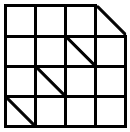


INSTITUTO DE ALTOS ESTUDIOS NACIONALES
UNIVERSIDAD DE POSTGRADO DEL ESTADO

REPÚBLICA DEL ECUADOR

INSTITUTO DE ALTOS ESTUDIOS NACIONALES
UNIVERSIDAD DE POSGRADO DEL ESTADO

IV MAESTRÍA EN ALTA GERENCIA

TÍTULO DE LA TESIS: "DISEÑO DE MODELO DE GESTIÓN PARA EL GERENCIAMIENTO DE LA SEGURIDAD DE LA INFORMACIÓN TECNOLÓGICA EN EL CONSEJO DE LA JUDICATURA" – PLANTA CENTRAL QUITO.

Tesis para optar el Título de Máster en Alta Gerencia.

Autor: Ing. Marco Vinicio Hidalgo Larco.

Directora: Msc. Mónica Ximena Hidalgo Andino.

Quito, Mayo 2017.

INSTITUTO DE ALTOS ESTUDIOS NACIONALES
LA UNIVERSIDAD DE POSGRADO DEL ESTADO

No.056- 2017.

ACTA DE GRADO

En la ciudad de Quito, a los diecinueve días del mes de mayo del año dos mil diecisiete, **MARCO VINICIO HIDALGO LARCO,** portador de la cédula de ciudadanía: 1713312039, **EGRESADO DE LA MAESTRÍA EN ALTA GERENCIA 2006-2007,** se presentó a la exposición y defensa oral de su Tesis, **con el tema: "DISEÑO DEL MODELO DE GESTIÓN PARA EL GERENCIAMIENTO DE LA SEGURIDAD DE LA INFORMACIÓN TECNOLÓGICA EN EL CONSEJO DE LA JUDICATURA – PLÀNTA CENTRAL QUITO"**, dando así cumplimiento al requisito, previo a la obtención del título de **MAGÍSTER EN ALTA GERENCIA.**

Habiendo obtenido las siguientes notas:

Promedio Académico:	8.88
Tesis Escrita:	8.46
Grado Oral:	7.94
Nota Final Promedio:	**8.54**

En consecuencia, **MARCO VINICIO HIDALGO LARCO,** se ha hecho acreedor al título mencionado.

Para constancia firman:

Mgs. Mónica Hidalgo
PRESIDENTA DEL TRIBUNAL

Mgs. Víctor Jácome
MIEMBRO

Dr. Romel Tintin
MIEMBRO

Abg. Lenin Melo
Director de Secretaria General

INSTITUTO DE ALTOS ESTUDIOS NACIONALES
LA UNIVERSIDAD DE POSGRADO DEL ESTADO

SECRETARÍA GENERAL

De conformidad con la facultad prevista en el estatuto del IAEN CERTIFICO que la presente es fiel copia del original

INSTITUTO DE ALTOS ESTUDIOS NACIONALES LA UNIVERSIDAD DE POSGRADO DEL ESTADO

Fojas 1

Fecha 17/04/2017

Secretaría General

INSTITUTO DE ALTOS ESTUDIOS NACIONALES

UNIVERSIDAD DE POSTGRADO DEL ESTADO

AUTORIA

Yo, MARCO VINICIO HIDALGO LARCO, ingeniero, con CC 171331203-9, declaro que las ideas, juicios, valoraciones, interpretaciones, consultas bibliográficas, definiciones y conceptualizaciones expuestas en el presente trabajo, así como los procedimientos y herramientas utilizadas en la investigación, son de absoluta responsabilidad de la tesis.

MARCO VINICIO HIDALGO LARCO.

CC: 171331203-9.

INSTITUTO DE ALTOS ESTUDIOS NACIONALES

UNIVERSIDAD DE POSTGRADO DEL ESTADO

AUTORIZACIÓN DE PUBLICACIÓN

"Yo, MARCO VINICIO HIDALGO LARCO cedo al IAEN, los derechos de publicación de la presente obra por un plazo máximo de cinco años, sin que deba haber un reconocimiento económico por este concepto. Declaro además que el texto del presente trabajo de titulación no podrá ser cedido a ninguna empresa editorial para su publicación u otros fines, sin contar previamente con la autorización escrita de la universidad"

Quito, 22 de mayo de 2017.

MARCO VINICIO HIDALGO LARCO.

CC: 171331203-9.

PREFACIO.

Las entidades del Estado ecuatoriano manejan y procesan información tecnológica diariamente, la misma que está expuesta a riegos de pérdida, manipulación o copiado, por lo que es imperativo contar con mecanismos y sistemas tecnológicos que garanticen la protección de la información generada por los usuarios institucionales y de la ciudadanía (público y privado), enmarcados en leyes, reglamentos y normativas institucionales o del servicio público.

Este trabajo de investigación de *Diseño de modelo de gestión para el gerenciamiento de la seguridad de la información tecnológica en el Consejo de la Judicatura*, planta central Quito, tiene por objetivo generar un modelo de gerenciamiento de la seguridad de la información para proteger y resguardar la información tecnológica institucional, por lo cual, se realizará un diagnóstico y un análisis de las vulnerabilidades de la información en el Consejo de la Judicatura, que ofrece servicios judiciales a toda la población ecuatoriana a nivel nacional a través de sus Unidades Judiciales[1]; por lo tanto, el contenido del presente trabajo tiene como fin la elaboración de un modelo de gestión que permita la articulación del Plan Estratégico Institucional, las atribuciones y productos establecidos en relación a la seguridad de la información, de acuerdo al Estatuto Integral de Gestión Organizacional por Procesos del Consejo de la Judicatura a Nivel Central y Desconcentrado.

[1]*Unidad Judicial:* Ver definición en la sección del glosario.

PREFACE.

Ecuadorian state entities handle and process technological information daily, that is exposed to risks of loss, manipulation or copy; so that it is important to have mechanisms and technological systems that ensure the protection of information generated by institutional users and citizenship, based in laws, rules and regulations of the institution or public service.

The research of design model for the management of security of information technology in the Judicial Council, central plant in Quito, which are intended to generate a model of management of security information to protect and safeguard the institutional information technology, therefore, a diagnosis and analysis of vulnerabilities of information in the Judicial Council[2], whose service is to provide justice to the entire Ecuadorian population nationwide through of Judicial Units; therefore, the content of this work whose propose is developing a management model that allows the articulation of institutional strategic plan, functions and products established in relation to information security, according to Status of Organizational Management by Processes Judicial Council to Central and Decentralized level.

[2] *Judicial Council:* The definition is in glossary.

DEDICATORIA

A mis padres, hermanos,

esposa y el equipo familiar Hidalgo.

A la institución de gobierno que me permitió dejar una semilla

para el desarrollo y beneficio del país en el sector de la justicia.

A los amigos que confían en los buenos y

malos momentos sin perder el apoyo y ayuda.

AGRADECIMIENTO

A Dios, a mis papis: Rosa y Jaime quienes apoyan incondicionalmente en todos los momentos a fomentar la tenacidad, a transferir su experiencia en la lucha diaria y a trascender el significado de esfuerzo, trabajo y dedicación para el cumplimiento de las metas personales.

A mis hermanos Mary y Patricio por su confianza depositada y respaldo desinteresado.

A Laura Nuñez y a todas las personas que participaron en el cierre este objetivo trazado.

No olvido a mi directora de tesis por su gran apoyo, colaboración y paciencia.

ÍNDICE GENERAL

TABLA DE APÉNDICES.

ÍNDICE DE ANEXOS.

ÍNDICE DE GRÁFICOS.

ÍNDICE DE TABLAS

LISTA ESPECIAL DE SIGLAS

CJ: Consejo de la Judicatura.

CGE: Contraloría General del Estado.

DINARDAP: Dirección Nacional de Registritos y Datos Públicos.

DNP: Directorio Nacional de Personal.

DNTICs: Dirección Nacional de Tecnologías de la Información y Comunicaciones.

FODA: Fortaleza, Oportunidades, Debilidades y Amenazas.

HPMS: HP Service Manager

INEN: Instituto Ecuatoriano de Normalización.

ISECOM: Institute for Security and Open Methodologies.

OSSTMM: Manual de la Metodología Abierta de Testeo de Seguridad (Open Source Security Testing Methodology Manual).

PDCA: Planificar – Hacer – Controlar - Actuar (Plan-Do-Check-Act).

SATJE: Sistema Automático de Trámite Judicial Ecuatoriano.

SEVRI: Sistema Específico de Valoración del Riesgo Institucional.

SGSI: Sistemas de Gestión de la Seguridad de la Información.

SNAP: Secretaría Nacional de Administración Pública.

SNIT: Subdirección Nacional de Infraestructura, Servicios y Telecomunicaciones.

SNSI: Subdirección Nacional de Seguridad de la Información.

SUPA: Sistema Único de Pensiones Alimenticias.

TICs: Tecnologías de la Información y Comunicaciones.

UPTICs: Unidades Provinciales de las Tecnologías de la Información y Comunicaciones.

VPN: Red Virtual Privada (Virtual Private Network).

GLOSARIO

Administración del riesgo.- Es el conjunto de acciones que realiza la administración activa para minimizar las consecuencias o efectos que pueden producirse si se materializa el riesgo (HMP SA, 2006).

Almacenamiento de la información tecnológica.- Son dispositivos electrónicos capaces de grabar datos con niveles elevados de memoria.

Anonymous.- Anónimo en redes informáticas. Todo recurso o servicio al que se accede de forma anónima, es decir, sin que se pueda descubrir la IP, computadora o persona que está detrás de la misma (Alegsa Dic, 2016).

Bases de datos.- Sistema formado por un conjunto de datos almacenados en arreglos de discos que permiten el acceso directo a ellos y un conjunto de programas que manipulen ese conjunto de datos (Estado del Arte de las Bases de Datos, 2016).

Benchmarking.- Definido como un proceso sistemático y continuo para evaluar los productos, servicios y procesos de trabajo de las organizaciones que son reconocidas como representantes de las mejores prácticas con el propósito de realizar superaciones en las organizaciones y que para nuestro caso, será aplicado para la seguridad de la información institucional responsable de la Justicia. Se plantea una comparación, no solo

entre la competencia sino con cualquier otra institución que le pueda proporcionar información para llevar a cabo las mejoras, ya sea de su misma actividad económica o no (Thompson, 2011).

Ciberataque.- Un comando de expertos delincuentes que utilizan Internet para operar una gran red de computadoras secuestradas, este ejército de computadoras (que recibe el nombre de redes robots o botnets) lanza un intenso bombardeo de códigos maliciosos, en cuestión de minutos se colapsan los cibersitios de las instituciones: militares, financieras y comerciales; los cajeros electrónicos, las redes telefónicas, se paraliza el tráfico aéreo, fallan los sistemas informáticos y/o la seguridad de una central nuclear (Biblioteca en línea, 2016)

Delito flagrante.- Guarda relación con la inmediatez; es decir, se considera así hasta 24 horas después de haberse cometido un delito. Además, se debe observar que haya un detenido, se encuentren armas, instrumentos, productos ilícitos y huellas o documentos relativos a la infracción. En delitos calificados como flagrantes se aplica el procedimiento directo, en ese juicio se centran todas las etapas del proceso en una sola audiencia, sentenciados con una pena máxima privativa de la libertad de hasta cinco años (Funcion Judicial de Pichincha, 2016).

Delitos informáticos tradicionales.- Actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos (Delitos informáticos, 2016).

Gestión del Riesgo Institucional.- (GRI) Es un elemento esencial de la buena gobernanza y rendición de cuentas de las organizaciones. Se trata de un enfoque sistemático que abarca toda la organización y que apoya el logro por la organización de sus objetivos estratégicos, mediante la determinación, la evaluación, la valoración, la fijación de prioridades y el control de riesgos de forma proactiva en toda la organización, (Naciones Unidas, 2010).

Hardware.-Parte física que conforma un sistema computación.

Incidentes de seguridad de la información.- Se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o cualquier otro acto que implique una violación a la Política de Seguridad de la Información en la institución (Universidad Nacional de Lujuan, 2016)

Información institucional.- Es todo aquel conjunto de datos organizados en poder de la institución en estudio que posean valor para la misma, independientemente de la forma en

que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

Institucional.- Todo aquello que se relaciona o se deriva con el Consejo de la Judicatura en calidad de Función del Estado como representante de la Justicia.

Impacto.- Consecuencias que puede ocasionar la materialización del riesgo(HMP SA, 2006).

Ignotos.- Sinónimo de desconocido, ignorado, incógnito o inexplorado. Adjetivo que designa aquello de lo que no se tiene conocimiento, de lo que nada se sabe, o que no ha sido descubierto aún". La palabra proviene del latín ignotus, que significa 'desconocido' (Significados, 2016)].

Kaspersky Anti-Virus.- Es un antivirus que realiza una combinación de protección reactiva y preventiva, protegiendo eficazmente de virus, troyanos y todo tipo de programas malignos. Adicionalmente, dentro del grupo de programas malignos, Kaspersky también se encarga de proteger el registro y todo tu sistema contra programas potencialmente peligrosos como los spyware (Kaspersky Anti-Virus, 2016).

Política de seguridad institucional.- Es un plan de acción para afrontar los riesgos de seguridad o un conjunto de reglas que tendrá buenas prácticas para la seguridad y las directrices de seguridad de la información en el Consejo de la Judicatura.

Probabilidad.- Es una medida (expresada como porcentaje o razón) para estimar la posibilidad de que ocurra un incidente o evento (HMP SA, 2006).

Prueba de penetración (Pen Test). Es una prueba que se realiza para detectar aquellas vulnerabilidades desconocidas en la infraestructura tecnológica de la institución antes que un atacante las explote. La evaluación de seguridad se puede realizar a cualquier nivel desde el entorno físico hasta las personas, pasando por las redes, sistemas operativos, sistemas de información, aplicaciones web y otros (Kali Linux Penetration Testing Tools, 2016).

Registro de incidente de seguridad.- Es un hecho o amenaza que atenta contra la confidencialidad, integridad o disponibilidad de un sistema de seguridad de información y se procede a colocar en un bitácora o histórico.

Repositorio de información.-Todo aquel dato o información que se reúne en un mismo lugar centralizado, facilitando el acceso a la misma. (Repositorio, 2016).

Software.- Es la parte lógica e intangible de un sistema computacional.

Salas o cuartos de comunicación.- Espacios físicos que permiten albergar infraestructura tecnológica ubicados en los edificios que se encuentran las Dependencias Judiciales (cortes y direcciones provinciales de Justicia, juzgados, flagrancias, unidades, entre otros).

Unidad de flagrancia.- Es el sitio de trabajo en conjunto con instituciones como el Consejo de la Judicatura, Defensoría Pública, Fiscalía, Ministerio del Interior, Ministerio de Justicia, Policía Nacional de criminalística, antinarcóticos, departamento de violencia intrafamiliar y DINAPEN, permitido que la atención al usuario sea prioritaria en esta Unidad**.** La Unidad de Flagrancia recibe denuncias de delitos penales como: hurto, robo, violencia contra la mujer o miembros del núcleo familiar, delitos sexuales como violación, estupro, abuso sexual, asesinato, drogas y lesiones(Funcion Judicial de Pichincha, 2016).

Unidades Judiciales.- Es un área de la Función Judicial que presta el servicio jurisdiccional de primer nivel, la misma que puede estar conformada por uno o más jueces en una o varias materias; y cuyo personal administrativo presta sus servicios por igual a mencionados jueces con el objeto de optimizar su funcionamiento a través del trabajo de áreas comunes, que aseguren la separación de las funciones jurisdiccionales de los

servicios de carácter administrativo (Resolución del Consejo de la Judicatura No. 003-2014, 2016).

Valoración de Riesgos.- Identificar y analizar los riesgos que enfrenta la institución, tanto de fuentes internas como externas relevantes para la consecución de los objetivos, para administrarlos (HMP SA, 2006).

Capítulo1. Introducción.

1.1 Antecedentes.

El presente trabajo pretende analizar el modelo de gestión con el que se gerencia la seguridad de la información tecnológica en el Consejo de la Judicatura y a su vez, conocer el estatus que se encuentra desde que el Consejo de la Judicatura de Transición entregó el mandato a las actuales autoridades, es decir, desde el miércoles, 09 de enero del 2013 hasta la fecha que se culminó el presente estudio. Es importante señalar que en mencionado Consejo de Transición se desarrollaron algunos proyectos tecnológicos con el objetivo de mejorar los servicios tecnológicos a la ciudadanía en cuanto a la justicia ecuatoriana. Las actuales autoridades, en aquel momento reorganizaron a esta institución en la parte interna y externa, para lo cual, se elaboró e implementó la normativa interna denominada "*Estatuto Integral de Gestión Organizacional por Procesos del Consejo de la Judicatura a nivel Central y Descentralizado"*, y también, se actualizó y aprobó el *"Código Orgánico de la Función Judicial"*, tomando en cuenta las últimas reformas que presenta la actual Constitución del Ecuador en el ámbito de la administración judicial y así alcanzar los objetivos internos y estratégicos en su período asignado; mientras tanto, la parte externa se visionó automatizar procesos judiciales en todas las materias de derecho que exige la Ley, según las causas que se presentan en las diferentes ventanillas a nivel

nacional de las *Unidades Judiciales*[3] y también se crearon la *Unidades Flagrancia*[4] como proyectos con carácter emblemático; se elaboró y se implementó el "Código Integral Penal (COIP)" y también el "Código Orgánico de Gestión Procesal (COGEP)", mismo que se implementó en mayo del 2016 a nivel tecnológico, incluyendo el proceso de grabación de audiencias. Se debe tomar en cuenta la implementación de otros servicios de justicia para la ciudadanía por medio de los portales WEB, tales como: denuncias de pérdidas de documentos personales, consulta de los juicios y demandas, servicios notariales y otros que estipula la Ley. Mismos que en la actualidad generan y almacenan diariamente elevadas cantidades de información tecnológica y que presentan riesgos o vulnerabilidades. Los detalles de la institución en estudio se revisarán en el siguiente capítulo.

Los mencionados servicios jurisdiccionales colocan a esta institución como líder y ejemplo a seguir en Latinoamérica con la articulación de la Justicia y la actual tecnología, ubicando en un excelente sitial de imagen institucional.

Es necesario e importante recordar que la seguridad de la información tecnológica es una disciplina que se encarga de proteger la integridad, privacidad y confidencialidad de los datos almacenados de un sistema o plataforma informática que pertenecen a una empresa o institución, y que no existe ninguna técnica totalmente segura que permita la inviolabilidad de dicho sistema o plataforma; adicionalmente, el cotidiano desarrollo

[3]*Unidades Judiciales:* Ver definición en la sección del glosario.
[4]*Unidades de Flagrancias:* Ver definición en la sección del glosario.

tecnológico que experimenta la sociedad exige una evolución en las formas de violar las seguridades, dando lugar: a la creación y diversificación de los *delitos informáticos tradicionales*[5], suspensión de los servicios, publicación de la información privada, obtener registro de incidentes de seguridad de la información tecnológica, entre otros problemas.

Por lo expuesto, la información del Consejo de la Judicatura en la actualidad tiene gran importancia por el contenido e información que éste significa para sí misma y para el Estado, en virtud que dispone de toda la información relacionada a la justicia de todo el Ecuador, más aún si la misma se encuentra concentrada en repositorios tecnológicos y ésta a su vez, presenta exposición de vulnerabilidad.

Las actuales Autoridades del Consejo de la Judicatura obtuvieron como herencia del Consejo de Transición, la implementación física y técnica de las tecnologías de la información y comunicaciones (**T**ICs), en la cual, se transmite, procesa y almacenan información, y, que está en relación con equipos tecnológicos, ubicados en el centro de datos principal; así también se cuenta con *salas o cuartos de comunicación*[6] a nivel nacional. El Centro de Datos Principal se compone básicamente de las siguientes partes:

- Infraestructura computacional: Son todos aquellos equipos tecnológicos tales como: servidores, almacenamiento de información (storages), seguridades informáticas, balanceadores de carga, computadores de escritorio y personales, racks, energía eléctrica

[5] *Delitos informáticos tradicionales:* Ver definición en la sección del glosario.
[6] *Salas o cuartos de comunicación:* Ver definición en la sección del glosario.

regulada, aire acondicionado industrial, teléfonos inteligentes, tabletas, entre los más importantes.

- Sistemas informáticos.- Son todos aquellos programas, aplicativos, librerías, archivos, códigos de programación (scripts), lenguajes de programación, licencias, software[7] base y otros en general, que conforman las denominadas: *base de datos*[8] y *repositorios de información*[9] para los servicios y aplicativos tecnológicos del tipo jurisdiccional y administrativo de la institución en estudio.

- Enlaces de datos.- Se refiere a la conectividad de datos por medio de las redes: WAN / LAN/ Wireless. Adicionalmente se considera el acceso a internet y otros tipos de enlaces de datos con el resto de instituciones públicas y privadas; y, según el convenio o acuerdo interinstitucional se contrata el servicio.

- Recurso humano.- Conformado por todo aquel personal técnico, administrativo, jurisdiccional y de terceros que cuenta la institución para el correcto funcionamiento del centro de datos como también para el resto de operaciones que requiere la institución en estudio, para lo cual, se clasifica como:

Usuarios internos.- Es el servidor judicial en los términos previstos en el "Código Orgánico de la Función Judicial".

---

[7] *Software:* Ver definición en la sección del glosario.
[8] *Base de datos:* Ver definición en la sección del glosario.
[9] *Repositorios de información:* Ver definición en la sección del glosario.

Usuarios externos.- Es el ciudadano y/o profesional del derecho que requiere atención del servicio público judicial.

1.2 Planteamiento del problema.

Por los antecedentes expuestos, el Consejo de la Judicatura es el responsable de administrar, controlar y asegurar la información tecnológica diaria, referente a la justicia del Ecuador, sin olvidar la parte administrativa institucional y considerando que éste servicio no se encuentra asignado a terceras personas; permitiendo asegurar la información institucional y que se describirán en los siguientes capítulos, además, se debe considerar la protección de la información institucional de los denominados *ignotos*[10], mismos que aprovechándose de cualquier vulnerabilidad existente en la infraestructura tecnológica de esta institución llegan a obtener datos de los servicios tecnológicos, considerados como activos críticos de la institución, mediante diversas formas de fraude, espionaje, sabotaje o vandalismo.

Adicionalmente, esta institución se encuentra expuesta a otros mecanismos de alta vulnerabilidad que son los virus informáticos, el hacking, ataques de denegación de servicio institucional, ataque de *anonymous*[11], llegando actualmente a lo que se conoce como *ciberataques*[12] y con el apoyo de la ingeniería social. Sumándose otros riesgos o

[10]*Ignoto:* Ver definición en la sección del glosario.
[11]*Anonymous:* Ver definición en la sección del glosario.
[12]*Ciberataque:* Ver definición en la sección del glosario.

incidentes de seguridad en forma voluntaria o involuntariamente que se debe reducir desde el interior de la institución o aquellos provocados por catástrofes naturales o pre-planificados.

Por tanto, para gerenciar la actual seguridad de la información del Consejo de la Judicatura es necesario conocer el estatus de la seguridad de la información institucional y con los recursos que éste cuente, para lo cual, se requiere realizar un análisis y obtener el diagnóstico que indique la necesidad de diseñar un modelo de gestión de la seguridad de la información institucional que se adapte a las actuales circunstancias, recursos y requerimientos de la información tecnológica con respecto al "core de negocio" institucional, basados en la normativa y Leyes del Ecuador vigentes.

1.3 Justificación.

De acuerdo al problema señalado, la información tecnológica en el Consejo de la Judicatura del Ecuador toma gran importancia por el contenido que éste significa para sí misma y para el Estado; por lo tanto, se requiere analizar y diagnosticar el actual modelo de gestión de la seguridad de la información tecnológica donde se pretende evaluar los mecanismos de seguridad que cuenta esta institución de acuerdo a los conceptos de: confidencialidad, disponibilidad e integridad de la información tecnológica institucional según estándares nacionales e internacionales vigentes; para lo cual, el presente estudio pretende conocer la actual ruta responsable del gerenciamiento de la seguridad de la

información en esta institución basado en un modelo de gestión, y, si el resultado lo amerita, se propondrá el planteamiento de un nuevo modelo de gestión para este fin.

1.4 Estado del Arte.

De acuerdo a la documentación que reposa en el Consejo de la Judicatura se puede verificar que entre las responsabilidades asignadas a la Dirección Nacional de Tecnologías de la Información y Comunicaciones (DNTICs) está la seguridad de la información, según describe el *"Estatuto Integral de Gestión Organizacional por Procesos del Consejo de la Judicatura a nivel Central y Descentralizado"*.

Según la investigación efectuada en esta dirección nacional se evidencia la carencia de documentos que describan un plan de ruta o una planificación estratégica referente a la seguridad de la información institucional. De acuerdo al estatuto integral mencionado, el responsable directo de la seguridad de la información para esta institución es el Director nacional de TICs[13], sin embargo, éste dispone de un delegado, denominado el Subdirector Nacional de Seguridad de la Información y, que por motivos de este documento se abreviará como *SNSI*; mismo que actualmente debe realizar y cumplir con las siguientes actividades, entre las más importantes son:

- Planificar, realizar el seguimiento y reportar los planes de actividades anuales a cargo del Subdirector.

[13]*TICs:* Ver definición en tabla de siglas.

- Generar proyectos de inversión anual relacionada con la seguridad de la información institucional.

- Coordinar el cumplimiento de convenios interinstitucionales en cuanto a la seguridad de la información.

- Es el responsable del servicio de firma electrónica de ésta institución orientada al uso de autoridades y servidores judiciales, actualmente, a cargo de otra Jefatura.

- Proponer planes, normativas, informes, reportes y lineamientos de seguridad de la información institucional, realizada con los debidos seguimientos.

- Desarrollar el mantenimiento y gestión de los equipos seguridad de la información que se encuentra bajo su responsabilidad, sin embargo, la operación y funcionamiento de éstos son a cargo de la *Subdirección nacional de infraestructura, servicios y telecomunicaciones* y, que por motivos de estudio se abreviara como *SNIT*[14] o simplemente se mencionará como *Dirección Nacional de Infraestructura*, que es adscrita a la DNTICs según el Estatuto institucional.

- Dispone de personal técnico y administrativo a cargo según las jerarquías definidas en la institución (técnico, analistas, supervisor, jefatura, asistente).

- Debe cumplir con indicadores de gestión solicitados por otras Direcciones Administrativas que tiene actualmente la institución.

---

[14] *SNIT:* Ver definición en tabla de siglas.

- Emitir pronunciamientos, recomendaciones, sugerencias y todo lo referente a la seguridad de la información institucional.

Por lo expuesto, el cargo para esta delegación va orientado a las actividades de un gerenciamiento responsable de la seguridad de la información.

En cuanto a la seguridad de la información institucional se cuenta con un registro de incidentes relacionados a la seguridad de la información, tales como: ataques a los portales web de la institución (suspensión del portal por anonymus), saturación del enlace o pérdida de la información de datos por ataques, consumo de aplicaciones y fenómenos de fuerza mayor como son los desastres naturales, accidentes o fallos de orden técnico. La autorización al centro de datos se realiza mediante aval escrito de acceso en la parte física o por medio de una red privada virtual (VPN[15]) para aquellos servidores judiciales que lo requieren y cumplen con el procedimiento establecido. El reporte de incidentes incluye al personal técnico que realiza mantenimiento a los equipos PC, impresoras, copiadoras y otros que tienen contacto directo con los servidores judiciales, mediante el uso de mesa de servicios.

Las bases de datos y los repositorios de información que posee ésta institución, se estima que diariamente se maneja miles de millones de datos (Tera Bits = TB) por segundo a nivel nacional, lo que se dispone de elevado nivel de procesamiento y también de almacenamiento del tipo dinámico (discos) y fijo (cintas). Sin embargo, se debe

[15]*VPN*: Ver definición en tabla de siglas.

evaluar el nivel de almacenamiento utilizado y el disponible actualmente, incluyendo los respectivos respaldos de toda la plataforma y sin afectar la operación normal de los servicios; mismos que servirán como contingencia luego de recibir un ataque, suspensión del servicio o vulnerando las protecciones de la información institucional.

En el inicio del año 2016 se mejoró la disponibilidad de los enlaces para cada una de las provincias y también para el centro de datos con el proveedor del servicio por medio de fibra óptica, llegando a obtener rutas alternas con cada enlace de datos principal y con una conmutación automática por demanda de fallas, denominado *enlace back up pasivo*; garantizándose una disponibilidad del servicio para cada enlace provincial del 99,80%.

El nivel de acceso y mecanismos de control hacia la información tecnológica institucional permite un registro y seguimiento por medio del directorio centralizado a nivel nacional, denominado Directorio Activo institucional. De igual manera, se dispone de un antivirus institucional que permite proteger algunos servicios. La autorización hacia otros programas o aplicativos informáticos se realizan de acuerdo al pedido por escrito que requiere un funcionario o servidor judicial y la autorización por parte de su inmediato superior y del propietario o dueño sistema.

Es importante indicar que los aplicativos informáticos que presta la institución en la actualidad son desarrollados internamente, por medio de la contratación de profesionales informáticos del Ecuador que conocen y traducen la normativa legal vigente en aplicaciones informáticas, para lo cual, se adquiere software base en código abierto o

aplicativos informáticos especiales si el caso lo amerita. La participación de los representantes del Derecho, personal técnico de TICs, responsables de la calidad en la gestión procesal, administrador del proyecto y los dueños o representantes del sistema permiten desplegar los aplicativos jurisdiccionales y administrativos de la institución a nivel nacional, obteniéndose los resultados planteados, bajo el uso de normas de seguridad de la información y con las respectivas coordinaciones.

La prestación de los mencionados servicios y otras aplicaciones informáticas que presta el Consejo de la Judicatura serán expuestos en los siguientes capítulos, permitiendo destacar a la institución en estudio a nivel Latinoamericano como un líder en la articulación de la tecnología con las normativas jurisdiccionales vigentes en el Ecuador, así señaló Ernesto Samper, Secretario General de la Unión de Naciones Suramericanas (UNASUR)[16] el 15 de septiembre de 2016, dando como resultado el funcionamiento de los modelos de Unidades de Fragancia que están implementados a nivel nacional y que otros países lo toman como referencia para replicar, como por ejemplo: Perú, Bolivia, Argentina, entre otros del mundo; sin embargo, el modelo de la seguridad de la información debe ajustarse de acuerdo a la normativa de derecho de cada país, a la normativa de seguridad de la información tecnológica vigente e implementada, entre otras Leyes o acuerdos internacionales e incluso a los recursos gestionados y asignados por parte de la institución para estos fines.

[16]http://www.ecuadorinmediato.com/index.php?module=Noticias&func=news_user_view&id=2818808436&umt=unasur_destaca_sistema_judicial_ecuador

Por lo tanto, el Subdirector de la seguridad de la información en el Consejo de la Judicatura debe verificar la existencia, aplicación y seguimiento de los procedimientos, modelos, teorías, guías o metodologías sobre la protección de la información según los estándares, lineamientos o normativas relacionados con la seguridad de la información, y, el nivel de madurez que éstos poseen actualmente en la institución, precisamente para proteger o reducir estas acciones imprevistas y que provocan grandes impactos a los dueños de la información.

1.5 Hipótesis.

El presente trabajo de investigación pretende demostrar las siguientes hipótesis:

- La institución en estudio requiere fortalecer la seguridad de la información bajo un modelo de gestión estratégico que permita generar confiabilidad y credibilidad en los servicios hacia la ciudadanía; de acuerdo a los resultados obtenidos del análisis y diagnósticos de las normas y estándares de gestión de la seguridad de la información institucional.

- El Consejo de la Judicatura del Ecuador diariamente presenta un alto riesgo en su información por la falta de apoyo de sus autoridades, desconocimiento o inexistencia de un modelo de gestión formal y la importancia que ésta representa a la seguridad de la información tecnológica como se analizará en los incidentes de seguridad registrados por la mesa de servicios y los riesgos de seguridad de la información institucional que se encuentra expuesta.

