	UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA			
Universidad Francisco de Paula Santander Ocaña - Colombia	Documento: FORMATO HOJA DE RESUMEN PARA TRABAJO DE GRADO	Código: F-AC-DBL-007	Fecha: 08-07-2021	Revisión: B
	Dependencia: DIVISIÓN DE BIBLIOTECA	Aprobado: SUBDIRECTOR ACADEMICO		Pág.: i(133)

RESUMEN – TRABAJO DE GRADO

AUTORES	Manuel Alejandro Caballero Paredes
FACULTAD	Facultad De Ingenierías
PLAN DE ESTUDIOS	Maestría En Gobierno De Ti
DIRECTOR	Doc. Libardo Flórez Villamizar
TÍTULO DE LA TESIS	Modelo De Gestión De Ti Para La Seguridad De La Información De La Jurisdicción Especial Para La Paz.
TITULO EN INGLES	It Management Model For Information Security Of The Special Jurisdiction For Peace.

RESUMEN
(70 palabras)

La elaboración de esta investigación es realmente significativa para la estructuración de procesos viables y de servicios que se prestan en la jurisdicción especial para la paz, dando orden a la efectividad de las directrices que se han planteado. Este documento es elaborado solo con fines educativos para la obtención del grado de Maestría en Gobierno de Tecnologías de la Información. Esta investigación beneficiará a la Universidad Francisco de Paula Santander Ocaña ya que contará con la disponibilidad de la información que logrará contribuir a más empresas que buscan tener mayor protección enfocadas en reducir las amenazas informáticas.

RESUMEN EN INGLES

The elaboration of this investigation is really significant for the structuring of viable processes and services that are provided in the special jurisdiction for peace, giving order to the effectiveness of the guidelines that have been proposed. This document is prepared only for educational purposes to obtain the Master's degree in Information Technology Government. This research will benefit the Francisco de Paula Santander Ocaña University since it will have the availability of information that will contribute to more companies that seek to have greater protection focused on reducing computer threats.

PALABRAS CLAVES	Seuridad Información Jurisdicción
PALABRAS CLAVES EN INGLES	Security Information Jurisdiction

CARACTERÍSTICAS

PÁGINAS: 133	PLANOS:	ILUSTRACIONES:	CD-ROM:

MODELO DE GESTIÓN DE TI PARA LA SEGURIDAD DE LA INFORMACIÓN DE LA JURISDICCIÓN ESPECIAL PARA LA PAZ.

AUTOR:

MANUEL ALEJANDRO CABALLERO PAREDES

PROYECTO PRESENTADO COMO REQUISITO PARA OBTENER EL TÍTULO DE MAESTRÍA EN GOBIERNO DE TI

DIRECTOR:

DOC. LIBARDO FLÓREZ VILLAMIZAR

Magister

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

FACULTAD DE INGENIERÍAS

MAESTRÍA EN GOBIERNO DE TI

OCAÑA, COLOMBIA **AGOSTO, 2021**

Índice

Lista de Figuras

Lista de tablas

Introducción

Según con la autoridad en asuntos de ciberseguridad en Colombia, la substracción de información donde se ven involucrados recursos tecnológicos, ha sido la mayor causa de delitos a nivel nacional desde 2018 hasta lo que va corrido del 2021, con más de 15.000 reclamos en los entes gubernamentales encargados de este tema. En referencia a este hecho:

Es necesario que las empresas hagan un esfuerzo e inversión en servicios de TI, que garanticen las condiciones de seguridad necesarias para proteger a los clientes y comercios. Righard Zwienenberg, que lleva más de 30 años estudiando los programas maliciosos, explica que el objetivo principal del "Malware" es conseguir información y dinero. Que en la actualidad el ransomware es una de las ciber amenazas más comunes y la gente continúa pagando incluso en campañas de ransomware que están muertas y no tienen a nadie activo detrás. (Rubio, 2019)

Es importante descubrir sobre, el fenómeno de los delitos informáticos, que se presentan en la "nube", por consiguiente, esto trae consigo muchas más vulnerabilidades y se han desarrollado varios proyectos para saber un poco más de ellos, a nivel internacional, en la ciudad de Los Ríos, Ecuador, se desarrolló un proyecto de grado titulado:

Uso de los modelos de control informático y su incidencia en la seguridad de la información en el sistema de control de calificaciones de la Universidad Técnica de Babahoyo, tiene como objetivo principal, Evaluar la incidencia de los modelos de control informático en la seguridad de la información en el sistema de control de calificaciones de la Universidad (Mosquera, 2018).

Por otro lado, a nivel nacional, en la ciudad de Bogotá, Colombia, se diseñó un Modelo para la implementación del sistema general de seguridad informática y protocolos de seguridad

informática en la oficina TIC de la alcaldía municipal de Fusagasugá, basados en la gestión del riesgo informático, donde la información es el activo más importante, en el que se realizó: “un análisis profundo de los riesgos a los que se ve expuesta y determinó cuáles son las medidas correctivas y preventivas que debe realizar la empresa, para garantizar los principios de la seguridad de la información: confidencialidad, integridad y disponibilidad” (Pulido y Mantilla, 2016, p. 19). A nivel local, en la ciudad de Ocaña, Norte de Santander, Colombia, se desarrolló un proyecto de grado titulado Diagnostico de seguridad al sistema informático de gestión de contratos de prestación de servicios (CPS) de la Universidad del Rosario: “donde su objetivo es evidenciar los riesgos y vulnerabilidades que existen en las empresas y los ataques cibernéticos a los que están expuestos, por tal razón, implementaron un protocolo de seguridad informática” (Peñaranda, 2017, p. 1).

La seguridad informática ha trazado caminos dentro de un proyecto especializado por el establecimiento de herramientas de software, que contrarresten la entrada ilegal y las irrupciones a los sistemas de información el cual presentan dentro de las empresas, donde, actualmente no cuentan con protocolos de respuesta en caso de que este siendo víctima de un ciber ataque, y los usuarios, en su mayoría logran tener información que debe ser confidencial para la oficina y debe de tener un estricto acceso ya sea por medio de la red o por medio físico en computadoras de la oficina, la falta de información para diseñar un modelo de gobierno de TI que logre implementar protocolos de buenas prácticas y COBIT 5 para una mayor gestión de la información dentro de la oficina y esto genera que los riesgos sean bastante altos al momento de estar teniendo un ataque informático ya sea causado intencionalmente por terceros o descuido del personal de la oficina.

En este trabajo se parte de la identificación de los estándares o buenas prácticas para constituir una guía de gestión de TI, que sirva a la jurisdicción especial para la paz y se realiza un diagnóstico previo de los riesgos inherentes.

Capitulo 1. Planteamiento del problema

Según con la autoridad en asuntos de ciberseguridad en Colombia, la substracción de información donde se ven involucrados recursos tecnológicos, ha sido la mayor causa de delitos a nivel nacional desde 2018 hasta lo que va corrido del 2021, con más de 15.000 reclamos en los entes gubernamentales encargados de este tema. En referencia a este hecho:

Es necesario que las empresas hagan un esfuerzo e inversión en servicios de TI, que garanticen las condiciones de seguridad necesarias para proteger a los clientes y comercios. Righard Zwienenberg, que lleva más de 30 años estudiando los programas maliciosos, explica que el objetivo principal del "Malware" es conseguir información y dinero. Que en la actualidad el ransomware es una de las ciber amenazas más comunes y la gente continúa pagando incluso en campañas de ransomware que están muertas y no tienen a nadie activo detrás. (Rubio, 2019)

Es importante descubrir sobre, el fenómeno de los delitos informáticos, que se presentan en la "nube", por consiguiente, esto trae consigo muchas más vulnerabilidades y se han desarrollado varios proyectos para saber un poco más de ellos, a nivel internacional, en la ciudad de Los Ríos, Ecuador, se desarrolló un proyecto de grado titulado:

Uso de los modelos de control informático y su incidencia en la seguridad de la información en el sistema de control de calificaciones de la Universidad Técnica de Babahoyo, tiene como objetivo principal, Evaluar la incidencia de los modelos de control informático en la seguridad de la información en el sistema de control de calificaciones de la Universidad (Mosquera, 2018).

Por otro lado, a nivel nacional, en la ciudad de Bogotá, Colombia, se diseñó un Modelo para la implementación del sistema general de seguridad informática y protocolos de seguridad

informática en la oficina TIC de la alcaldía municipal de Fusagasugá, basados en la gestión del riesgo informático, donde la información es el activo más importante, en el que se realizó: “un análisis profundo de los riesgos a los que se ve expuesta y determinó cuáles son las medidas correctivas y preventivas que debe realizar la empresa, para garantizar los principios de la seguridad de la información: confidencialidad, integridad y disponibilidad” (Pulido y Mantilla, 2016, p. 19). A nivel local, en la ciudad de Ocaña, Norte de Santander, Colombia, se desarrolló un proyecto de grado titulado Diagnostico de seguridad al sistema informático de gestión de contratos de prestación de servicios (CPS) de la Universidad del Rosario: “donde su objetivo es evidenciar los riesgos y vulnerabilidades que existen en las empresas y los ataques cibernéticos a los que están expuestos, por tal razón, implementaron un protocolo de seguridad informática” (Peñaranda, 2017, p. 1).

La seguridad informática ha trazado caminos dentro de un proyecto especializado por el establecimiento de herramientas de software, que contrarresten la entrada ilegal y las irrupciones a los sistemas de información el cual presentan dentro de las empresas, donde, actualmente no cuentan con protocolos de respuesta en caso de que este siendo víctima de un ciber ataque, y los usuarios, en su mayoría logran tener información que debe ser confidencial para la oficina y debe de tener un estricto acceso ya sea por medio de la red o por medio físico en computadoras de la oficina, la falta de información para diseñar un modelo de gobierno de TI que logre implementar protocolos de buenas prácticas y COBIT 5 para una mayor gestión de la información dentro de la oficina y esto genera que los riesgos sean bastante altos al momento de estar teniendo un ataque informático ya sea causado intencionalmente por terceros o descuido del personal de la oficina.

1.1 Formulación del problema

¿Cuáles serían los componentes que integrarían un modelo de gestión de ti para la seguridad de la información de la jurisdicción especial para la paz?

1.2 Objetivos

1.2.1 Objetivo general

Diseñar un modelo de gestión de ti para la seguridad de la información de la jurisdicción especial para la paz.

1.2.2 Objetivos específicos

- Diagnosticar los riesgos inherentes a la JEP.
- Identificar estándares o buenas prácticas para establecer un modelo de gestión de TI, para la JEP.
- Integrar los componentes identificados en un modelo de gestión de TI que sirvan a la jurisdicción especial para la paz.

1.3 Justificación

Hablar de seguridad informática, es enfocarse en la protección de toda la infraestructura computacional, tanto física como lógica, Gómez, explico, que: “las empresas que deseen sobrevivir a los cambios y tener éxito deben centrarse en preservar, proteger desarrollar y aplicar su capital intelectual, deben evaluar el impacto potencial de los riesgos informáticos que se presentan dentro de la empresa” (2015, p. 13). Por otro lado, Rincón:

Presentan COBIT 5, como la guía de gobierno y gestión de TI, más usada por las organizaciones a nivel mundial; donde han diseñado varias versiones con base al uso, implantación y necesidades que presentan las empresas, el cual muestra que el gobierno implica conocer las necesidades del negocio, priorizarlas, establecer una dirección por medio de

objetivos, roles y responsabilidades para que la gestión pueda operar y con base en esta operación poder monitorear el desempeño de los procesos (ISACA, 2016, p. 12).

De acuerdo con Pillo, COBIT 5: “es robusto, flexible e integrador, y permite a las organizaciones alinear sus objetivos estratégicos con TI apoyando el uso adecuado de recursos, disminución de costos y riesgos” (ISACA, 2017, p. 13). Por otro lado, Pinto y Cañón, explican que, provee un marco de trabajo integral que ayuda a: “las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas, ayudando a las empresas a crear valor manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo” (ISACA, 2017, p. 73).