- Los servidores judiciales como los actores más expuestos al incumplimiento de los procedimientos, normativas y leyes establecidas en materia de la seguridad de la información tecnológica, provoca el riesgo de copia, modificación o eliminación de los datos; para lo cual, se utilizará una herramienta informática para efectuar una prueba de penetración y su resultado permitirá conocer un diagnóstico institucional referente a estos temas.

- La seguridad de la información tecnológica es una responsabilidad exclusiva de las TICs para cualquier institución pública o privada y requiere del apoyo, colaboración y cumplimiento del resto de direcciones, unidades o áreas que conforman la estructura organizacional del Consejo de la Judicatura en el cumplimiento de las normativas de seguridad de la información; para lo cual, se revisará la actual organización de la información en los repositorios compartidos de información institucional por medio de la prueba de penetración.

1.6 Objetivos.

1.6.1 Objetivo general.

Analizar y diseñar un modelo de gestión para el gerenciamiento de la seguridad de la información tecnológica en el Consejo de la Judicatura del Ecuador.

1.6.2 Objetivos específicos.

- Analizar el marco institucional y normativo, referente a la seguridad de la información que regula al sector de justicia.

- Analizar y diagnosticar el uso y aplicabilidad de las normas y estándares nacionales e internacionales mediante el sistema de gestión de seguridad de la información tecnológica en el Consejo de la Judicatura del Ecuador.
- Diseñar un modelo de gestión según los resultados obtenidos del diagnóstico y que permita asegurar los datos tecnológicos en el Consejo de la Judicatura bajo un proceso de madurez, permitiendo el gerenciamiento responsable desde el encargado de la seguridad de la información en la institución de estudio.

1.7. Marco Teórico.

El marco teórico que respalda a la Institución como responsable de la Justicia Ecuatoriana se origina en la vigente Constitución de la República del Ecuador; definida como parte de la Función Judicial; posee autonomía administrativa y económica, se rige por leyes, códigos y/o normativas jurídicas, propias de la Función Judicial del Ecuador, no forma parte de otras Funciones del Estado. La institución en estudio se conforma de dos partes: la *Administrativa*, misma que brinda el apoyo físico, material, económico, humano y tecnológico; y la segunda parte, denominada *Jurisdiccional*, misma que se encarga de brindar justicia por medio de personal especializado en materia de derecho.

La institución en estudio posee la mayor parte de información tecnológica centralizada y una reducida información desconcentrada, misma que se maneja como se describe en la tabla 1:

Tabla 1.Información tecnológica centralizada y descentralizada.

INFORMACIÓN TECNOLÓGICA.	LOCAL Y/O NACIONAL	PUBLICA Y/O PRIVADA	INSTITUCIONAL Y/O GUBERNAMENTAL
	IMPORTANCIA BAJA	IMPORTANCIA MEDIA	IMPORTANCIA ALTA
	PORTALES WEB	INTRANET INSTITUCIONAL	REPOSITORIOS Y/O ALMACENAMIENTO

Fuente: Consejo de la Judicatura, 2016. *Elaborado por:* el autor, 2016.

1.7.1 Aseguramiento de la información y activos de la institución en estudio.

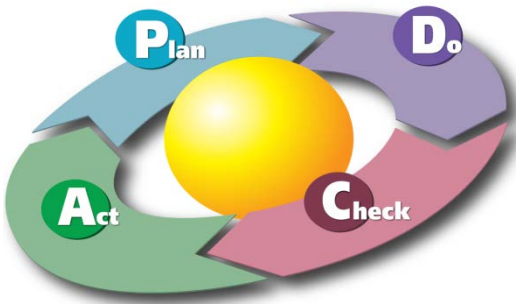
Para el aseguramiento de la información y activos de la institución en estudio se propone llevar a cabo, mediante un control físico, técnico y administrativo; como se describirá en los siguientes capítulos.

1.7.2 Sistema de Gestión de Seguridad de la Información.

Un Sistema de Gestión de Seguridad de la Información (SGSI) es una parte del sistema general que se enfocará al *riesgo institucional*, para establecer, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información institucional**.**

La ISO/IEC 27001 incorpora el típico Plan-Do-Check-Act (PDCA) que significa "Planificar-Hacer-Controlar-Actuar" siendo este un enfoque de mejora continua:

Figura 1. Círculo de Deming.



Fuente: Norma ISO/IEC 27001, 2013.*Elaborado por:* Norma INEN, 2016.

- Plan *(planificar)*: es una fase de diseño del SGSI, realizando la evaluación de riesgos de seguridad de la información y la selección de controles adecuados.

- Do *(hacer)*: es una fase que envuelve la implantación y operación de los controles.

- Check *(controlar)*: es una fase que tiene como objetivo revisar y evaluar el desempeño (eficiencia y eficacia) del SGSI.

- Act *(actuar)*: en esta fase se realizan cambios cuando sea necesario para llevar de vuelta el SGSI a máximo rendimiento.

El objetivo principal de la seguridad informática es garantizar que los recursos y la información estén protegidos; y para salvaguardar, es necesario conseguir los siguientes aspectos:

- Integridad: Sólo los usuarios autorizados podrán modificar la información.

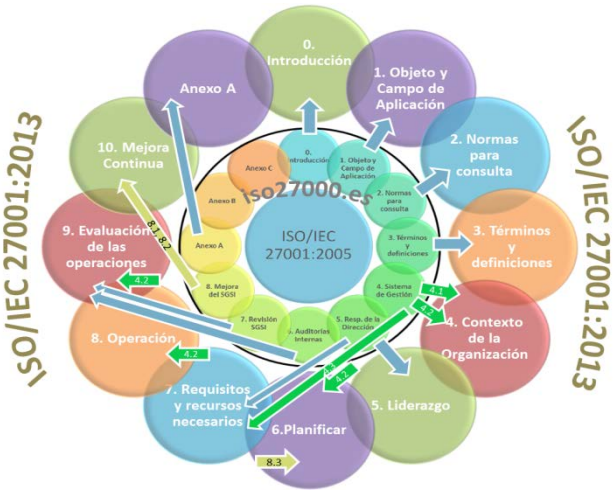
- Confidencialidad: Sólo los usuarios autorizados tendrán acceso a los recursos y a la información que utilicen.

- Disponibilidad: La información institucional debe estar disponible cuando se necesite.

- Irrefutabilidad: El usuario no puede refutar o negar una operación realizada.

A continuación, se describe gráficamente la normativa ISO/IEC27001, aprobada por el Instituto Ecuatoriano de Normalización (INEN) y que proviene de una normativa internacional.

Figura 2. ISO/IEC27001:2005.



Fuente: Norma ISO/IEC 27001, 2013.*Elaborado por:* Norma INEN, 2016

La evaluación del Sistema de Gestión de la Seguridad de la Información en forma gráfica se presenta en la siguiente figura:

Figura 3. Visualización de SGSI

Fuente: Norma ISO/IEC 27001, 2013.*Elaborado por:* Norma INEN, 2016

La *política de seguridad institucional*[17]será un documento de alto nivel que revela el compromiso de las Autoridades Institucionales, la DNTICs con la seguridad de la información y los servidores judiciales, para lo cual, debe contener la definición de la seguridad de la información desde el punto de vista que esta institución en estudio lo requiriese, además de complementar con el enriquecimiento y compatibilidad con otras políticas dependientes de ésta índole, objetivos de seguridad y procedimientos de otras instituciones. También, debe estar fácilmente accesible a los servidores judiciales, tanto de la existencia como de su contenido; será un documento único y asignado a un responsable para el mantenimiento y actualización.

El objetivo de la política de seguridad es proteger, preservar y administrar objetivamente la información del Consejo de la Judicatura, junto con las tecnologías utilizadas para su procesamiento, transmisión y almacenamiento frente a amenazas internas y externas con el fin de asegurar el cumplimiento de las características de confidencialidad, integridad, disponibilidad, legalidad, confiabilidad y no repudio de la información.

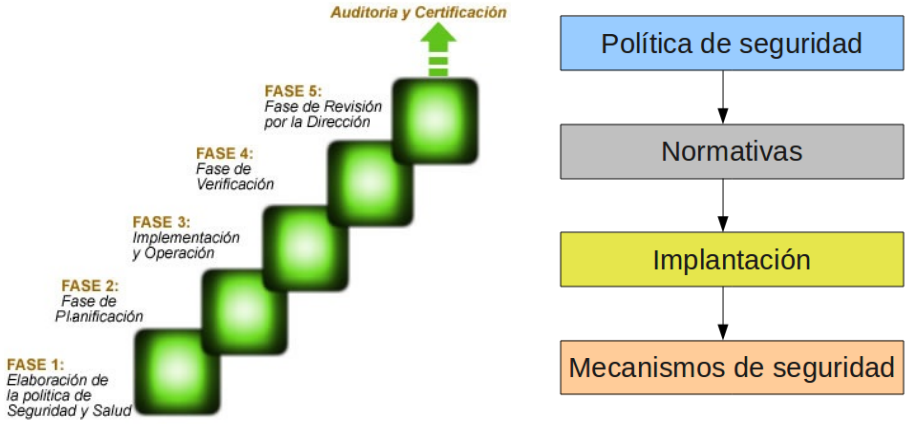
Es importante recordar que la información es un activo institucional que requiere de una gestión responsable, segura, oportuna y de calidad. El establecimiento, seguimiento, mejora continua y aplicación de las Políticas de Seguridad de la Información garantiza un compromiso ineludible de protección frente a la amplia gama de amenazas.

[17]*Política de seguridad institucional:* Ver definición en la sección del glosario.

Con estas políticas se contribuye a minimizar los riesgos asociados al manejo de información.

El desarrollo de la política de seguridad se muestra en la siguiente figura:

Figura 4. Desarrollo de las políticas.

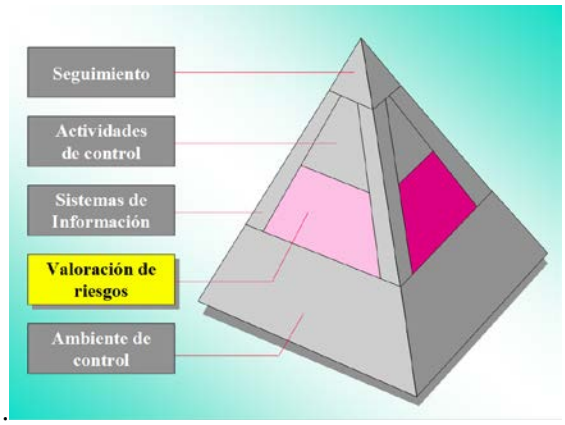


Fuente: Norma ISO/IEC 27001, 2013. *Elaborado por:* Norma INEN, 2016

1.7.3 La seguridad de la información y el riesgo.

Esta relación es fuertemente vinculada, por cuanto, si se logra identificar y analizar los riesgos que enfrenta la institución en cuanto a su información, tanto de fuentes internas como externas relevantes para la consecución de los objetivos es digno de alcanzar una administración, como se detalla a continuación:

Figura 5. Modelo de admiración del riesgo



Fuente: Curso de valoración de riesgos. *Elaborado por:* (HMP SA, 2006)

Por lo tanto, corresponde identificar y analizar los riesgos relevantes asociados al logro de los objetivos y las metas institucionales. De igual forma, se requiere analizar el efecto potencial de los riesgos, su importancia, probabilidad de ocurrencia y decidir las acciones a tomar para administrar dichos riesgos.

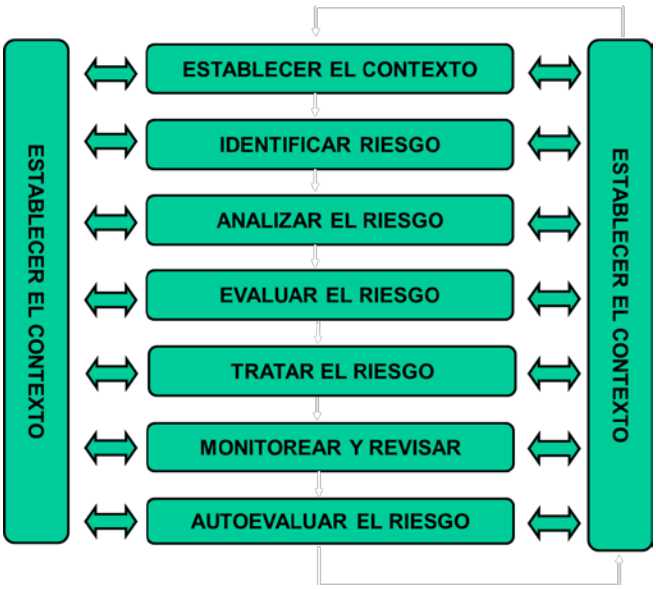
1.8 Marco metodológico.

El marco metodológico del presente trabajo se basará en la utilización de técnicas cuantitativas tales como: indicadores, estadísticas, evaluaciones, diagrama de flujo, modelos y otros procesos a ser implementados con referencia a la seguridad de la información institucional. Los datos extraídos pertenecen a fuentes primarias, tales como: memorando, informes internos, informes de la Contraloría General del Estado (CGE), talleres, reportes, entre otros documentos propios del área de seguridad de la información

y del área de infraestructura tecnológica de ésta institución que desemboca en información fidedigna (DNTICs), en la cual, el presente autor es partícipe directo de la Seguridad de la Información en calidad de supervisor; esto significa que se gestionó con el personal técnico, Director y Subdirectores de la DNTICs para revisar, analizar y realizar el diagnóstico correspondiente a la seguridad de la información institucional, y, que por motivos del contenido de la misma, se encuentran catalogados como reservados, para lo cual, se solicita las acciones específicas.

El esquema de la administración del riesgo propuesto tendrá la siguiente organización como señala la siguiente figura:

Figura 6. Esquema de la administración del riesgo.



Fuente: Curso de valoración de riesgos. *Elaborado por:* (HMP SA, 2006)

En cuanto al *contexto* se debe tomar en cuenta los siguientes puntos de enfoque: comprender la razón de ser de la institución, realización de una FODA, diseño de

procesos no ejecutados e inexistentes y el respectivo establecimiento de los objetivos de los procesos.

A continuación, se describe en que consiste el *Sistema Específico de Valoración de Riesgo Institucional* (SEVRI) según normativa interna de la institución en estudio: Se identifica y declaran los riesgos, se analizan y evalúan los riesgos, se aplica un tratamiento mediante una planificación, se monitorea el tratamiento mediante un seguimiento y se vuelve a evaluar para conocer el nuevo estatus; así se mantiene hasta que el riesgo sea mitigado o eliminado por completo. Los detalles serán ampliados en los siguientes capítulos del presente documento y, que visto en forma de proceso se presenta en la siguiente figura:

Figura 7. Proceso para desarrollar el SEVRI.

Fuente: Curso de valoración de riesgos. *Elaborado por:* (HMP SA, 2006)

Para el presente estudio, nuestro análisis para la gestión y gerenciamiento de la seguridad de la información institucional se basa en la metodología señalada en la

herramienta de *Benchmarking*[18], misma que permitirá al gerente, en nuestro caso, el Subdirector actual permita *tomar decisiones* referente a la seguridad de la información institucional tecnológica. La razón de tomar esta herramienta se debe al tipo de actividad que requiere cumplirse con la seguridad de la información institucional (cíclico), alcanzando *credibilidad para todas las operaciones institucionales* y *la posición de un gerente si ha buscado lo mejor de la industria (en cuanto a la seguridad de la información tecnológica) incorporado a los planes y procesos (institucionales), (*Robert Camp Benchmarking).

El Benchmarking contribuye al logro de los objetivos del negocio de la organización, facilitando la detección de las mejores prácticas que conducen en forma rápida, ordenada y eficiente a la generación de ventajas competitivas y a nuevas oportunidades de negocios (enfocado a la seguridad de la información institucional) a fin de motivar la mejora en el desempeño organizacional (Thompson, 2011).

Los principales beneficios de esta herramienta referente a la seguridad de la información institucional se apreciarán de la siguiente forma:

- Aprender de otra organización pública y privada, cuyos procesos son los mejores (como por ejemplo: petrolero, farmacéutico, instituciones financieras del Ecuador, Presidencia de la República, entre otros).
- Se adaptará lo aprendido para mejorar (cumpliendo lo que señala SGSI).

[18]*Benchmarking:* Ver definición en la sección del glosario.

- Se llegará a un mejoramiento organizacional en cuanto a seguridad de la información mediante un proceso continuo y sistemático de evaluaciones a los servicios y procesos de trabajo de la institución (aplicación del ciclo de Deming); debiéndose laborar las gestiones a corto, mediano y largo plazo.
- Se establecerán metas de desempeño en relación con las prácticas de vanguardia según la necesidad de la seguridad de la información institucional (propia y externa).

Se conoce que el proceso de Benchmarking según el modelo puede ser de diez pasos como lo tiene la organización Xerox, nueve pasos en AT&T, cinco fases y catorce pasos en IBM, entre otros; pero, en el caso de la seguridad de la información del Consejo de la Judicatura se aplicará las cinco principales fases que el modelo de Benchmarking debe cumplir:

1. Definición de objetivos
2. Diagnóstico interno
3. Comparación
4. Definición de actividades
5. Implementación.

El Benchmarking a pesar de ser una herramienta excepcional con muchas ventajas, tiene críticas, por cuanto provoca a las organizaciones a la copia, al espionaje y a la falta de interés por generar conocimientos propios y nuevos, mismos que se ha visto en algunas instituciones públicas y privadas. Sin embargo, se considera también que éstas críticas son

resultado de aquellas organizaciones que no pueden aplicar el verdadero Benchmarking y que solo se interesaron por la copia y no por el aprender, como es el objetivo de esta herramienta; incluso se puede constatar que ciertas normas ISO 27000 no se articula con el negocio de ciertas instituciones.

Por lo expuesto, en este trabajo se establece los objetivos y alcance de esta investigación (capítulo 1); se describe a la institución (capítulos 2), se realiza un análisis y diagnóstico interno referente a la seguridad de la información tomando muestras reales de su estatus (capítulo 3), se propone el diseño de un modelo de gestión para el gerenciamiento de la seguridad de la información tecnológica del Consejo de la Judicatura siempre y cuando los resultados arrojen la necesidad de elaboración de una nueva ruta del modelo de gestión con la descripción de las actividades gerenciales (capítulo 4); y, en cuanto al cumplimiento de mencionado modelo de gestión una vez diseñado, se entregará a las autoridades de la Dirección Nacional de Tecnologías de la Información y Comunicaciones (DNTICs) para su revisión, aprobación y el respectivo despliegue.

Capítulo 2. Estado y análisis del marco institucional y normativo, y su aplicación en la seguridad de la información tecnológica para el Consejo de la Judicatura.

2.1 Antecedentes.

De acuerdo a la Constitución vigente del Ecuador, aprobada en el año 2008, se establecen las responsabilidades de las Funciones del Estado, para lo cual, en el capítulo cuarto se describe a la *Función Judicial* y *Justicia Indígena*, y, que para motivos de estudio del presente trabajo de investigación se tomará en cuenta las siguientes secciones y artículos de mencionado capítulo, teniendo como alcance, la justicia en el Ecuador, como se presenta en la siguiente tabla:

Tabla 2. Secciones y artículos de la Constitución del Ecuador referentes a este estudio.

CAPÍTULO	SECCIÓN	TÍTULO DE LA SECCIÓN	ARTÍCULOS
Cuarto: *Función Judicial y justicia indígena*	Primera	Principios de la administración de justicia.	167-170
	Segunda	Justicia indígena*****.	171
	Tercera	Principios de la Función Judicial.	172-176
	Cuarta	Organización y funcionamiento.	177-178
	Quinta	Consejo de la Judicatura.	179-181
	Sexta	Justicia Ordinaria.	182-188
	Séptima	Jueces de Paz.	189
	Octava	Medios alternativos de solución de conflictos.	190
	Duodécima	Servicio Notarial.	199-200
	Decimotercera	Rehabilitación social.	201-203

***** Según jurisdicción. *Fuente:* Constitución vigente del Ecuador, 2015.*Elaborado por:* el autor, 2016.

De acuerdo a lo expuesto, el Consejo de la Judicatura es un órgano del gobierno ecuatoriano que administra, vigila y disciplina la Función Judicial. Se compone de órganos jurisdiccionales y auxiliares, sin perjuicio de otros órganos con iguales potestades reconocidos en la Constitución, y, son los encargados de administrar justicia (Nacional, 2008).

Los Órganos Jurisdiccionales se componen bajo la siguiente jerarquía: La Corte Nacional de Justicia, Cortes Provinciales de Justicia, Tribunales y Juzgados que establezca la ley y los Juzgados de Paz.

Mientras los Órganos Auxiliares se forman del Servicio Notarial, Martilladores Judiciales, Depositarios Judiciales y los demás que determine la Ley. Por lo tanto, el Consejo de la Judicatura tiene a su cargo y responsabilidad: la Justicia Ordinaria, Jueces de Paz, Medios Alternativos de Solución de Conflictos, Servicio Notarial y la Rehabilitación Social (notificaciones de encarcelamiento y desencarcelamiento).

Los Órganos señalados anteriormente y otras unidades relacionadas con la justicia del Ecuador; y, por motivos de sintetizar el texto en el presente estudio, se los denominarán como estamentos judiciales o dependencias judiciales.

El Consejo de la Judicatura en su Plan Estratégico de la Función Judicial 2013-2019 tiene como visión “la consolidación al sistema de justicia ecuatoriano como un referente de calidad, confianza y valores que promueva y garantice el ejercicio de los derechos individuales y colectivos”; mientras que su misión es “proporcionar un servicio de administración de justicia eficaz, eficiente, efectivo, íntegro, oportuno, intelectual y

accesible, que contribuya a la paz social y a la seguridad jurídica, afianzando la vigencia del Estado constitucional de los derechos y justicia. Sus principios fundamentales son: idoneidad y probidad; sujeción a la Constitución y a todo el ordenamiento jurídico; imparcialidad e independencia; igualdad y equidad; vocación de servicio; transparencia y rendición de cuentas; y, compromiso con la sociedad (Consejo de la Judicatura, 2015)".

Los objetivos estratégicos del Consejo de la Judicatura son "asegurar la transparencia y la calidad en la prestación de los servicios de justicia; promover el óptimo acceso a la justicia; impulsar la mejora permanente y modernización de los servicios; institucionalizar la Meritocracia en el sistema de justicia; y, combatir la impunidad contribuyendo a mejorar la seguridad ciudadana"(Consejo de la Judicatura, 2015).

Otro instrumento normativo institucional es el *Estatuto Integral de Gestión Organizacional por Procesos del Consejo de la Judicatura a Nivel Central y Desconcentrado*; entre los cuales, determina la responsabilidad de la seguridad de la información institucional y del servicio de firma electrónica en la Subdirección Nacional de Seguridad de la Información (SNSI), y ésta a su vez, es adscrito a la Dirección Nacional de Tecnologías de la Información y Comunicaciones (DNTICs).

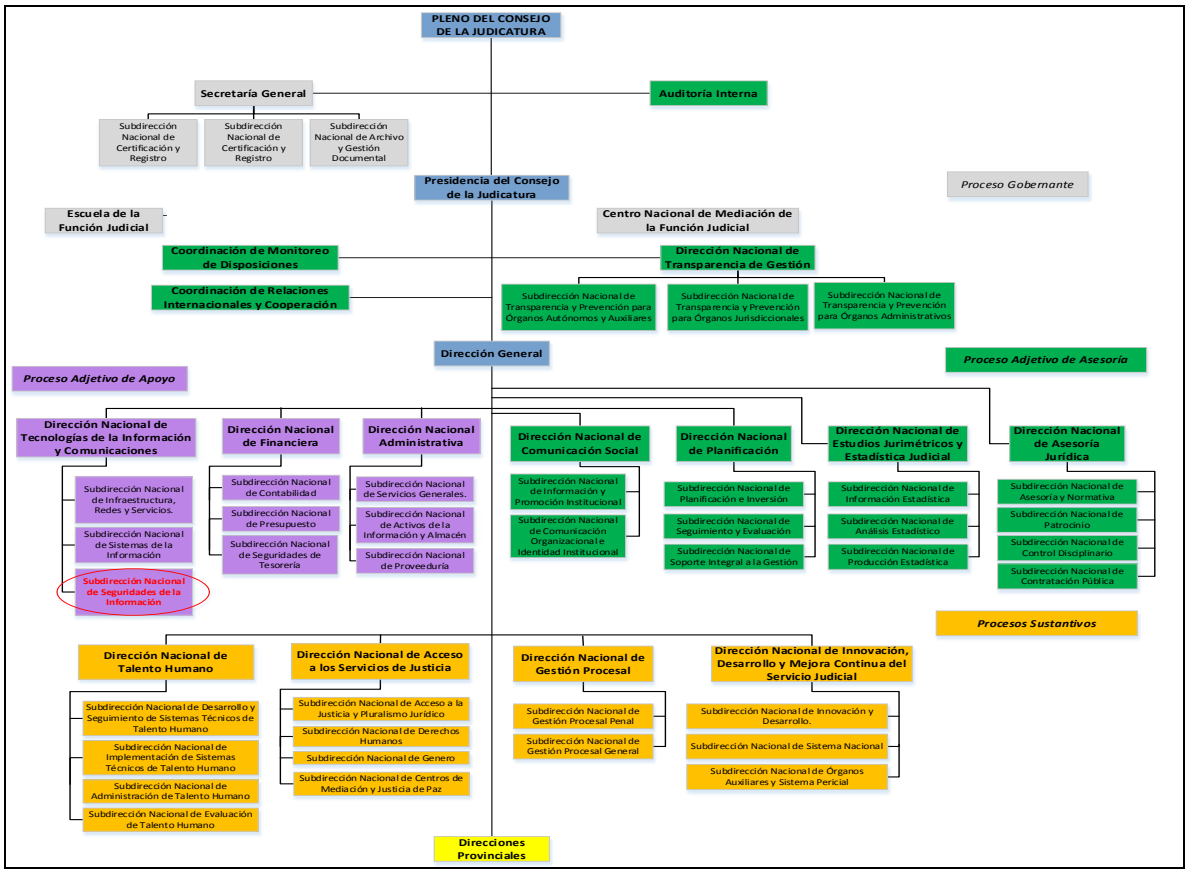
2.2 Estructura organizacional del Consejo de la Judicatura.

Esta institución actualmente cuenta de una compleja estructura orgánica piramidal; donde, la DNTICs tiene como misión el "gestionar y administrar las soluciones y servicios de

tecnología para los procesos de la Función Judicial" (Consejo de la Judicatura, 2015)y está definido como un proceso adjetivo de apoyo para la institución.

La estructura Orgánica del Consejo de la Judicatura se presenta en la *figura* 1, en la cual, la Subdirección nacional de seguridad de la información se encuentra resaltada en la parte inferior de la DNTICs.

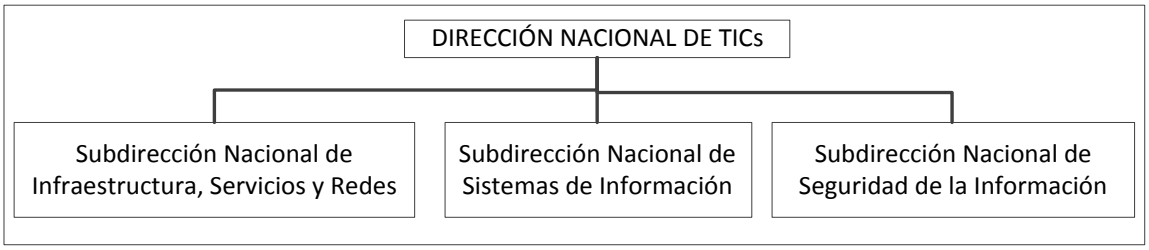
Figura 8. Estructura Orgánica del Consejo de la Judicatura.



Fuente: Estatuto Integral de Gestión Organizacional por Procesos del Consejo de la Judicatura a nivel central y descentralizado, 2015.*Elaborado por:* Institución, 2014, transcrito por el autor.

La DNTICs se compone de tres Subdirecciones: Sistemas de información; Infraestructura, servicios y redes; y finalmente, Seguridades de la información. La siguiente figura presenta la estructura de la DNTICs con sus Subdirecciones nacionales:

Figura 9. Estructura Organizacional de la Dirección Nacional de Tecnologías de la Información y Comunicaciones.



Fuente: Estatuto Integral de Gestión Organizacional por Procesos del Consejo de la Judicatura a nivel central y descentralizado, 2015.*Elaborado por:* el autor, 2016.

Toda política, normativa o lineamiento que son generadas en estas Subdirecciones nacionales se replica con al resto de las direcciones provinciales con el aval del Director nacional de TICs, a través del respectivo *Director Provincial*, se comunica al *Coordinador Provincial* de TICs y éste a su vez, comunica al personal técnico de las tecnologías de la información provinciales para su cumplimiento.

2.3 Normativa, atribución y productos de la Subdirección nacional de seguridad de la información del Consejo de la Judicatura.

De acuerdo al *Estatuto Integral de Gestión Organizacional por Procesos del Consejo de la Judicatura a nivel central y descentralizado* (Consejo de la Judicatura, 2015), la Subdirección nacional de seguridad de la información tiene definido como misión la "preservación de la confidencialidad, integridad y seguridad de la infraestructura

tecnológica y de la información que se procesa, almacena y transmite a través de los diferentes sistemas informáticos institucionales”; para lo cual, tiene que cumplir con sus atribuciones, responsabilidades y productos descritos en el mencionado Estatuto.

2.3.1 Atribuciones y responsabilidades de la Subdirección nacional de seguridad de la información.

Las atribuciones y responsabilidades que tiene la Subdirección nacional de seguridad de la información(Consejo de la Judicatura, 2015), entre las más importantes se describen a continuación:

- Desarrollar y supervisar la ejecución de los planes de respaldo de la información, seguridad de instalaciones físicas, seguridad de hardware y software, planes de contingencia, continuidad de operaciones de TICs y recuperación de desastres de TICs.
- Desarrollar y supervisar el cumplimiento de la gestión de riesgos, de incidentes y continuidad de operaciones de TICs y de los procedimientos internos para la gestión de seguridad de la información;
- Elaborar informes de gestión y cumplimiento de planes de la Subdirección nacional de seguridad de la información.
- Las demás que disponga la autoridad competente.

2.3.2 Productos de la Subdirección nacional de seguridad de la información.

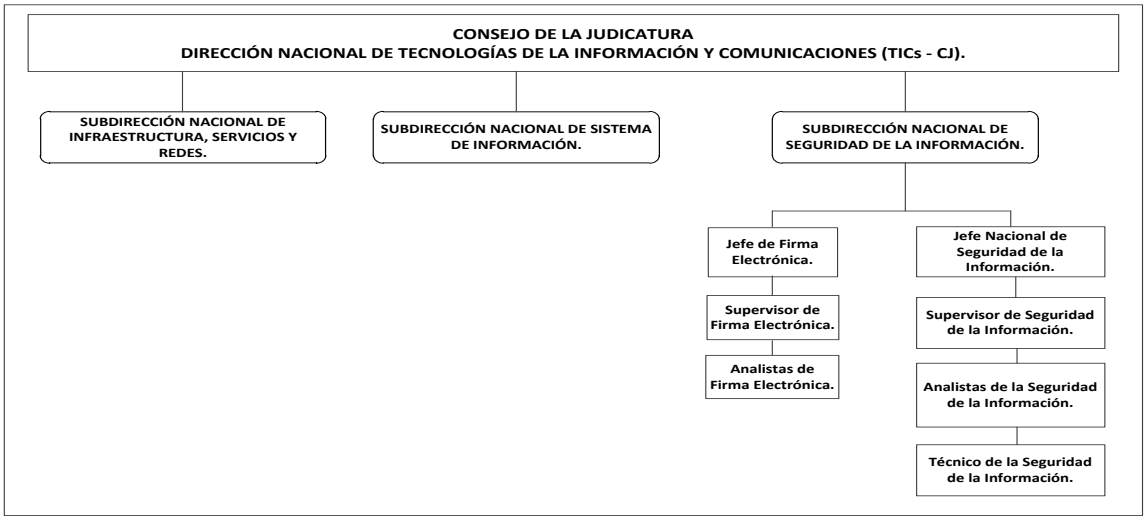
Los productos a cargo de la Subdirección nacional de seguridad de la información(Consejo de la Judicatura, 2015)se ajusta a un proceso de gestión, administración y políticas de seguridad, para lo cual, se debe elaborar, implementar y dar seguimiento a mencionados productos para garantizar la seguridad en la información institucional. A continuación se describen los más importantes:

- Planes de remediación, continuidad de operaciones, recuperación de desastres y contingencias de TICs basados en la gestión de riesgos.
- Propuestas de reglamentos relacionados con la seguridad de la información para el procesamiento y almacenamiento de datos.
- Informes de análisis, vulnerabilidades, tendencias, y riesgos relacionados con la seguridad de la información.
- Indicadores de incidencias y casos de violaciones de políticas de seguridad.
- Informes de auditoría de acceso a plataformas, aplicaciones o servicios de forma interna y externa.