Actualmente, en la JEP se dispone de unas instalaciones técnica extensa, el cual contiene apoyo completo de recursos tecnológicos y alrededor de más de 2000 usuarios que manipulan los dispositivos, como lo es el uso de los servicios de la intranet, los aplicativos, los sistemas Web, toda la infraestructura es administrada por el área de sistemas, por lo tanto, se considera importante que se establezca un modelo de gobierno de TI que optimice los procesos el cuál garanticen la reacción inmediata al momento de tener algún ciberataque, de proteger la información confidencial que se maneja dentro de la oficina.

La elaboración de esta investigación es realmente significativa para la estructuración de procesos viables y de servicios que se prestan en la jurisdicción especial para la paz, dando orden a la efectividad de las directrices que se han planteado. Este documento es elaborado solo con fines educativos para la obtención del grado de Maestría en Gobierno de Tecnologías de la Información. Esta investigación beneficiará a la Universidad Francisco de Paula Santander Ocaña ya que contará con la disponibilidad de la información que logrará contribuir a más empresas que buscan tener mayor protección enfocadas en reducir las amenazas informáticas.

1.4 Delimitaciones

Delimitación Operativa

El desarrollo del proyecto establece las bases para una futura implementación del Modelo de Gestión de TI el cual sirva de protección ante la ocurrencia de un delito informático.

Delimitación Conceptual

Para lograr tener información de los conceptos existentes nos limitamos a trabajar con la aplicación de buenas prácticas de la Gestión de TI, modelo de Gestión de TI, Delitos Informáticos, Cyber Crimen, protección y estándares existentes enfocados a las buenas prácticas.

Delimitación Geográfica

En cuanto a la posición geográfica se aplicará esta guía dentro de la Jurisdicción Especial para la Paz (JEP) que se encuentra ubicada en la carrera 7 #63-44 en la ciudad de Bogotá.

Delimitación Temporal

Este modelo de Gestión de TI tiene como objetivo la aprobación de la investigación. En un periodo de estudio que será de 12 (doce) meses a partir de la aprobación del proyecto.

Capítulo 2. Marco Referencial

2.1 Marco histórico

El Vínculo que existe a partir de las ciencias aplicadas y las violaciones informáticas no empezó a partir de los computadores. Al nacer el telégrafo en la época de XIX, ya se realizaban interceptaciones en las líneas en el que se transmitían todo tipo de datos falsos monetarios. Por otro lado, con el surgimiento del teléfono, en los años 60, Parada y Errecaborde, dan una breve historia sobre como:

Diferentes programadores informáticos o especialistas en sistemas intentaban boicotear el financiamiento gubernamental a la guerra de Vietnam mediante el uso gratuito del servicio, los phreakers (neologísmo proveniente de las palabras en inglés “Freak”, de rareza; “phone”, de teléfono; y “free”, gratis) utilizaban una blue boxes o cajas azules que reproducían tonos de llamadas similares a los utilizados por la Bell Corporation, y la ATT establecía comunicaciones gratuitas de larga distancia. En cuanto a la utilización de computadoras a partir del almacenamiento y procesamiento de datos personales producto de obras de ficción como 1984 de Orwell. (Parada y Errecaborde, 2018, p. 7)

Según la UNODC (United Nations Office on Drugs and Crime) recopilo información, de cómo la perspectiva global, se ha transformado económicamente, a nivel mundial, las agencias encargadas de hacer cumplir la ley no dan abasto por el gran crecimiento acelerado que ha tenido las tecnologías de la información, y con ello aumentaron los niveles de delitos cibernético:

En 2011, al menos 2.300 millones de personas, el equivalente a más de un tercio de la población total del mundo, tenía acceso a Internet. Más del 60 por ciento de todos los usuarios de internet se encuentran en países en desarrollo, y el 45 por ciento de todos los usuarios de Internet tienen menos de 25 años de edad. Para el año 2017 se calcula que las suscripciones a banda

ancha móvil llegarán al 70 por ciento de la población total del mundo. Para el año 2020, el número de dispositivos interconectados por la red rebasará a las personas en una proporción de seis a uno, transformando las concepciones actuales de lo que es internet. En el mundo hiperconectado del mañana, será difícil imaginarse un "delito informático", y quizás cualquier otro delito que no involucre evidencia electrónica vinculada con la conectividad del protocolo de internet "IP" (UNODC, 2013, p. 15).

Para el Doctor Cano, el chantaje informático es un ambiente real que afecta: "A todos los participantes de la sociedad; su capacidad de adaptación y reinvención en contextos digitales, le permite asumir distintas formas y aproximaciones de tal manera que, establecer esquemas referentes que enfrentarlo, resulta una tarea exigente y de visión multidisciplinar" (Cano, 2016, p. 4).

2.1.1 En el ámbito internacional. Levet, Espinoza, Macgluf y Fragozo, realizaron un proyecto titulado "La inconclusa reforma al Código penal federal en materia de delitos informáticos", en Veracruz, México, en el que hablaron sobre los delitos informáticos; en el que la aparición de las tecnologías de información y comunicación en los años noventa, motivó de reformas al Código Penal Federal Mexicano:

Para incluir la figura de delito informático, a la fecha no se ha actualizado dicha ley en esa materia, por lo que, no se puede sancionar a las personas por conductas no previstas en la legislación penal, quedando desfasado dicho delito. Teniendo como finalidad tipificar como delito la conducta de aquellas personas que sin autorización modifiquen, destruyan o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad que sean tanto de particulares, como del gobierno federal (Levet, Espinoza, Macgluf y Fragozo, 2019, p. 1). El proyecto de grado tiene relación ya que se busca

que se implementen nuevas leyes, para contrarrestar los delitos informáticos y lograr establecer un límite con los cibernautas a nivel mundial.

Los autores concluyeron que la reforma al Código Penal Federal de 1999 para implementar los delitos informáticos en México, se encuentra rebasada por los avances tecnológicos y por la sofisticación de las conductas delictivas que existen en esta materia. En el que los intentos legislativos para implementar reformar a la Ley Penal Federal y al Código Nacional de Procedimiento Penales, han sido insuficiente y socialmente han sido ignorados o desconocidos (Levet, Espinoza, Macgluf y Fragozo, 2019, p. 11).

De acuerdo con López, el cual realizo un proyecto titulado "Gobierno de TI basado en el Esquema Gubernamental de seguridad de la Información (EGSI) en el Hospital San Luis de OTAVALAO", en Ibarra, Ecuador, que tiene como enfoque primordial para el desarrollo del proyecto, elaborar una estructura de protección de datos para la entidad de salud de Otavalao:

Con el alcance de comprender acerca de la legislación del Estado enmarcado en el cuadro de la seguridad de la información en instituciones Públicas, se realizará un estudio de referencias afines a los principios del EGSI y políticas propias del ministerio de Salud Pública para obtener una perspectiva del punto de partida para el diseño del Gobierno de TI. Esto permite identificar los procesos que la institución necesita mejorar con relación al uso de las TI y apoyar al cumplimiento de sus objetivos estratégicos; para ello se realizó el análisis de Gestión de Riesgos según el estándar NTE INEN-ISO/IEC 27005:2012 donde se determinan los activos de información críticos, se identifican sus principales amenazas y vulnerabilidades, y a partir de los riesgos encontrados se formula una Política de Seguridad de la Información para reducir, controla o mitigar cada riesgo encontrado (López, 2019, p. 2-7).

El autor concluye que con el marco de trabajo de COBIT 5 se logró diseñar el Gobierno de TI en Otavalao, donde se trabajó con la guía de buenas prácticas aplicadas a la dirección estratégica de la empresa con el fin de mejorar la protección y la interacción de los procesos y los servicios que se prestan mediante el cumplimiento de las actividades planteadas dentro del marco de gestión, logrando reducir las amenazas y riesgos que se puedan presentar dentro de ella. (López, 2019, p. 179).

Por otro lado, Gómez, en su proyecto titulado "Gobernanza Corporativa de la Tecnología de la Información (T.I) (Auditoría y Control según la Norma UNE-ISO/IEC 38500:2013)"; desarrollado en la ciudad de Leganés, España; en el que perfilan el contexto de las organizaciones, como deben valorar, y establecer, sus transformaciones y los peligros coherentes en cuanto a la protección de la infraestructura tecnológica:

El cual tiene como objetivo profundizar en dos aspectos principales; el primero es comentar el papel estratégico de la tecnología de la información en la empresa y mencionar los riesgos asociados. El segundo es dar a conocer los requisitos de gobierno corporativo y gobierno de TI y orientar acerca de los marcos y estándares relacionados. Cada una de estas normas y marcos tiene un carácter decisivo y de generación de valor en las organizaciones; el desafío es integrarlos de manera que cada uno cumpla el fin para el que fueron diseñados y que permitan a la entidad diseñar su propio gobierno de TI, en base a sus requerimientos y necesidades. Teniendo en cuenta estos aspectos, y como se solución, se elabora una guía de implantación de gobierno de TI y un modelo de autoevaluación, diseñado para mejorar el gobierno de las operaciones TI y hacerlas más eficientes (Gómez, 2015, p. 6).

El presente proyecto tiene relación con la elaboración de la investigación ya que se busca controlar y mejorar el control interno de las empresas para disminuir los riesgos en los delitos

cibernéticos. El autor concluye que el panorama actual de la mayoría de las empresas no contempla la T.I como un activo más e incluso acaban delegando sus servicios y procesos a terceros (outsourcing). Esto trae desventajas ya que la empresa externa adquiere el conocimiento de los sistemas de información de la organización en la que están trabajando. Generando adicionalmente otro riesgo asociado en que la organización seguirá el ritmo que marque la empresa externa, logrando vulnerar la seguridad de la información o exponerla a delitos informáticos (Gómez, 2015, p. 108).

2.1.2 En el ámbito nacional. Mediante el trabajo de grado realizado por, Montañez, titulado "Análisis de los delitos informáticos en el actual Sistema Penal Colombiano", desarrollado en la ciudad de Bogotá, Colombia, en el que proponen un concepto sobre la protección de datos, el cual tiene una conexión con lo que se vive actualmente dentro de las empresas colombianas:

Su objetivo general del proyecto es verificar cuanto apoyo brinda los estatutos planteados por Min Tic, para que las empresas logren tener una excelente calidad en los servicios de protección prestados, para lograr disminuir la substracción de información de manera arbitraria, el proyecto tiene relación con la presente investigación, ya que se necesita verificar si las leyes vigentes ayudan a promover la seguridad de la información.

En la cual el autor concluye que a lo largo del trabajo investigativo, se generan distintas conclusiones, de las cuales se puede empezar indicando que se debe resaltar el esfuerzo generado por Colombia, con la creación de la Ley 1273 de 2009, la cual fortalece el sistema jurídico frente a la nueva tendencia global, que se basa en el tratamiento digital de la información; sin embargo, al generar un análisis detallado del articulado, se puede constatar vacíos, que pueden generar contradicciones, ya que si bien la ley pretende proteger la integridad, disponibilidad y

confidencialidad de la información, se pueden generar errores en la interpretación (Montañez, 2017, p. 81).

Mediante el trabajo de grado realizado por Parra, titulado “Delitos informáticos y Marco normativo en Colombia”, desarrollado en la ciudad de Bogotá, Colombia; el cual, para entender de manera más profunda y sencilla, el uso de las TIC, y si son accesibles, el cual permite el canje de información, pero en general y de manera detalla mirar el procedimiento criminal de los ciberdelincuentes, el cual el proyecto:

Tiene como objetivo principal analizar el estado actual de la seguridad informática a través del marco normativo colombiano para combatir los delitos informáticos que se presentan con más regularidad en el país, así como determinar el marco normativo colombiano y reconocer la relación con otros países en cuanto a la normatividad sobre el cibercriminal, motivo por el cual se presenta el análisis de la norma, su aporte y alcance en las organizaciones y de esta manera poder visualizar la implementación de políticas y estrategias sobre seguridad informática. Tiene como alcance presentar un análisis de la normatividad colombiana en lo que refiere a delitos informáticos, la adaptación, aplicación y las diferentes modificaciones que se han presentado desde el año 1980; en el que se pueda regular el uso de nuevas tecnologías en el territorio nacional (Parra, 2017, p. 16).

El autor logro proponer un modelo de análisis denominado normo grama, el cual contiene la una guía de buenas practicas el cual se basa en las leyes actuales de Colombia, para el apoyo en la protección de datos y de infraestructura tecnológica, que sirve para el apoyo en caso tal de que ocurra un delito cibernético y que la gerencia no sepa que hacer en este caso. Esto ayuda mucho a las empresas a saber qué hacer y por donde comenzar al momento de que un posible riesgo exista y se deba solucionar de manera inmediata. (Parra, 2017, p. 119).

En la ciudad de Bogotá, Colombia, Vásquez y Rodríguez, realizaron un proyecto titulado "Propuesta de Buenas Prácticas para fortalecer los controles de prevención y Detección Temprana del Cibercriminal en las Empresas Colombianas"; el cual a través de los años han resultado potencias negativamente perturbando así la protección tecnológica, logrando proponer:

Como objetivo principal la investigación proponía: Fortificar cada habilidad que tienen los profesionales encargados de la seguridad de la información, para así lograr prever las posibles amenazas y riesgos presentes en el ambiente laboral brindando así protección en la web y credenciales para poder cumplir con la confidencialidad de los documentos. (Vásquez y Rodríguez, 2016, p. 30). El proyecto de investigación tiene relación ya que se buscar fortalecer los controles y prevención para lograr prevenir ataques cibernéticos, proteger el activo de la información y lograr mejorar los tiempos de respuestas para los riesgos que se presenten.

Las autores del proyecto lograron concluir que las buenas prácticas fortalecen los controles de prevención y detección temprana de la cibercriminal en las empresas colombianas, aporta conceptualmente un beneficio que integra al sector público, privado y a la academia, en cuando su intención es la de establecer un punto en el estado del arte nacional e internacional, sobre los lineamientos de ciberseguridad y ciberdefensa, buscando en un plano comparativo resaltar los avances nacionales, y los puntos de mejora teniendo en cuenta las mejores prácticas de países que han logrado disminuir las pérdidas económicas a causa del cibercrimen y los adelantos en la infraestructura cibercriminal (Vásquez y Rodríguez, 2016, p. 144). A nivel de gobierno corporativo de TI En el trabajo de Velásquez se establecieron los lineamentos para adoptar criterios de gobierno de TI en empresas Colombianas, tomando la empresa en cuatro niveles, aplicando los dominios de COBIT y los niveles de madurez CMMI (Velásquez, T, 2010).

2.1.3 En el ámbito local. En la ciudad de Ocaña, Norte de Santander, se realizó un proyecto de grado titulado, "Modelo de Gobierno de Tratamiento de la información para la empresa Colombiana en la Globalización en la prospectiva del desarrollo Organizacional", que tiene como objetivo principal "Diseñar un modelo de Gobierno de Tratamiento de la Información de la Información para la Empresa Colombia, como un elemento fundamental en la organización permitiendo la protección de datos personales, en cumplimiento de los derechos fundamentales de sus titulares". (Camargo Barbosa, et, al, 2020, p. 4).

El autor concluyo que el inadecuado tratamiento de la información en la empresa a nivel interno y externo puede con llevar a la pérdida de la imagen frente a sus clientes, ser menos adaptables, competitivas y sostenibles en el mercado, afectando la productividad y utilidades, y en efecto, el cumplimiento de sus objetivos y metas estratégicas. Por tal motivo, es indispensable establecer estrategias adecuados de tratamiento de la información en la organización como base fundamental en cumplimiento de su misión y visión empresarial en términos empresariales y legales actuales. Es necesario que la empresa de hoy tome conciencia de la importancia que tiene el adecuado tratamiento de la información personal en cumplimiento de su misión, visión y todo el marco estratégico corporativo, de tal manera que se estructure a nivel organizacional un gobierno sobre la misma, con el fin de cumplir los requisitos legales y generar un valor agregado a un negocio, haciéndola más sólida, sostenible y competitiva en las nuevas tendencias empresariales". (Camargo Barbosa, et, al, 2020, p. 184).

2.2 Marco conceptual

2.2.1 Gobierno Corporativo. El gobierno corporativo se basa en determinar el incremento en las empresas el cual sirve de apoyo para dar respaldo a los posibles inversionistas y seguridad

en sus ganancias. Son los encargados de todo el funcionamiento empresarial, desde la dirección estratégica hasta el más mínimo detalle de los procesos que se realizan dentro de ella, para lograr la eficiencia dentro de ella. (Gómez, 2015, p. 24).

2.2.2 Gobierno de TI. Se encarga de dirigir todas las estrategias planteadas dentro de las empresas para así lograr garantizar el cumplimiento de todas las metas y los objetivos que se establezcan, el cual sirve para realizar una gestión adecuada de las amenazas y riesgos latentes dentro de la organización. El gobierno de TI, se enfoca en verificar que todos los procesos dentro de la empresa se cumplan y se completen a cabalidad todas las actividades planteadas por la gerencia. (Gómez, 2015, p. 25)

2.2.3 Delito Informáticos. Fuentes, explica que para prevenir los delitos informáticos se debe realizar: “La auditoría informática es un proceso en evolución, ya que cada vez hay nuevos riesgos asociados a la materialización sobre la tecnología que está en constante movimiento; que también es cambiante e innovadora” (2019, p. 9).

2.2.4 Ingeniería Social. No se pude hablar de seguridad e información de una forma aislada de la vida del ser humano, él es quien, maneja y direcciona la misma. Igualmente, no podemos desligar estos conceptos de la formación o educación, puesto que se da en los diversos escenarios en los que el sujeto interacciona y se forma. (Novoa, 2018, p. 19).

2.2.5 Seguridad de la información. Se encarga de la protección de la infraestructura tecnológica dentro y fuera de la empresa así como la de los activos de la información, plantea trabajos el cual apoyen la logística para determinar posibles amenazas dentro de la empresa y lograr minimizar los riesgos existentes (López, 2019, p. 6)

2.3 Marco contextual.

El trabajo se desarrollará para la Jurisdicción especial para la Paz (JEP) como apoyo para mejorar los controles de prevención y detección temprana ante la ocurrencia de un delito informático para la jurisdicción especial para la paz y acciones que se deban tomar para manejar la información de los usuarios de la mejor manera posible y evitar posibles altercados con ellos.

Misión

Nuestra misión es administrar justicia para consolar la transición hacia la paz y restaurar el tejido social, garantizado los derechos de las víctimas y la seguridad jurídica de los comparecientes, con enfoque territorial, diferencial y de género. (JEP, 2018)

Visión

Nuestra visión a 2023 es haber hecho justicia, esclareciendo y estableciendo las responsabilidades penales individuales sobre los crímenes más graves y representativos cometidos durante el conflicto armado colombiano y resolviendo la situación jurídica de todos los comparecientes a la JEP, contribuyendo así a la construcción de la paz y la reconciliación nacional. (JEP, 2018)

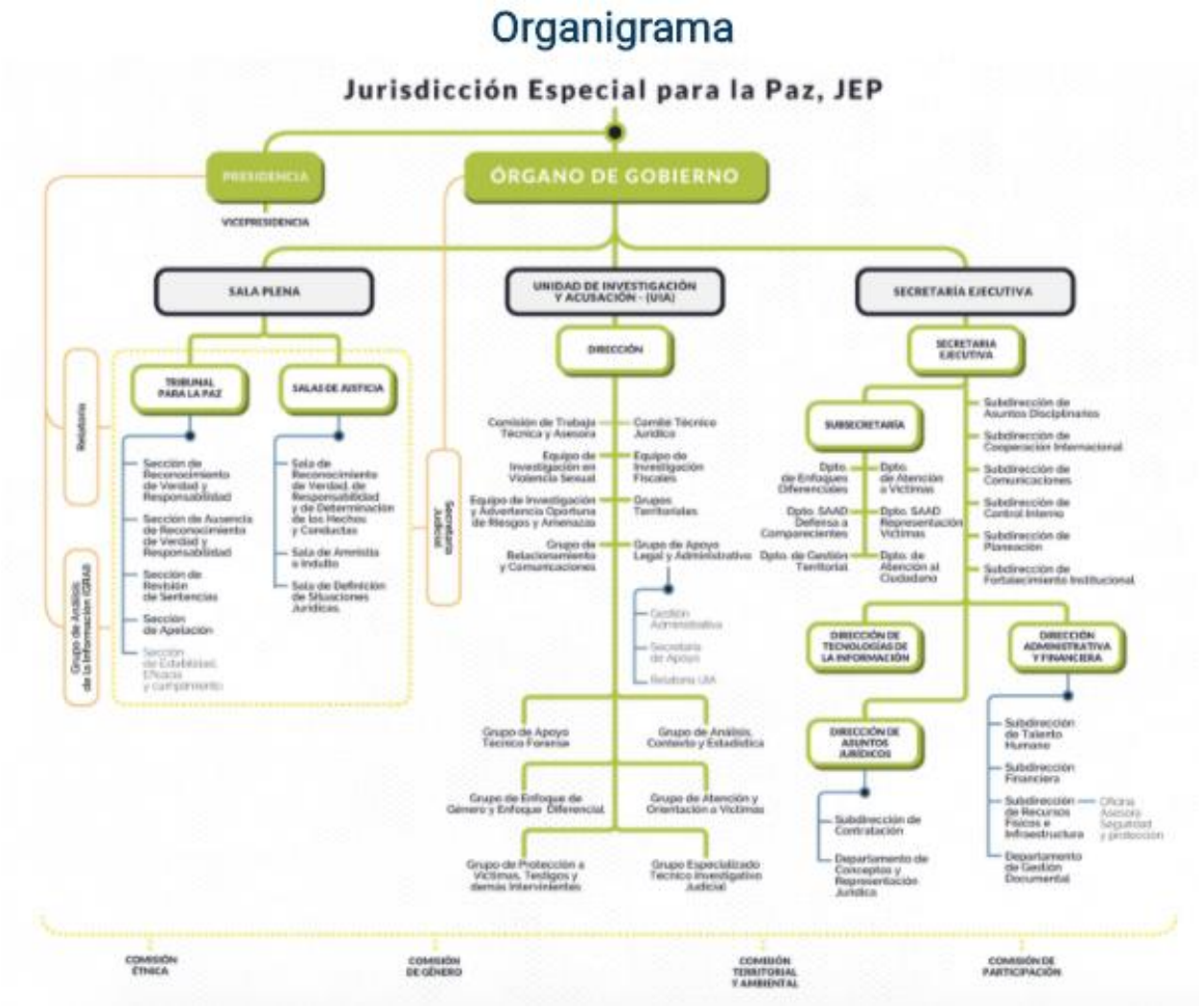


Figura 1. Organigrama JEP Obtenido de:

https://www.jep.gov.co/Paginas/Transparencia/Talento/Organigrama.aspx

2.4 Marco teórico

Los actos de substracción de información dentro de las empresas a nivel nacional, para Parra, fueron encaminados a la observación de los datos que sirven para "proteger la información digitalizada y la manera legal de castigar a quien de una forma u otra acceda a los servicios de almacenamiento de documentos, en su mayoría confiables y de gran valor para las personas, empresas, entidades u organizaciones" (Parra, 2019, p. 28). Por otro lado, según Novoa:

Cabe resaltar que el impacto del Cibercrimen es global, afecta a to mundo, no únicamente a las organizaciones legalmente constituidas. Una organización con un buen SGSI (Sistema de Gestión de Seguridad en la Información) puede prevenir los ataques informáticos, más no se puede decir que nunca vaya a sufrir uno, pero si se hará menos vulnerable a una amenaza. Así mismo, es importante recordar que el proceso de transformación frente a seguridad informática debe ser constante, puesto que los pilares de la seguridad en la información son la confidencialidad, integridad y disponibilidad (Novoa, 2018, p. 19).