La SNSI del Consejo de la Judicatura tiene la siguiente distribución organizacional, donde el número del personal asignado es reducido, no se incluye firma

electrónica[19] y, se requiere de servidores judiciales con conocimientos y experiencia ligada a la seguridad de la información, como señala la *figura 4*:

Figura 10. Estructura organizacional de la Subdirección nacional de seguridad de la información.



Fuente: Subdirección Nacional de Seguridad de la Información, 2015. *Elaborado por:* el autor, 2016.

2.4 Infraestructura tecnológica del Consejo de la Judicatura.

2.4.1 Sistemas informáticos.

El Consejo de la Judicatura actualmente tiene sistemas y aplicativos informáticos que brindan servicios del tipo jurisdiccional (core del negocio referente a la justicia) y del administrativo (como soporte coadyuvante en el desarrollo institucional) logrando: brindar, agilizar y optimizar las actividades de justicia a la ciudadanía y también a los

[19]*Nota*: El área de firma electrónica para este estudio se considera como un servicio externo que brinda la institución a la ciudadanía y que aún no se plasma en el Estatuto Integral de Gestión Organizacional por Procesos del Consejo de la Judicatura a Nivel Central y Desconcentrado.

servidores judiciales (clientes internos). Al interior del Consejo de la Judicatura se desarrollan, actualizan y plantean sistemas y aplicativos institucionales para mejorar los servicios de justicia y administración institucional. El Consejo de la Judicatura cuenta con los siguientes servicios jurisdiccionales, entre los más principales son: el Sistema Autónomo de Trámite Judicial Ecuatoriano (**S**ATJE), Sistema Único de Pensiones Alimenticias (**S**UPA), Sistema Notarial, Sistema de Subastas Judiciales, proyecto del Código Orgánico General de Procesos (**C**OGEP) que pertenece a la Dirección nacional de gestión procesal, el Sistema de la Dirección de Personal, Sistema Administrativo y otros aplicativos que suman un total de 83 sistemas. A continuación, se describe un resumen a los sistemas informáticos en la tabla No. 3 (*Resumen de los sistemas o aplicaciones informáticas de la institución)*; sin embargo, los detalles de los dueños o propietarios de los sistemas se detallan en el *Anexo 1* (*Detalle de los sistemas o aplicaciones informáticas de la institución*).

Tabla 3. Resumen de los sistemas o aplicaciones informáticas de la institución.

DUEÑO	**NÚMERO DE SISTEMAS**
EXTERNO	***32***
COMUNICACIÓN	3
CONCURSOS	5
ESCUELA JUDICIAL	3
FINANCIEROS	3
INFRAESTRUCTURA	1
JURISDICCIONAL	15
LA SECRETARIA	1
TALENTO HUMANO	1

INTERNO	***51***
ADMINISTRATIVO	1
COMUNICACIÓN	5
DESARROLLO	2
ESCUELA JUDICIAL	2
FINANCIEROS	9
INFRAESTRUCTURA	4
JURISDICCIONAL	15
MESA DE SERVICIOS	8
TALENTO HUMANO	5
Total general	83

Fuente: Subdirección Nacional de Infraestructura, redes y servicios de la DNTICs, 2015.*Elaborado por:* el autor, 2016.

2.4.2 Servicios indispensables de las tecnologías de la información.

Los sistemas antes señalados deben complementarse con otros servicios tecnológicos básicos que requiere toda institución y que se resumen en la *tabla 4* (*Resumen de servicios y responsabilidad de la DNTICs*) y el detalle de estos servicios se encuentra en el *Anexo 2* (*Detalle de los servicios y responsabilidad de la DNTICs*).

Tabla 4. Resumen de servicios y responsabilidad de la DNTICS.

RESPONSABLE: DNTICs.	**NÚMERO DE SERVICIOS**
INFRAESTRUCTURA	9
INFRAESTRUCTURA - REDES	1
MESA DE SERVICIOS	1
OPERACIONES	2
REDES	9
REDES - SEGURIDADES	1

SEGURIDADES	1
Total general	24

Fuente: Subdirección Nacional de Infraestructura, redes y servicios de la DNTICs, 2015.*Elaborado por:* el autor, 2016.

2.4.3 Infraestructura computacional.

En los párrafos anteriores, se presentaron las aplicaciones y servicios que el Consejo de la Judicatura presta y necesita (prácticamente orientado a software[20]); a continuación, se presentarán los equipos tecnológicos o infraestructura tecnológica con los que cuenta la institución para el correcto funcionamiento (prácticamente orientado a *hardware*[21] y/o *software* base). Esta institución dispone de mencionada infraestructura en todos sus estamentos judiciales, como por ejemplo: Unidades de Flagrancia y otros que define la Ley; pero, los más importantes y de mayor cantidad reposan actualmente en el centro de datos principal (el mismo que cumple con la norma internacional TIER 2[22]); en virtud que la información institucionales concentrada. En cada estamento judicial, la infraestructura tecnológica reposa en las denominadas salas o cuartos de comunicaciones y que por normativa de seguridad de la información, no será revelado a detalle. La infraestructura tecnológica que reposan en el centro de datos principal se encuentran resumidos en la tabla No. 5 (*Resumen de los equipos del centro de datos)* y su detalle se encuentra en el *Anexo 3* (*Descripción de los equipos del centro de datos*).

[20]*Software:* Ver definición en la sección del glosario.
[21]*Hardware:* Ver definición en la sección del glosario.
[22] Estándar de la norma ANSI/TIA-942 Telecommunications Infrastructure Standard for Data Centers

Tabla 5. Resumen de los equipos en el centro de datos.

TIPO DE EQUIPOS	NÚMERO DE EQUIPOS
ALMACENAMIENTO	12
VIDEOCONFERENCIA	15
DE AIRE ACONDICIONADO	7
DE ENERGÍA ELECTRICA	4
DE OFICINA (lote)	1
DE RED	191
DE SEGURIDAD	11
SERVIDORES FÍSICOS	103
Total general	344

Fuente: Subdirección Nacional de Infraestructura, redes y servicios de la DNTICs, 2015. *Elaborado por:* el autor, 2016.

El centro de datos principal ubicado en la ciudad de Quito se compone de otros elementos de apoyo, tales como: energía de respaldo: UPS y generados eléctrico, aire acondicionado forzado, sistemas de monitoreo y control interno, almacenamiento o respaldos de información por medio de arreglos de discos duros, cintas y brazo robótico, sistemas de alarma, sistemas de incendios y otros de origen tecnológico. Este centro de datos principal funciona desde el año 2012.

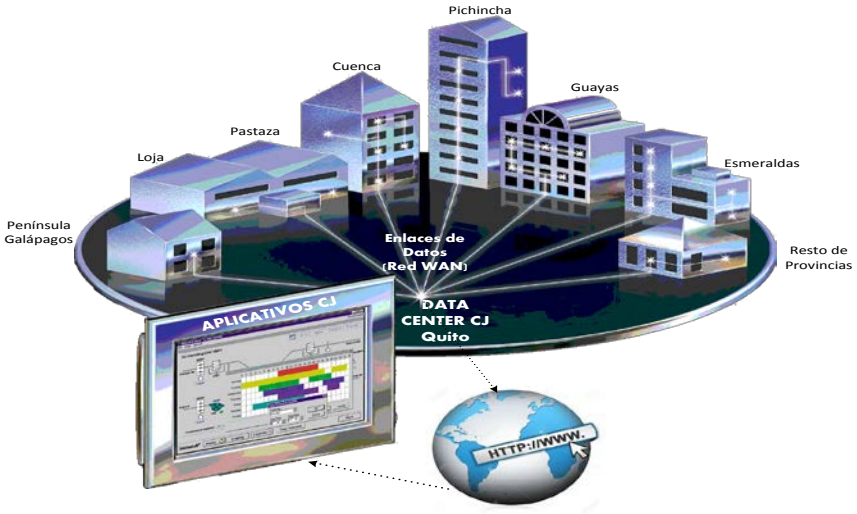
2.4.4 Enlaces de datos.

El portador o proveedor de datos mediante el servicio de enlaces de datos hacia el resto de provincias permite la centralización y procesamiento de la información tecnológica a nivel nacional (cumpliendo el centro de datos la función de nodo principal), es importante

recalcar que desde cada Dirección Provincial o cabecera provincial se brinda conectividad hacia el resto de cantones; teniendo una red de datos institucional del tipo estrella.

La actual topología de la red de datos permite administrar, controlar y monitorear los aplicativos y servicios: jurisdiccionales y administrativos del Consejo de la Judicatura a nivel nacional, como se plasma en la *figura 4:*

Figura 11. Diagrama figurativo de la red tecnológica de la institución a nivel de capitales de provincia.



Fuente: Subdirección Nacional de Infraestructura, redes y servicios de la DNTICs, 2015. *Elaborado por:* el autor, 2016.

2.4.5 Arquitectura tecnológica del Consejo de la Judicatura.

Con el fin de proporcionar el servicio jurisdiccional a los clientes externos e internos se dispone de una arquitectura tecnológica tipo estrella, diseñada bajo el concepto de flexibilidad en el crecimiento de datos y ampliaciones tecnológicas según el presupuesto económico anual asignado; donde sin necesidad de cambiar la estructura tecnológica actual, se puede ampliar procesamiento, repositorios de información, incrementar anchos

de banda, entre otras necesidades tecnológicas a cubrirse. Por lo tanto, los servicios no serán interrumpidos al momento de aplicar un crecimiento y/o ampliación. A continuación, se presenta un ejemplo de la arquitectura implementada con el Sistema Autónomo de Trámite Judicial Ecuatoriano (**S**ATJE), el mismo que está en el *Anexo 4* (*Arquitectura tecnológica del Sistema Autónomo de Trámite Judicial Ecuatoriano – SATJE*).

La Dirección nacional de tecnología de la información y comunicaciones, tiene la jefatura de mesa de servicios, unidad adscrita a la Subdirección nacional de infraestructura, servicios y redes. Esta jefatura registra los incidentes y requerimientos de los servidores judiciales.

La jefatura de operaciones se encarga de garantizar el funcionamiento y operaciones de los servicios y aplicaciones institucionales para los clientes externos e internos; para lo cual, esta jefatura también es adscrita a la Subdirección nacional de infraestructura, servicios y redes.

Capítulo 3. Análisis y diagnóstico del estado actual de uso y aplicabilidad de las normas y estándares nacionales e internacionales para un sistema de gestión de seguridad de la información tecnológica en el Consejo de la Judicatura.

Para el análisis de la seguridad de la información tecnológica en el Consejo de la Judicatura se toma información de primera mano y que son remitidos periódicamente, tales como: reporte del antivirus institucional, informe de incidentes trimestrales relacionados con la seguridad de la información, disponibilidad de los servicios jurisdiccionales, talleres de trabajo entre las Subdirecciones que conforman la Dirección Nacional de TICs, entre otros documentos catalogados de carácter reservado.

Sin embargo, los documentos que requiere el análisis y diagnóstico del estado actual referente a la seguridad de la información tecnológica en el Consejo de la Judicatura, permitiendo conocer la gestión del gerenciamiento actual y el estatus, objeto de esta investigación, se describe a continuación:

3.1 Diagnóstico del uso y aplicabilidad de las normas y estándares nacionales e internacionales para un sistema de gestión de seguridad de la información tecnológica en el Consejo de la Judicatura del Ecuador.

En referencia al análisis del uso y aplicabilidad de las normas y estándares nacionales e internacionales para la actual gestión de seguridad de la información tecnológica en el Consejo de la Judicatura se considera el acceso libre a la información generada en

entidades públicas o que realicen las Funciones Públicas y ninguna entidad pública podrá negar dicha información, como se señala la Carta Magna en su artículo 18; sin embargo, la Carta Magna no especifica la normativa que debe acogerse el Consejo de la Judicatura para proteger sus datos.

También, se considera que la seguridad de la información de origen tecnológico en el sector público, específicamente, en la Función Ejecutiva está bajo la responsabilidad de la Secretaria Nacional de la Administración Pública (**S**NAP), para lo cual, el Consejo de la Judicatura deberá ajustarse con parámetros de seguridad de la información definidos por este ente de Gobierno, en virtud que existe intercambio de información, como es el caso de la validación de datos con la Dirección Nacional de Registros y Datos Públicos (**D**INARDAP).

El Estado tiene a disposición el Instituto Ecuatoriano de Normalización (**I**NEN), el mismo que como organismo técnico nacional, eje principal del Sistema Ecuatoriano de la Calidad en el país, competente en la Normalización, Reglamentación Técnica y Metrología, que contribuye a garantizar el cumplimiento de los derechos ciudadanos relacionados con la seguridad; la protección de la vida y la salud humana, animal y vegetal; la preservación del medio ambiente; la protección del consumidor y la promoción de la cultura de la calidad y el mejoramiento de la productividad y competitividad en la sociedad ecuatoriana (INEN, 2016); provocando el cumplimiento de éstas normativas y reglamentaciones que debe ser acatado en el Ecuador por medio del **I**NEN, se procede a tomar como referencia su normativa, estándares y guías para la implementación de

sistemas de gestión de la seguridad de la información (**S**GSI), considerando que el **I**NEN regula el sistema Ecuatoriano, de tal forma, que el Consejo de la Judicatura se ajustará a estas normas y también debe interactuar con otras instituciones público y/o privadas del Ecuador.

El Consejo de la Judicatura al momento de desarrollar con las aplicaciones o servicios informáticos debe observar y cumplir con lo que señala la información pública y privada en la Constitución, Código Orgánico de la Función Judicial, Ley Orgánica de Transparencia y Acceso a la Información, Ley de Propiedad Intelectual, Ley del Sistema Nacional de Registros de Datos Públicos, Estatuto de Gestión Organizacional por Procesos, Normas de Control Interno de la Contraloría General del Estado y entre otros que sean considerados los órganos de control en el Ecuador.

3.1.1 Análisis de cumplimiento según normativas de seguridad de la información según INEN.

Se realiza un análisis del cumplimiento de las normativas que señala el **I**NEN referente a la seguridad de la información para el Consejo de la Judicatura, como se describe en el *Anexo 5* (Análisis del uso y aplicabilidad según las normas INEN para un sistema de gestión de seguridad de la información tecnológica institucional); y su resumen, se presenta en la siguiente tabla:

Tabla 6. Resumen de normativas o estándares INEN cumplidos por el Consejo de la Judicatura.

DESCRIPCIÓN	SI	NO	PARCIAL	TOTAL
Normativa / Estándares de Seguridad de la Información en el CJ.	0	15	9	24
Peso o participación.	0,00%	62,50%	37,50%	100%

Fuente: INEC, catálogo de documentos normativos vigentes, responsable: dirección de normalización, actualización: marzo 2016.
Elaborado por: El autor, 2016.

El resultado de la tabla anterior presenta que no se cumple 15 normativas y estándares que señala el **I**NEN con respecto a la seguridad de la información institucional y también, el Consejo de la Judicatura se encuentran desarrollando 9 normativas.

3.1.2 Matriz de complimiento según norma ISO27001-2013.

Se elaboró la evaluación de la denominada "matriz de complimiento de la seguridad de la información" de acuerdo a lo que señala norma ISO27001-2013 (*Ver Anexo 6*), cuyo resultado por el cumplimiento por sección de la norma se expone en la siguiente tabla:

Tabla 7. El tablero de cumplimiento por sección de la norma ISO 27001-2013.

Sección	Estatus
Políticas de seguridad	30%
Aspectos organizativos de la seguridad de la información	50%
Seguridad ligada a los recursos humanos	82%
Gestión de Activos	56%
Control de accesos	75%
Cifrado	0%
Seguridad física y ambiental	78%
Seguridad en la operación	72%
Seguridad en las telecomunicaciones	81%
Adquisición, desarrollo y mantenimiento de los sistemas de información	91%
Relaciones con suministradores	61%

Gestión de incidentes en la seguridad de la información	70%
Aspectos de seguridad de la información en la gestión de la continuidad del negocio	45%
Cumplimiento	60%

Fuente: INEC, catálogo de documentos normativos vigentes, responsable: dirección de normalización, actualización: marzo 2013.
Elaborado por: ISO y el autor, 2016.

Mientras que el resultado por cumplimiento de control se expresa en la siguiente tabla:

Tabla 8. Tablero de cumplimiento por control de la norma ISO 27001-2013.

Estándar	Sección	Estatus
A.5.1	Directrices de la Dirección en la seguridad de la información	30%
A.6.1	Organización interna	54%
A.6.2	Dispositivos para movilidad y teletrabajo	40%
A.7.1	Antes de la contratación	83%
A.7.2	Durante la contratación	80%
A.7.3	Cese o cambio de puesto de trabajo	85%
A.8.1	Responsabilidad sobre los activos	85%
A.8.2	Clasificación de la Información	47%
A.8.3	Manejo de los soportes de almacenamiento	25%
A.9.1	Requisitos de negocio para el control de acceso	85%
A.9.2	Gestión de acceso para los usuarios	53%
A.9.3	Responsabilidades del usuario	100%
A.9.4	Control de acceso a sistemas y aplicaciones	91%
A.10.1	Controles criptográficos	0%
A.11.1	Áreas seguras	83%
A.11.2	Seguridad de los equipos	75%
A.12.1	Responsabilidades y procedimientos de operación	69%
A.12.2	Protección contra código malicioso	95%
A.12.3	Copias de seguridad	90%
A.12.4	Registro de actividades y supervisión	88%
A.12.5	Control de software en explotación	60%
A.12.6	Gestión de vulnerabilidad técnica	68%
A.12.7	Consideraciones de las auditorías de los sistemas de información	0%
A.13.1	Gestión de la seguridad en las redes	78%
A.13.2	Intercambio de información con partes externas	84%
A.14.1	Requisitos de seguridad en los sistemas de información	95%
A.14.2	Seguridad en los procesos de desarrollo y soporte	90%
A.14.3	Datos de prueba	75%
A.15.1	Seguridad de la información en las relaciones con suministradores	78%
A.15.2	Gestión de la prestación del servicio por suministradores	35%

A.16.1	Gestión de incidentes de seguridad de la información y mejoras	70%
A.17.1	Continuidad de la seguridad de la información	40%
A.17.2	Redundancias	60%
A.18.1	Cumplimiento de los requisitos legales y contractuales	57%
A.18.2	Revisiones de la seguridad de la información	65%

Fuente: INEC, catálogo de documentos normativos vigentes, responsable: dirección de normalización, actualización: marzo 2013. ***Elaborado por:*** El autor, 2016.

De acuerdo a los resultados presentados, el cumplimiento de la norma ISO 27001 del 2013, tanto por la sección como por el nivel de control, se observa que el Consejo de la Judicatura presenta algunas falencias en el cumplimiento en cuanto a la seguridad de la información institucional; para lo cual, se requiere tomar los correctivos necesarios en cada uno de los ítems incumplidos.

3.1.3 Matriz de riesgos institucional.

Se elaboró la matriz de riesgo institucional bajo pedido de la Máxima Autoridad a finales del año 2015 (*Ver Anexo 7*), cuyo resultado se expone en el siguiente cuadro:

Tabla 9. Matriz de riesgos institucional.

Riesgos Inherente	**Cantidad**	**Peso**
INACEPTABLE	0	0,0%
IMPORTANTE	1	14,3%
MODERADO	2	28,6%
TOLERABLE	2	28,6%
ACEPTABLE	2	28,6%
TOTAL	**7**	**100%**

Fuente: Consejo de la Judicatura 2015. ***Elaborado por:*** El autor, 2016.

Según los resultados presentados, se observa que el Consejo de la Judicatura no presenta riesgos inherentes inaceptables, apenas un riesgo inherente importante, mientras

que el resto de riesgos son moderados y también tolerables; lo que implica trabajar en soluciones finales o de remediación; sin embargo, es importante señalar que dicho resultado está globalizado yes transversal para toda la institución por lo que se requiere la gestión como DNTICs y el apoyo por parte de la Máxima Autoridad, sin olvidar que el riesgo importante también incluye los equipos de seguridad perimetral institucional.

3.2 Análisis de vulnerabilidades con prueba de penetración (Pen test).

La "prueba de penetración"[23] o "pen test" se efectuó en el mes de marzo del 2016, y, permite diagnosticar vulnerabilidades en los servicios, servidores, redes y servicios informáticos del Consejo de la Judicatura mediante el uso de una herramienta informática de nivel avanzado, apoyado en el "Manual de la Metodología Abierta de Testeo de Seguridad (OSSTMM)[24]", convirtiéndose en un manual estándar para pruebas y análisis de seguridad de la información, debido a que considera un primer nivel de acercamiento al concepto global de seguridad, pasando a desarrollar pruebas de calidad, ordenada y eficiente. Los resultados de la información encontrada se catalogará como: importante, media o leve. El nivel de la prueba se lo realizó en modo escucha por medio del aplicativo informático denominado *Kali Linux* (Kali Linux Penetration Testing Tools, 2016) es decir, no se acudió a un ataque violento o uno del tipo ataque bruto que torture o

[23] *Prueba de penetración:* Ver definición en la sección del glosario.
[24] *Manual de la Metodología Abierta de Testeo de Seguridad (OSSTMM):* Ver definición en la sección del glosario.

fuerce a los sistemas o infraestructura tecnológica de la institución al momento de su funcionamiento.

La metodología utilizada en esta herramienta para el Consejo de la Judicatura se describe brevemente en los siguientes detalles:

- Recopilación de información**.-** Incorpora internamente una herramienta para el análisis de red, presenta una gráfica del diseño e incorpora información técnica de la institución a nivel de capa de red, permitiendo explorar la información de los documentos, imágenes y otro tipo de archivos a nuestro alcance por medio de la navegación web (metadatos).

- Enumeración.- Presenta y explora las direcciones IPs de los equipos pertenecientes a la institución en estudio, entrega nombres de usuarios, contraseñas válidas en su entorno, nombres de los servicios, aplicaciones accesibles y todo aquello que puede ayudar a lanzar un ataque. Esta primera fase permite investigación, no se lleva a cabo ningún ataque pero se posee información muy valiosa.

- Análisis.- Se actúa sobre los sistemas encontrados según lo descrito en el paso anterior. Mediante navegación web se busca vulnerabilidades en la infraestructura tecnológica, sistemas operativos, servicios disponibles o las aplicaciones existentes.

- Explotación**.-** Se realiza la intrusión a los servicios, servidores, redes y servidor de archivos del Consejo de la Judicatura y se obtiene las evidencias del trabajo realizado.

- Identificación de los componentes**.-** Se realiza la recopilación de la información, enumeración, análisis y explotación; es decir, permite clasificar la información navegada.

- Documentación.- Se procede a elaborar un informe de forma entendible y digerible para ser presentado a las autoridades, donde constan todos los descubrimientos, en virtud que el aplicativo seleccionado no emite reportes autónomos.

El aplicativo mencionado presenta pantallas con resultados gráficos y detalles técnicos que brindan un modo amigable para el encargado de realizar la prueba. El informe del análisis de vulnerabilidades se encuentra en el *Anexo 8* (*Informe del análisis de vulnerabilidades del CJ*), mientras que los hallazgos y el tipo de información encontrada se detallan en la *tabla 10*.

Tabla 10. Tabla de hallazgos con la prueba de penetración.

HALLAZGOS		
SECCIÓN	**DETALLES**	**TIPO DE INFORMACIÓN**
Sistema Alfesco (repositorio) acceso a toda la información: memorandos, archivos institucionales, archivos personales, otros.	Archivos con información de todos los funcionarios, incluyendo correos electrónicos.	Importante
	Archivos del tipo script (archivo de programación ejecutable y que funciona para los sistemas informáticos del CJ, varias versiones).	Importante
	Archivos con información de los servidores, nombres, direcciones IP.	Importante
	Archivos del tipo Script con credenciales y direcciones IP	Importante
	Listados de usuarios y datos personales que utiliza el SUPA (Sistema Único de Pensiones Alimenticias)	Importante
	Respaldos de bases de datos	Importante
	Instaladores de programas, configuración, credenciales de sistemas SAAR	Importante
	Información de usuarios para ingeniería social	Importante
	Publicaciones de aplicativos o servicios con IIS, Jboss, otros.	Importante
	Instaladores de software pirata	Importante
Redes informáticas	Navegación y escaneo de la red del CJ desde cualquier punto de red.	Importante

	Acceso a las estaciones de trabajo como administrador con las credenciales por defecto	Importante
	Configuración y acceso a los teléfonos IP	Importante
	Configuración y acceso a las cámaras IP	Importante
	Servidores con puertos abiertos de uso innecesario	Importante
	Acceso a los servidores de impresión, credenciales por defecto e ingreso a la configuración	Importante
	Servidores FTP sin uso	Importante

Fuente: *Subdirección Nacional de Seguridad de la Información de la* DNTICs, 2016. *Elaborado por*: SNSI, *2016.*

De acuerdo a lo señalado en la tabla anterior, toda la información está catalogada como importante, en virtud, que existen datos de los servidores judiciales, acceso a los programas de los aplicativos y servicios jurisdiccionales e incluso, información de la misma institución en calidad de memorandos; para la cual, cualquiera de esta información tecnológica está comprometida y expuesta a pérdidas, substracción, extorciones, venta o un mal uso.

3.3 Desarrollo y análisis FODA de la Subdirección Nacional de Seguridad de la Información.

Luego de realizar un diagnóstico de la seguridad de la información del Consejo de la Judicatura, a continuación es necesario realizar un diagnóstico de la Subdirección nacional de seguridad de la información mediante un análisis FODA que se detalla a continuación:

3.3.1 Análisis Interno.

Para el diagnóstico interno de la Subdirección nacional de la seguridad de la información es necesario analizar las fuerzas internas que están incidiendo para facilitar el logro de los objetivos trazados, y, definir las limitaciones que impiden el alcance de las metas de una manera eficiente y efectiva. Es decir, en el primer caso se refiere a las fortalezas y en el segundo caso a las debilidades. Entre ellos se puede mencionar los principales recursos: humanos, materiales, financieros, tecnológicos y físicos.

- Fortalezas.- El Consejo de la Judicatura realizó la adquisición de modernos bienes tecnológicos para la seguridad de la información en el período 2012 al 2014, incluyendo la capacitación de sus funcionarios a cargo del área de tecnología, por lo que se cuenta con personal de altos conocimientos técnicos de los equipos tecnológicos implementados institucionalmente, mismos que utilizan, configuran, operan y actualizan, de acuerdo a las necesidades diarias.

La institución cuenta con herramientas tecnológicas que permiten controlar sectores de la seguridad de la información como son el antivirus los equipos de seguridad perimetral institucional (equipos Cisco bajo lineamientos de seguridad); los mismos que actualmente son controlados por la Subdirección de Infraestructura.

La SNSI elaboró el manual de políticas de seguridad de la información V1.0, basada en las normativas nacionales e internacionales, en este caso, se aplica la normativa **I**NEN referente a seguridades de la información de la ISO.

La SNSI al ser una nueva área institucional que lleva apenas dos años en funcionamiento, dispone de personal técnico y administrativo con la capacidad en la elaboración de planes y programas que permitan proteger la información institucional; y, los estudios profesionales mínimos para la contratación en esta área corresponde a nivel 3 y relacionados con la seguridad de la información.

- *Debilidades*.- El Consejo de la Judicatura no cuenta con la aprobación formal del manual de políticas de la información a nivel de la Máxima Autoridad, solamente, se encuentra aprobado a nivel de la Dirección nacional de tecnologías de la información y comunicaciones, limitando ciertas acciones; y, se cuenta con determinados procedimientos para este fin.

La SNSI no cuenta con ciertas definiciones y estandarizaciones básicas de documentos, procesos, roles y funciones legalmente definidas que apoyen el buen desarrollo de las actividades operativas y funcionales del personal de seguridad de la información y sus jerarquías.

También se conoce la existencia de ataques involuntarios a los servicios, aplicativos o a la infraestructura tecnológica institucional por el desconocimiento de los servidores judiciales en materia de seguridad de la información, el mismo que origina reparaciones constantes a sus computadores, suspensión de actividades por el desconocimiento en el uso de correos no deseados (SPAM), código malicioso, phising y

otros que afectan el rendimiento en el procesamiento de información en los equipos tecnológicos.

La Subdirección mencionada dispone de un plan de contingencia probado técnicamente con ciertas limitaciones y que las Autoridades institucionales tienen conocimiento debido al gran impacto que esto conlleva al momento de detener el centro de datos, originado por el elevado volumen de información procesada, almacenada y que debe ser transmitida.

Los sistemas e infraestructura de la seguridad de la información institucional tienen pendiente el cumplimiento de las garantías de licencias y mantenimiento en los equipos tecnológicos en el centro de datos, lo que limita la emisión de reportes automáticos, pero, se continúa protegiendo la información institucional según licenciamiento caducado. Como es de conocimiento público en este período de tiempo, el Gobierno del Ecuador dispuso recorte en el gasto y presupuesto anual del estado, lo que genera recursos económicos insuficientes para esta institución; cabe mencionar que al interior de la Subdirección se mantiene la gestión e insistencia en los trámites para las garantías de licencias y mantenimiento de los equipos y otras necesidades que se vinculan con la parte económica.

3.3.2. Análisis Externo.

Para realizar este tipo de diagnóstico en la SNSI es necesario analizar las condiciones o circunstancias ventajosas de su entorno que la pueden beneficiar; identificadas como las oportunidades; así como también con las tendencias del contexto, que en cualquier momento pueden ser perjudiciales y que constituyen las amenazas, con estos dos elementos se podrá integrar el diagnóstico externo.

- *Oportunidades*.- Frente al actual papel que desempeña la SNSI al interior de la DNTICs del Consejo de la Judicatura y éste a la vez, desarrolla, implementa y brinda los servicios informáticos a la ciudadanía, en el cual, la SNSI debe monitorear y controlar la seguridad de la información institucional, mediante el uso de software, preferible que no requieran licencias en virtud de las condiciones económicas señaladas anteriormente.

El análisis, implementación y seguimiento a los planes y programas de la seguridad de la información que permitan proteger y mejorar continuamente los servicios y aplicaciones institucionales relacionadas a la seguridad de la información institucional; mismos que contribuirán a la protección de los datos tecnológicos y alcanzar la eficiente, eficaz y efectivo uso de los recursos institucionales para un prudente tiempo de implementación.

- *Amenazas*.- Dentro de las amenazas que está expuesta la SNSI, se tienen los desastres naturales que pueden afectar a las dependencias judiciales, como por ejemplo, el caso en la provincia de Manabí. Ataques de ignotos hacia los servicios, aplicativos o

infraestructura tecnológica institucional, como es el caso de los portales web en las provincias de Loja y Machala.

Ataques a los servicios, aplicativos o infraestructura tecnológica desde el exterior con código malicioso, spam, fishing, ingeniería social, entre otros; incluso se puede suplantar el acceso de los usuarios hacia los sistemas o aplicativos asignados desde computadores no autorizados, eliminación de tablas con el contenido de claves de acceso a usuarios externos.

El intercambio de información entre instituciones se encamina por medio de la DINARDAP y administrativamente se maneja la figura de convenio institucional.