Según Quintero, un plan de Seguridad Informática reúne todos los procesos y servicios que se implican dentro de la protección de los datos. Este cumple con todos los requerimientos que se instauran dentro del plan de seguridad de la empresa, para lograr cumplir con la mayor efectividad y eficiencia de los servicios prestados de TI. Apoya el cumplimiento de las directrices planteadas para lograr tener confidencialidad en la información recolectada cumpliendo con la Misión y Visión de la organización. (Quintero, 2018, p. 17-18).

2.4.1 ISO 27002. La norma ISO 27002 es una recopilación de buenas prácticas para implementar en una empresa, Quintero, explica que son: "Una herramienta que permite establecer políticas con el objetivo de reducir los riesgos que presentan los activos de la empresa, de tal forma que al momento de generarse una incidencia se minimizan y se asegura la

continuidad del negocio" (Quintero, 2018, p.18) con esto se lograr tomar medidas para afianzar la seguridad de la empresa y reducir los detonantes para que existan amenazas y riesgos dentro de ella.

2.4.2 Sistema de Información. En la actualidad los Sistemas de Información son utilizados en todas las empresas, Pulido y Mantilla, explican que: "Pueden ser cualquier combinación organizada de personas, hardware, software, redes de comunicaciones y recursos de información que almacene, recupere y transforme y disemine información en la organización" (Pulido y Mantilla, 2016, p. 28).

2.4.3 Seguridad Informática. El mundo hoy en día está expuesto a eventos en las que sus derechos e incluso su propia seguridad se ven expuestas a riesgos y amenazas debido a la gran cantidad de información que se genera día a día, en los sistemas informáticos y estos son el blanco de los ciber delincuentes, hackers, el cual son riesgos que se corren por el uso de las tecnologías y su constante evolución e innovación, para, Peñaranda:

La Seguridad Informática, es también conocida como ciberseguridad o seguridad de tecnologías de la información, es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información (Peñaranda, 2019, p. 26).

2.4.4 Objetivo de la Seguridad Informática. La Seguridad Informática debe establecer normas que minimicen los riesgos a la información o en las instalaciones de cómputo. El cual tienen reglas que contienen agendas de trabajo, prohibiciones de entrada, credenciales, negaciones, procedimientos para amenazas, pautas en cuanto a que se debe hacer dentro de la

empresa para así lograr un excelente manejo de todos los activos de la información. (Peñaranda, 2019, P. 26).

2.5 Marco legal

La investigación se basa en razón de la elaboración de un modelo de gestión el cual sirva para robustecer cada área dentro de la empresa y ayude a localización anticipada de una amenaza ante la ocurrencia de un delito informático dentro de la JEP se fundamenta en las siguientes leyes:

- LEY 1581 DE 2012: se expidió el régimen General de Protección de Datos Personales, el cual, de conformidad con su artículo 1, tiene por objeto, Desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la constitución Política; así como el derecho a la información en el artículo 20 de la misma. (Congreso de la República, 2012)
- LEY 1273 DE 2009: por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado, denominado, De la protección de la información y de los datos. Y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. (Congreso de la República, 2009)
- LEY 594 DE 2000: por medio de la cual se dicta la Ley general de Archivos y se dictan otras disposiciones. (Congreso de la República, 2000)
- LEY 1266 de 2008: “por el cual se dictan las disposiciones generales del Habeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones” (Congreso de la República, 2008).

- LEY 527 de 1999: “Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones” (Congreso de la República, 1999).
- LEY 1341 de 2009: “por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la información y las Comunicaciones, TIC, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones” (Congreso de la República, 2009).

Capítulo 3. Diseño Metodológico

3.1 Tipo de investigación

El proyecto se enfoca en una forma Cuantitativa, de acuerdo a lo explicado por, Rodríguez, Erazo y Narváez, tienen como objetivo "Cuantificar los resultados, deben ser estadísticamente representativas mediante la aplicación de un muestro representativo, de tal forma que, la información obtenida pueda sacar conclusiones estadísticas de la población en estudio" (2019, p. 4) Por otro lado, Valdiviezo, la investigación cuantitativa es aquella que: "Se encarga de la recopilación y análisis de información, se pone a prueba o comprueba mediante hipótesis, para lo cual utiliza un análisis estadísticos basadas en valores numéricos, lo cual tiene como propósito explicar el fenómeno estudiado" (2019, p. 8).

El enfoque que toma es de forma Descriptivo, en el que se toma el planteamiento hecho por, Valdiviezo, el cual explica como su nombre lo indica: "describe las características o funciones de personas o cosas en un determinado espacio y en tiempo real, es requerido para obtener datos relevantes y precisos que han sido descubiertos por las investigaciones exploratorias" (2019, p. 9).

3.2 Seguimiento metodológico del proyecto

Tabla 1. Seguimiento Metodológico

OBJETIVOS DE LA INVESTIGACIÓN	ACTIVIDADES POR OBJETIVO	INDICADOR POR ACTIVIDAD
Diagnosticar los riesgos inherentes a la seguridad	Act 1. Identificar los estándares y normativa	Ind 1. Normatividad, Estándares, dominios,

de la información dentro de la unidad de investigación y acusación de la jurisdicción especial para la paz.	requeridos de la protección de datos aplicados en la JEP	controles y objetivos de control identificados
	Act 2. Análisis estadístico	Datos analizados
	Act3. Diseño de instrumento	Instrumento diseñado
	Act4. Aplicación del instrumento	Sistematización de la información
	Act 5. Análisis de información	Diagnostico
• **Integrar los componentes identificados en un modelo de gobierno de ti para la jurisdicción especial para la paz**	Act 6. Seleccionar los componentes que integrarían el modelo	Componentes seleccionados
	Act 7. Elaborar un documento que integre los componentes seleccionados para el diseño del modelo	Diseño del modelo
	Act 8. Selección del tipo de validación	Validación seleccionada

• **Validar el modelo propuesto**	Act 9. Aplicación de la validación	Validación aplicada
	Act 10. Documentación de la validación	Documento de la validación

Fuente: Autor, 2020

3.3 Población y muestra

La población que se tomó como objeto de estudio para la realización del proyecto fueron todos los funcionarios que se conforman dentro de la JEP; debido a la Población con la que se cuenta es limitada, se tomó como muestra toda la población que conforma la unidad dentro de la JEP.

3.4 Técnicas de recolección de la información

Las fuentes primarias se obtendrá a través de encuestas y entrevistas, validación por expertos, pruebas estadísticas, al encargado de la JEP y empleados que laboren dentro de la institución, lo que servirá para establecer causas y posibles vulnerabilidades que se presentan, las fuentes secundarias serán obtenidas a través de las bases de datos de la Universidad Francisco de Paula Santander Ocaña, Google Académico, Science Direct y textos adicionales con información a fin del proyecto de investigación. Sistema de información

3.5 Análisis de la información

Este análisis se ejecutó mediante el análisis cuantitativo de información el cual se lleva a cabo mediante técnicas de análisis estadístico: “Estos datos estadísticos no se utilizan únicamente para producir unos resultados finales y dar respuesta a los objetivos e hipótesis, también se utilizan en el procedimiento de muestreo o para probar la fiabilidad y validez de los instrumentos de recogida de información” (Navarro, Jiménez, Rappoport y Thoilliez, 2017, p. 40)

Capítulo 4. Resultado

Como resultado del proyecto de TI de los componentes que integran un modelo gestión hacia el apoyo a la seguridad en los activos de información dentro de la JEP, se inicia con un diagnostico que se realiza para conocer los riesgos inherentes, luego se identifica los estándares y buenas practicas que pueden establecer en un modelo de gestión de ti y finalizamos con la integración de los componentes identificados.

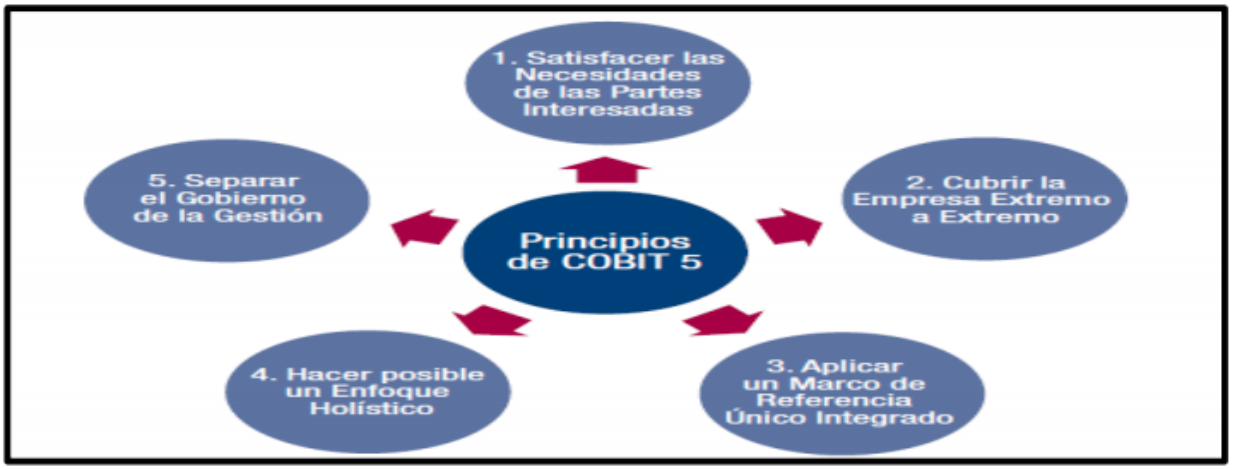
4.1. Diagnosticar los riesgos inherentes para la JEP.

Para lograr realizar la aplicación del diagnóstico en cuanto a los riesgos inherentes dentro de la JEP, se crea una matriz de operacionalización de variables (Ver Anexo A) el cual sirve de base para diseñar el guion de preguntas que se realizó a la parte administrativa y oficina de gestión de TI, aplicados a la JEP. Se toma de referencia el marco de COBIT 5, partiendo de DSS05 y APO13 el cual tienen como objetivo gestionar servicios de seguridad.

El modelo COBIT 5 tiene un acople dentro de la organización el cual sirve de apoyo como un modelo de buenas prácticas, el cual sirve de apoyo para, la protección y eficiencia, en el cual se comprueban cada uno de los activos que se distinguen dentro de las TI, por medio del talento profesional, infraestructura tecnológica, por el cual, se evalúa en la última etapa, la metodología implementada para la elaboración de este modelo. (Figueroa, Paladines, Paladines, Caicedo y Romero, 2017, p. 37).

Por otra parte, la estructura del modelo COBIT 5, propone un marco de acción, donde se evalúan los criterios de información, como por ejemplo la seguridad y calidad, se auditan los recursos humanos, instalaciones, sistemas, entre otros; y, finalmente, se realiza una evaluación sobre los procesos involucrados en la empresa.

Figura 2. Principios del COBIT 5.