Los nuevos métodos o herramientas tecnológicas para vulnerar la seguridad de la infraestructura, sistemas y aplicativos tecnológicos institucionales cada día son más asombrosos debido al desarrollo de la tecnología; donde inicialmente se busca buenos fines pero su uso se convierte en perverso.

Por lo expuesto, es importante tener buenas prácticas de seguridad de la información pero, el principal reto es reducir la obtención de información confidencial a través de los servidores judiciales; como parte más frágil de la cadena de información.

Tabla 11. Análisis FODA de la SNSI.

FORTALEZAS	**DEBILIDADES**
• Cuenta con profesionales especializados en políticas, infraestructura y software de TICs, y, con experiencia de seguridades de la información. • Cuenta con protección reactiva y preventiva; protegiendo eficazmente los	• No se cuenta con la aprobación del manual de políticas de la información a nivel de la Máxima Autoridad. • No se cuenta con una definición de estandarización de documentos, procesos, roles y funciones en la

virus, troyanos y todo tipo de programas malignos. • Se dispone de una solución perimetral para proteger información tecnológica institucional. • Manual elaborado de políticas de seguridad de la información basado en las normativas nacionales e internacionales (ISO). • Capacidad para el desarrollo de planes y programas que permitan proteger la información institucional.	Subdirección. • Ataques involuntarios a los servicios, aplicativos o a la infraestructura tecnológica institucional por el desconocimiento de los servidores judiciales en materia de seguridad de la información. • Plan de contingencia no aplicable técnicamente. • Falta de aprovechamiento de las capacidades de la infraestructura tecnológica de la seguridad de la información institucional. • Recursos económicos insuficientes.
OPORTUNIDADES	**AMENAZAS**
• Flexibilidad y escalabilidad en el uso de herramientas tecnológicas respecto a la seguridad de la información. • Implementación de nuevos planes y programas que permitan proteger y mejorar continuamente los servicios y aplicaciones institucionales relacionadas a la seguridad de la información institucional.	• Desastres naturales. • Ataques externos dirigidos a los servicios, aplicativos o infraestructura tecnológica institucional. • Cambios en la normativa legal para el manejo de la seguridad de la información a nivel institucional. • Nuevos métodos o herramientas tecnológicas para vulnerar la seguridad de la infraestructura, sistemas y aplicativos tecnológicos institucionales. • Novedosas prácticas modernas para obtener información confidencial a través de los servidores judiciales.

Fuente: *El autor, 2016*. ***Elaborado por:*** *El autor, 2016.*

3.9 Propuesta de estrategia según análisis FODA.

De acuerdo al análisis FODA del numeral anterior, se convierte en la base del fortalecimiento de la SNSI, para lo cual, se planeta las siguientes estrategias:

Tabla 12. Propuesta de estrategia.

	Amenazas	**Oportunidades**
Fortalezas	**Estrategias defensivas:** • Realizar planes y programas que permitan reducirlos impactos ante desastres o ataques externos dirigidos a los servicios, aplicativos o infraestructura tecnológica institucional. • Elaboración de procedimientos para el cumplimiento del manual de políticas de seguridad de la información. • Capacitación permanente al personal de seguridad de la información sobre los nuevos métodos o herramientas tecnológicas de la seguridad de la información. • Informar, concientizar y socializar periódicamente a los servidores judiciales sobre las distintas formas de estafa en materia de seguridad de la información.	**Estrategias ofensivas:** • Ejecución de pruebas periódicas que se relacionan con la seguridad de la información institucional e informar. • Seguimiento y evaluación de planes y programas que permitan proteger y mejorar continuamente los servicios y aplicaciones institucionales relacionadas a la seguridad de la información. • Creación de un plan de catálogos de cuentas de usuario para el ingreso a los servicios, aplicativos y plataforma tecnológica institucional. • Creación de un programa informático para la gestión de la seguridad de la información, permitiendo el control de acceso a los servicios, aplicativos y plataforma tecnológica institucional.

Debilidades	**Estrategias de supervivencia:** • Desarrollar un plan o programa de continuidad en los servicios o aplicativos institucionales de acuerdo al manual de políticas. • Registro de incidentes relacionados a la seguridad de la información. • Actualizar el plan de contingencia de acuerdo a los nuevos métodos o herramientas tecnológicas.	**Estrategias de reorientación:** • Implementación de herramientas tecnológicas que permitan el cumplimiento del manual de políticas de seguridad de la información. • Implementación de planes y programas que permitan proteger y mejorar continuamente los posibles ataques involuntarios a los servicios, aplicativos e infraestructura tecnológica institucional. • Diseñar un manual de indicadores que están relacionados con la seguridad de la información.

Fuente: *El autor, 2016*. ***Elaborado por:*** *El autor, 2016.*

3.9.1 Validez y gestión de la estrategia planteada.

De acuerdo a los anteriores numerales referente al análisis y propuesta de estrategia FODA, el presente estudio tiene una validez por dos años a partir de la aprobación o hasta la entrega de una nueva versión.

La SNSI procederá con la revisión del presente documento, efectuarán las observaciones y actualizaciones necesarias, previa aprobación. El documento se evaluará en el período de un año y tendrá una validez no mayor al año 2019.

Por lo expuesto en este capítulo y el anterior, se requiere el diseño de una modelo de gestión para el gerenciamiento de la seguridad de la información del Consejo de la Judicatura bajo la competencia de la Subdirección Nacional de Seguridad de la Información, como señala el Estatuto Institucional vigente.

Capítulo 4. Diseño de un modelo de gestión para el gerenciamiento de la seguridad de la información tecnológica del Consejo de la Judicatura.

Un modelo de gestión "se entiende como esquema o marco de referencia que una organización utiliza para planear, organizar, dirigir, coordinar y controlar un proceso, de tal forma que el tratamiento de las entradas genere las salidas adecuadas con las cuales se pretende obtener uno o más objetivos organizacionales" (Enríquez B, 2014). Un modelo de gestión puede ser aplicado a una empresa, negocios privados y a la administración pública, por lo tanto los gobiernos tienen un modelo de gestión que se basan para desarrollar políticas y acciones, consiguiendo así sus objetivos. El modelo de gestión que utiliza el sector público normalmente no busca obtener ganancias económicas pero busca el bienestar social.

4.1 Antecedentes.

El modelo de gestión propuesto para el gerenciamiento de la seguridad de la información tecnológica del Consejo de la Judicatura toma como insumo a las responsabilidades, atribuciones y productos de la SNSI, definidos en el *Estatuto Integral de Gestión Organizacional por Procesos del Consejo de la Judicatura a Nivel Central y Desconcentrado*, misma que se describió en el capítulo I.

El siguiente insumo corresponde al resultado de la *Matriz de cumplimiento de la norma ISO 27001-2013* sobre la seguridad de la información, descrito en el capítulo

anterior y que presenta un valor promedio de los controles implementados en la institución de estudio.

La herramienta de gestión gerencial para la seguridad de la información que permiten integrar los dos insumos señalados y que permite realizar una mejora continua con respecto a nuestros propios indicadores con respecto a la seguridad de la información es la herramienta de *Benchmarking,* descrita en el capítulo I; permitiendo tomar decisiones gerenciales sobre el estado de la seguridad de la información tecnológica institucional según los resultados de la evaluación inicial (punto de partida); y, así reportar a las autoridades de la institución; para lo cual, se describe en los próximos subcapítulos.

4.2 Análisis documental.

4.2.1 Productos de la SNSI:

De acuerdo a los productos de la SNSI definidos en el capítulo I y manteniendo el mismo orden, se presentan las fases que debe cumplir cada uno de estos productos y el tiempo estimado hasta la implementación, información detalla en el *Apéndice A*, mismo que servirá para describir el porcentaje de avance y el número de entregables para un período de tiempo. Estos avances servirán para el desarrollo del Programa Anual de Política Pública (PAPP), Programa Plurianual de Política Pública (PPPP) y del Plan Operativo Anual (POA) que corresponde a la SNSI.

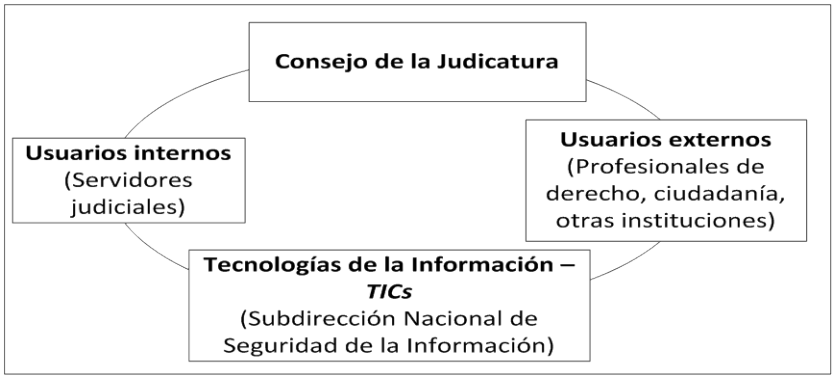
4.2.2 Evaluación de la Matriz de cumplimiento de la ISO 27001-2013:

Por medio de esta Matriz se obtiene valores preliminares de la seguridad de la información tecnológica institucional y que por asunto de este estudio, se los denominará *estatus base*; mismos que pertenecen al *cumplimiento por control de la norma ISO 27001-2013*; este resultado presenta actualmente un valor promedio del 64,50% y se propone alcanzar un crecimiento anual, dando como resultado el tiempo de vencimiento en años; mismo que será desarrollado en el modelo de gestión según los niveles descritos en el *Apéndice B (Modelo de crecimiento propuesto según crecimiento propuesto por año basado en el tablero de cumplimiento por control de la norma ISO 27001-2013*) y definir valores de umbral institucional; conservando el mismo número de personal que cuenta la SNSI.

4.3 Enfoque sistemático.

De acuerdo a lo expuesto en los párrafos anteriores del presente trabajo de investigación se puede determinar a los actores principales y su relación con la seguridad de la información en la institución de estudio, como se ilustra en la siguiente figura:

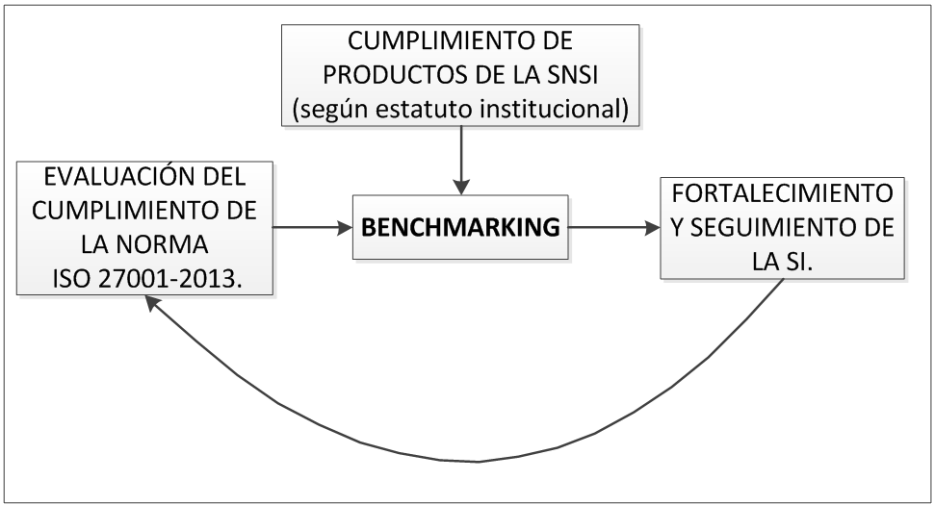
Figura 12. Descripción de actores.



Fuente: El autor. *Elaborado por:* el autor, 2016.

La representación para el gerenciamiento de la seguridad de la información del Consejo de la Judicatura (operativa y lógica) se ilustra en la siguiente figura:

Figura 13. Ilustración de un ataque a los servicios jurisdiccionales y su restauración.



Fuente: SNSI, 2016. *Elaborado por*: el autor, 2016.

4.4 Diseño del modelo.

La SNSI como parte inicial de este modelo de gestión debe proponer la regularización de los procedimientos internos, tales como: estandarizar ciertos documentos internos y almacenar esta información en un repositorio digital; y, por motivos del presente estudio se denominará: "Estándar de conocimiento y documentación de la **S**NSI", para lo cual, se requiere cumplir con los siguientes detalles:

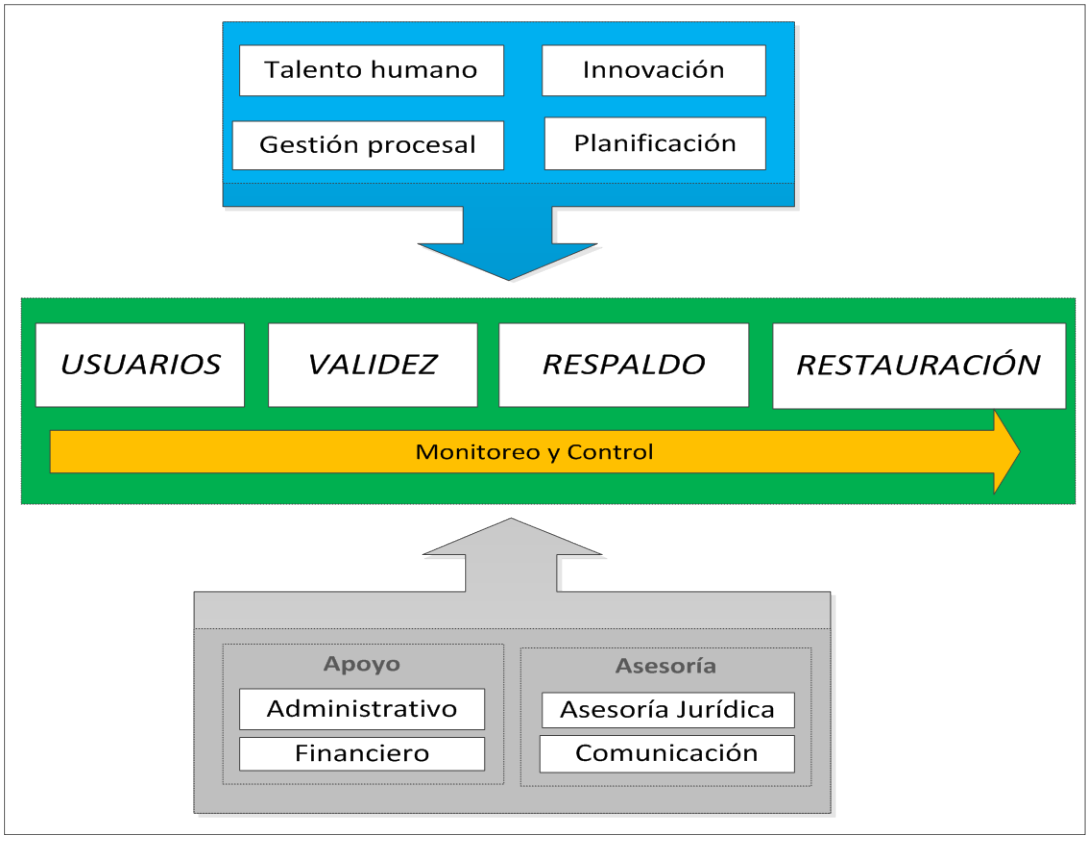
- Elaborar los documentos necesarios que describan las normas, métodos, procesos y prácticas internas que establece la SNSI y que debe cumplir el personal de esta Subdirección tomando cuenta que muchos de éstos documentos serán emitidos hacia otras Direcciones y Autoridades, e incluso llegarán a ser documentos de conocimiento público o privado, tales como: planes, informes, memorandos, auditorías, catálogos, normativas, lineamientos, entre otros; de tal forma que la comunicación contenida en éstos, presenten la mayor objetividad y claridad referente a la seguridad de la información institucional y el plan estratégico de la SNSI, como detalla el *Anexo 9* (Procesos, indicadores y tiempo estimado de los documentos SNSI). Adicionalmente, se definirán las carátulas, formatos, nivel de importancia, versión, plantillas de los títulos, tipo de letra, espacios, codificación y otros detalles para la presentación de cada uno de estos documentos, y, muchos de ellos serán de carácter público y reservado.

- Creación de una estructura jerárquica digital para esta Subdirección denominada "**S**NSI" o "Seguridades" ubicada en el repositorio institucional, organizado por el tipo de documento, carácter (público o reservado), catálogo de acceso y una codificación

establecida por esta Subdirección. El detalle de los procesos para este lineamiento se describe en el *Apéndice C* (Procesos de estandarizar los formatos para los documentos de la SNSI).

La propuesta del diseño de modelo de gestión para el gerenciamiento de la seguridad de la información en el Consejo de la Judicatura como parte externa de la SNSI, se ilustra en la siguiente figura y se describe a continuación:

Figura 14. Propuesta del diseño del Modelo de Gestión para el gerenciamiento de la seguridad de la información en el CJ.



Fuente: El autor. *Elaborado por:* El autor, 2016.

A continuación, la descripción de la propuesta:

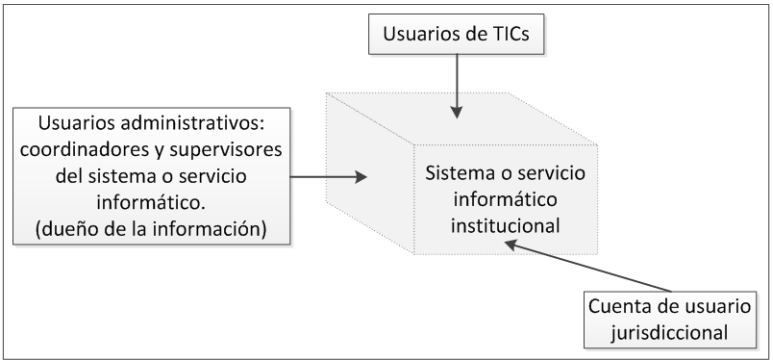
4.4.1 Submodelo de gestión de usuarios.

Este submodelo de gestión de usuarios pretende regularizar, normar y controlar la creación y eliminación de cuentas de usuarios institucionales para hacer uso de sus recursos tecnológicos, para lo cual, se definen los siguientes directrices:

- Elaboración, implementación y seguimiento de los procedimientos para la creación y eliminación de usuarios en el directorio activo institucional en colaboración con talento humano, dirección nacional de: TICs e innovación.
- Elaboración, implementación y seguimiento del documento de confidencialidad para los servidores judiciales que poseen relación laboral directa e indirecta con el Consejo de la Judicatura, para lo cual, se debe firmar una declaración de confidencialidad y un acuerdo de confidencialidad respectivamente. Será requisito indispensable para los servidores judiciales que ingresan a la institución el cumplimiento de este documento, al igual que su regularización.
- Elaboración, implementación y seguimiento de un catálogo de acceso para los servicios y programas informáticos institucionales por medio de la cuenta de usuario que pertenece a cada servidor judicial, según la tarea encomendada como describe el *Anexo 10* (*Cargo y tareas de los servidores judiciales*), donde se relacionen: la atribución (definido como el tipo de lectura, escritura o ambos) y el perfil de usuario en cada aplicativo, como se ilustra

en la siguiente figura; para lo cual se debe activar los módulos de auditoría y el almacenamiento de los registros de cuentas de usuarios.

Figura 15. Descripción de cuentas de usuario para sistema o servicio informáticos institucional.



Fuente: El autor. *Elaborado por:* el autor, 2016.

A continuación se presenta el siguiente cuadro de los clientes internos que conforman el Consejo de la Judicatura (servidores judiciales) según el roll y funciones asignadas:

Tabla 13. Clasificación de los clientes internos en el Consejo de la Judicatura.

Tipo	Clasificación	Roll	Funciones
Clientes internos	Personal de TICs	Super administrador	Dueño o propietario del sistema. Crea al menos a un administrador. Define niveles de acceso a los administradores.
		Administrador	Administra el sistema, crea coordinadores, soporte técnico, soporte técnico. Define los acceso de lectura, escritura o los dos simultáneamente.
		Operador	Visualiza y exporta reportes de los aplicativos o herramientas de TICs. Visualiza información ingresada por los técnicos.
		Soporte técnico	Brinda asesoría técnica a los servidores judiciales en general, acuerdo a necesidades de los usuario.
	Personal administrativo	Vocal	Miembro del Pleno del Consejo de la Judicatura para la toma de decisiones institucionales.
		Asesor	Asesoramiento a un vocal.

		Directores	Dirige y gestiona las distintas direcciones nacionales o provinciales.
		Subdirectores	Dirige y gestiona las distintas unidades que posee las direcciones nacionales.
		Supervisores	Validación y seguimiento de las gestiones, proyectos y actividades de las unidades.
		Analistas	Análisis de los proyectos, tareas y documentos internos pertenecientes a su unidad.
		Técnicos	Extracción de datos, aplica mediciones, realiza la parte operativa técnica.
	Personal Jurisdiccional	Juez	Brindar justicia por medio del dictamen de sentencias según el tipo de materia jurisdiccional.
		Secretario	Proporciona el soporte y colaboración al juez, mediante la elaboración de documentos, actos judiciales, petitorios, entre otros.
		Ayudante judicial	Realiza la parte operativa de las casusas en base a normativas y solicitudes que el Juez creo conveniente.
		Personal de Ventanilla	Persona quien recibe causas, escritos, anexos y otros documentos legales provenientes del personal de derecho y a su vez, procede a entregar al Secretario.

Fuente: El autor. *Elaborado por:* El autor, 2016.

4.4.2 Modelo de gestión de validez.

Se requiere de una herramienta informática que permita el control y monitoreo de todos los cambios que se realiza en la información institucional, esto es principalmente en la base de datos y el repositorio institucional, obteniendo un registro de la cuenta de usuario quien procedió a modificar los datos y conocer el dato exacto que se alteró. Se debe agregar una forma de encriptación a los datos; entre ellos, el mercado se la seguridad de la información presenta una solución en la cual, mediante el uso de un complejo y algoritmo propietario permite que los datos visualizados en la base de datos sean modificados en el contenido pero se conserva el formato del dato (numérico, texto o alfanumérico) pero solo

sirve esta técnica para aquellos usuarios que no son parte de la organización; aliviando el procesamiento de la codificación y decodificación de toda la base o repositorio, evitando la lentitud en el servicio por falto de procesamiento y memoria del sistema.

4.4.3 Modelo de gestión de respaldo.

Esta gestión consiste en cumplir con el objetivo de almacenar hasta los últimos datos posibles de configuración e información que almacenen las bases de datos y los repositorios institucionales propiamente dichos, pero éstas deben ser albergadas en otro sitio físico, preferiblemente muy cercano para evitar costos o molestias con la logística. Se debe utilizar herramientas informáticas automatizadas para controlar la correcta grabación y transferencia de los respaldos de la información institucional con las debidas validaciones y etiquetaciones. Se debe elaborar, implementar y controlar el cumplimiento de un plan de respaldos de la información institucional, tanto de los equipos activos (storage) y de las cintas magnéticas. Se definirán lineamientos para eliminar información que cumpla determinado período de vigencia y que permitan reutilizar recursos de almacenamiento institucional, previa aprobación de las autoridades. Adicionalmente, se pretende ampliar la capacidad de almacenamiento para disponer de otros ambientes de preproducción y producción de manera que la información institucional permita una conmutación automática en el caso de fallos, desperfectos, ataques, desastres u otros que permitan la suspensión de los servicios institucionales.

4.4.4 Modelo de gestión de restauración.

Esta gestión tiene como fin, el permitir restaurar el servicio o aplicativo tecnológico institucional luego de sufrir un desastre, ataque o fallo técnico de mediana y alta magnitud en la cual, se permita reducir las horas de indisponibilidad. También, es indispensable aplicar un monitoreo y control por parte de SNSI para este fin, de tal forma que la información no sea manipulada.

Otra forma de mitigar la disponibilidad de los servicios y aplicativos informáticos institucionales son la elaboración, cumplimiento y control de los planes de mantenimiento preventivo y correctivo, donde se incluye partes y piezas de los equipos o sistemas complementarios que requiere las TICs.

4.4.5 Modelo de gestión habilitante.

El modelo de gestión propuesto considera los siguientes modelos de gestión habilitantes para cumplir lo descrito en los numerales anteriores, estos son: talento humano, gestión procesal, planificación e innovación.

- *Talento humano*: Siendo la parte fundamental de un sistema de administración de justicia, por cuanto, se selecciona, administra, gestiona el desarrollo, habilidades, destrezas para el desarrollo de las actividades al servidor judicial jurisdiccional y administrativo de la institución. En nuestro caso se desarrolla un tiempo estimado de trabajo para conocer las horas-hombre que se requiere un proyecto para el desarrollo de

los productos que debe cumplir la SNIS y por ende, se planifica las actividades anuales de seguridad de la información institucional, como se presenta en la siguiente tabla:

Tabla 14. Catálogo de tiempo estimado para elaboración y entrega de productos SNSI para 12 meses.

ITEM	PRODUCTOS DE LA SNSI	TIEMPO ESTIMADO DE ELABORACION DOCUMENTO (meses).
1	Planes de remediación, continuidad de operaciones, seguridad de hardware y software, recuperación de desastres y contingencias de TICs	3,5 - 04
2	Propuestas de reglamentos relacionados con la seguridad de la información para el procesamiento y almacenamiento de datos, gestión de riesgos, uso de los servicios de telecomunicaciones	01–1,5
3	Informes de seguimiento y gestión de seguridad de la información	0,5–01
4	Informes de análisis, vulnerabilidades, tendencias, y riesgos relacionados con la seguridad de la información	0,5 – 01
5	Procedimiento para la actualización y robustecimiento de las seguridades del hardware	02 - 03
6	Medir los indicadores de incidencias y casos de violaciones de las políticas de seguridad, una vez definidos los indicadores.	02 - 03
7	Informes de auditoría de acceso a las plataformas, las aplicaciones y los servicios de forma interna y externa	02 - 03
8	Informes de gestión y cumplimiento de planes	01 –1,5

Fuente: El autor. *Elaborado por:* El autor, 2016.

El objetivo de establecer estos tiempos y con ayuda de los documentos estandarizados de SNSI permitirán al personal de esta Subdirección evaluar las metas asignadas.

- *Gestión procesal*: Se encuentra representado por la Dirección nacional de gestión procesal, misma que desarrolla el sistema de gestión procesal penal y general para prestar servicios de justicia de calidad; encargada de modernizar la justicia por medio de sus proyectos emblemáticos a nivel nacional basado en la tecnología para controlar procesos e

información; por lo tanto, la SNSI se convierte en un asesor estratégico y se verificará con un test de pruebas y el uso de otras herramientas informáticas para asegurar los sistemas institucionales, tanto los adquiridos como los desarrollados. Por lo tanto, esta Dirección guía en la parte jurisdiccional y en coordinación con la DNTICs se solventarán los procesos e incidentes reportados.

- *Innovación*: Representado por la Dirección Nacional de innovación, desarrollo y mejoramiento de la calidad en los servicios judiciales, mismo que gestiona la innovación, desarrollo y modernización y, mejora continua de los procesos de la función judicial a nivel nacional. Permite organizar y normar los procesos internos y externos de acuerdo al proyecto, resalta a los actores e indicadores que se definan en cada proceso o procedimiento, otorgando un amplio beneficio de la Institución en estudio.

- *Planificación*: Representado por la Dirección nacional de planificación y permite elaborar, dar seguimiento y evaluar la planificación estratégica, operativa y de inversión institucional, como es principalmente, el PAPP y POA de cada una de las Direcciones y Subdirecciones, reportándose periódicamente los avances, productos y los gastos de inversión según la normativa vigente institucional. De igual forma, se trabaja en conjunto para revisar los proyectos de inversión e integrar la aprobación de los términos de referencia en la parte técnica.

Tabla 15. Plan PAPP de SNSI 2017.

PRODUCTOS	CUMPLIMIENTO	CANTIDAD	TIEMPO	UNIDAD	# ENTREGABLES
Planes de remediación, continuidad de operaciones, seguridad de hardware y software, recuperación de desastres y contingencias de TICs	1 / Cuatrimestre	1	4	Meses	3
Propuestas de reglamentos relacionados con la seguridad de la información para el procesamiento y almacenamiento de datos, gestión de riesgos, uso de los servicios de telecomunicaciones	4 / Semestre	4	6	Meses	2
Informes de seguimiento y gestión de seguridad de la información	3 / Trimestre	3	3	Meses	4
Informes de análisis, vulnerabilidades, tendencias, y riesgos relacionados con la seguridad de la información	3 / Trimestre	3	3	Meses	4
Procedimiento para la actualización y robustecimiento de las seguridades del hardware	1 / Trimestre	1	3	Meses	4
Medir los indicadores de incidencias y casos de violaciones de las políticas de seguridad, una vez definidos los indicadores.	1 / Trimestre	1	3	Meses	4
Informes de auditoría de acceso a las plataformas, las aplicaciones y los servicios de forma interna y externa	1 / Semestre	1	6	Meses	2
Informes de gestión y cumplimiento de planes	1 / Cuatrimestre	1	4	Meses	3

Fuente: El autor. *Elaborado por:* El autor, 2016.

4.4.6 Modelo de gestión de apoyo.

Como parte del modelo de gestión propuesto se considera de apoyo a las siguientes Direcciones Nacionales: Administrativa, Financiera, Asesoría Jurídica y Comunicación.

- *Administrativa*: Representado por la *Dirección nacional administrativa* que permite gestionar, administrar y proveer de una manera eficaz, bienes y servicios para la institución: La SNSI por medio de la Dirección nacional de TICs realiza las coordinaciones y gestiones para la adquisición de servicios y bienes tecnológicos respecto

a la seguridad de la información por medio del portal de compras públicas; por lo tanto, se requiere el aval de esta Dirección para el trámite de adquisición.

- *Financiera*: Representado por la *Dirección nacional financiera*, misma que permite gestionar y administrar los recursos financieros de manera eficaz y transparente para nuestro caso, todos los proyectos tecnológicos relacionados con la seguridad de la información, vinculado con los anticipos y pagos (flujos de caja o forma de pago) que se definieron en los TDRs y visualizados en los proyectos de adquisición de bienes y servicios de la seguridad de la información institucional. Esta Dirección debe gestionar los fondos económicos con el aval del Ministerio de Finanzas.

- *Asesoría Jurídica*: Representado por la *Dirección nacional de asesoría jurídica*; misma que asesora, patrocina y desarrolla la normativa institucional de manera jurídica o legal propiamente dicha, precautelando la constitucionalidad y legalidad de todos los actos. Entre sus actividades con la SNSI se lleva a cabo la revisión, asesoramiento y guía legal con los contratos de adquisición de bienes y servicios, documentos delicados como son: manuales de políticas, normativas, reglamentos y otros documentos de orden legal que se utiliza interna y externamente (ejemplo los documentos de confidencialidad).

- *Comunicación*: Representado por la *Dirección nacional de comunicación social*, misma que se encarga de comunicar y difundir de manera integral y estratégica, afianzando los vínculos con la sociedad. La SNSI propone la coordinación y utilización de los medios de difusión institucional para llegar a la conciencia de los servidores judiciales en cuanto a un planteamiento de programas masivos vinculados con la seguridad de la información

institucional; rescatando su importancia, consecuencias y formas de contrarrestar posibles riesgos o vulnerabilidades.

4.4.7 Agregado de valor para el Modelo de gestión propuesto.

El modelo de gestión propuesto considera un agregado de valor para el monitoreo y control de la seguridad de la información en forma transversal.

- *Monitoreo y control*: Este agregado de valor se aplicar en todo el modelo de gestión propuesto y que se relaciona con la seguridad de la información; es decir, la SNSI debe elaborar, implementar y monitorear los controles propuestos por las TICs; siendo éste del tipo automático y autónomo (no depender de otros equipos tecnológicos vinculados a la seguridad de la información), permitiendo la menor posibilidad de intervenciones humanas, comparando y analizando datos a nivel de auditorías, alcanzando resultados puros (no intervenidos por el personal interno o externo).

De acuerdo a lo señalado en el numeral 1.7.1 (Aseguramiento de la información y activos de la institución en estudio) se procede a realizar una evaluación de mencionados aseguramientos en la siguiente tabla:

Tabla 16. Estatus del aseguramiento de la información y activos de la institución en estudio.