Fuente: tomado de COBIT 5

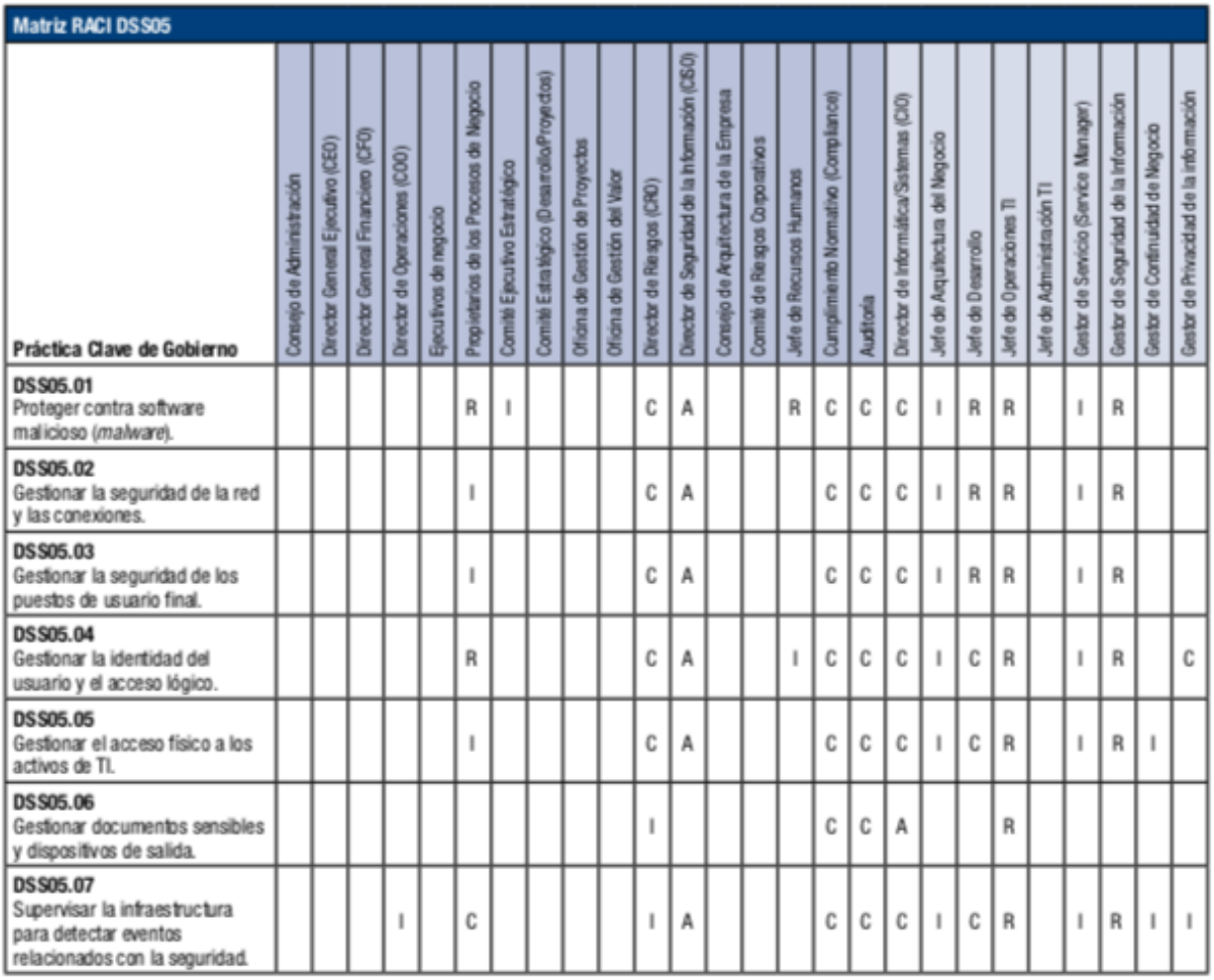
En base a lo anterior, se entiende que es un modelo que integra una serie de procesos y subprocesos el cual apoyan dentro de las organizaciones a conseguir las metas enfocadas a la tecnología de información empresarial, esto les permite a las organizaciones obtener una importancia por estas actividades que se realizan para buscar mejores resultados y optimizar cada uno de los riesgos que se presenten. Todo esto encaminado al control y supervisión de los servicios que se ofrecen y van orientados al estándar, ya sean, Procesos Catalizadores que contienen un plan para apoyar los subprocesos que se brindan dentro de la organización, mientras que, Información Catalizadora es una guía de referencia para pensar en forma estructurada sobre la información y los aspectos típicos de gobierno y gestión de la información (Monfort, 2016, p. 10)

Figura 3. Matriz RACI APO13

Matriz RACI APO13																									
Práctica Clave de Gobierno	Consejo de Administración	Director General Ejecutivo (CEO)	Director General Financiero (CFO)	Director de Operaciones (COO)	Ejecutivos de negocio	Propietarios de los Procesos de Negocio	Comité Ejecutivo Estratégico	Comité Estratégico (Desarrollo/Proyectos)	Oficina de Gestión de Proyectos	Oficina de Gestión del Valor	Director de Riesgos (CRO)	Director de Seguridad de la Información (CISO)	Consejo de Arquitectura de la Empresa	Comité de Riesgos Corporativos	Jefe de Recursos Humanos	Cumplimiento Normativo (Compliance)	Auditoría	Director de Informática/Sistemas (CIO)	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	Gestor de Servicio (Service Manager)	Gestor de Seguridad de la Información	Gestor de Continuidad de Negocio	Gestor de Privacidad de la información
APO13.01 Establecer y mantener un SGSI.		C		C	C	I	C	I	I		C	A	C	C		C	C	R	I	I	I	R	I	R	C	C
APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.		C		C	C	C	C	I	I		C	A	C	C		C	C	R	C	C	C	R	C	R	C	C
APO13.03 Supervisar y revisar el SGSI.					C	R	C		R			A				C	C	R	R	R	R	R	R	R	R	R

Fuente: Tomada de "COBIT 5 Un marco de negocios para el gobierno y la gestión de las TI de la empresa" por ISACA (2016). p. 114.

Figura 4. Matriz RACI DSS05.



Matriz RACI DSS05

Práctica Clave de Gobierno	Consejo de Administración	Director General Ejecutivo (CEO)	Director General Financiero (CFO)	Director de Operaciones (COO)	Ejecutivos de negocio	Propietarios de los Procesos de Negocio	Comité Ejecutivo Estratégico	Comité Estratégico (Desarrollo/Proyectos)	Oficina de Gestión de Proyectos	Oficina de Gestión del Valor	Director de Riesgos (CRO)	Director de Seguridad de la Información (CISO)	Consejo de Arquitectura de la Empresa	Comité de Riesgos Corporativos	Jefe de Recursos Humanos	Cumplimiento Normativo (Compliance)	Auditoría	Director de Informática/Sistemas (CIO)	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	Gestor de Servicio (Service Manager)	Gestor de Seguridad de la Información	Gestor de Continuidad de Negocio	Gestor de Privacidad de la información
DSS05.01 Proteger contra software malicioso (*malware*).						R	I				C	A			R	C	C	C	I	R	R		I	R		
DSS05.02 Gestionar la seguridad de la red y las conexiones.						I					C	A				C	C	C	I	R	R		I	R		
DSS05.03 Gestionar la seguridad de los puestos de usuario final.						I					C	A				C	C	C	I	R	R		I	R		
DSS05.04 Gestionar la identidad del usuario y el acceso lógico.						R					C	A			I	C	C	C	I	C	R		I	R		C
DSS05.05 Gestionar el acceso físico a los activos de TI.						I					C	A				C	C	C	I	C	R		I	R	I	
DSS05.06 Gestionar documentos sensibles y dispositivos de salida.											I					C	C	A			R					
DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad.				I		C					I	A				C	C	C	I	C	R		I	R	I	I

Fuente: Tomada de "COBIT 5 Un marco de negocios para el gobierno y la gestión de las TI de la empresa" por ISACA (2016). p. 192

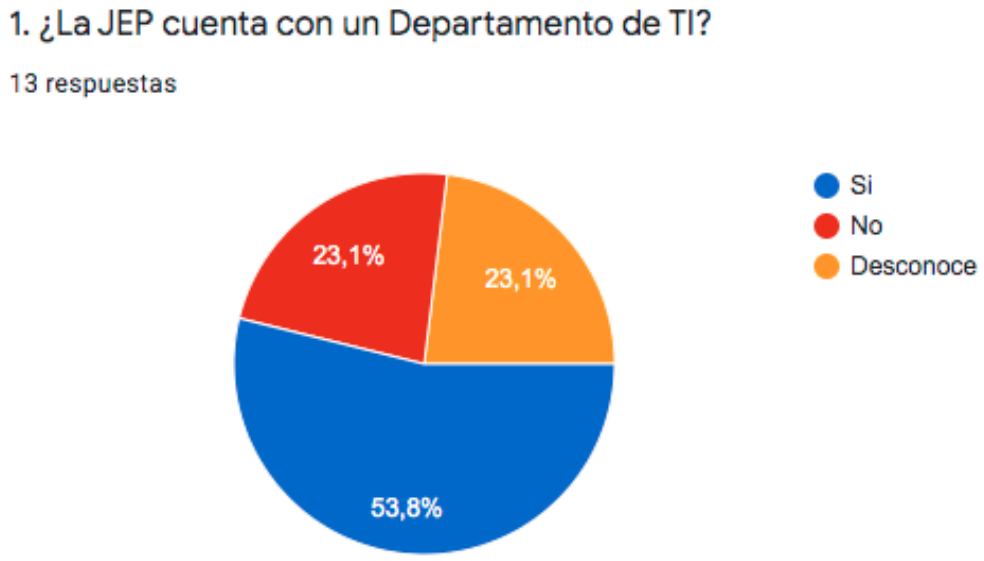
Tabla 2. Requisitos organizacionales y de seguridad de la información.

REQUISITOS ORGANIZACIONALES Y DE SEGURIDAD DE LA INFORMACIÓN	
Sociedad en conjunto o población en general	Mecanismos que faciliten la realización de trámites y la solicitud de servicios. Mecanismos para interponer PQRS. Mecanismos para ejercer derechos como titulares de información.
Servidores, servidoras y contratistas	Sensibilización y capacitación en seguridad de la información para el ejercicio de funciones.
Órgano de Gobierno, Presidencia de la JEP Salas de justicia y secciones Secretaría Ejecutiva	Acatamiento de estrategias y ordenamientos de protección de datos por parte de los funcionarios y contratistas. Revisión periódica del cumplimiento de estrategias por parte de los Jefes de Dependencia. Realizar auditorías internas con el fin de verificar el cumplimiento de políticas y procedimientos de seguridad de la información y, por ende, verificar el cumplimiento con la Estrategia de Gobierno Digital

Fuente: Oficina TI - JEP.

4.1.1 Análisis de instrumentos para validar la incorporación de los estándares de COBIT 5 dentro de los procesos de gestión de TI de la JEP. El instrumento diseñado está conformado por 15 preguntas en las cuales se buscó identificar el estado actual en el que se encuentra la parte administrativa dentro de la JEP, en la manera que gestiona la seguridad, como está actualmente la infraestructura y las prioridades de inversión, para lograr obtener un diagnóstico de acuerdo a los resultados que se muestran en la encuesta. La encuesta se aplicó a los encargados de las oficinas de la parte administrativa de la JEP el cual fue enviado a 15 profesionales, de los cuales respondieron 12 la encuesta enviada.

Figura 5. Pregunta 1.



Fuente: Autor del proyecto.

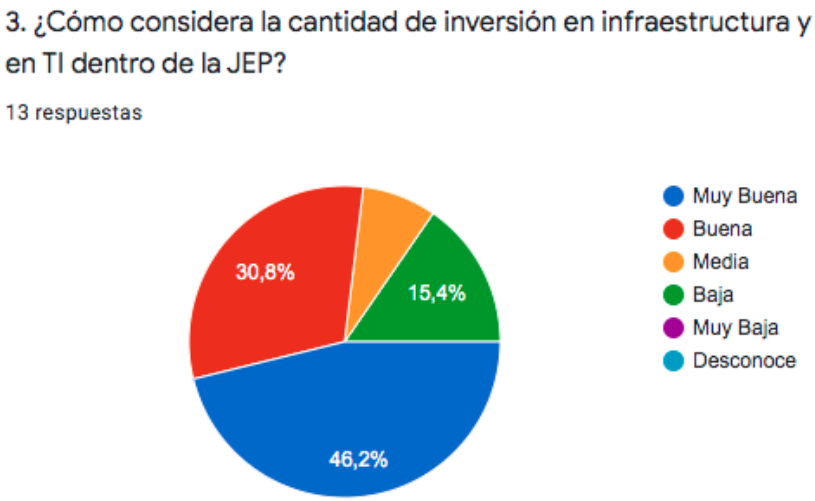
De acuerdo a lo evidenciado en la gráfica de la encuesta que el 23,1% de los encuestados afirma que no existe un departamento de TI y el otro 23,1% desconoce que exista esta dependencia, lo que resulta bastante alarmante, ya que los empleados al no conocer toda la información de la empresa pueden traer problemas a futuro.