TIPO DE CONTROL	DESCRIPCION DE LA SEGURIDAD	DISPONE	OBSERVACIÓN
CONTROL FISICO	Protección de instalaciones	Parcial	Física e infraestructura adecuada, sitio estratégico.
	Guardias de seguridad	No	Suspendido los guardias privados.
	Cerraduras	Si	Sistemas Biométricos (electrónicos).
	Supervisión	Si	Siempre acompaña personal de TICs.

	Control ambiental	Si	Sensores y aire acondicionado.
	Detección de intrusos.	Si	Utilización de cámaras de vigilancia.
CONTROL TECNICO	Control de acceso lógico	Si	Centralizado para usuarios internos y concentrado para usuario externos.
	Encriptación	Si	Utilizados en los medios de transmisión.
	Dispositivos de seguridad	Parcial	Sistema perimetral de SI
	Identificación y autenticación.	Si	Mediante usuario y clave del usuario.
CONTROL ADMINISTRATIVO	Políticas	Parcial	No aprobado por la Máxima Autoridad.
	Estándares	Parcial	Existen protocolos y ciertas normas de regulación según requerimientos.
	Procedimientos	Parcial	Existen algunos procedimientos aprobados por el Director Nacional de TICs, Dirección General y resoluciones del Pleno.
	Directrices	Parcial	Existen pocas directrices emitidas a la presente fecha.
	Declaración personal	Parcial	Procedimiento elaborado y en aprobación.
	Formación de conciencia de seguridad.	No	
DATOS Y ACTIVOS DEL CJ	Centro de datos	Si	Principal en Quito, respaldo en Cuenca.
	Sala de comunicaciones	Si	En todas las edificaciones del CJ a nivel nacional.

Fuente: El autor. *Elaborado por:* El autor, 2016.

- *Buenas prácticas:* El Consejo de la Judicatura presenta algunas buenas prácticas relacionadas con la seguridad de la información, tanto de iniciativa propia como también de otras instituciones público o privadas, descritas en la siguiente tabla:

Tabla 17. Buenas prácticas recomendadas por la SNSI.

No.	DESCRIPCION
1	Usuarios internos no compartir usuarios y claves en base a la experiencia.
2	Los usuarios deben cambiar su clave personal en períodos establecidos.
3	Aplicar un cronograma de respaldos de la información periódica, sin embargo, se tienen factores que lo limitan y el respaldo no es totalmente completo.
4	Controlar la entrada y salida de computadores portátiles pertenecientes al institución.
5	Poseer un registro actualizado de los principales activos de la información, mismos que están albergados en el Centro de Datos Principal.
6	Contar con un manual de políticas de seguridad a nivel de la Dirección nacional de TICs sin aprobación de la Máxima Autoridad. Sin embargo, se está tratando de implementar y socializar con el personal técnico debido a su importancia.
7	Desarrollar software en el Consejo de la Judicatura mediante procedimientos o metodologías definidas con la Subdirección de proyectos y en participación con la Dirección nacional de gestión procesal o con el propietario del sistema.
8	Respaldar la configuración de todos los equipos tecnológicos, al igual que los sistemas de información.

Fuente: El autor. *Elaborado por:* El autor, 2016.

Capítulo 5. Conclusiones y recomendaciones.

5.1 Conclusiones.

De acuerdo a la investigación desarrollada para el "Diseño de modelo de gestión para el gerenciamiento de la seguridad de la información tecnológica en el Consejo de la Judicatura" y, según los objetivos propuestos como también las hipótesis planteadas, se concluye que:

- Actualmente, el Consejo de la Judicatura cuenta con la Subdirección Nacional de Seguridad de la Información (**S**NSI) adscrita a la Dirección Nacional de Tecnologías de la Información y Comunicaciones (**D**NTICs), siendo la responsable del cumplimiento con lo establecido en el Estatuto Integral de Gestión Organizacional por Procesos del Consejo de la Judicatura a nivel Central y Descentralizado; cuya misión es "la preservación de la confidencialidad, integridad y seguridad de la infraestructura tecnológica y, de la información que se procesa, almacena y transmite a través de los diferentes sistemas informáticos institucionales"; por lo tanto, las atribuciones, responsabilidades y productos de la seguridad de la información institucional se encuentran definidas y recae sobre la SNSI.

- El Consejo de la Judicatura no cuenta con una disposición específica y legal que señale uso y aplicabilidad de las normas y estándares nacionales e internacionales de la seguridad de la información tecnológica, por lo tanto, actualmente no se dispone de un

modelo de gestión formal. El Consejo de la Judicatura para la ejecución de ciertas actividades relativas a la seguridad de la información hace uso de las normativas y estándares determinados por el Instituto Ecuatoriano de Normalización (**I**NEN), el mismo que se basa en estándares internacionales.

- El Consejo de la Judicatura referente a la seguridad de la información presenta una gestión de acuerdo a la demanda de incidentes que se reportan por parte de los servidores judiciales o autoridades y, se actúa con un tratamiento de acuerdo a la criticidad; lo que conlleva a un uso ineficiente de los recursos, afectando a la confianza y credibilidad en sus servicios hacia la ciudadanía.

- El incremento de riesgos para realizar una copia, modificación o eliminación de los datos en los repositorios o base de datos jurisdiccional o administrativa del Consejo de la Judicatura no se debe solamente al incumplimiento de los procedimientos, normativas y leyes establecidas en materia de la seguridad de la información tecnológica por parte de los servidores judiciales; también se originan por el mal uso de los sistemas o servicios tecnológicos que dispone la institución y también, por la falta de una herramienta tecnológica que alerte sobre las modificaciones de los datos fuera de un patrón normal de comportamiento.

- El modelo de gestión diseñado permite organizar eficientemente los procesos internos y externos de la Subdirección nacional de seguridad de la información, optimizando los principales recursos (financieros y de talento humano); así como también, determina las futuras acciones para atender los incidentes críticos.

- La Subdirección nacional de seguridad de la información debe observar que el Plan Estratégico Institucional tiene una vigencia hasta 2019, por lo tanto, el modelo de gestión propuesto debe ser analizado de acuerdo a los detalles que tendrá el nuevo Plan Estratégico Institucional.

- El desarrollo, análisis y el planteamiento de estrategias según el FODA, se ajusta a las necesidades actuales de la Subdirección nacional de seguridad de la información y a la vez, se articula con la responsabilidad, atribuciones y productos señalados en el Plan Estratégico Institucional vigente; sin tener que modificar el contenido de estos documentos.

5.2 Recomendaciones.

De acuerdo a las conclusiones y la investigación realizada para el "Diseño de modelo de gestión para el gerenciamiento de la seguridad de la información tecnológica en el Consejo de la Judicatura" se procede a señalar las siguientes recomendaciones:

- Revisar e implementar el presente modelo de gestión como herramienta organizacional para gestionar eficientemente el uso de los recursos existente en la Subdirección nacional de seguridad de la información del Consejo de la Judicatura mediante el aval de la Dirección Nacional de TICs.

- Revisar y aprobar una disposición o normativa que permita la elaboración, implementación y seguimiento de un modelo de gestión para el gerenciamiento de la seguridad de la información del Consejo de la Judicatura según aval de la Dirección Nacional de TICs.

- Implementar herramientas tecnológicas que permitan el control, monitoreo y seguimiento de los indicares del presente modelo de gestión para el gerenciamiento de la seguridad de la información del Consejo de la Judicatura.

- Registrar todos los incidentes de acuerdo el nivel de criticidad que permitan construir una base de conocimientos, elaborar estadísticas periódicas y formular patrones de comportamiento.

- Realizar pruebas periódicas de vulnerabilidades a los sistemas y servicios del Consejo de la Judicatura mediante el uso de la metodología abierta de testeo de seguridad.

- Crear y habilitar una carpeta pública de “seguridades” que permita albergar documentos, manuales, formularios y otras publicaciones que los servidores judiciales pueden hacer uso interno.

- De acuerdo al nuevo planteamiento del modelo de gestión, la **S**NSI debe trazar una nueva misión, visión, objetivos y lineamientos que necesita cumplirse con el nuevo Plan Estratégico Institucional a partir del 2019, el mismo que deberá ser aprobado, socializado e implementado bajo la colaboración de las otras Direcciones y Subdirecciones del Consejo de la Judicatura.

- Registrar y actualizar los avances y cumplimientos del presente modelo de gestión de la seguridad de la información para los posteriores Subdirectores asignados a la seguridad de la información, de tal forma que se mantenga un seguimiento y continuidad de las actividades y tareas programadas para el beneficio del Consejo de la Judicatura.

- Dar cumplimiento a las propuestas estratégicas definidas como "Estándar de conocimiento y documentación de la **S**NSI", de tal forma que permita el conocimiento, desarrollo de las habilidades, conciencia y el desenvolvimiento del resto de estrategias en forma ordenada por parte del personal que conforma la Subdirección nacional de seguridad de la información.

BIBLIOGRAFÍA

Aguilar J, A. I. (2001). *Metodología para el Desarrollo de Modelos de Gestión en Instituciones Públicas.* Merida, Venezuela: Fundacite-Mérida.

Alegsa Dic. (01 de 04 de 2016). *Definición Anonymous.* Obtenido de Definición Anonymous: www.alegsa.com.ar/Dic/anonymous.php

Biblioteca en línea. (01 de 04 de 2016). *Definición Cyberataques.* Obtenido de Definición Cyberataques: http://wol.jw.org/es/wol/h/r4/lp-s

Cabezas, M. M. (03 de 04 de 2016). *La Firma Electrónica en el Ecuador y sus aplicaciones - Data Security S.A.* Obtenido de Administradora del sistema PKI: http://www.lacamara.org/website/images/Seminarios/Material/ABRIL2011/m-%20aplicaciones%20empresariales.pdf

Consejo de la Judicatura - portal web. (03 de 04 de 2016). *Portal del Consejo de la Judicatura*. Obtenido de http://www.funcionjudicial-azuay.gob.ec/index.php?option=com_content&view=article&id=214%3Aconsejo-de-la-judicatura-implementa-firma-electronica&catid=34%3Ainstitucion&Itemid=68

Consejo de la Judicatura. (28 de 05 de 2015). Estatuto Integral de Gestión Organizacional por Procesos del Consejo de la Judicatura a nivel Central y Descentralizado. Quito, Pichincha, Ecuador.

Contraloría General del Estado - CGE. (2010). *Informe de Observaciones de normas internas 410-10.* Quito: CGE.

Core One. (05 de 04 de 2016). *Coreoneit*. Obtenido de Consultoría, auditoría, diseño, seguridad, cloud segurity: http://www.coreoneit.com/disponibilidad-de-la-informacion/

Definicion de. (01 de 04 de 2016). *Definicion.de*. Obtenido de Definicion.de: http://definicion.de/confidencialidad/

Delitos informaticos. (01 de 04 de 2016). *Delitos informaticos.* Obtenido de Delitos informaticos: http://delitosinformaticos.info/delitos_informaticos/definicion.html.

Díaz N, F. M. (1997). *Gestión Estratégica del cambio institucional.* Quito-Ecuador: Servicio Internacional para la Investigación Nacional (ISNAR).

Enríquez B, C. J. (28 de 04 de 2014). Modelo de Gestión de Proyectos de Tecnología. Quito, Pichincha, Ecuador: Consejo de la Judicatura.

Estado del Arte de las Bases de Datos. (01 de 04 de 2016). *Estado del Arte BBDD.* Obtenido de Estado del Arte BBDD: http://es.scribd.com/doc/84999565/Estado-Del-Arte-de-Las-Bases-de-Datos#scribd

Fernando, P. H. (2007). *Gobierno de las Tecnologías y los Sistemas de Información.* Madrid: RA -MA.

Funcion Judicial de Pichincha. (25 de 05 de 2016). *http://www.funcionjudicial-pichincha.gob.ec*. Recuperado el 25 de 05 de 2016, de funcion judicial pichincha:

http://www.funcionjudicial-pichincha.gob.ec/index.php?option=com_content&view=article&id=911:unidad-de-flagrancia-servicio-de-justicia-continuo&catid=41:noticias-home

Gobierno Electrónico. (30 de 12 de 2015). Obtenido de http://www.gobiernoelectronico.gob.ec

Gualan, L. M. (01 de 04 de 2016). *ARQUITECTURAS DE SEGURIDAD*. Obtenido de ARQUITECTURAS DE SEGURIDAD: http://www.personal.fi.upm.es/~lmengual/ARQ_REDES/Arquitecturas_Seguridad.pdf

HMP SA. (2006). *Curso Taller Interno de Valoración del Riesgo*. Recuperado el 22 de 10 de 2016, de www.hmp.sa.cr/files/control_interno/Otros/Riesgos/Valoración%20Riesgos.ppt

INEN. (01 de 04 de 2016). *INEN - Normalización*. Obtenido de INEN - Normalización: http://www.normalizacion.gob.ec/la-institucion/

ISECOM. (s.f.). *ISECOM, Institute for Security and Open Methodologies*. Obtenido de https://foro.elhacker.net/seguridad/osstmm_3_en_espanol-t415117.0.html, 2016: https://foro.elhacker.net/seguridad/osstmm_3_en_espanol-t415117.0.html, 2016

Kali Linux Penetration Testing Tools. (01 de 03 de 2016). *Pen Testing*. Obtenido de http://tools.kali.org/

Kaspersky Anti-Virus. (01 de 04 de 2016). *Kaspersky_Anti-Virus*. Obtenido de Kaspersky_Anti-Virus: http://www.ecured.cu/Kaspersky_Anti-Virus

(2008). Art. 179 de la Constitución del Ecuador. En A. Nacional, *Constitución del Ecuador 2008* (pág. 98). Quito: Registro Oficial.

Naciones Unidas. (Jun de 2010). EXAMEN DE LA GESTIÓN DEL RIESGO. Ginebra, Ginebra, Ginebra.

Networks CISCO Security. (01 de Abril de 2016). *Cisco Security*. Obtenido de http://www.cisco.com/cisco/web/support/LA/7/75/75923_confaccesslists.pdf

Real Academia de la Lengua - Diccionario. (01 de 04 de 2016). *Diccionario de la lengua española*. Obtenido de Diccionario de la lengua española: http://dle.rae.es/?id=AFGgKxB

Repositorio. (01 de 04 de 2016). *Definicion de repositorio*. Obtenido de Definicion de repositorio: http://definicion.de/repositorio/#ixzz3p43XxRwx

Resolución del Consejo de la Judicatura No. 003-2014. (15 de 04 de 2016). *Resolución del Consejo de la Judicatura No. 003-2014*. Obtenido de Resolución del Consejo de la Judicatura No. 003-2014: http://www.funcionjudicial.gob.ec/www/pdf/resoluciones/2014cj/003-2014.pdf

Secretaría Nacional de la Adminstración Pública - SNAP. (19 de 09 de 19). Acuerdo No. 166. Quito, Pichincha, Ecuador.

Significados. (01 de 04 de 2016). *Significados.com.* Obtenido de Significados.com: http://www.significados.com/ignoto

Thompson, J. M. (09 de 03 de 2011). *Administración en teoría*. Recuperado el 08 de 10 de 2016, de http://administracionenteoria.blogspot.com/2011/03/herramientas-administrativas-o.html

Universidad Nacional de Lujuan. (01 de 04 de 2016). *Incidente de seguridad de la información*. Obtenido de Incidente de seguridad de la información: http://www.seguridadinformatica.unlu.edu.ar/?q=node/4

APÉNDICES.

APÉNDICE A. FASES Y TIEMPO ESTIMADO PARA EL DESARROLLO DE PRODUCTOS.

PRODUCTO No.	PRODUCTOS ENTRANTES	DEFINICION DEL INDICADOR	PROCESOS									TIEMPO ESTIMADO GLOBAL HASTA IMPLEMENTACIÓN
(Detallado)	(Según el Estatuto Integral de Gestión Organizacional por Procesos del CJ)	(Según el alcance o cumplimiento)	**Fase 1**	**Fase 2**	**Fase 3**	**Fase 4**	**Fase 5**	**Fase 6**	**Fase 7**	**Fase 8**	**Fase 9**	(Meses)
1	Planes de remediación		Recopilar y depurar la información	Aplicar metodología o estándar de evaluación y/o modelo de gestión para el Plan	Resultado del análisis.	Elaboración del plan (documento).	Presentar, revisar y aprobar el plan por Subdirector/Director.	Aplicación o Pruebas Demo	Evaluación	Reajuste	Evaluación	15
1	Continuidad de operaciones		Recopilar y depurar la información	Aplicar análisis	Definir proceso alterno o paralelo	Elaboración del documento: "Continuidad operaciones	Presentar, revisar y aprobar el plan por Subdirector/Director.	Prueba funcionamiento DEMO	Reajuste	Prueba final	Funcionamiento	18
1	Seguridad de hardware y software		Recopilar información y/o verificar estado	Aplicar metodología o sistema a las seguridades	Presentación de resultados	Propuesta de seguridad	Implementación y verificación	Evaluación				3
1	Recuperación de desastres y contingencias de TICs.		Recopilar y depurar la información	Aplicar metodología o estándar de evaluación y/o modelo a la información	Resultado del análisis.	Elaboración del plan a recuperar (documento).	Presentar, revisar y aprobar la recuperación por Subdirector/Director.	Aplicación o Pruebas Demo	Evaluación	Reajuste	Evaluación	18
2	Propuestas de reglamentos relacionados con la seguridad de la información para: el procesamiento y almacenamiento de datos		Desarrollar la propuesta	Aprobación	Implementar	Socializar	Gestionar el cumplimiento					12

2	Propuestas de reglamentos relacionados con la seguridad de la información para: Gestión de riesgos		Desarrollar la propuesta	Aprobación	Implementar	Socializar	Gestionar el cumplimiento					9
2	Propuestas de reglamentos relacionados con la seguridad de la información para: Uso de los servicios de telecomunicaciones.		Desarrollar la propuesta	Aprobación	Implementar	Socializar	Gestionar el cumplimiento					9
3	Informes de seguimiento y gestión de la seguridad de información en la Institución.		Recopilar y depurar la información	Aplicar análisis	Elaboración del informe	Entrega del Informe	Respuesta u observación del informe.	Seguimiento del resultado o culminación.				12
4	Informe de análisis, vulnerabilidades, tendencias y riesgos relacionados con la seguridad de la información.		Recopilar y depurar la información	Aplicar análisis	Elaboración del informe	Entrega del Informe	Respuesta u observación del informe.	Seguimiento del resultado o culminación.				12
5	Procedimiento para la actualización y robustecimiento de las seguridades del hardware.		Recopilar y depurar la información	Aplicar metodología o estándar de evaluación y/o modelo a la información	Resultado del análisis.	Elaboración del procedimiento	Presentar, revisar y aprobar el procedimiento por Subdirector/Director.	Aplicación o Pruebas del procedimiento Demo	Evaluación	Reajuste		12
6	Indicadores de incidencias y casos de violación de políticas de seguridad.		Recopilar y depurar la información	Elaboración del informe	Evaluación	Plan de mitigación	Monitoreo y control					12
7	Informes de auditoría de acceso a plataformas, aplicaciones, servicios de forma interna y externa.		Definición de los formularios	Aplicación de la Auditoria	Recomendaciones	Seguimiento						4

8	Informes de gestión y de cumplimiento de planes.		Recopilar y depurar la información	Aplicar análisis	Elaboración del informe	Entrega del Informe	Respuesta u observación del informe.	Seguimiento del resultado o culminación.				15
9	Proyectos y TDRs		Estudio técnico para el proyecto.	Informe técnico del proyecto.	Estudio Técnico - Económico.	Elaboración y presentación del TDR según formatos SERCOP.	Aprobación y validación de DNA / DG	Subasta inversa	Entrega/Implementación	Funcionamiento	Mantenimiento	1

Fuente: SNSI, 2016. *Elaborado por:* El autor, 2016.

APÉNDICE B. MODELO DE CRECIMIENTO PROPUESTO SEGÚN CRECIMIENTO PROPUESTO POR AÑO.

		2016	2017	2018	2019	2020	2021
Estándar	**Sección**	**Estatus base**	9%	9%	9%	9%	9%
A.10.1	Controles criptográficos	0%					
A.12.7	Consideraciones de las auditorías de los sistemas de información	0%					
A.8.3	Manejo de los soportes de almacenamiento	25%					
A.5.1	Directrices de la Dirección en la seguridad de la información	30%					
A.15.2	Gestión de la prestación del servicio por suministradores	35%					
A.6.2	Dispositivos para movilidad y teletrabajo	40%					
A.17.1	Continuidad de la seguridad de la información	40%					
A.8.2	Clasificación de la Información	47%					
A.9.2	Gestión de acceso para los usuarios	53%					
A.6.1	Organización interna	54%					
A.18.1	Cumplimiento de los requisitos legales y contractuales	57%					
A.12.5	Control de software en explotación	60%					
A.17.2	Redundancias	60%					
A.18.2	Revisiones de la seguridad de la información	65%					
A.12.6	Gestión de vulnerabilidad técnica	68%					
A.12.1	Responsabilidades y procedimientos de operación	69%					
A.16.1	Gestión de incidentes de seguridad de la información y mejoras	70%					
A.11.2	Seguridad de los equipos	75%					
A.14.3	Datos de prueba	75%					
A.13.1	Gestión de la seguridad en las redes	78%					
A.15.1	Seguridad de la información en las relaciones con suministradores	78%					
A.7.2	Durante la contratación	80%					
A.7.1	Antes de la contratación	83%					
A.11.1	Áreas seguras	83%					
A.13.2	Intercambio de información con partes externas	84%					
A.7.3	Cese o cambio de puesto de trabajo	85%					
A.8.1	Responsabilidad sobre los activos	85%					
A.9.1	Requisitos de negocio para el control de acceso	85%					
A.12.4	Registro de actividades y supervisión	88%					
A.12.3	Copias de seguridad	90%					
A.14.2	Seguridad en los procesos de desarrollo y soporte	90%					

A.9.4	Control de acceso a sistemas y aplicaciones	91%					
A.12.2	Protección contra código malicioso	95%					
A.14.1	Requisitos de seguridad en los sistemas de información	95%					
A.9.3	Responsabilidades del usuario	100%					
	PORCENTAJE PROPUESTO	9,00%					
	PORCENTAJE PROMEDIO Y PROYECTADO	**64,50%**	*70,31%*	*76,63%*	*83,53%*	*91,05%*	*99,24%*

Fuente: SNSI, 2016. *Elaborado por:* El autor, 2016.

APÉNDICE C. PROCESOS DE ESTANDARIZACIÓN PARA LOS DOCUMENTOS DE LA SNSI.

No.	Lineamiento	Nombre del proceso	Insumos	Salida	Actividades intervinientes	Rol de la SNSI	Subprocesos asociados.
1	*Estandarizar los formatos para los documentos de la SNSI.*	Estandarización de formatos para documentos del SNSI	Memorandos	Notificar o comunicar	Elaborar, revisar, aprobar, emitir, enviar y registrar la recepción del memorando	Controlar y registrar el envío y su recepción.	.
2			Informes	Recomendaciones o informar	Extraer información, elaborar, revisar, aprobar el informe y adjuntar el respectivo memorando	Seguimiento al cumplimiento de recomendaciones y registrar	.
3			Programas y planes	Cronograma de cumplimiento y recursos requeridos	Elaborar, revisar, aprobar el programa o plan y adjuntar el respectivo memorando	Cumplimiento de programa o plan y su control	.
4			Protocolos	Compromiso de los actores y la responsabilidad con sus actividades	Coordinar y extraer información, elaborar, revisar, aprobar el protocolo y adjuntar el respectivo memorando	Controlar o evaluar el cumplimiento del protocolo	.
5			Lineamientos, normativas, políticas o reglamentos	Dar cumplimiento	Generar y responder lineamientos, normativas, políticas o reglamentos	Cumplimiento, control y monitoreo	.
6			Catálogos	Lista ordenada o clasificada	Elaborar, revisar, aprobar el catálogo y adjuntar el respectivo memorando	Cumplimiento, control y monitoreo	.
7			Procesos y procedimientos	Indicador(es)	Responsabilidad bajo la DNIDMCSJ	Coordinación con DNIDMCSJ y otras unidades competentes.	Depende del proceso o procedimiento.
8			Evaluaciones	Resultado del diagnóstico y recomendaciones	Generar formulario, coordinar y evaluar, emitir informe con recomendaciones y adjuntar el respectivo memorando	Cumplimiento de recomendaciones y seguimiento	Depende del resultado de la evaluación.

9			Auditorías	Estatus del cumplimiento y recomendaciones	Generar formulario, coordinar y auditar, emitir informe con observaciones y adjuntar el respectivo memorando	Cumplimiento de observaciones y seguimiento	Depende del resultado de la auditoría.
10		Repositorio digital de SNSI	Crear repositorio como carpeta compartida y otra pública	Almacenamiento en un repositorio y acceso a carpetas (SNSI y pública)	Solicitar almacenamiento y creación de acceso al personal de SNSI Para compartir información al resto de Direcciones y Subdirecciones del Consejo de la Judicatura.	Cumplir con la codificación para los documentos digitales de SNSI	Autorización del Subdirector para colocar en carpeta pública la información pertinente.
11			Digitalizar todo documento a ser despachado	Árbol jerárquico en un repositorio o carpeta compartida SNSI	Creación del árbol jerárquico en un repositorio o carpeta compartida SNSI y también en la carpeta pública. Alimentar la información de manera inmediata.	Subir al repositorio los documentos digitales codificados	.

Fuente: *Dirección Nacional de Talento Humano, 2016.* Elaborado por: *El autor, 2016*

ANEXOS.

ANEXO 1. DETALLE DE LOS SISTEMAS O APLICACIONES INFORMÁTICAS DE LA INSTITUCIÓN Y EL DUEÑO DEL SISTEMA.

CÓD.	SISTEMA	DUEÑO DEL SISTEMA
APLI01	SISTEMA DE DIRECCIÓN NACIONAL ADMINISTRATIVA “DNA”	ADMINISTRATIVO
APLI02	SISTEMA DE "CARTELERAS DIGITALES"	COMUNICACIÓN
APLI03	PORTAL INFORMATIVO INTERNO “INTRANET”	COMUNICACIÓN
APLI04	PORTAL DE BIBLIOTECAS “PORTAL PMB”	COMUNICACIÓN
APLI05	"PORTAL WEB DEL CONSEJO DE LA JUDICATURA"	COMUNICACIÓN
APLI06	"PORTAL WEB DE LA ESCUELA JUDICIAL"	COMUNICACIÓN
APLI07	PORTAL WEB DE MEDIACIÓN	COMUNICACIÓN
APLI08	PORTAL WEB LOTAIP	COMUNICACIÓN
APLI09	SISTEMA DE PRESENTACIÓN "INFOCHANNEL"	COMUNICACIÓN
APLI10	SISTEMA DE CONCURSOS CORTE NACIONAL “sisperfujv1.4”	CONCURSOS
APLI11	SISTEMA DE CONCURSOS 101 JUECES “sisperfujv1.5”	CONCURSOS
APLI12	SISTEMA DE CONCURSOS 313 JUECES “sisperfujv1.7”	CONCURSOS
APLI13	SISTEMA DE CONCURSOS 1284 JUECES Y NOTARIOS “sisperfujv1.8”	CONCURSOS
APLI14	SISTEMA DE CONCURSOS NACIONALES	CONCURSOS
APLI15	SISTEMA JENKINS	DESARROLLO
APLI16	SISTEMA NEXUS	DESARROLLO
APLI17	SISTEMA DE CAPACITACIÓN VIRTUAL “E-LEARNING”	ESCUELA JUDICIAL
APLI18	SISTEMA AULA VIRTUAL MOODLE	ESCUELA JUDICIAL
APLI19	SISTEMA DE BIBLIOTECAS “PMB”	ESCUELA JUDICIAL
APLI20	SISTEMA DE META BUSCADOR WEB	ESCUELA JUDICIAL
APLI21	SISTEMA DE PRÁCTICAS “PRE-PROFESIONALES”	ESCUELA JUDICIAL
APLI22	SISTEMA DE DEUDORES ALIMENTICIOS	FINANCIEROS
APLI23	SISTEMA DE PARTICIPACIÓN DEL ESTADO	FINANCIEROS
APLI24	SISTEMA DE PROTOCOLOS Y DILIGENCIAS NOTARIALES	FINANCIEROS
APLI25	INVENTARIO DE PROTOCOLOS Y DILIGENCIAS NOTARIALES	FINANCIEROS
APLI26	SISTEMA NOTARIAL	FINANCIEROS
APLI27	SISTEMA NOTARIAL	FINANCIEROS
APLI28	SISTEMA DE PENSIONES ALIMENTICIAS - CUENCA -LOJA	FINANCIEROS
APLI29	SISTEMA DE PENSIONES ALIMENTICIAS - PICHINCHA	FINANCIEROS
APLI30	SISTEMA DE PENSIONES ALIMENTICIAS PILOTO NACIONAL	FINANCIEROS
APLI31	SISTEMA FINANCIERO DE “VIÁTICOS”	FINANCIEROS
APLI32	SISTEMA FINANCIERO DE “VIÁTICOS WEB”	FINANCIEROS

APLI33	SISTEMA DE CÁLCULOS NOTARIALES	FINANCIEROS
APLI34	SISTEMA DE CONTROL DE ACCESO “SICOP”	INFRAESTRUCTURA
APLI35	SISTEMA DE CONTROL E INVENTARIO “SIMEV”	INFRAESTRUCTURA
APLI36	SISTEMA GENERAL DE SEGURIDADES	INFRAESTRUCTURA
APLI37	SISTEMA DE INFORMACIÓN DOCUMENTAL “ALFRESCO COMUNITY”	INFRAESTRUCTURA
APLI38	SISTEMA SWITHYARD	INFRAESTRUCTURA
APLI39	SISTEMA DE SEGUIMIENTO DE ACUERDOS PRESIDENCIALES	JURISDICCIONAL
APLI40	SISTEMA DE INGRESO DE INFORMACIÓN PARA "AUDIENCIAS PENALES"	JURISDICCIONAL
APLI41	SISTEMA DE VISUALIZACIÓN DE AUDIENCIAS DE SATJE WEB	JURISDICCIONAL
APLI42	SISTEMA DE INFORMACIÓN DE UNIDADES JUDICIALES CATASTRAL	JURISDICCIONAL
APLI43	SISTEMA DE "COMISARIAS DE LA MUJER Y FAMILIA"	JURISDICCIONAL
APLI44	SISTEMA DE DEPURACIÓN DE CAUSAS SATJE	JURISDICCIONAL
APLI45	SISTEMA DE REGISTROS DE UNIDADES JUDICIALES FLAGRANTES	JURISDICCIONAL
APLI46	SISTEMA DE FORO DE ABOGADOS "SISFA"	JURISDICCIONAL
APLI47	SISTEMA DE ABOGADOS NO REGISTRADOS	JURISDICCIONAL
APLI48	SISTEMA DE CASILLEROS ELECTRÓNICOS	JURISDICCIONAL
APLI49	SISTEMA DE CONSULTA TERRITORIAL “GEO REFERENCIAL”	JURISDICCIONAL
APLI50	SISTEMA DE PROCESAMIENTO DE JURISPRUDENCIA “SIPJUR”	JURISDICCIONAL
APLI51	SISTEMA DE INFORMACIÓN JUDICIAL “JUSTICIA 2.0”	JURISDICCIONAL
APLI52	SISTEMA DE AUTENTICACIÓN BIOMÉTRICA COMPORTAMENTAL	JURISDICCIONAL
APLI53	SISTEMA DE "PERITOS WEB"	JURISDICCIONAL
APLI54	SISTEMA DE "ELEGIBLES WEB"	JURISDICCIONAL
APLI55	SISTEMA AUTOMÁTICO DE TRÁMITES JUDICIALES ECUATORIANO “SATJE”	JURISDICCIONAL
APLI56	SISTEMA DE EQUIVALENCIAS "SATJE - JUSTICIA"	JURISDICCIONAL
APLI57	SISTEMA DE CONSULTA DE CAUSAS EXTERNAS	JURISDICCIONAL
APLI58	SISTEMA DE CONSULTA INTERNA Y REPORTES	JURISDICCIONAL
APLI59	SISTEMA DE GENERACIÓN DE BOLETAS	JURISDICCIONAL
APLI60	SISTEMA DE REGISTRO Y CONTROL DE PRESOS Y SENTENCIAS "CYR"	JURISDICCIONAL
APLI61	SISTEMA DE CONTROL DISCIPLINARIO “QUEJAS”	JURISDICCIONAL
APLI62	PORTAL DE DENUNCIA DE FUNCIONARIOS	JURISDICCIONAL
APLI63	SISTEMA DE SORTEOS MASIVOS PARA CORTE NACIONAL	JURISDICCIONAL
APLI64	SISTEMA DE CONSTANCIA DE PÉRDIDA DE DOCUMENTOS	JURISDICCIONAL
APLI65	SISTEMA DE COLAS PARA LAS UNIDADES JUDICIALES “TURNEROS”	JURISDICCIONAL
APLI66	SISTEMA DE ACTAS RESUMEN	JURISDICCIONAL
APLI67	SISTEMA DE GACETA JUDICIAL	JURISDICCIONAL
APLI68	SISTEMA DE ABOGADOS NO SANCIONADOS	JURISDICCIONAL

APLI69	SISTEMA DE CERO PAPELES “PPLESS”	LA SECRETARIA
APLI70	SERVICIO DE ASISTENCIA REMOTA	MESA DE SERVICIOS
APLI71	SISTEMA DE INVENTARIO DE PARQUE TECNOLÓGICO “OSCVENTORY”	MESA DE SERVICIOS
APLI72	SERVICIO DE MENSAJERÍA INTERNA “SPARK” - CUENCA	MESA DE SERVICIOS
APLI73	SISTEMA DE DIRECTORIO TELEFÓNICO	MESA DE SERVICIOS
APLI74	SISTEMA DE DIRECTORIO TELEFÓNICO “INFORMATIVO”	MESA DE SERVICIOS
APLI75	SISTEMA DE SOPORTE AL USUARIO “GLPI”	MESA DE SERVICIOS
APLI76	SISTEMA HP SERVICE MANAGER 9 x “MESA DE SERVICIOS”	MESA DE SERVICIOS
APLI77	SISTEMA DE PROYECTOS “PROJECT SERVER”	MESA DE SERVICIOS
APLI78	SISTEMA DE REGISTRO PARA LA BOLSA DE EMPLEO “BOLSA DE EMPLEO”	TALENTO HUMANO
APLI79	SISTEMA DE BUSSINES INTELIGENT BI SAIKU	TALENTO HUMANO
APLI80	SISTEMA DE CENSO JUDICIAL	TALENTO HUMANO
APLI81	SISTEMA DE NÓMINA	TALENTO HUMANO
APLI82	SISTEMA DE DIRECCIÓN NACIONAL DE PERSONAL “DNP”	TALENTO HUMANO
APLI83	SISTEMA DE EVALUACIÓN DE FUNCIONARIAS Y FUNCIONARIOS “SISTEMA MODULAR”	TALENTO HUMANO

Fuente: SNIT, 2015.*Elaborado por:* El autor (2016).

ANEXO 2. DETALLE DE LOS SERVICIOS Y RESPONSABILIDAD AL INTERIOR DE LA DNTICs.

COD.	SERVICIOS	RESPONSABLE DEL SERVICIO
S01	Internet	REDES
S02	Correo Electrónico	INFRAESTRUCTURA
S03	Video conferencia	REDES
S04	Autenticación Corporativa	INFRAESTRUCTURA
S05	Red LAN	REDES
S05-01	Red Inalámbrica	REDES
S06	Telefonía	REDES
S07	Servicios de RED	INFRAESTRUCTURA
S07-01	DNS	INFRAESTRUCTURA
S07-02	DHCP	INFRAESTRUCTURA
S07-03	NTP	INFRAESTRUCTURA
S8	SISTEMA JUDICIAL	OPERACIONES
S9	SOPORTE EN OFIMÁTICA	MESA DE SERVICIOS
S10	Almacenamiento Centralizado	INFRAESTRUCTURA
S11	Redes WAN	REDES
S11-01	Soporte Enlaces	REDES
S13	Antivirus	REDES - SEGURIDADES
S15	VPN	REDES
S16	Apoyo a los aplicativos	OPERACIONES
S17	Firma Electrónica	SEGURIDADES
S18	Base de Datos	INFRAESTRUCTURA
S19	Actualización de Software Base	INFRAESTRUCTURA
S20	Monitoreo	INFRAESTRUCTURA - REDES
S21	Mensajería Instantánea (Chat Institucional)	REDES

Fuente: SNIT, 2015. Elaborado por: El autor, 2016.

ANEXO 3. DESCRIPCIÓN DE LOS EQUIPOS DEL CENTRO DE DATOS.

EQUIPOS DE ALMACENAMIENTO.

DISPOSITIVO	MARCA	MODELO	FUNCIÓN	# DE SERIE
CAJA DE DISCOS-DISKSHELF	NETAPP	DS4243	Cantidad: 2 unidades.	
STORAGE	NETAPP	FAS3210	Almacenamiento para Telefonía X 2 Módulos	700000912522
STORAGE	IBM	TS3200 / 3573 4UL	TAPE BACKUP	78P5452
STORAGE	IBM	XIV		7805022
STORAGE	HP	Storage Works P2000		2S6120C451
STORAGE	DELL	MD3600		
STORAGE	DELL	MD1200f	Cantidad: 2 unidades.	
STORAGE	NETAPP	V6240	Almacenamiento Servidores, Cantidad: 2 unidades.	
STORAGE	NETAPP	FAS6240		

Fuente: SNIT, 2015. Elaborado por: El autor, 2016.

EQUIPOS DE VIDEOCONFERENCIA.

DISPOSITIVO	MARCA	MODELO	FUNCIÓN	# DE SERIE
VIDEOCONFERENCIA	SONY	IPELA PCS-XG80	Equipo de Video Conferencia	104616
PANTALLA PLANA 50"	SONY		Equipo de Video Conferencia	
PIZARRON PROYECTOR	RIPP		Equipo de Video Conferencia	
VIDEOCONFERENCIA	POLYCOM	DMA 7000	DMA 1-1, Cantidad: 4 unidades.	
VIDEOCONFERENCIA	POLYCOM	POLYCOM RPRM 1	RPRM 1 y 2, Cantidad: 2 unidades.	
VIDEOCONFERENCIA	POLYCOM	RSS 4000	RSS, Cantidad: 2 unidades.	
VIDEOCONFERENCIA	POLYCOM	Real Presence Collaboration server 2000	RMX 1 Servidor de Multiconferencia MCU, Cantidad: 2 unidades.	
VIDEOCONFERENCIA	RADVISION	SCOPIA ELITE 5100	MCU de videoconferencia SCOPIA	1138080011
VIDEOCONFERENCIA	POLYCOM	2200-78700-500	RPAD1 Servidor de Conexión Universal	

Fuente: SNIT, 2015. Elaborado por: El autor, 2016.

EQUIPOS DE AIRE.

DISPOSITIVO	MARCA	MODELO	FUNCIÓN	# DE SERIE
AIRE ACONDICIONADO DE PRECISIÓN	CANNATAL	8AD10	Aire de Precisión-1 Carrier A y B, Cantidad: 2 unidades	11-1208-C06-02A
AIRE ACONDICIONADO DE CONFORT	LG	TV-C602LLA0	Aire de Confort-1 Energía, Cantidad: 2 unidades.	
AIRE ACONDICIONADO DE PRECISIÓN	CANNATAL	9AD14	Aire de Precisión-1 y 2 Servidores, Cantidad: 2 unidades	11-1208-C07-02A
AIRE ACONDICIONADO DE PRECISIÓN	CANNATAL	8AD10	Aire de Precisión-2 Telecom B	11-1208-C06-03A

Fuente: SNIT, 2015. Elaborado por: El autor, 2016.

EQUIPOS DE ENERGÍA.

DISPOSITIVO	MARCA	MODELO	FUNCIÓN	# DE SERIE
UPS 's ON LINE	EATON POWERWARE	9390(160KVA), Cantidad: 2 unidades	UPS A y B	EF025CBB05
POWER DISTRIBUTION UNIT (PDU)	PDI	WAVESTAR 150 KVA, Cantidad: 2 unidades		110-3059 UNIT 4

Fuente: SNIT, 2015. Elaborado por: El autor, 2016.

EQUIPOS DE OFICINA.

COMPUTADORES LAPTOP EN EL CJ.

MARCA	CANTIDAD
HP PRO BOOK 440 G1	1
ACER	32
ACERASPIRE 4752G	1
APPLE	1
DELL	352
DELL 6420	22
DELL 6430	34
DELL 6440	51
HACER	1
HP	14
HP 440	1
HP 8570P	1
HP14-V014LA	1
HP-PROBOOK-640-G1	1
No definidos.	20
Total Laptop:	**533**

COMPUTADORES DESKTOP EN EL CJ.

MARCA	CANTIDAD
500	1
ACER	57
APPLE	6
CPU 9010	1
DELL	407
DELL 790	4
DELL 9010	11
DELL 990	3
FUJIPSON	1
HACER	1
HP	43
HP DC5700	
MAC	4
OPTIPLEX	1
XEROX	1
No definidos.	5
Total desktop:	**546**

Total Computadores: 1.079 unidades

Fuente: SNIT, 2016. *Elaborado por:* El autor, 2016.

EQUIPOS DE RED.

DISPOSITIVO	MARCA	MODELO	FUNCION
SWITCH LAN	CISCO	3750-X 48P	Switch de Distribución en Frontera
ACELERADORES	CISCO	WAVE-8541-K9	WAAS Acelerador de tráfico Central Manager
ROUTER	CISCO	CISCO 800	Prestados por CNT
SWITCH LAN	CISCO	3750-X 48P	Switch de Distribución en Frontera

SWITCH LAN	CISCO	Catalyst 2960-s PoE+	
FABRIC INTERCONNECT	CISCO	UCS-FI-6120XP	Fabric InterConnect de Telefonía, Cantidad: 2 unidades.
FABRIC INTERCONNECT	CISCO	UCS-FI-6248UP	Fabric InterConnect Chasis seguridades, Cantidad: 2 unidades.
SWITCH LAN	CISCO	N2K-C2248TP-1GE	Aumento capacidad de Nexus 5K, Cantidad: 2 unidades.
SWITCH LAN	CISCO	N5K-C5548P	Cantidad: 2 unidades.
SWITCH SAN	HP		
FABRIC INTERCONNECT	CISCO	UCS-FI-6248UP	FI para servidores principales (Primary y Back up), Cantidad: 2 unidades
SWITCH LAN	CISCO	N2K-C2232PP-10GE	FEX Extensión para Fabric Interconect, Cantidad: 2 unidades.
SWITCH SAN	BROCADE	BROCADE 300	Cantidad: 3 unidades.
SWITCH LAN	ENTERASYS	Horizon GH-2402S2	
ACELERADORES	CISCO	WAE 7300	NO ESTA INSTALADO ES DE PROVINCIA
SWITCH LAN	CISCO	N2K-C2248TP-1GE	Aumento capacidad de Nexus 5K, Cantidad: 2 unidades.
SWITCH SAN	BROCADE	5100	Switch SAN para el NetAPP, Cantidad: 2 unidades.
AIRE ACONDICIONADO DE PRECISIÓN	CANNATAL	8AD10	Aire de Precisión-2 Telecom A
iPATCH	SISTIMAX	iPatch Network Manager	Cantidad: 22 unidades.
PATCH PANEL FO	SISTIMAX	Bandeja de 24 puertos	Cantidad: 10 unidades.
PATCH PANEL CO	SISTIMAX	Panel de 48 puertos	Cantidad: 13 unidades.
PATCH PANEL CO	PANDUIT	panel de 24 puertos	Cantidad: 10 unidades.
BALANCEADOR	CISCO	ACE 4710-2PAK	Balanceador de Aplicaciones
BALANCEADOR	CISCO	GSS-4492R-K9	Balanceadores DNS
ACELERADORES	CISCO	WAVE 294	WAAS Acelerador de tráfico desde DC
SWITCH LAN	CISCO	N7K-C7010	Switch de Core
ROUTER	CISCO	3900	Gateway de Voz
SWITCH LAN	CISCO	Catalyst 3560	
SWITCH LAN	CISCO	Catalyst 2960-s PoE+ 10g	Switch para Operadores, Cantidad: 2 unidades.
SWITCH LAN	CISCO	Catalyst 2960-s PoE+	Switch para las cámaras
SWITCH LAN	CISCO	Catalyst 2960-s PoE+	Switch para datos
SWITCH LAN	CISCO	Catalyst 2960-s PoE+ 10g	Switch para Operadores
GRABADOR DE VIDEOSEGURIDAD	ACTI	XNR-4200	Administrador de cámaras de video
KVM	BELKIN	F1DC108H	
G4	GAMATRONIC	G4	RED IP DE TABLERO CONTRA INCENDIOS
FIREWALL	CISCO	ASA 5585-X IPS SSP 10	Firewall IPS Perimetral
UTM	CHEKPOINT	CHECK POINT 12600	Filtrado Web
BALANCEADOR	CISCO	CISCO ACE 4710	Balanceador de Aplicaciones
SWITCH LAN	CISCO	N7K-C7010	Switch de Core
RF Coder			Lector RFC
PDU-Rackmount	EATON	PW103MI0U236	Cantidad: 58 unidades.
CAMARA	ACTI	TCM-3511	Cantidad: 21 unidades.
CONTROL DE ACCESO	ZK	ZEM500	Cantidad: 8 unidades.
PANTALLA PLANA 50"	SONY	GXDL52H1	Cantidad: 4 unidades.

Fuente: SNIT, 2015. Elaborado por: El autor, 2016.

EQUIPOS DE SEGURIDAD.

DISPOSITIVO	MARCA	MODELO	FUNCIÓN	# DE SERIE
ADM ANCHO DE BANDA	EXINDA	6060	Control de Ab para Internet	GGCV7V1
ADM ANCHO DE BANDA	EXINDA	6060	Control de Ab para Regionales	GG9V7V1
FIREWALL	RADVISION	Firewall Transversal	Firewall Transversal	114080120
FIREWALL	CISCO	ASA 5585-X IPS SSP 10	Firewall IPS Perimetral	JMX1553703U
UTM	CHEKPOINT	CHECK POINT 12600	Filtrado Web	1145B00564
LOG SERVER	CHEKPOINT	SMART ONE-EVENT		
SECURITY MAIL GATEWAY	CISCO	ESA X1070 AIRONPORT MAIL	Appliance para el filtrado de correos	848F69E72F2E-8DDJYV1
UTM	CHEKPOINT	CHECK POINT 12600		
FIREWALL	CISCO	ASA 5505		JMX155340WU
SECURITY SERVER	CISCO	ACS 1121	Control de Acceso	KQ53AHA
SECURITY MAIL GATEWAY	CISCO	ESA X1070 AIRONPORT MAIL	Appliance para el filtrado de correos	848F69E6999F-8DCLYV1

Fuente: SNIT, 2015. Elaborado por: El autor (2016).

SERVIDORES FÍSICOS.

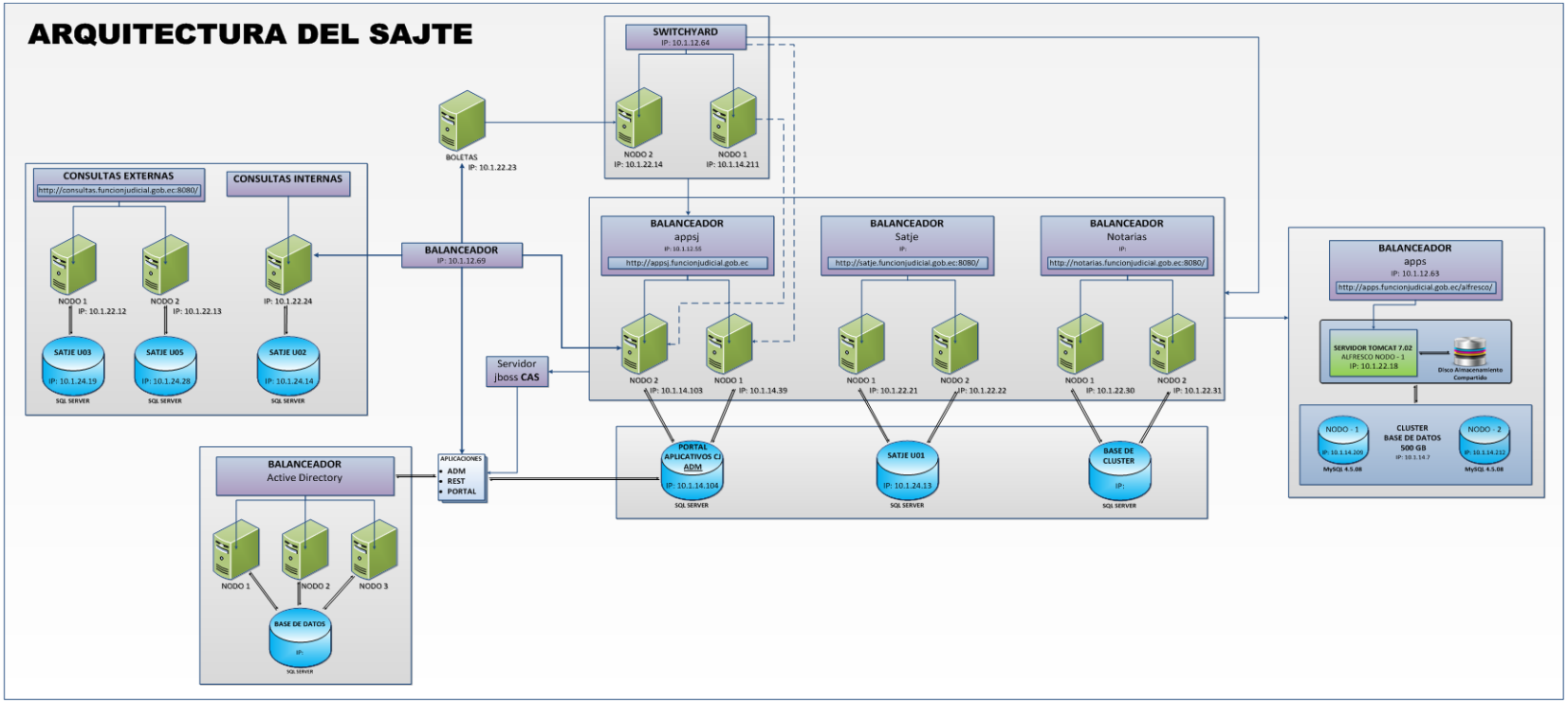
DISPOSITIVO	MARCA	MODELO	FUNCIÓN	# DE SERIE
SERVIDOR	HP	DL380 G6		2UX01001DR
APPLIANCE	CISCO	SMART SERVICE CONNECTION 2000	Cantidad: 2 unidades.	
CHASIS	CISCO	UCS 5108	Chasis de servidores de Telefonía	FOX1537G5DQ
SERVIDOR	CISCO	UCS B200 M2	UBICACIÓN: RST-CH1-SL1 TELEFONIA 1 a 6, Cantidad: 6 unidades.	FCH154378GF
CHASIS	CISCO	UCS 5108	Chasis de servidores de seguridades	FOX1549H9AC
SERVIDOR	CISCO	UCS B200 M2	UBICACIÓN: RSS-CH1-SL1 CISCO LMS	FCH160172MV
SERVIDOR	CISCO	UCS B200 M2	UBICACIÓN: RSS-CH1-SL2 CISCO SCURITY MANAGER / Slot-2	QCI1551A8H9
SERVIDOR	CISCO	UCS B200 M2	UBICACIÓN: RSS-CH1-SL3 Athen Ware de Producción, Cantidad: 2 unidades.	FCH1601774Z
SERVIDOR	HP	ML110G7 E3-1220	Servidor Authen Ware Pruebas	BRC06115WP
SERVIDOR	HP	DL160G6	Logs	
SERVIDOR	HP	Proliant DL380 G4	Servidor de Backups	2UX61500E7
SERVIDOR	HP	ML110G7 E3-1220	Servidor para Pruebas Concurso	
SERVIDOR	HP	DL380G7 E5649	Servidor BD Oracle 10g y Web	2M22030669
SERVIDOR	HP	DL360 G7	Base de Datos Portales	MXQ1170CLR
SERVIDOR	HP	DL160 G6	Ipatch	MXQ1350B6Q
SERVIDOR	HP	HPDL360 G6	Cantidad: 2 unidades.	MXQ84601GR
CHASIS	IBM	Blade Center H	CHASIS IBM RACK IBM.	698369
SERVIDOR	IBM	HS22 7870AC1	Plataforma ESX Virtualización, Cantidad: 6 unidades.	06PAZ57
SERVIDOR	IBM	IBM HX5 (2 espacios)	SQL Server prueba para correo (Ex virtualización CITRIX), Cantidad: 2 unidades.	
SERVIDOR	IBM	IBM HX5 (2 espacios)	SQL Server Cluster 1 y 2, Cantidad: 2 unidades.	
SERVIDOR	CISCO	UCS C240 M3	SERV1 UCS. Sistema institucional administrativos y financieros	FCH1623V116
SERVIDOR	CISCO	UCS C240 M3	SERV3 UCS, Base de Datos SATJE05 Guayas,	FCH1618V0AM

			Cantidad: 2 unidades.	
CHASIS	CISCO	UCS 5108	CHASIS 8, RS5-U27	FOX1627GLFL
CHASIS	CISCO	UCS 5108	CHASIS 1, RS5-U21	FOX1621GXZ1
SERVIDOR	CISCO	UCS B200 M2	UBICACIÓN: RS5-CH1-SL1 Justicia	QCI1629A7SR
SERVIDOR	CISCO	UCS B200 M2	UBICACIÓN: RS5-CH1-SL2 General	QCI1629A81P
SERVIDOR	CISCO	UCS B200 M2	UBICACIÓN: RS5-CH1-SL3 General	QCI1629A820
SERVIDOR	CISCO	UCS B200 M2	UBICACIÓN: RS5-CH1-SL4 Justicia	QCI1629A82V
SERVIDOR	CISCO	UCS B200 M2	UBICACIÓN: RS5-CH1-SL5 General	FCH160272MN
SERVIDOR	CISCO	UCS B200 M2	UBICACIÓN: RS5-CH1-SL6 Preproducción	FCH162874L4
SERVIDOR	CISCO	UCS B200 M2	UBICACIÓN: RS5-CH1-SL7 Justicia	QCI1629A7RU
SERVIDOR	CISCO	UCS B200 M2	UBICACIÓN: RS5-CH1-SL8 General	QCI1629A7S2
CHASIS	CISCO	UCS 5108	CHASIS 2, RS5-U15	FOX1627GLF6
SERVIDOR	CISCO	UCS B200 M2	UBICACIÓN: RS5-CH2-SL1 Preproducción	QCI1629A83Q
SERVIDOR	CISCO	UCS B200 M2	UBICACIÓN: RS5-CH2-SL2 Justicia	QCI1629A7TJ
SERVIDOR	CISCO	UCS B200 M2	UBICACIÓN: RS5-CH2-SL3 General	FCH16297HG6
SERVIDOR	CISCO	UCS B200 M2	UBICACIÓN: RS5-CH2-SL4 General	FCH16297HLB
SERVIDOR	CISCO	UCS B200 M2	UBICACIÓN: RS5-CH2-SL5 Justicia	FCH16277BWP
SERVIDOR	CISCO	UCS B200 M2	UBICACIÓN: RS5-CH2-SL6 General	QCI1629A7XH
SERVIDOR	CISCO	UCS B200 M3	UBICACIÓN: RS6-CH9-SL1	FCH1651J07E
SERVIDOR	CISCO	UCS C240 M3	SERV5 UCS, Servidor Base de datos STJE05	FCH1618V0AH
SERVIDOR	CISCO	UCS C240 M3	SERV4 UCS, Servidor Base de datos STJE05	FCH1623V07L
CHASIS	CISCO	UCS 5108	CHASIS 9, RS6-U33	FOX1625H024
CHASIS	CISCO	UCS 5108	CHASIS 3, RS6-U27	FOX1627GLE8
SERVIDOR	CISCO	UCS B200 M2	UBICACIÓN: RS6-CH3-SL1 N1 Cluster MYSQL	QCI1629A7RZ
SERVIDOR	CISCO	UCS B200 M2	UBICACIÓN: RS6-CH3-SL3 Justicia	QCI1629A7UW
SERVIDOR	CISCO	UCS B200 M2	UBICACIÓN: RS6-CH3-SL4 General	QCI1629A7VZ
SERVIDOR	CISCO	UCS B200 M2	UBICACIÓN: RS6-CH3-SL5 Preproducción	QCI1629A82C
SERVIDOR	CISCO	UCS B200 M2	UBICACIÓN: RS6-CH3-SL6 Justicia	QCI1629A803
SERVIDOR	CISCO	UCS B200 M2	UBICACIÓN: RS6-CH3-SL7 General	QCI1629A7W5
SERVIDOR	CISCO	UCS B200 M2	UBICACIÓN: RS6-CH3-SL8 Justicia	QCI1629A7YY
CHASIS	CISCO	UCS 5108	CHASIS 4, RS6-U21	FOX1627GLDZ
SERVIDOR	CISCO	UCS B200 M2	UBICACIÓN: RS6-CH4-SL1 N2 Cluster MYSQL	QCI1629A7WZ
SERVIDOR	CISCO	UCS B200 M2	UBICACIÓN: RS6-CH4-SL3 General	QCI1629A7ZE
SERVIDOR	CISCO	UCS B200 M2	UBICACIÓN: RS6-CH4-SL4 Justicia	FCH16297HHA
SERVIDOR	CISCO	UCS B200 M3	UBICACIÓN: RS6-CH4-SL5 SATJEU04 - G	FCH1651J0E4
SERVIDOR	CISCO	UCS B200 M2	UBICACIÓN: RS6-CH4-SL6 Preproducción	FCH16297HTH
SERVIDOR	CISCO	UCS B440 M2	UBICACIÓN: RS6- CH4, SL7-8 Preproducción	FCH1613752X
CHASIS	CISCO	UCS 5108	CHASIS 5, RS6-U15	FOX1626GQ5E
SERVIDOR	CISCO	UCS B200 M2	UBICACIÓN: RS6-CH5-SL1 CICERO	QCI1629A7Z0
SERVIDOR	CISCO	UCS B200 M2	UBICACIÓN: RS6-CH5-SL2 Justicia	QCI1629A7UB
SERVIDOR	CISCO	UCS B200 M3	UBICACIÓN: RS6-CH5-SL3 ACTIVE DIRECTO	FCH1651J08P
SERVIDOR	CISCO	UCS B440 M2	UBICACIÓN: RS5-CH8, SL7-8	FCH161577VR
SERVIDOR	CISCO	UCS B440 M2	UBICACIÓN: RS6-CH5-SL7-8 N2 SATJE NAC	FCH16177D47

SERVIDOR	DELL	POWEREDGE R720	Cantidad: 2 unidades.	FW28F5J
KVM	MINICOM	SMART 108IP		
SERVIDOR	HP	GL380 G7	Oracle Rack Nodo1	2M212700UH
SERVIDOR	HP	GL380 G7	Oracle Rack Nodo2	2M212700V3
SERVIDOR	HP	GL360 G7		MXQ1340265
SERVIDOR	HP	DL380G4	Cantidad: 3 unidades.	2UX61500E4
VIDEOCONFERENCIA	POLYCOM	2200-78700-500	RPAD1 Servidor de Conexión Universal	1Y4YFX1
VIDEOCONFERENCIA	RADVISION	SCOPIA PATHFINDER	Scopiapathfinder	
SERVIDOR	IBM	7945-AC1 System x 3650	Servidor de VDC	KQ74WRN
SERVIDOR	IBM	7945-AC1 System x 3650	Servidor de VDC	KQ74WLT
SERVIDOR	HP	ProLiant DL380 G7	Virtualizado con HyperV (Traído del CJ, está libre), Cantidad: 2 unidades.	2M203700KV
SERVIDOR	HP	Proliant DL360 G7	Servidor de BDD MYSQL	EA72LJC138
SERVIDOR	HP	ProLiant DL380 G7	Virtualizado con HyperV	2M203700HT
SERVIDOR	CISCO	UCS B200 M2	UBICACIÓN: RS5-CH2-SL7 Preproducción	FCH162971JN
SERVIDOR	CISCO	UCS B200 M3	UBICACIÓN: RS5-CH2-SL8 Pruebas Replica	FCH1651J0VY
SERVIDOR	CISCO	UCS B200 M2	UBICACIÓN: RS5-CH8, SL1 Preproducción	FCH16287JQE
SERVIDOR	CISCO	UCS B200 M3	UBICACIÓN: RS5-CH8, SL2 Apagado	FCH16507FHN
SERVIDOR	CISCO	UCS B200 M2	UBICACIÓN: RS6-CH9-SL2 Preproducción	FCH162971PU

Fuente: SNIT, 2016. *Elaborado por:* El autor, 2016.

ANEXO 4. ARQUITECTURA TECNOLÓGICA DEL SISTEMA AUTOMÁTICO DE TRÁMITE JUDICIAL ECUATORIANO - SATJE.



Fuente: Jefatura de Operaciones de la DNTICs. *Elaborado por:* El autor, 2016.

ANEXO 5. ANÁLISIS DEL USO Y APLICABILIDAD SEGÚN LAS NORMAS *INEN* PARA UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN TECNOLÓGICA INSTITUCIONAL.