Figura 6. Pregunta 2.

Fuente: Autor del proyecto.

De acuerdo a lo plasmado por los encuestados en esta grafica el 61,5% de los administrativos están informados de que existe una división de Seguridad de la información, frente a un 23,1% que no expresa que no existe y un 15,4% que desconoce de su existencia, es importante que toda la parte administrativa esté informada de la existencia de esta dependencia, si se trata de la seguridad de la información de la empresa.

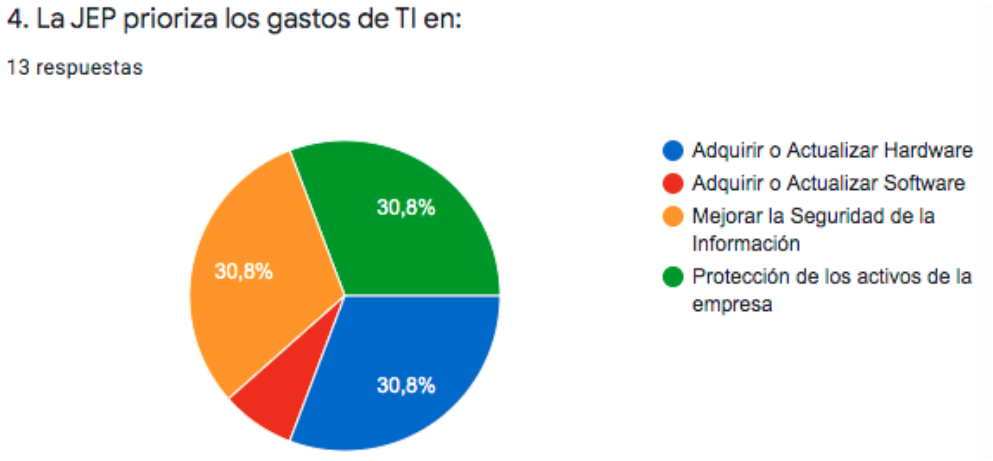
Figura 7. Pregunta 3.



Fuente: Autor del proyecto.

Se puede observar en la pregunta que a pesar de que el 46,2% de la inversión es Muy buena para TI, aún no se cubre en su totalidad con una inversión, el cual le sirva para evitar riesgos o amenazas.

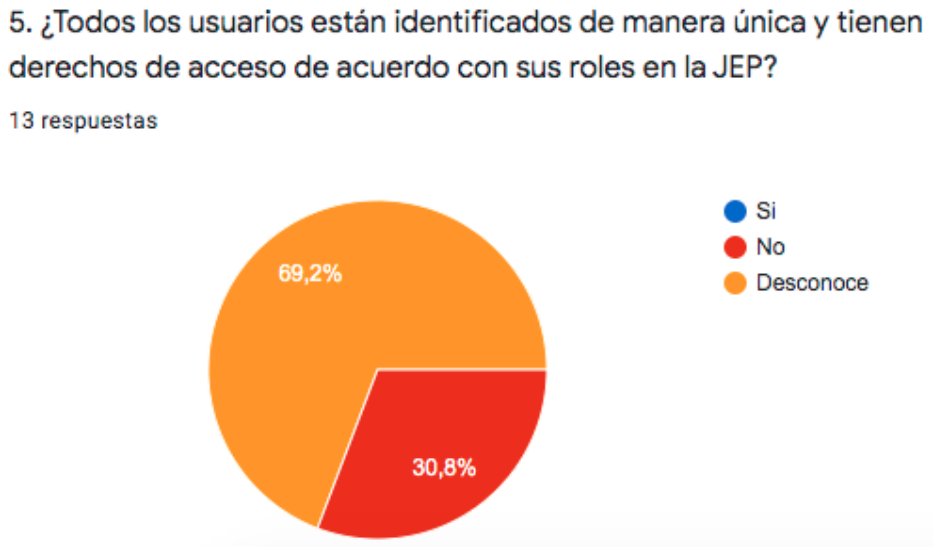
Figura 8. Pregunta 4.



Fuente: Autor del proyecto.

De acuerdo a lo expresado por los encuestados, se priorizan los gastos en varios recursos tecnológicos que aportan seguridad y ayudan a reducir riesgos dentro de la empresa, el cual pueden reducir las amenazas dentro de la empresa.

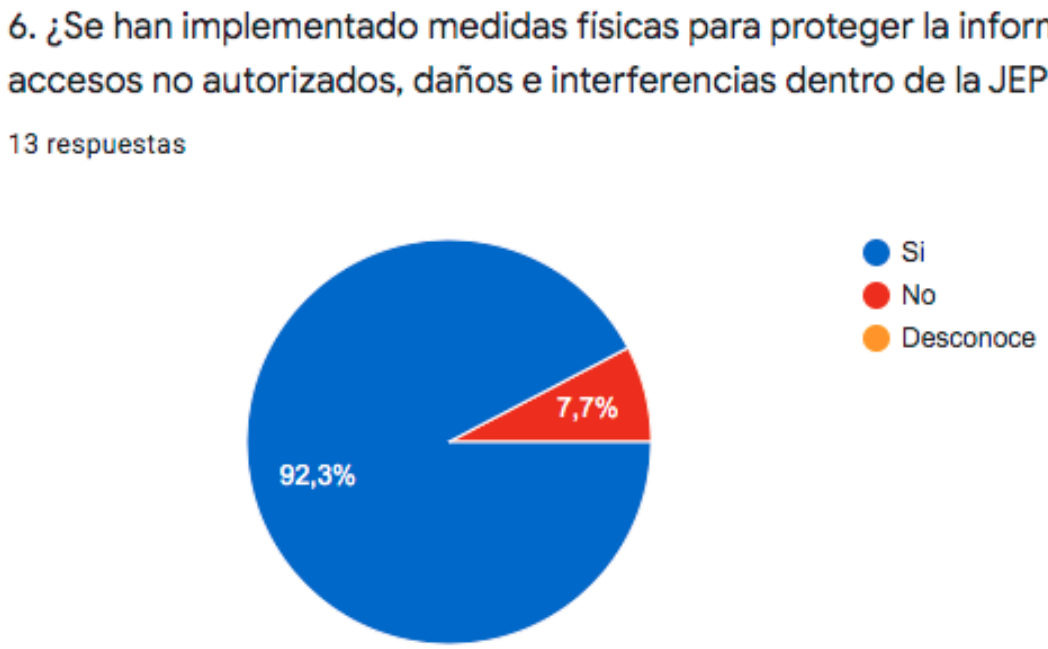
Figura 9. Pregunta 5.



Fuente: Autor del proyecto.

De acuerdo con lo expresado por los encuestados, aunque se realizan inversiones para TI, no se implementan los requisitos mínimos de seguridad para los puestos de trabajo, el cual puede causar una amenaza a futuro y un riesgo con los activos de información.

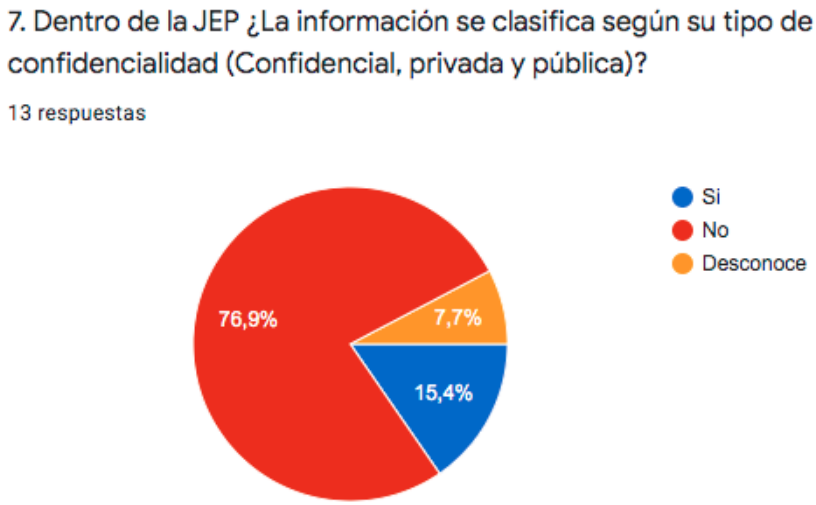
Figura 10. Pregunta 6.



Fuente: Autor del proyecto.

De acuerdo a la gráfica, el 92,3% contesto que se implementan medidas para proteger la información, pero al compararla con la pregunta 5 los resultados muestran que no se hace un seguimiento adecuado dentro de la JEP, para lograr tener la máxima seguridad en los activos de información.

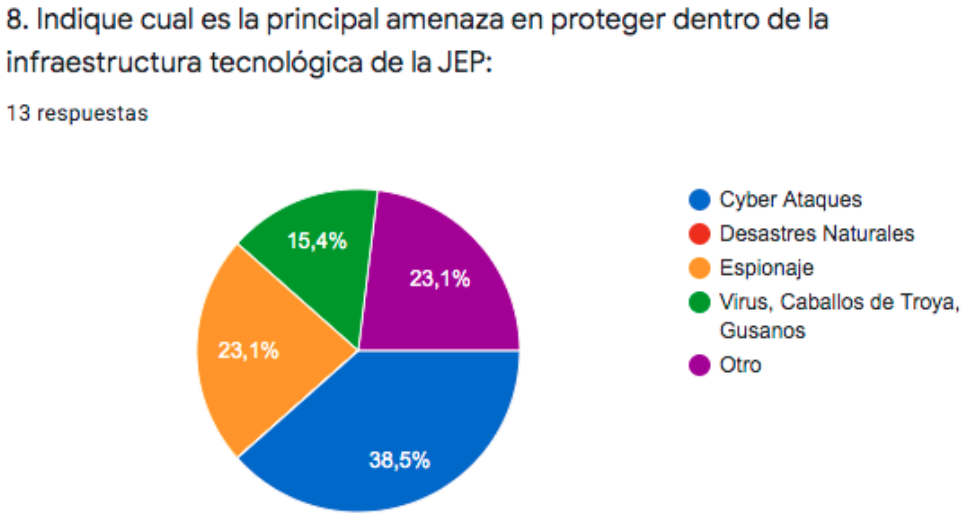
Figura 11. Pregunta 7.



Fuente: Autor del proyecto.

De acuerdo a la gráfica, el 75,9% no conoce cómo se clasifica la información dentro de la JEP y el 7,7% desconoce que se realice este proceso, lo que lleva a pensar que no se realiza seguimientos a los procesos de la seguridad de la información.

Figura 12. Pregunta 8.



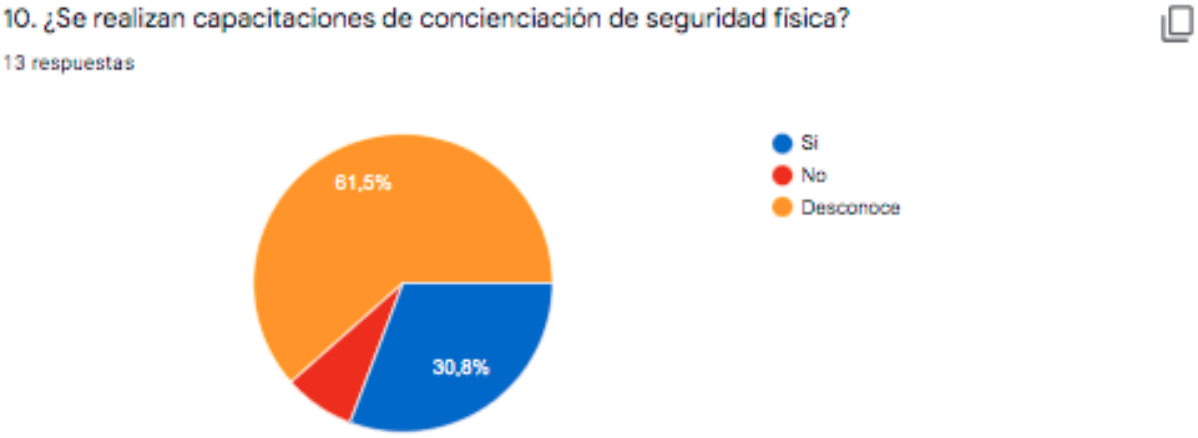
Fuente: autor del proyecto

Figura 13. Pregunta 9.

Fuente: autor del proyecto.

Según la gráfica, el 38,5% no tiene conocimiento de que se realicen revisiones para lograr detectar incidentes potenciales y el 38,5% desconoce que se realicen estos eventos dentro de la empresa, el cual resulta muy preocupante ya que no se conoce a ciencia cierta cuales son los riesgos o amenazas que se pueden presentar.

Figura 14. Pregunta 10.



Fuente: Autor del proyecto.

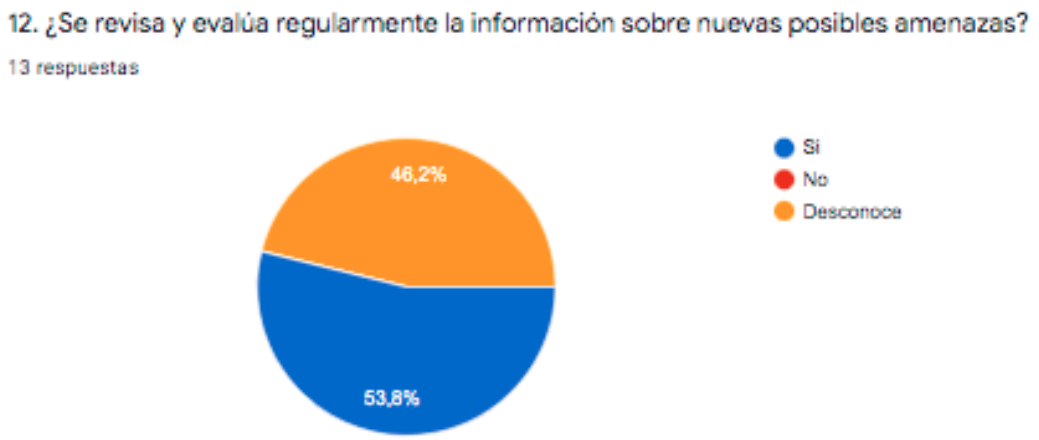
El 61,5% de los encuestados, afirmo desconoce que se realicen capacitaciones dentro de la empresa, el cual resulta muy preocupante no capacitar al personal, frente a un 30,8% que dice que, si se capacitan, impactando negativamente el uso de los activos de la información y el uso de los recursos tecnológicos.

Figura 15. Pregunta 11.

Fuente: autor del proyecto.

De acuerdo con la gráfica, el 61,5% de los encuestados desconoce que se aplique un Modelo dentro de la JEP, mejore los procesos y aumente la probabilidad de reducir los riesgos y amenazas que se puedan presentar con los activos de la información y los recursos tecnológicos que están presente dentro de la empresa.

Figura 16. Pregunta 12.



Fuente: autor del proyecto.

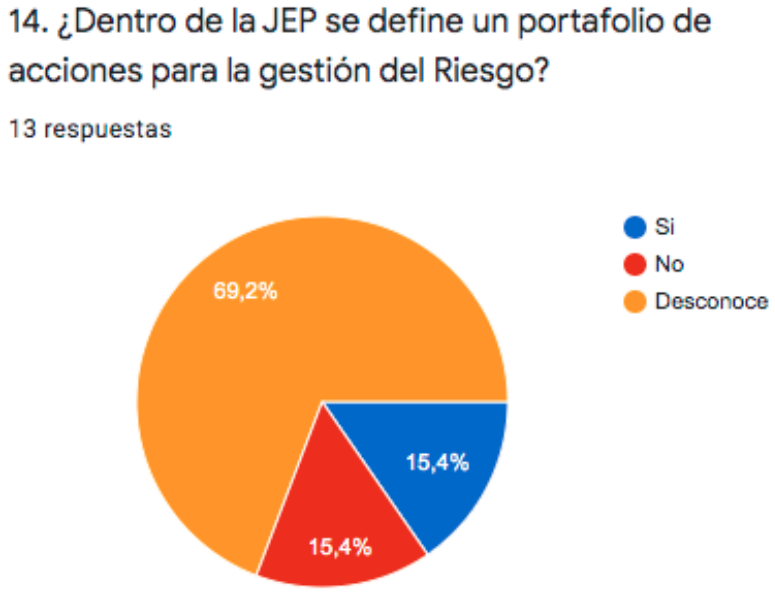
De acuerdo a la gráfica, el 46,2% de los encuestados desconoce que dentro de la empresa se revise y evalué la información sobre si existe nuevas amenazas en el cual se vean involucrados los activos en la infraestructura tecnológica en la organización.

Figura 17. Pregunta 13.

Fuente: autor del proyecto.

De acuerdo a la gráfica, el 61,5% desconoce que exista un plan de tratamiento del riesgo de la seguridad de la información, mientras que el 30,8% dice que no existe un plan, por lo que se pueden presentar problemas al momento de presentarse una amenaza dentro de la empresa.

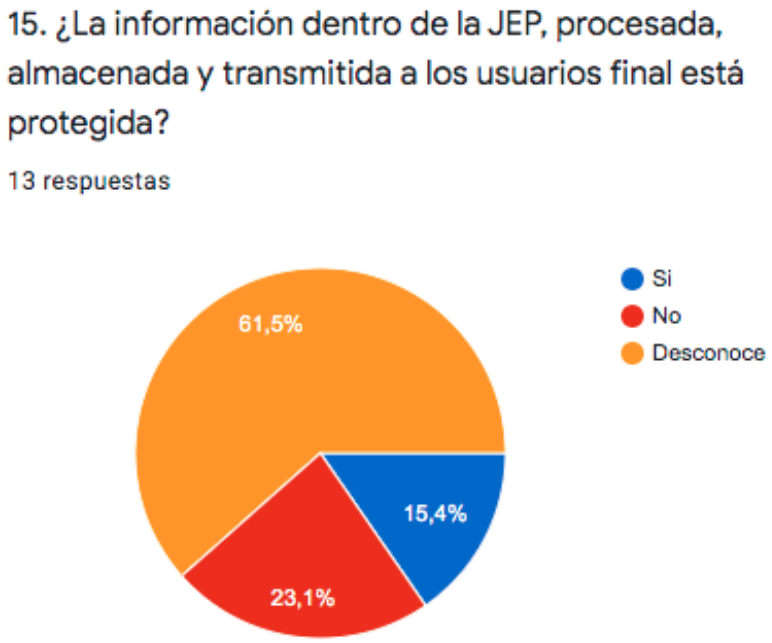
Figura 18. Pregunta 14.



Fuente: autor del proyecto.

De acuerdo a la gráfica, el 69,2% menciono desconocer que exista un portafolio de acciones para gestionar los riesgos que se presenten dentro de la JEP; por el contrario, el 15% contesto que si cuentan con este portafolio.

Figura 19. Pregunta 15.



Fuente: autor del proyecto.

De acuerdo a la gráfica, el 61,5% de los encuestados desconoce que exista una política de confidencialidad que brinde a las partes interesadas que los reportes estén encriptados o protegidos.

4.1.1 Análisis de resultados. De acuerdo a la encuesta realizada a la parte administrativa dentro de la JEP, se puede evidenciar que el personal no está capacitado para gestionar riesgos de TI, no se cumplen con los protocolos de seguridad física, donde el personal no cuenta con las competencias o habilidades necesarias para manejar la información y su respectiva clasificación, afectando al usuario final poniendo en riesgo la divulgación o perdida de esta información.

Se evidencia que, en el catalizador de persona, habilidades y competencias, existen grandes vacíos en cuanto a la gestión de TI, por no contar con un modelo o estándar de buenas prácticas el cual les sirva de apoyo para la ejecución de los mismos. Es por ello que se pueden

presentar inconvenientes o demoras al momento de solucionar un riesgo o una amenaza que se esté presentando dentro de la JEP. Por otro lado, en la encuesta realizada, no se cuenta con los principios de construcción de sistemas seguros, dejando vacíos a fin de garantizar que se tengan en cuentas aspectos de protección de datos dentro de los lineamientos de la 27001:2013.

Finalmente, de acuerdo a la encuesta realiza no se presencia conocimiento de la existencia de un modelo de gestión de TI, en el cual se contemplen los lineamientos para la gestión de la seguridad dentro de la JEP, como se estipula en DSS05, que tiene como objetivo principal Gestionar los servicios de seguridad. Por otro lado, tampoco se establecen lineamientos basados en APO13, que tiene como objetivo, gestionar la seguridad y dar cumplimiento y soporte de TI. De igual manera y de acuerdo a la revisión, no existen lineamientos para la gestión de servicios de seguridad que estén contemplados dentro de la JEP en su plan de desarrollo.

4.2 Estándares para establecer una guía de buenas prácticas

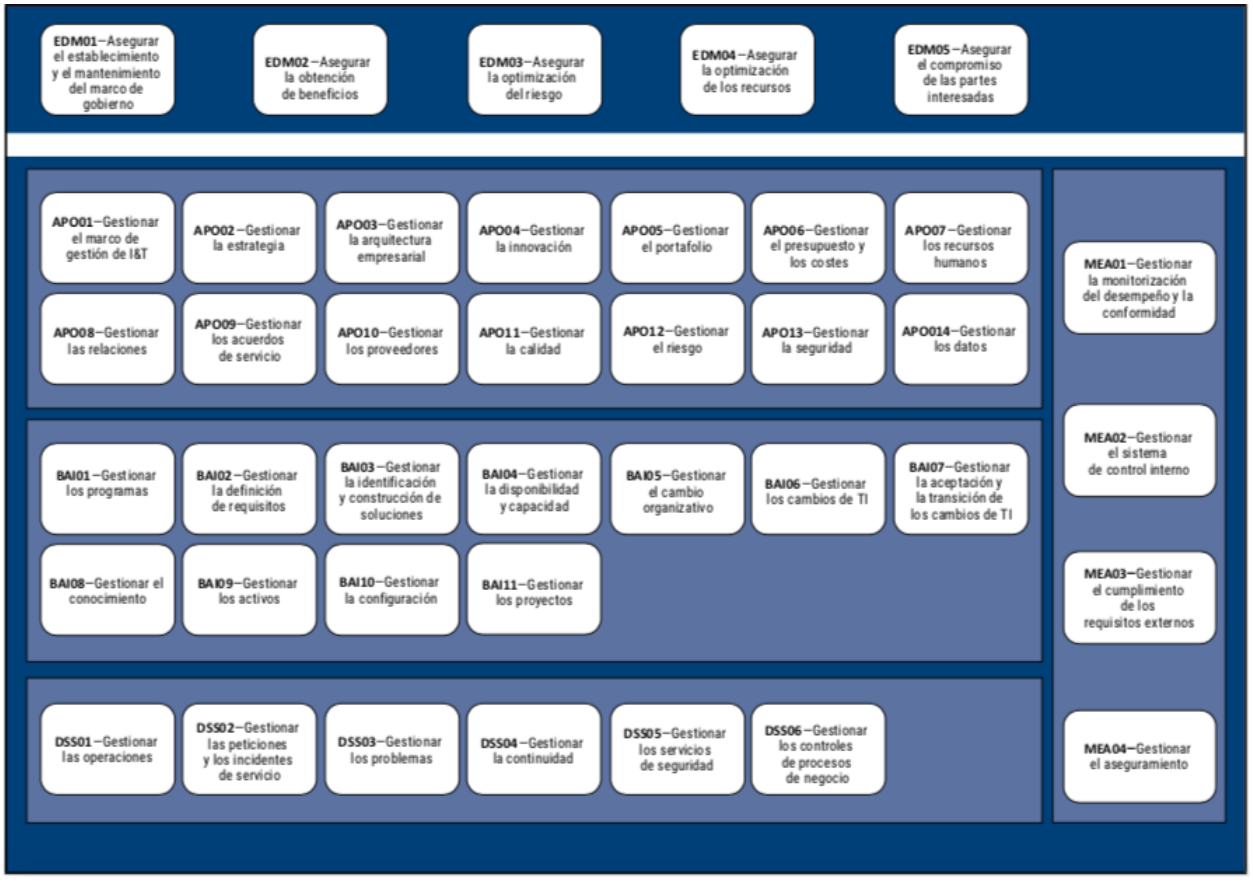
4.2.1 Estándares existentes. Existen recomendaciones o lineamientos a nivel de gobierno de tecnología de la información (Velásquez Pérez, 2010), donde se aplican marcos o referencias de gobierno y gestión de TI aplicable o todo tipo de organizaciones (Castro Márquez, et al., 2020), entre los más comunes están COBIT.