CÓDIGO ICS			SECTOR	SUBSECTOR	DOCUMENTO NORMATIVO					ANÁLISIS EN EL CJ			
NIVEL 1	NIVEL 2	NIVEL 3			TIPO DE DOCUMENTO	NÚMERO DE DOCUMENTO	AÑO	REVISIÓN	TÍTULO	SI	NO	PARCIAL	OBSERVACIÓN
35	040		ELECTRÓNICA, TECNOLOGÍA DE LA INFORMACIÓN Y TELECOMUNICACIONES	TECNOLOGÍA DE LA INFORMACIÓN. MÁQUINAS DE OFICINA	NTE INEN-ISO/IEC	27000	2012	0	TECNOLOGÍA DE LA INFORMACIÓN - TÉCNICAS DE SEGURIDAD - SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - DESCRIPCIÓN GENERAL Y VOCABULARIO		X		
35	040		ELECTRÓNICA, TECNOLOGÍA DE LA INFORMACIÓN Y TELECOMUNICACIONES	TECNOLOGÍA DE LA INFORMACIÓN. MÁQUINAS DE OFICINA	NTE INEN-ISO/IEC	27001	2011	0	TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI). REQUISITOS			X	Utilizado para el manual de políticas (parte del SGSI).
35	040		ELECTRÓNICA, TECNOLOGÍA DE LA INFORMACIÓN Y TELECOMUNICACIONES	TECNOLOGÍA DE LA INFORMACIÓN. MÁQUINAS DE OFICINA	NTE INEN-ISO/IEC	27002	2009	0	TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE LA SEGURIDAD. CÓDIGO DE PRÁCTICA PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN		X		
35	040		ELECTRÓNICA, TECNOLOGÍA DE LA INFORMACIÓN Y TELECOMUNICACIONES	TECNOLOGÍA DE LA INFORMACIÓN. MÁQUINAS DE OFICINA	NTE INEN-ISO/IEC	27003	2012	0	TECNOLOGÍA DE LA INFORMACIÓN - TÉCNICAS DE SEGURIDAD - GUÍA DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN			X	Utilizado para el desarrollo del manual de políticas de seguridad de la información institucional.
35	040		ELECTRÓNICA, TECNOLOGÍA DE LA INFORMACIÓN Y TELECOMUNICACIONES	TECNOLOGÍA DE LA INFORMACIÓN. MÁQUINAS DE OFICINA	NTE INEN-ISO/IEC	27004	2012	0	TECNOLOGÍA DE LA INFORMACIÓN - TÉCNICAS DE SEGURIDAD - GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN - MEDICIÓN		X		
35	040		ELECTRÓNICA, TECNOLOGÍA DE LA INFORMACIÓN Y TELECOMUNICACIONES	TECNOLOGÍA DE LA INFORMACIÓN. MÁQUINAS DE OFICINA	NTE INEN-ISO/IEC	27005	2012	0	TECNOLOGÍA DE LA INFORMACIÓN - TÉCNICAS DE SEGURIDAD - GESTIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN			X	Utilización de ciertas técnicas de seguridad básica.
35	040		ELECTRÓNICA, TECNOLOGÍA DE LA INFORMACIÓN Y TELECOMUNICACIONES	TECNOLOGÍA DE LA INFORMACIÓN. MÁQUINAS DE OFICINA	NTE INEN-ISO/IEC	27007	2015	0	TECNOLOGÍAS DE LA INFORMACIÓN — TÉCNICAS DE SEGURIDAD — DIRECTRICES PARA LA AUDITORÍA DE SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (ISO/IEC 27007:2011, IDT)			X	Utilizado para la auditoría de telefonía IP.
35	040		ELECTRÓNICA, TECNOLOGÍA DE LA INFORMACIÓN Y TELECOMUNICACIONES	TECNOLOGÍA DE LA INFORMACIÓN. MÁQUINAS DE OFICINA	NTE INEN-ISO/IEC	27010	2015	0	TECNOLOGÍAS DE LA INFORMACIÓN – TÉCNICAS DE SEGURIDAD – GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA COMUNICACIONES INTERSECTORIALES E INTERORGANIZACIONALES (ISO/IEC 27010:2012, IDT)		X		Se canaliza por medio de la DINARDAP y de acuerdo al convenio interinstitucional se puede requerir.
35	040		ELECTRÓNICA, TECNOLOGÍA DE LA INFORMACIÓN Y	TECNOLOGÍA DE LA INFORMACIÓN. MÁQUINAS DE	NTE INEN-ISO/IEC	27031	2015	0	TECNOLOGÍAS DE LA INFORMACIÓN – TÉCNICAS DE SEGURIDAD – DIRECTRICES PARA LA ADECUACIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y			X	Se encuentra en elaboración el plan de continuidad del

			TELECOMUNICACIONES	OFICINA					COMUNICACIÓN PARA LA CONTINUIDAD DEL NEGOCIO (ISO/IEC 27031:2011, IDT)				negocio de uno de los servicios judiciales.
35	040		ELECTRÓNICA, TECNOLOGÍA DE LA INFORMACIÓN Y TELECOMUNICACIONES	TECNOLOGÍA DE LA INFORMACIÓN. MÁQUINAS DE OFICINA	NTE INEN-ISO/IEC	27032	2015	0	TECNOLOGÍAS DE LA INFORMACIÓN – TÉCNICAS DE SEGURIDAD – DIRECTRICES PARA CIBERSEGURIDAD (ISO/IEC 27032:2012, IDT)		X		
35	040		ELECTRÓNICA, TECNOLOGÍA DE LA INFORMACIÓN Y TELECOMUNICACIONES	TECNOLOGÍA DE LA INFORMACIÓN. MÁQUINAS DE OFICINA	NTE INEN-ISO/IEC	27033-1	2015	0	TECNOLOGÍAS DE LA INFORMACIÓN – TÉCNICAS DE SEGURIDAD – SEGURIDAD DE LA RED – PARTE 1: DESCRIPCIÓN Y CONCEPTOS (ISO/IEC 27033-1:2009, IDT)			X	Utilizado una parte de la seguridad de la red.
35	040		ELECTRÓNICA, TECNOLOGÍA DE LA INFORMACIÓN Y TELECOMUNICACIONES	TECNOLOGÍA DE LA INFORMACIÓN. MÁQUINAS DE OFICINA	NTE INEN-ISO/IEC	27034-1	2015	0	TECNOLOGÍAS DE LA INFORMACIÓN – TÉCNICAS DE SEGURIDAD – SEGURIDAD DE LA APLICACIÓN – PARTE 1: DESCRIPCIÓN Y CONCEPTOS (ISO/IEC 27034-1:2011 + Cor 1:2014, IDT)			X	Utilizado una parte de la seguridad de la aplicación.
35	080		ELECTRÓNICA, TECNOLOGÍA DE LA INFORMACIÓN Y TELECOMUNICACIONES	TECNOLOGÍA DE LA INFORMACIÓN. MÁQUINAS DE OFICINA	NTE INEN-ISO/IEC	38500	2014	0	GOBIERNO CORPORATIVO DE LA TECNOLOGÍA DE LA INFORMACIÓN (ISO/IEC 38500:2008, IDT)		X		
35	080		ELECTRÓNICA, TECNOLOGÍA DE LA INFORMACIÓN Y TELECOMUNICACIONES	TECNOLOGÍA DE LA INFORMACIÓN. MÁQUINAS DE OFICINA	NTE INEN-ISO/IEC	40500	2014	0	TECNOLOGÍA DE LA INFORMACIÓN – DIRECTRICES DE ACCESIBILIDAD PARA EL CONTENIDO WEB DEL W3C (WCAG) 2.0 (ISO/IEC 40500:2012, IDT)		X		
35	040		ELECTRÓNICA, TECNOLOGÍA DE LA INFORMACIÓN Y TELECOMUNICACIONES	TECNOLOGÍA DE LA INFORMACIÓN. MÁQUINAS DE OFICINA	NTE INEN-ISO/IEC TR	14516	2013	0	TECNOLOGÍAS DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. DIRECTRICES PARA EL USO Y GESTIÓN DE SERVICIOS CONFIABLES DE TERCERAS PARTES			X	Aprobado el documento de confidencialidad para terceros.
35	040		ELECTRÓNICA, TECNOLOGÍA DE LA INFORMACIÓN Y TELECOMUNICACIONES	TECNOLOGÍA DE LA INFORMACIÓN. MÁQUINAS DE OFICINA	NTE INEN-ISO/IEC TR	15446	2014	0	TECNOLOGÍAS DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. GUÍA PARA LA PRODUCCIÓN DE PERFILES DE PROTECCIÓN Y OBJETIVOS DE SEGURIDAD (ISO/IEC/TR 15446:2009, IDT).		X		
35	040		ELECTRÓNICA, TECNOLOGÍA DE LA INFORMACIÓN Y TELECOMUNICACIONES	TECNOLOGÍA DE LA INFORMACIÓN. MÁQUINAS DE OFICINA	NTE INEN-ISO/IEC TR	19791	2014	0	TECNOLOGÍAS DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. EVALUACIÓN DE LA SEGURIDAD DE SISTEMAS OPERACIONALES (ISO/IEC/TR 19791:2010, IDT)		X		
35	080		ELECTRÓNICA, TECNOLOGÍA DE LA INFORMACIÓN Y TELECOMUNICACIONES	TECNOLOGÍA DE LA INFORMACIÓN. MÁQUINAS DE OFICINA	NTE INEN-ISO/IEC TR	20000-3	2014	0	TECNOLOGÍA DE LA INFORMACIÓN. GESTIÓN DEL SERVICIO. PARTE 3: DIRECTRICES PARA LA DEFINICIÓN DEL ALCANCE Y APLICABILIDAD DE LA NORMA ISO/IEC 20000-1:2005 (ISO/IEC/TR 20000-3:2009, IDT)		X		
35	240	30	ELECTRÓNICA, TECNOLOGÍA DE LA INFORMACIÓN Y TELECOMUNICACIONES	TECNOLOGÍA DE LA INFORMACIÓN. MÁQUINAS DE OFICINA	NTE INEN-ISO/TR	20983	2014	0	INFORMACIÓN Y DOCUMENTACIÓN. INDICADORES PARA LOS SERVICIOS BIBLIOTECARIOS ELECTRÓNICOS. (ISO/TR 20983:2003, IDT)		X		
35	100	05	ELECTRÓNICA, TECNOLOGÍA DE LA INFORMACIÓN Y TELECOMUNICACIONES	TECNOLOGÍA DE LA INFORMACIÓN. MÁQUINAS DE OFICINA	NTE INEN-ISO/IEC	29361	2014	0	TECNOLOGÍA DE LA INFORMACIÓN - INTEROPERABILIDAD DE SERVICIOS WEB - PERFIL BÁSICO WS-L VERSIÓN 1.1 (ISO/IEC 29361:2008, IDT)		X		Requerido para interoperabilidad institucional, actualmente se lo realiza por medio de la DINARDAP.
35	100	05	ELECTRÓNICA, TECNOLOGÍA DE LA INFORMACIÓN Y TELECOMUNICACIONES	TECNOLOGÍA DE LA INFORMACIÓN. MÁQUINAS DE OFICINA	NTE INEN-ISO/IEC	29362	2014	0	TECNOLOGÍA DE LA INFORMACIÓN - INTEROPERABILIDAD DE SERVICIOS WEB - PERFIL DE ADJUNTOS WS-L VERSIÓN 1.0 (ISO/IEC 29362:2008, IDT)		X		Requerido para interoperabilidad institucional, actualmente se lo realiza por medio de la DINARDAP.

35	100	05	ELECTRÓNICA, TECNOLOGÍA DE LA INFORMACIÓN Y TELECOMUNICACIONES	TECNOLOGÍA DE LA INFORMACIÓN. MÁQUINAS DE OFICINA	NTE INEN-ISO/IEC	29363	2012	0	TECNOLOGÍA DE LA INFORMACIÓN - INTEROPERABILIDAD DE SERVICIOS WEB - PERFIL DE ENLACE SIMPLE SOAP WS-I VERSIÓN 1.0.		X		Requerido para interoperabilidad institucional, actualmente se lo realiza por medio de la DINARDAP.
35	040		ELECTRÓNICA, TECNOLOGÍA DE LA INFORMACIÓN Y TELECOMUNICACIONES	TECNOLOGÍA DE LA INFORMACIÓN. MÁQUINAS DE OFICINA	NTE INEN-ISO/IEC	27006	2012	0	TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. REQUISITOS PARA ORGANIZACIONES QUE PROVEEN AUDITORÍA Y CERTIFICACIÓN DE SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN		X		No aplica en este momento.
35	040		ELECTRÓNICA, TECNOLOGÍA DE LA INFORMACIÓN Y TELECOMUNICACIONES	TECNOLOGÍA DE LA INFORMACIÓN. MÁQUINAS DE OFICINA	NTE INEN-ISO/IEC	27011	2015	0	TECNOLOGÍAS DE LA INFORMACIÓN – TÉCNICAS DE SEGURIDAD – DIRECTRICES DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA ORGANIZACIONES DE TELECOMUNICACIONES BASADAS EN ISO/IEC 27002 (ISO/IEC 27011:2008, IDT)			X	Solicitado al proveedor del servicio y limitado por la institución a nivel económico.

Fuente: INEC, catálogo de documentos normativos vigentes, responsable: dirección de normalización, actualización: marzo 2016. *Elaborado por*: El autor, 2016.

.

ANEXO 6. MATRIZ DE CUMPLIMIENTO DE LA NORMA ISO 27001-2013.

Referencia		Área de evaluación de cumplimiento		Resultados	
Checklist	Estándar	Sección	Puntos de evaluación inicial	Hallazgos	Estado
	A.5	**Políticas de seguridad**			
	A.5.1	**Directrices de la Dirección en seguridad de la información**			
	A.5.1.1	Conjunto de políticas para la seguridad de la información	1. ¿Existen políticas de seguridad? 2. ¿Están todas las políticas aprobadas por la Máxima Autoridad? 3. ¿Las políticas son comunicadas adecuadamente a los empleados?	No existen políticas aprobadas. Se actualizó el documento como primer borrador. Las políticas dispersas (según emisión de los memorandos).	40%
	A.5.1.2	Revisión de las políticas para la seguridad de la información	1. ¿Se revisan las políticas de seguridad de la información? 2. ¿Las revisiones se realizan a intervalos regulares? 3. ¿Las revisiones se realizan cuando cambian las circunstancias?	No.	20%
	A.6	**Aspectos organizativos de la seguridad de la información**			
	A.6.1	**Organización interna**			
	A.6.1.1	Asignación de responsabilidades para la seguridad de la información	¿Están las responsabilidades para la protección de los activos individuales, y para llevar a cabo los procesos específicos de seguridad, claramente identificados, definidos y comunicados a las partes pertinentes?	Parcialmente implementado	15%
	A.6.1.2	Segregación de tareas	¿Están las funciones y áreas de responsabilidad separadas, con el fin de reducir las oportunidades de modificación o mal uso de la información o los servicios no autorizados?	Parcialmente implementado	60%
	A.6.1.3	Contacto con las autoridades	1. ¿Existe un procedimiento documentando cuando y quién debe ponerse en contacto con las autoridades pertinentes (aplicación de la ley, etc.)? 2. ¿Existe un proceso que detalla cómo y cuándo se requiere el contacto? 3. ¿Existe un proceso para el contacto de rutina y el intercambio de inteligencia?	Parcialmente implementado	35%
	A.6.1.4	Contacto con los grupos de interés especial	¿Los individuos relevantes de la Institución mantienen membresía activa en grupos de intereses especiales relevantes?	Parcialmente implementado	80%
	A.6.1.5	Seguridad de la información en la gestión de proyectos	¿Se formulan todos los proyectos evaluando de alguna forma la seguridad de la información?	Parcialmente implementado	80%
	A.6.2	**Dispositivos para movilidad y teletrabajo**			
	A.6.2.1	Política de uso de dispositivos para movilidad	1. ¿Existe una política de uso de dispositivos móviles? 2. ¿La política tiene aprobación de la Máxima Autoridad? 3. ¿La política documenta y brinda directrices adicionales acerca de riesgos por el uso de dispositivos móviles (por ejemplo, el robo de activos, el uso de puntos de acceso inalámbricos abiertos, etc.)?	1. Política desarrollada. 2. Política no aprobada por la Máxima Autoridad. 3. Si documento y brinda directrices.	80%
	A.6.2.2	Teletrabajo	1. ¿Existe una política de teletrabajo? 2. ¿Cuenta con la aprobación de la Máxima Autoridad? 3. ¿Existe un proceso establecido para los trabajadores remotos para obtener acceso? 4. ¿Han sido los teletrabajadores capacitados para proteger sus activos y se les ha otorgado el equipamiento necesario?	1. No existe política de teletrabajo. 2. No cuenta aprobación de la Máxima Autoridad. 3. No existe proceso establecido para trabajos remotos. 4. No.	0%

	A.7	**Seguridad ligada a los recursos humanos**			
	A.7.1	**Antes de la contratación**			
	A.7.1.1	Investigación de antecedentes	1. ¿Se verifica los antecedentes de los nuevos candidatos para su empleo? 2. ¿Los controles para la verificación del personal nuevo se encuentran aprobados por la autoridad pertinente? 3. ¿Los controles para la verificación del personal nuevo cumplen con las leyes, regulaciones y ética pertinente? 4. ¿Los niveles de controles de verificación cumplen con la evaluación de los riesgos institucionales?	1. No. Propuesto en la nueva versión de políticas. 2. No se encuentran aprobados por la autoridad. 3. Si se cumplen desde este año. 4. Cumplen parcialmente.	70%
	A.7.1.2	Términos y condiciones de contratación	1. ¿Se solicita a todos los empleados, contratistas y/o terceros la firma de acuerdos de confidencialidad y no divulgación? 2. ¿Los contratos de empleo y/o de servicios cubren las especificaciones para proteger la información de la institución?	1. Aprobado este año los acuerdos de confidencialidad. 2. SI, en una de las cláusulas lo detalla.	95%
	A.7.2	**Durante la contratación**			
	A.7.2.1	Responsabilidades de gestión	1. ¿Participan los directores, subdirectores o jefaturas de la administración y conducción de la seguridad en la institución? 2. ¿Se gestiona las políticas de seguridad y se alienta a todos los servidores judiciales y contratistas aplicar la seguridad de la información de conformidad con las políticas y procedimientos establecidos?	1. Parcialmente participan. 2. Se está gestionando.	90%
	A.7.2.2	Concienciación, educación y capacitación en seguridad de la información	¿Todos los servidores judiciales, contratistas y usuarios de terceros, se someten regularmente a una formación adecuada referente a la concienciación sobre el papel y función de la seguridad de la información en la organización?	Parcialmente implementado	95%
	A.7.2.3	Proceso disciplinario	1. ¿Existe un proceso disciplinario formal que permita a la institución, tomar medidas contra los servidores judiciales que han cometido una violación de la seguridad de la información? 2. ¿Se comunica a los servidores judiciales de este proceso disciplinario?	1. Parcialmente implementado el proceso. 2. Parcialmente implementado el proceso.	55%
	A.7.3	**Cese o cambio de puesto de trabajo**			
	A.7.3.1	Cese o cambio de puesto de trabajo	1. ¿Existe un procedimiento documentado para la terminación o cambio de las funciones del servidor judicial? 2. ¿Existe alguna información respecto a las tareas de seguridad que se haya comunicado al servidor judicial y/o contratista mientras dure el empleo? 3. ¿La institución es capaz de garantizar el cumplimiento de las funciones del empleo?	1. Definido y aprobado este año el procedimiento en DA. Realizando lo mismo para el DNP. 2. Parcialmente implementado. 3. Parcialmente implementado.	85%
	A.8	**Gestión de activos**			
	A.8.1	**Responsabilidad sobre los activos**			
	A.8.1.1	Inventario de activos	1. ¿Existe un inventario de todos los activos asociados con la información y/o procesamiento de la información? 2. ¿Existe un inventario exacto y este se mantiene actualizado a la fecha?	1. Parcialmente implementado. 2. Parcialmente implementado	95%
	A.8.1.2	Propiedad de los activos	Todos los activos de información deben tener claramente definido un propietario que sea consciente de sus responsabilidades.	Parcialmente implementado	95%

	A.8.1.3	Uso aceptable de los activos	1. ¿Existe una política de uso aceptable para cada clase / tipo de activo de información? 2. ¿Los usuarios son conscientes de esta política antes de su uso?	1. Política desarrollada, aún no aprobada. 2. Parcialmente implementado.	55%
	A.8.1.4	Devolución de activos	¿Existe un proceso para asegurar que todos los servidores judiciales y usuarios externos devuelvan los activos de la institución a la terminación de su empleo, contrato o acuerdo de trabajo?	SI	95%
	A.8.2	**Clasificación de la información**			
	A.8.2.1	Directrices de clasificación	1. ¿Existe una política que rija la clasificación de la información? 2. ¿Existe un proceso por el cual toda la información se puede clasificar de manera adecuada?	1. Política desarrollada, aún no aprobada. 2. No definido el proceso.	45%
	A.8.2.2	Etiquetado y manipulado de la información	¿Existe un proceso o procedimiento para asegurar que la clasificación de la información está debidamente marcada en cada activo?	Parcialmente implementado	70%
	A.8.2.3	Manipulación de activos	1. ¿Existe un procedimiento para el manejo de la información clasificada? 2. ¿Los usuarios encargados de los activos de información están al tanto de este procedimiento?	1. No definido el procedimiento. 2. Parcialmente implementado.	25%
	A.8.3	**Manejo de los soportes de almacenamiento**			
	A.8.3.1	Gestión de soportes extraíbles	1. ¿Existe una política que rija a los medios extraíbles? 2. ¿Existe un proceso que abarque la forma de gestionar los medios extraíbles? 3. ¿Existe una política o proceso comunicado a todos los empleados que utilizan medios extraíbles?	1. Política desarrollada, aún no aprobada. 2. No existe el proceso. 3. No existe socialización del proceso.	30%
	A.8.3.2	Eliminación de soportes	¿Existe un procedimiento formal dispuesto para medios extraíbles?	No existe procedimiento formal.	0%
	A.8.3.3	Soportes físicos en tránsito	1. ¿Existe una política documentada y/o un proceso que detalle como los medios físicos deben ser transportados? 2. ¿El medio de transporte cuenta con las garantías de protección contra el acceso no autorizado, mal uso y corrupción?	1. Política desarrollada, aún no aprobada. No existe el proceso. 2. No existe garantías de protección.	45%
	A.9	**Control de accesos**			
	A.9.1	**Requisitos de negocio para el control de accesos**			
	A.9.1.1	Política de control de accesos	1. ¿Existe una política documentada del control de acceso? 2. ¿La política está basada según los requerimientos de la institución? 3. ¿Está la política comunicada de forma apropiada?	1. Política desarrollada, aún no aprobada. 2. Si. 3. Parcialmente socializada la política.	75%
	A.9.1.2	Control de acceso a las redes y servicios asociados	¿Los controles establecidos para el acceso a los recursos de red, se aseguran que estén autorizados y sean los necesarios para el desarrollo de sus funciones?	Controles habilitados y asegurados en los accesos	95%
	A.9.2	**Gestión de acceso de usuario**			
	A.9.2.1	Gestión de altas/bajas en el registro de usuarios	¿Existe un proceso de registro formal para el acceso de los usuarios en la institución?	Parcialmente implementado	25%
	A.9.2.2	Gestión de los derechos de acceso asignados a usuarios	¿Existe un proceso de aprovisionamiento formal para el acceso en lugar de asignar derechos de acceso y servicios a todos los tipos de usuarios?	Parcialmente implementado	60%
	A.9.2.3	Gestión de los derechos de acceso con privilegios especiales	¿Las cuentas de acceso privilegiado son gestionadas y separadas por separado?	Implementado	95%

	A.9.2.4	Gestión de información confidencial de autenticación de usuarios	¿Existe un proceso de control formal para la gestión de la información cuando se asigne la información de forma confidencial?	Parcialmente implementado	25%
	A.9.2.5	Revisión de los derechos de acceso de los usuarios	1. ¿Existe un proceso a los propietarios de activos para revisar los derechos de acceso a sus activos de forma regular? 2. ¿Se ha verificado este proceso de revisión?	1. Parcialmente implementado. 2. No.	20%
	A.9.2.6	Retirada o adaptación de los derechos de acceso	¿Existe un proceso que garantice los derechos de acceso del usuario cuando este termine su contrato y este cambie de rol?	Si.	95%
	A.9.3	**Responsabilidades del usuario**			
	A.9.3.1	Uso de información confidencial para la autenticación	1. ¿Existe una política documentada que cubra las prácticas de la institución en el manejo de la confidencialidad de la información? 2. ¿Está comunicado a todos los usuarios?	Si, implementado-	100%
	A.9.4	**Control de acceso a sistemas y aplicaciones**			
	A.9.4.1	Restricción del acceso a la información	¿Está el acceso a la información y las funciones de los sistemas de aplicación restringido de acuerdo con la política de control de accesos?	Parcialmente implementado	90%
	A.9.4.2	Procedimientos seguros de inicio de sesión	¿Cuándo se requiere una política de control de acceso, es el acceso controlado por un procedimiento de conexión segura?	Parcialmente implementado	95%
	A.9.4.3	Gestión de contraseñas de usuario	1. ¿Son los sistemas de contraseñas interactivas? 2. ¿Se requiere contraseñas complejas?	1. Parcialmente implementado. 2. Si.	80%
	A.9.4.4	Uso de herramientas de administración de sistemas	¿Son restringidos y monitoreados los programas de utilidad privilegiada?	Parcialmente implementado	95%
	A.9.4.5	Control de acceso al código fuente de los programas	¿Se protege el acceso al código fuente del sistema de control de acceso?	Parcialmente implementado	95%
	A.10	**Cifrado**			
	A.10.1	**Controles criptográficos**			
	A.10.1.1	Política de uso de los controles criptográficos	¿Existe una política para el uso de controles criptográficos?		0%
	A.10.1.2	Gestión de claves	¿Existe una política que rija todo el ciclo de vida de las claves de cifrado?		0%
	A.11	**Seguridad física y ambiental**			
	A.11.1	**Áreas seguras**			
	A.11.1.1	Perímetro de seguridad física	1. ¿Existe un perímetro de seguridad designado? 2. ¿Las áreas de información sensible o críticas son segregadas y controladas de manera adecuada?	1. Parcialmente implementado 2. Parcialmente implementado	80%
	A.11.1.2	Controles físicos de entrada	¿Las áreas seguras tienen sistemas de control de entrada adecuados, para garantizar que solo el personal autorizado tenga acceso?	Parcialmente implementado	95%
	A.11.1.3	Seguridad de oficinas, despachos y recursos	1. ¿Están las oficinas, habitaciones e instalaciones diseñadas y configuradas pensando en la seguridad? 2. ¿Los procesos para mantener la seguridad (ejemplo, cerraduras, escritorios limpios, etc.) existen?	1. Parcialmente implementado 2. Parcialmente implementado	90%
	A.11.1.4	Protección contra las amenazas externas y ambientales	¿Se cuenta con medidas de protección física diseñadas para prevenir desastres naturales, ataques maliciosos o accidentes?	Parcialmente implementado	80%
	A.11.1.5	El trabajo en áreas seguras	1. ¿Existen zonas seguras? 2. ¿Dónde existen áreas seguras, tienen políticas y procesos adecuados?	1. Parcialmente implementado 2. Parcialmente implementado	85%

			3. ¿Son las políticas y procesos aplicados y monitoreados?	3. Parcialmente implementado	
	A.11.1.6	Áreas de acceso público, carga y descarga	1. ¿Están separadas las zonas de entrega / carga? 2. ¿Existen controles en estas áreas? 3. ¿Está el acceso de las zonas de carga aisladas de instalaciones de procesamiento de información?	1. Parcialmente implementado 2. Parcialmente implementado 3. Parcialmente implementado	65%
	A.11.2	**Seguridad de los equipos**			
	A.11.2.1	Emplazamiento y protección de equipos	1. ¿Identificar los peligros ambientales y considerar la selección de sus ubicaciones? 2. ¿Se considera los riesgos por el ingreso de personal no autorizado, una forma para desplazar los equipos?	1. Parcialmente implementado 2. Parcialmente implementado	65%
	A.11.2.2	Instalaciones de suministro	1. ¿Existe un sistema UPS o generador de respaldo? 2. ¿Se ha probado el tiempo aproximado de respaldo?	1. Si. 2. Parcialmente implementado	95%
	A.11.2.3	Seguridad del cableado	1. ¿Existen evaluaciones del riesgo sobre la ubicación de los cables de energía y telecomunicaciones? 2. ¿Se encuentran los cables protegidos y localizados para intercepción o daños?	1. Parcialmente implementado 2. Si.	95%
	A.11.2.4	Mantenimiento de los equipos	¿Existe un riguroso programa de mantenimiento de equipos?	Parcialmente implementado	25%
	A.11.2.5	Salida de activos fuera de las dependencias de la empresa	1. ¿Existe un proceso de control para la salida de activos de la institución? 2. ¿Se respeta este proceso? 3. ¿Se ha llevado a cabo controles en sitio?	1. Parcialmente implementado 2. Parcialmente implementado 3. Parcialmente implementado	75%
	A.11.2.6	Seguridad de los equipos y activos fuera de las instalaciones	1. ¿Existe una póliza de seguros para los activos que se encuentren fuera de la institución? 2. ¿Está política se encuentra ampliamente comunicada?	1. Parcialmente implementado 2. Parcialmente implementado	75%
	A.11.2.7	Reutilización o retirada segura de dispositivos de almacenamiento	1. ¿Existe una política que cubra la reutilización de activos de información? 2. ¿Cuándo se limpia la data, esta se controló y verifico de manera adecuada antes de su reutilización y/o eliminación?	1. Política desarrollada, aún no aprobada por la M.A. 2. Parcialmente implementado	90%
	A.11.2.8	Equipo informático de usuario desatendido	1. ¿Tiene la institución una política entorno: como es la protección de equipo desatendido? 2. ¿Los controles técnicos aseguran que el equipo este siendo inadvertidamente corregido?	1. Parcialmente implementado 2. Parcialmente implementado	75%
	A.11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla	1. ¿Existe una política de escritorio limpio y bloqueo de pantalla? 2. ¿Esta se cumple de forma correcta?	1. Política desarrollada, aún no aprobada por la M.A. 2. Parcialmente cumplido	80%
	A.12	**Seguridad en la operación**			
	A.12.1	**Responsabilidades y procedimientos de operación**			
	A.12.1.1	Documentación de procedimientos de operación	1. ¿Los procedimientos de operación están bien documentados? 2. ¿Los procedimientos están disponibles a todos los usuarios cuando lo necesiten?	1. Parcialmente desarrollados 2. Parcialmente disponibles	70%
	A.12.1.2	Gestión de cambios	¿Hay un proceso de gestión de cambio controlado en su institución?	Parcialmente implementado	70%
	A.12.1.3	Gestión de capacidades	¿Hay un proceso de gestión de capacidad en su institución?	Parcialmente implementado	40%
	A.12.1.4	Separación de entornos de desarrollo, prueba y producción	¿La organización cumple con la segregación de los ambientes de desarrollo, pruebas y operaciones?	Parcialmente implementado	95%
	A.12.2	**Protección contra código malicioso**			
	A.12.2.1	Controles contra el código malicioso	1. ¿Existe procesos para detectar malware en su institución? 2. ¿Existe procesos para evitar la propagación de malware en su institución? 3. ¿Tiene la organización un proceso y la capacidad para recuperarse de una infección de malware?	1. Parcialmente implementado 2. Parcialmente implementado 3. Parcialmente implementado	95%

	A.12.3	**Copias de seguridad**			
	A.12.3.1	Copias de seguridad de la información	1. ¿Existe una política de copia de seguridad? 2. ¿La política de copia de seguridad de la institución cumple con los marcos legales pertinentes? 3. ¿Las copias de seguridad que se realiza están conforme a la política de seguridad? 4. ¿Se prueban las copias de seguridad?	1. Política desarrollada, aún no aprobada por la M.A. 2. Parcialmente implementado 3. Parcialmente implementado 4. No	90%
	A.12.4	**Registro de actividad y supervisión**			
	A.12.4.1	Registro y gestión de eventos de actividad	¿Se mantienen los registros de eventos apropiados y revisados con regularidad?	Parcialmente implementado	80%
	A.12.4.2	Protección de los registros de información	¿Las instalaciones están protegidas contra la manipulación y acceso no autorizado?	Parcialmente implementado	80%
	A.12.4.3	Registros de actividad del administrador y operador del sistema	¿Los registros sysadmin / sysop se mantienen, protegidos y revisados con regularidad?	Parcialmente implementado	90%
	A.12.4.4	Sincronización de relojes	¿Están todos los relojes sincronizados en la institución	Parcialmente implementado	100%
	A.12.5	**Control del software en explotación**			
	A.12.5.1	Instalación del software en sistemas en producción	¿Existe un proceso para la instalación de software en los sistemas operativos?	Parcialmente implementado	60%
	A.12.6	**Gestión de la vulnerabilidad técnica**			
	A.12.6.1	Gestión de las vulnerabilidades técnicas	1. ¿Tiene la institución el acceso a información actualizada y oportuna sobre las vulnerabilidades técnicas? 2. ¿Existe un proceso para evaluar el riesgo y reaccionar a medida que se van descubriendo nuevas vulnerabilidades?	1. Parcialmente implementado 2. Parcialmente implementado	55%
	A.12.6.2	Restricciones en la instalación de software	¿Existen procesos para restringir que los usuarios instalen software?	Parcialmente implementado	80%
	A.12.7	**Consideraciones de las auditorías de los sistemas de información**			
	A.12.7.1	Controles de auditoría de los sistemas de información	1. ¿Hay sistemas sujetos a la auditoría? 2. ¿El proceso de auditoría asegura la reducción al mínimo de interrupciones en la institución?	1. Si. 2. Parcialmente implementado	0%
	A.13	**Seguridad en las telecomunicaciones**			
	A.13.1	**Gestión de la seguridad en las redes**			
	A.13.1.1	Controles de red	¿Hay un proceso de gestión de la red en la institución?	Parcialmente implementado	80%
	A.13.1.2	Mecanismos de seguridad asociados a servicios en red	1. ¿Tiene la organización implementada un enfoque de gestión de riesgos que identifique todos los servicios de red y los acuerdos de servicio? 2. ¿Se exige seguridad de la información en acuerdos y contratos con los proveedores de servicios (permanente y subcontratado)?. 3. ¿Tiene acuerdos de nivel de servicio relacionados con la seguridad de la información?	1. Parcialmente implementado 2. Si. 3. Parcialmente implementado.	65%
	A.13.1.3	Segregación de redes	¿La topología de la red cumple con la segregación de las redes para diferentes tareas?	Si	90%
	A.13.2	**Intercambio de información con partes externas**			
	A.13.2.1	Políticas y procedimientos de intercambio de información	1. ¿Existen políticas en la institución para determinar cómo se transfiere la información? 2. ¿Existen procedimientos de como la información debe ser transferida a todos los empleados? 3. ¿Existen controles técnicos relevantes para evitar formas no autorizadas de transferencia	1. Parcialmente implementado. 2. Parcialmente implementado. 3. Si.	80%

			de información?		
	A.13.2.2	Acuerdos de intercambio	¿Se realiza contratos y/o acuerdos con terceros de parte de la institución, donde detalle los requisitos para obtener transferencia de información?	Parcialmente implementado	90%
	A.13.2.3	Mensajería electrónica	¿Se incluye políticas de seguridad para la transferencia de información durante el uso de sistemas de mensajería electrónica?	Parcialmente implementado	95%
	A.13.2.4	Acuerdos de confidencialidad y secreto	1. ¿Los empleados, contratistas y agentes firman un acuerdo de confidencialidad y no divulgación? 2. ¿Los acuerdos se revisan periódicamente? 3. ¿Se mantiene registro de los acuerdos?	1. No. 2. Parcialmente implementado. 3. Si.	70%
	A.14	**Adquisición, desarrollo y mantenimiento de los sistemas de información**			
	A.14.1	**Requisitos de seguridad de los sistemas de información**			
	A.14.1.1	Análisis y especificación de los requisitos de seguridad	1. ¿Se especifican los requisitos de seguridad de la información cuando se introducen nuevos sistemas? 2. ¿Cuándo los sistemas están siendo mejorados o actualizados, se especifica y direcciona los requisitos de seguridad?	1. Parcialmente implementado. 2. Si.	90%
	A.14.1.2	Seguridad de las comunicaciones en servicios accesibles por redes públicas	¿Para las aplicaciones que envíen información a través de redes públicas se protege adecuadamente la información contra la actividad fraudulenta, disputa contractual, divulgación y modificación no autorizada?	Parcialmente implementado	95%
	A.14.1.3	Protección de las transacciones por redes telemáticas	¿Existen controles para prevenir la transmisión incompleta, alteración de mensajes no autorizados, duplicación no autorizada o mensajes de ataque de replicación?	Si	100%
	A.14.2	**Seguridad en los procesos de desarrollo y soporte**			
	A.14.2.1	Política de desarrollo seguro de software	1. ¿La organización desarrolla software o sistemas? 2. ¿Si es así, Existen políticas que ordenen la implementación y evaluación de los controles de seguridad?	1. Si. 2. Parcialmente implementado.	90%
	A.14.2.2	Procedimientos de control de cambios en los sistemas	¿Existe un proceso de control de cambios?	Si	100%
	A.14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	¿Existe un proceso para garantizar la revisión técnica que se lleva a cabo cuando se cambian las plataformas de operación?	Si	100%
	A.14.2.4	Restricciones a los cambios en los paquetes de software	¿Existe una política que especifique cuando un paquete de software puede ser cambiado o modificado?	Parcialmente implementado	90%
	A.14.2.5	Uso de principios de ingeniería en protección de sistemas	¿La institución tiene documentación de los principios de ingeniería de como los sistemas debe asegurar la seguridad?	Parcialmente implementado	85%
	A.14.2.6	Seguridad en entornos de desarrollo	1. ¿Se ha establecido un entorno de desarrollo seguro? 2. ¿Todos los proyectos utilizan el entorno de desarrollo seguro apropiadamente durante el ciclo de vida del desarrollo de los sistemas?	1. Parcialmente implementado. 2. Parcialmente implementado. 3. Si.	80%
	A.14.2.7	Externalización del desarrollo de software	1. ¿Cuándo el desarrollo se realiza externamente este es supervisado? 2. ¿El código desarrollado externamente está sujeto a una revisión de seguridad antes de la implementación?	1. Parcialmente implementado. 2. Parcialmente implementado. 3. Si.	75%
	A.14.2.8	Pruebas de funcionalidad durante el	¿Cuándo un sistema o aplicación son desarrollados, existen pruebas de seguridad como parte	Parcialmente implementado	95%

		desarrollo de los sistemas	del proceso de desarrollo?		
	A.14.2.9	Pruebas de aceptación	¿Existe un proceso establecido para aceptar nuevo sistemas/aplicaciones o actualizaciones, antes de su puesta en producción?	Parcialmente implementado	95%
	A.14.3	**Datos de prueba**			
	A.14.3.1	Protección de los datos utilizados en pruebas	1. ¿Existe un proceso para la selección de los datos de prueba? 2. ¿Los datos de prueba son adecuadamente protegidos?	1. Parcialmente implementado. 2. Parcialmente implementado.	75%
	A.15	Relaciones con proveedores			
	A.15.1	**Seguridad de la información en las relaciones con proveedores**			
	A.15.1.1	Política de seguridad de la información para proveedores	1. ¿La seguridad de la información está incluida en los contratos establecidos con los proveedores y prestadores de servicios? 2. ¿Existe un enfoque de gestión de riesgos en toda la institución para relaciones con los proveedores?	1. Parcialmente implementado. 2. Parcialmente implementado	90%
	A.15.1.2	Tratamiento del riesgo dentro de acuerdos de proveedores	1. ¿Se proporciona a los proveedores la documentación de requisitos de seguridad? 2. ¿El acceso a los activos de información e infraestructura para proveedores es controlada y monitoreada?	1. Parcialmente implementado. 2. Parcialmente implementado.	70%
	A.15.1.3	Cadena de suministro en tecnologías de la información y comunicaciones	¿Los acuerdos con los proveedores incluyen requisitos para hacer frente a la seguridad de la información dentro de la cadena de servicios y suministro de productos?	Parcialmente implementado	75%
	A.15.2	**Gestión de la prestación del servicio por suministradores**			
	A.15.2.1	Supervisión y revisión de los servicios prestados por terceros	¿Los proveedores son sujetos a revisión periódica y la auditoria?	No.	30%
	A.15.2.2	Gestión de cambios en los servicios prestados por terceros	¿Los cambios en la prestación de los servicios son sujetos a un proceso de gestión que incluya la seguridad y la evaluación de riesgos?	Parcialmente implementado	40%
	A.16	**Gestión de incidentes en la seguridad de la información**			
	A.16.1	**Gestión de incidentes de seguridad de la información y mejoras**			
	A.16.1.1	Responsabilidades y procedimientos	¿Las responsabilidades de gestión son claramente identificadas y documentados en los procesos de gestión de incidentes?	Parcialmente implementado	75%
	A.16.1.2	Notificación de los eventos de seguridad de la información	1. ¿Existe un procedimiento para la comunicación oportuna de eventos de seguridad de la información? 2. ¿Existe un proceso para revisar y actuar sobre los eventos de seguridad de la información detectados?	1. Parcialmente implementado. 2. Parcialmente implementado.	60%
	A.16.1.3	Notificación de puntos débiles de la seguridad	1. ¿Existe un procedimiento para la notificación de los fallos de seguridad de la información que se identifique? 2. ¿Este proceso está ampliamente comunicado? 3. ¿Existe un proceso para revisar y hacer frente a los informes de manera oportuna?	1. Parcialmente implementado. 2. Parcialmente implementado. 3. Si.	70%
	A.16.1.4	Valoración de eventos de seguridad de la información y toma de decisiones	¿Los procesos para asegurar la información y los eventos de seguridad se evalúan y clasifican correctamente?	Parcialmente implementado	65%
	A.16.1.5	Respuesta a los incidentes de seguridad	¿Existe un proceso de respuesta a incidentes que refleja la clasificación y la gravedad de los incidentes de seguridad de la información?	Parcialmente implementado	60%
	A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	¿Existe un proceso o marco de referencia que permita a la institución aprender de los incidentes de seguridad de la información para reducir el impacto / probabilidad de eventos futuros?	Parcialmente implementado	75%

	A.16.1.7	Recopilación de evidencias	1. ¿Existe una política de preparación forense? 2. ¿En el caso de un incidente de seguridad de la información se recoge los datos relevantes de una manera que permita ser utilizado como pruebas?	1. No. 2. Parcialmente implementado.	85%
	A.17	**Aspectos de seguridad de la información en la gestión de la continuidad del negocio**			
	A.17.1	**Continuidad de la seguridad de la información**			
	A.17.1.1	Planificación de la continuidad de la seguridad de la información	¿La seguridad de la información está incluida en los planes de continuidad de la organización?	Parcialmente implementado	45%
	A.17.1.2	Implantación de la continuidad de la seguridad de la información	¿La seguridad de la información de la institución está documentada, implementada los procesos para mantener la continuidad del servicio durante una situación adversa?	Parcialmente implementado	45%
	A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	¿Los planes de continuidad son validados y verificados en intervalos regulares?	Parcialmente implementado	30%
	A.17.2	**Redundancias**			
	A.17.2.1	Disponibilidad de instalaciones para el procesamiento de la información	¿Las instalaciones de procesamiento de información tienen la suficiente redundancia para satisfacer los requisitos de disponibilidad de la organización?	Parcialmente implementado	60%
	A.18	**Cumplimiento**			
	A.18.1	**Cumplimiento de los requisitos legales y contractuales**			
	A.18.1.1	Identificación de la legislación aplicable	1. ¿La institución ha identificado y documentado todos los requisitos legales, regulatorios o contractuales respecto a la seguridad de la información? 2. ¿Está documentado el cumplimiento?	1. Parcialmente implementado. 2. Parcialmente implementado.	55%
	A.18.1.2	Derechos de propiedad intelectual (DPI)	1. ¿La institución mantiene un registro de todos los derechos de propiedad intelectual y el uso de software propietario? 2. ¿Se monitorea en la organización el uso de software sin licencia?	1. Parcialmente implementado. 2. Parcialmente implementado.	60%
	A.18.1.3	Protección de los registros de la organización	¿Los registros están protegidos contra pérdida, destrucción, falsificación y acceso no autorizado de conformidad con los requisitos legales, reglamentos y contratos de la institución?	Parcialmente implementado	60%
	A.18.1.4	Protección de datos y privacidad de la información personal	1. ¿Se identifican los datos personales y son clasificados apropiadamente? 2. ¿Los datos personales están protegidos de conformidad a la legislación pertinente?	1. Parcialmente implementado. 2. Parcialmente implementado.	75%
	A.18.1.5	Regulación de los controles criptográficos	¿Existen controles criptográficos protegidos de acuerdo con todos los acuerdos pertinentes, la legislación y los reglamentos?	No.	35%
	A.18.2	**Revisiones de la seguridad de la información**			
	A.18.2.1	Revisión independiente de la seguridad de la información	1. ¿El enfoque de la institución para la gestión de la seguridad de la información está sujeto a una revisión periódica independiente? 2. ¿La implementación de controles de seguridad está sujeta a una revisión periódico independiente?	1. Parcialmente implementado. 2. Parcialmente implementado.	70%
	A.18.2.2	Cumplimiento de las políticas y normas de seguridad	1. ¿La institución instruye a los responsables de revisar periódicamente el cumplimiento de las políticas y procedimientos dentro de su área de responsabilidad? 2. ¿Se mantienen registros de estas revisiones?	1. Parcialmente implementado. 2. Parcialmente implementado.	40%

	A.18.2.3	Comprobación del cumplimiento	¿La institución lleva a cabo periódicamente revisiones de cumplimiento técnico en los sistemas de información?	Parcialmente implementado	85%

Fuente: INEC, catálogo de documentos normativos vigentes, responsable: dirección de normalización, actualización: marzo 2016. *Elaborado por*: El autor, 2016.

ANEXO 7. MATRIZ DE RIESGOS INSTITUCIONAL.

PROCESOS (ATRIBUCIÓN)	OBJETIVO ESTRATÉGICO	IDENTIFICACIÓN DE RIESGOS	CAUSA	PROBABILIDAD		IMPACTO		RESULTADO	RIESGO INHERENTE	CONTROL	TIPO DE CONTROL	¿Está documentado el control del riesgo?	¿Se aplicado en la actualidad el control?	¿Es efectivo el control para mitigar el riesgo?	EVALUACIÓN	RIESGO RESIDUAL
				VALOR	PROBABILIDAD	VALOR	IMPACTO			¿Cuál es el control?						
Proponer, analizar, diseñar y supervisar la implementación de proyectos de innovación orientados a mejorar la gestión de la Función Judicial en el ámbito de TICs;	Impulsar a la mejora permanente y modernización de los servicios	Generación de sistemas no acordes a la realidad	Falta de planeación institucional, capacidades y estudios previos limitado acceso de información,	02-ene-00	Muy baja	08-ene-00	Mayor	16-ene-00	TOLERABLE	Gestión de Proyectos, mediante Metodologías por parte de la Jefatura Área de Proyectos TICS	PREVENTIVO	SI	SI	SI	MUY BUENO	ACEPTABLE
Proponer, analizar, diseñar y supervisar la implementación de proyectos de innovación orientados a mejorar la gestión de la Función Judicial en el ámbito de TICs;	Impulsar a la mejora permanente y modernización de los servicios	Ausencia de implementación y supervisión de proyectos de innovación de TICs	Falta de acompañamiento de la Dirección Requirente Falta de recursos administrativos, recursos humanos y tecnológicas para la implementación y supervisión de proyectos	6	Moderada	6	Media	36	MODERADO	Gestión de Proyectos, mediante Metodologías por parte de la Jefatura Área de Proyectos TICS	PREVENTIVO	SI	SI	SI	MUY BUENO	TOLERABLE
Elaborar y ejecutar el plan estratégico de TICs;	Impulsar a la mejora permanente y modernización de los servicios	Deficiente alineación a los OEIS del Consejo de la Judicatura en la elaboración del Plan Estratégico de TICs	No utilización de metodologías que permitan alinear el PETIC a los OEIS del Consejo de la Judicatura	2	Muy baja	8	Mayor	16	TOLERABLE	Control de Indicadores del Plan Estratégico	PREVENTIVO	SI	SI	SI	MUY BUENO	ACEPTABLE
Elaborar y administrar la arquitectura de tecnología de información de la Función Judicial;	Impulsar a la mejora permanente y modernización de los servicios	Infraestructura y arquitectura tecnológica sin mantenimiento y sin renovación	Priorización Institucional Recursos económicos no asignados.	8	Alta	8	Mayor	64	IMPORTANTE	Evaluación de Riesgos Internos para Alertar a las Autoridades	PREVENTIVO	SI	SI	NO	MEJORABLE	IMPORTANTE
Elaborar y administrar la arquitectura de tecnología de información de la Función Judicial;	Impulsar a la mejora permanente y modernización de los servicios	No contar con el servicio de Telecomunicaciones	Depender de un único proveedor para el tema de comunicaciones	4	Baja	8	Mayor	32	TOLERABLE	Informes mensuales de disponibilidad del servicio	PREVENTIVO	SI	SI	SI	MUY BUENO	ACEPTABLE

Elaborar y administrar el modelo de interoperabilidad de la Función Judicial;	Impulsar a la mejora permanente y modernización de los servicios	No disponer de un modelo de interoperabilidad definido	Falta de coordinación interna y externa	4	Baja	8	Mayor	32	TOLERABLE	Seguimiento de convenios interinstitucionales	PREVENTIVO	NO	NO	NO	DEFICIENTE	MODERADO
Administrar la demanda de servicios tecnológicos de la Función Judicial;	Impulsar a la mejora permanente y modernización de los servicios	Incumplimiento de los requerimientos por falta de capacidad humana y tecnológica	No contar con los recursos tecnológicos y humanos para satisfacer la demanda	4	Baja	6	Media	24	TOLERABLE	Gestión de Recursos (Personal y tecnológico)	PREVENTIVO	SI	SI	SI	MUY BUENO	ACEPTABLE
Administrar los activos tecnológicos e informáticos de la Función Judicial;	Impulsar a la mejora permanente y modernización de los servicios	Inventario desactualizado de los activos tecnológicos e informáticos	Falta de procedimiento coordinado entre la unidad administrativa y DNTICS	6	Moderada	6	Media	36	MODERADO	Gestión de Recursos	CORRECTIVO	NO	NO	NO	DEFICIENTE	IMPORTANTE
Elaborar y administrar normas, procedimientos, políticas de seguridad y estándares de TICs de la Función Judicial;	Impulsar a la mejora permanente y modernización de los servicios	Desactualización y no aplicación de las Normas, procedimientos, políticas de seguridad y estándares de TICs	Falta de procesos de control a nivel desconcentrado	4	Baja	8	Mayor	32	TOLERABLE	Revisión de Manual de políticas de seguridad. Informes mensuales de las Directrices y lineamientos de la Dirección.	PREVENTIVO	SI	SI	SI	MUY BUENO	ACEPTABLE
Desarrollar, supervisar y ejecutar planes de seguridad de la información, contingencias, recuperación de desastres y continuidad de operaciones de tecnología de información;	Impulsar a la mejora permanente y modernización de los servicios	Falta de generación de planes de contingencias, desastres y continuidad de operaciones para todos los sistemas de información	Falta de priorización en la generación y aprobación de planes de contingencia y continuidad	4	Baja	8	Mayor	32	TOLERABLE	Presentación de los Planes de contingencia y continuidad	PREVENTIVO	SI	NO	NO	MEJORABLE	TOLERABLE
Coordinar y supervisar las acciones de las unidades desconcentradas;	Impulsar a la mejora permanente y modernización de los servicios	Ausencia de coordinación con las unidades desconcentradas de TICs	Deficiente comunicación Falta de claridad en los roles administrativos a nivel desconcentrado	4	Baja	6	Media	24	TOLERABLE	Seguimiento a las directrices establecidas por la Dirección de TICs	PREVENTIVO	NO	NO	NO	DEFICIENTE	MODERADO

Fuente: *Consejo de la Judicatura, 2016*. Elaborado por: *El autor, 2016*

ANEXO 8. INFORME DEL ANÁLISIS DE VULNERABILIDADES DEL CJ.

(Se imprime el informe del análisis de vulnerabilidades del CJ en PDF – documento interno confidencial SNSI).

Fuente: SNSI, 2016. *Elaborado por*: SNSI y participación del autor, *2016*.

ANEXO 9. PROCESOS, INDICADORES Y TIEMPO ESTIMADO DE LOS DOCUMENTOS SNSI.

OBJETIVO No.	PRODUCTOS ENTRANTES	DEFINICIÓN DEL INDICADOR	PROCESOS									TIEMPO ESTIMADO GLOBAL
(Detallado)	(Según el Estatuto Integral de Gestión Organizacional por Procesos del CJ)	(Según el alcance o cumplimiento)	**Fase 1**	**Fase 2**	**Fase 3**	**Fase 4**	**Fase 5**	**Fase 6**	**Fase 7**	**Fase 8**	**Fase 9**	(Meses)
1	Planes de remediación		Recopilar y depurar la información	Aplicar metodología o estándar de evaluación y/o modelo de gestión a la información	Resultado del análisis.	Elaboración del plan (documento).	Presentar, revisar y aprobar el plan por Subdirector/Director.	Aplicación o Pruebas Demo	Evaluación	Reajuste		15
1	Continuidad de operaciones		Recopilar y depurar la información	Aplicar análisis	Definir proceso alterno o paralelo	Elaboración del documento: "Continuidad operaciones	Presentar, revisar y aprobar el plan por Subdirector/Director.	Prueba funcionamiento DEMO	Reajuste	Prueba final	Funcionamiento	18
1	Seguridad de hardware y software		Recopilar información y/o verificar estado	Correr metodología o sistema a las seguridades	Presentación de resultados	Propuesta de seguridad	Implementación y verificación	Evaluación				3
1	Recuperación de desastres y contingencias de TICs.		Recopilar y depurar la información	Aplicar metodología o estándar de evaluación y/o modelo a la información	Resultado del análisis.	Elaboración del plan a recuperar (documento).	Presentar, revisar y aprobar la recuperación por Subdirector/Director.	Aplicación o Pruebas Demo	Evaluación	Reajuste		18
2	Propuestas de reglamentos relacionados con la seguridad de la información para: el procesamiento y almacenamiento de datos		Desarrollar la propuesta	Aprobación	Implementar	Socializar	Gestionar el cumplimiento					12
2	Propuestas de reglamentos relacionados con la seguridad de la información para: Gestión de riesgos		Desarrollar la propuesta	Aprobación	Implementar	Socializar	Gestionar el cumplimiento					9
2	Propuestas de reglamentos relacionados con la seguridad de la información para: Uso de los servicios de telecomunicaciones.		Desarrollar la propuesta	Aprobación	Implementar	Socializar	Gestionar el cumplimiento					9

3	Informes de seguimiento y gestión de la seguridad de información en la Institución.		Recopilar y depurar la información	Aplicar análisis	Elaboración del informe	Entrega del Informe	Respuesta u observación del informe.	Seguimiento del resultado o culminación.				12
4	Informe de análisis, vulnerabilidades, tendencias y riesgos relacionados con la seguridad de la información.		Recopilar y depurar la información	Aplicar análisis	Elaboración del informe	Entrega del Informe	Respuesta u observación del informe.	Seguimiento del resultado o culminación.				12
5	Procedimiento para la actualización y robustecimiento de las seguridades del hardware.		Recopilar y depurar la información	Aplicar metodología o estándar de evaluación y/o modelo a la información	Resultado del análisis.	Elaboración del procedimiento	Presentar, revisar y aprobar el procedimiento por Subdirector/Director.	Aplicación o Pruebas del procedimiento Demo	Evaluación	Reajuste		12
6	Indicadores de incidencias y casos de violación de políticas de seguridad.		Recopilar y depurar la información	Elaboración del informe	Evaluación	Plan de mitigación	Monitoreo y control					12
7	Informes de auditoría de acceso a plataformas, aplicaciones, servicios de forma interna y externa.		Definición de los formularios	Aplicación de la Auditoria	Recomendaciones	Seguimiento						4
8	Informes de gestión y de cumplimiento de planes.		Recopilar y depurar la información	Aplicar análisis	Elaboración del informe	Entrega del Informe	Respuesta u observación del informe.	Seguimiento del resultado o culminación.				15
9	Proyectos y TDRs		Estudio técnico para el proyecto.	Informe técnico del proyecto.	Estudio Técnico - Económico.	Elaboración y presentación del TDR según formatos SERCOP.	Aprobación y validación de DNA / DG	Subasta inversa	Entrega/Implementación	Funcionamiento	Mantenimiento	1

Fuente: SNSI, 2016. *Elaborado por*: El autor, 2016

ANEXO 10. CARGO Y TAREAS DE LOS SERVIDORES JUDICIALES.

CARGO	TAREA
ANALISTA DE ADMINISTRACIÓN Y TALENTO HUMANO 1	Sin catálogo
ANALISTA DE ADMINISTRACIÓN Y TALENTO HUMANO 2	Sin catálogo
ANALISTA DE ASESORÍA JURÍDICA 1	Sin catálogo
ANALISTA DE ASESORÍA JURÍDICA 2	Sin catálogo
ANALISTA DE BIBLIOTECA, GACETA JUDICIAL Y MUSEO 1	Sin catálogo
ANALISTA DE BIBLIOTECA, GACETA JUDICIAL Y MUSEO 2	Sin catálogo
ANALISTA DE COOPERACIÓN JUDICIAL INTERNACIONAL 1	Sin catálogo
ANALISTA DE COOPERACIÓN JUDICIAL INTERNACIONAL 2	Sin catálogo
ANALISTA DE GESTIÓN DOCUMENTAL Y ARCHIVO 1	Sin catálogo
ANALISTA DE GESTIÓN DOCUMENTAL Y ARCHIVO 2	Sin catálogo
ANALISTA DE INVESTIGACIONES JURÍDICAS 1	Sin catálogo
ANALISTA DE INVESTIGACIONES JURÍDICAS 2	Sin catálogo
ANALISTA DE PROCESAMIENTO DE JURISPRUDENCIA 1	Sin catálogo
ANALISTA DE PROCESAMIENTO DE JURISPRUDENCIA 2	Sin catálogo
ANALISTA DE RELACIONES PÚBLICAS Y COMUNICACIÓN SOCIAL 1	Sin catálogo
ANALISTA DE RELACIONES PÚBLICAS Y COMUNICACIÓN SOCIAL 2	Sin catálogo
ANALISTA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES 1	Sin catálogo
ANALISTA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES 2	Sin catálogo
ASISTENTE ADMINISTRATIVO 2	Sin catálogo
ASISTENTE DE COORDINACIÓN DE UNIDAD JUDICIAL	Sin catálogo
AUXILIAR DE ENFERMERÍA	Sin catálogo
AYUDANTE JUDICIAL	DIGITALIZACIÓN
	INGRESA ACTIVIDADES ANTERIORES
	INGRESO DE JUICIOS HISTÓRICOS
	MODIFICAR CARATULA
	MODIFICAR FIRMAS Y CARGOS
	PONER/CAMBIAR RESPONSABLE
	PUEDE ASIGNAR DATOS PARA CITACIÓN
	RECIBIR ESCRITOS EN LA JUDICATURA
	SACAR REPORTES
	TERMINAR ACTIVIDAD
	TRAMITE
CONJUEZ	HACER RESOLUCIONES
	MODIFICAR CARATULA
	TERMINAR ACTIVIDAD
	TRAMITE
COORDINADOR DE UNIDAD JUDICIAL	Sin catálogo

COORDINADOR JURÍDICO DE CORTE NACIONAL	SACAR REPORTES
DIRECTOR TÉCNICO DE ASESORÍA JURÍDICA Y COOPERACIÓN JUDICIAL INTERNACIONAL	Sin catálogo
DIRECTOR TÉCNICO DE PROCESAMIENTO DE JURISPRUDENCIA E INVESTIGACIONES JURÍDICAS	Sin catálogo
GESTOR DE ARCHIVO	DIGITALIZACIÓN
	RECIBIR ESCRITOS EN LA JUDICATURA
JEFE DE ADMINISTRACIÓN Y TALENTO HUMANO	Sin catálogo
JEFE DE BIBLIOTECA, GACETA JUDICIAL Y MUSEO	Sin catálogo
JEFE DE GESTIÓN DOCUMENTAL Y ARCHIVO	DIGITALIZACIÓN
	SACAR REPORTES
JEFE DE GESTIÓN DOCUMENTAL Y ARCHIVO	DIGITALIZACIÓN
	SACAR REPORTES
JEFE DE RELACIONES PÚBLICAS Y COMUNICACIÓN SOCIAL	Sin catálogo
JEFE DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES	Sin catálogo
JUEZ	ANULAR SORTEO DE PERITO
	ASIGNAR CAMBIAR JUEZ
	DEPÓSITOS JUDICIALES
	DIGITALIZACIÓN
	EJECUTA RESORTEO A NUEVA JUDICATURA
	EJECUTAR REORGANIZACIÓN
	ELIMINAR AGENDA PENDIENTE
	ENVÍO A SUPERIOR
	ESCUCHAR AUDIO
	HABILITAR SORTEO SEGUNDO PERITO
	HACER CITACIONES
	HACER RESOLUCIONES
	INGRESA ACTIVIDADES ANTERIORES
	INGRESAR JUICIOS DIRECTAMENTE
	INGRESAR JUICIOS DIRECTAMENTE PARA JUDICATURAS NO AUTOMATIZADAS
	INGRESAR PROCESOS DIRECTAMENTE
	INGRESO DE JUICIOS HISTÓRICOS
	MODIFICAR CARATULA
	MODIFICAR FIRMAS Y CARGOS
	MODIFICAR TIPO ACCIÓN\DELITO
	PONER/CAMBIAR RESPONSABLE
	PUEDE ASIGNAR DATOS PARA CITACIÓN
	PUEDE CONFIGURAR ZONAS
	PUEDE MODIFICAR CITADOR
	REASIGNACIÓN TOTAL
	RECIBIR ESCRITOS EN LA JUDICATURA

	RESORTEAR A NUEVA JUDICATURA
	SACAR REPORTES
	SORTEA DEPOSITARIOS
	SORTEA PERITOS
	TERMINAR ACTIVIDAD
	TRAMITE
LIQUIDADOR - PAGADOR	SACAR REPORTES
MÉDICO INSTITUCIONAL	Sin catálogo
MÉDICO PERITO	DIGITALIZACIÓN
	SACAR REPORTES
NOTIFICADOR - CITADOR	DIGITALIZACIÓN
	HACER CITACIONES
	SACAR REPORTES
ODONTÓLOGO	Sin catálogo
OFICINISTA AUXILIAR	Sin catálogo
OFICINISTA AUXILIAR PROVINCIAL	Sin catálogo
PARVULARIA/O DE ÓRGANOS JURISDICCIONALES	DIGITALIZACIÓN
	SACAR REPORTES
PRESIDENTE DE LA CORTE NACIONAL DE JUSTICIA	HACER RESOLUCIONES
	TERMINAR ACTIVIDAD
	TRAMITE
PRESIDENTE DE SALA	Sin catálogo
PROSECRETARIO GENERAL	Sin catálogo
PSICÓLOGO PERITO	DIGITALIZACIÓN
	SACAR REPORTES
SECRETARIO	ANULAR SORTEO DE PERITO
	DEPÓSITOS JUDICIALES
	ELIMINAR ACTIVIDADES Y ESCRITOS
	ENVÍO A SUPERIOR
	ESCUCHAR AUDIO
	HABILITAR SORTEO SEGUNDO PERITO
	HACER CITACIONES
	INGRESA ACTIVIDADES ANTERIORES
	INGRESAR JUICIOS DIRECTAMENTE
	INGRESAR JUICIOS DIRECTAMENTE PARA JUDICATURAS NO AUTOMATIZADAS
	INGRESO DE JUICIOS HISTÓRICOS
	MODIFICAR CARATULA
	MODIFICAR FIRMAS Y CARGOS
	MODIFICAR TIPO ACCIÓN\DELITO

	PONER/CAMBIAR RESPONSABLE
	PUEDE ASIGNAR DATOS PARA CITACIÓN
	REASIGNACIÓN TOTAL
	RECIBIR ESCRITOS EN LA JUDICATURA
	SACAR REPORTES
	SORTEA DEPOSITARIOS
	SORTEA PERITOS
	TERMINAR ACTIVIDAD
	TRAMITE
SUB COORDINADOR JURÍDICO DE CORTE NACIONAL	Sin catálogo
SUBDIRECTOR TÉCNICO DE ASESORÍA JURÍDICA	Sin catálogo
SUBDIRECTOR TÉCNICO DE COOPERACIÓN JUDICIAL INTERNACIONAL	Sin catálogo
SUBDIRECTOR TÉCNICO DE INVESTIGACIONES JURÍDICAS	Sin catálogo
SUBDIRECTOR TÉCNICO DE PROCESAMIENTO DE JURISPRUDENCIA	Sin catálogo
TÉCNICO DE AUDIENCIAS Y DILIGENCIAS	SACAR REPORTES
TÉCNICO DE BIBLIOTECA, GACETA JUDICIAL Y MUSEO	Sin catálogo
TÉCNICO DE GESTIÓN DOCUMENTAL Y ARCHIVO	DIGITALIZACIÓN
	RECIBIR ESCRITOS EN LA JUDICATURA
TÉCNICO DE SALA Y CÁMARA GESSEL	DIGITALIZACIÓN
	SACAR REPORTES
TÉCNICO DE VENTANILLA E INFORMACIÓN	DIGITALIZACIÓN
	RECIBIR ESCRITOS EN LA JUDICATURA
	SACAR REPORTES
	TRAMITE
TÉCNICO OPERATIVO	SACAR REPORTES
TRABAJADOR SOCIAL PERITO	DIGITALIZACIÓN
	SACAR REPORTES

Fuente: *Dirección Nacional de Seguridad de la Información y Talento Humano, 2016*. Elaborado por: *El autor, 2016.*

FIN DEL DOCUMENTO.