4.2.1.1 COBIT 5. Se enfoca en cumplir una serie de lineamientos, mediante una guía de buenas prácticas para optimizar los procesos y subprocesos dentro de la organización, para lograr disminuir los riesgos de amenazas y saber que debilidades están presente dentro de la empresa misma. Todo lo relacionado con la infraestructura tecnológica enfocada a la empresa, el estándar lo apoya para lograr cumplir con todas las actividades propuestas desde la dirección estratégica y así lograr cumplir con las metas propuestas en cada uno de los proyectos. Esto quiere decir, que

todos los activos de TI, no están limitados solo a la oficina de sistemas, al contrario, debe estar incluido todo lo que sea recurso tecnológico dentro del inventario. (ISACA, 2018).

Por otro parte, se enfoca en proyectar, determinar, elaborar y/o monitorear los procesos que se encuentran dentro de los lineamientos para su próxima ejecución dentro de la gestión de TI, logrando cumplir las metas propuestas por la organización. Este estándar se basa en cuatro objetivos de dominio. (ISACA, 2018)

Figura 20. Modelo Core de COBIT



Fuente: (ISACA, 2018)

- **APO - Alinear, planificar y Organizar:** se encarga de todos los procesos establecidos por la dirección estratégica, el cual es estructurada por la alta gerencia y los encargados de Ti de la organización. (ISACA, 2018, p. 12)
- **BAI - Construir, Adquirir e Implementar:** se enfoca en definir, adquirir e implementar posibles procedimientos de mejoras el cual se logren integrar a partir de los servicios prestados. (ISACA, 2018, p. 12)
- **DSS - Entregar, Dar Servicio y Soporte:** se enfoca en el cumplimiento de los procesos al momento de realizar actividades de mantenimiento o cumplimiento de servicios específicos de TI, basados en la protección de datos. (ISACA, 2018, p. 12)
- **MEA - Monitorizar, Evaluar y Valorar:** se enfoca en medir el rendimiento de los procesos y subprocesos que se realizan dentro de la empresa para su posterior mejora continua y posibles respuestas a amenazas, debilidades y/o riesgos que se presenten. (ISACA, 2018, p. 12)

4.2.2 Elemento a incorporar para el modelo. Descripción de los objetivos que se presentan en la matriz de operacionalización de variables conceptos de dominios y catalizadores, para el modelo.

4.2.2.1 Gestionar la Seguridad - APO13. Se encarga de especificar, aplicar y vigilar que se cumpla con los requisitos mínimo para la protección de todos los activos dentro de la infraestructura tecnológica de la organización. Lo anterior hace referencia, a que se prevé algún evento ya sea amenaza o riesgo de ataques cibernéticos dentro de la empresa, se establecen unos niveles de riesgos dentro de cada área. Dando acatamiento y viabilidad a los servicios prestado dentro del marco legal y los requisitos de las partes interesadas. (ISACA, 2018).

Metas

1. Requerimientos de protección de datos.
2. Establecer, aceptar y comunicar a toda la empresa un plan de protección para los datos.
3. Viabilidad en las soluciones de la protección de datos.

Métricas

- Roles y responsabilidades.
- Incidentes relacionados.
- Satisfacción por las partes interesadas.
- Soluciones de seguridad.
- Soluciones para la infraestructura organizacional.
- Alineamiento del modelo de protección.
- Incidentes causados por el no cumplimiento del modelo de protección.

4.2.2.1.1 APO13.01 Establecer y mantener un SGSI. Establece y mantiene un SGSI el cual logre proporcionar una serie de pasos a seguir, el cual apoya los procesos dentro de la infraestructura tecnológica, y ayuda a mejorar los servicios prestados dentro de la organización logrando disminuir debilidades que se presenten dentro de ella. Definiendo alcances e incluyendo límites para lograr determinar en términos generales las particularidades empresariales y sus instalaciones. Incluyendo complementos y reportes de cada uno de los riesgo y amenazas que se presenten. (ISACA, 2018)

4.2.2.1.2 Definir y gestionar un plan tratamiento del riesgo de la seguridad la información - APO13.02. Se encarga de conservar los lineamientos el cual se basa en las directrices planteadas por la gerencia en el que se prioriza la seguridad de todos los recursos tecnológicos dentro de la empresa. Asegurando, cada una de las reglas que se expresan sean implementadas para mejorar la seguridad basándose en los negocios que se muestren las partes interesadas como parte fundamental del proceso, el cual llegan a un acuerdo para el cumplimiento del proyecto. Formulando o manteniendo las estrategias para disminuir las amenazas que se presentan por ataques cibernéticos dentro de la organización. (ISACA, 2018)

4.2.2.1.3 Supervisar y revisar el SGSI - APO13.03. Se encarga de salvaguardar e informar normalmente la insuficiencia en la realización de las actividades establecidas dentro de la empresa. Se enfoca en recoger y examinar la información que se encuentra en los sistemas de información para mejorar la eficiencia en cada uno de los procesos. Mejorar cada una de las posibles amenazas encontradas dentro de la empresa para evitar posibles riesgos e incumplimiento dentro de los proyectos en curso. Realizando supervisiones que se establecen dentro del calendario, para que se logre cumplir con los reportes de las actividades realizadas. (ISACA, 2018)

4.2.2.2 Gestionar Servicios de Seguridad - DSS05. Se enfoca en resguardar los datos el cual se recolectan en la organización para poder medir el nivel de confidencialidad de cada uno de ellos y lograr establecer quien es apto para acceder a esta información cumpliendo con las normas establecidas. Establece las responsabilidades de cada uno de los encargados de las áreas de TI, si tienen credenciales o no para acceder a estos activos y realiza el control dentro de las instalaciones. (ISACA, 2018).

Metas

1. Seguridad de las redes y las comunicaciones.
2. Información procesada, almacenada y transmitida.
3. Usuarios identificados de manera única.
4. Medidas físicas para proteger la información.
5. Protección para los datos electrónicos.

4.2.2.2.1 Proteger contra software malicioso - DSS05.01. Se encarga de implementar y conservar efectivas las medidas preventivas y correctivas (fundamentalmente parches de protección actualizados e inspección de softwares maliciosos) a lo amplio de la organización para salvaguardar los sistemas (como lo pueden ser, gusanos, software espía – spyware – y correspondencia infectada). Divulgando concienciación en cuanto a los virus y exigir procedimientos y responsabilidades de precaución. (ISACA, 2018).

4.2.2.2.2 Gestionar la seguridad de la red y las conexiones - DSS05.02. Se enfoca en aplicar medidas de protección y procedimientos de servicios conectados para salvaguardar los datos en todos los modos de enlace. Basándose en el examen de riesgos y en los requerimientos de la empresa, logrando instaurar y conservar una dirección de protección para las conexiones. Permitiendo exclusivamente a los dispositivos autorizados gozar de credenciales para obtener datos y acceder al internet de la organización. Configurando estos dispositivos para obligar la demanda de contraseña. (ISACA, 2018)

4.2.2.2.3 Gestionar la seguridad de los puestos de usuario final - DSS05.03. Se encarga de proteger y verificar que cada uno de los empleados tengan credenciales para el uso de los recursos tecnológicos dentro de las instalaciones de la organización, el cual les permita

realizar sus labores con mayor seguridad y no tengan riesgo de amenazas o de vulnerabilidad de la información el cual están manejando o recolectando de los usuarios finales. (ISACA, 2018).

4.2.2.2.4 Gestionar la identidad del usuario y el acceso lógico - DSS05.04. Se encarga de brindar acceso a las partes interesadas de acuerdo al nivel de confidencialidad establecida por la alta gerencia dentro de la organización, para así lograr tener una infraestructura tecnológica dentro de la empresa, que está protegida de ataques cibernéticos. Y a su vez que cada uno conserve las credenciales para futuras investigaciones o reportes que necesiten. (ISACA, 2018)

4.2.2.2.5 Gestionar el acceso físico a los activos de TI - DSS05.05. Define e implementa las instrucciones el cual cada encargado de área debe cumplir a cabalidad para poder delimitar e invalidar los intentos de ataques cibernéticos dentro de la empresa, ya sean remotos o por medio de virus, riesgos naturales, entre otros. El personal que desee ingresar a las instalaciones de la empresa de reportarlo en el momento de ingreso y de salida, para poder controlarlo y verificar que exista la credencial. (ISACA, 2018)

4.2.2.2.6 Gestionar documentos sensibles y dispositivos de salida - DSS05.06. Se encarga de instaurar protecciones a la infraestructura tecnológica empresarial, el cual sirva de apoyo a todas las áreas en específico, por si se presenta alguna falla de TI, o necesiten soporte técnico para lograr cubrir una amenaza que se presente o salvaguardar datos confidenciales para su posterior uso. (ISACA, 2018).

4.2.2.2.7 Supervisar la infraestructura para detectar eventos relacionados con la seguridad - DSS05.07. Se enfoca en aprovechar los recursos tecnológicos para la localización de delitos, supervisando cada uno de los activos de la información dentro de la organización el cual sirve para descubrir pasos no considerados y certificar los reportes de los incidentes esté compuesto con la vigilancia habitual de incidentes. Registrando los sucesos coherentes de la

protección obtenidos con los recursos tecnológicos que monitorean la empresa, emparejando los datos que se deben asegurar en las bases de datos para medir su nivel de confidencialidad. Reteniéndola durante un tiempo determinado el cual servirá a futuro para su posterior uso. (ISACA, 2018)

4.2.2.3 NORMA ISO 27001:2013. La gestión de TI de COBIT 5 con unión a la protección de los datos el cual tiene los siguientes fines, para conseguir afirmar que, adentro de la organización, los activos están protegidos con la propagación por usuarios no autorizados (confidencialidad), alteración inapropiada (honestidad) y no ingreso cuando es requerida (acceso al recurso) (Márquez y Vega, 2017, p. 48).

- **Confidencialidad:** significa resguardar las restricciones autorizadas en el ingreso y publicidad, incluyendo la seguridad de privacidad y poseedor de los datos.
- **Integridad:** significa no autorizar la alteración inapropiada o detrimento e incluye cerciorarse de la no repudiación de los datos y su legitimidad.
- **Disponibilidad:** significa comprobar el ingreso adecuado y Íntegro a los datos y su utilización.

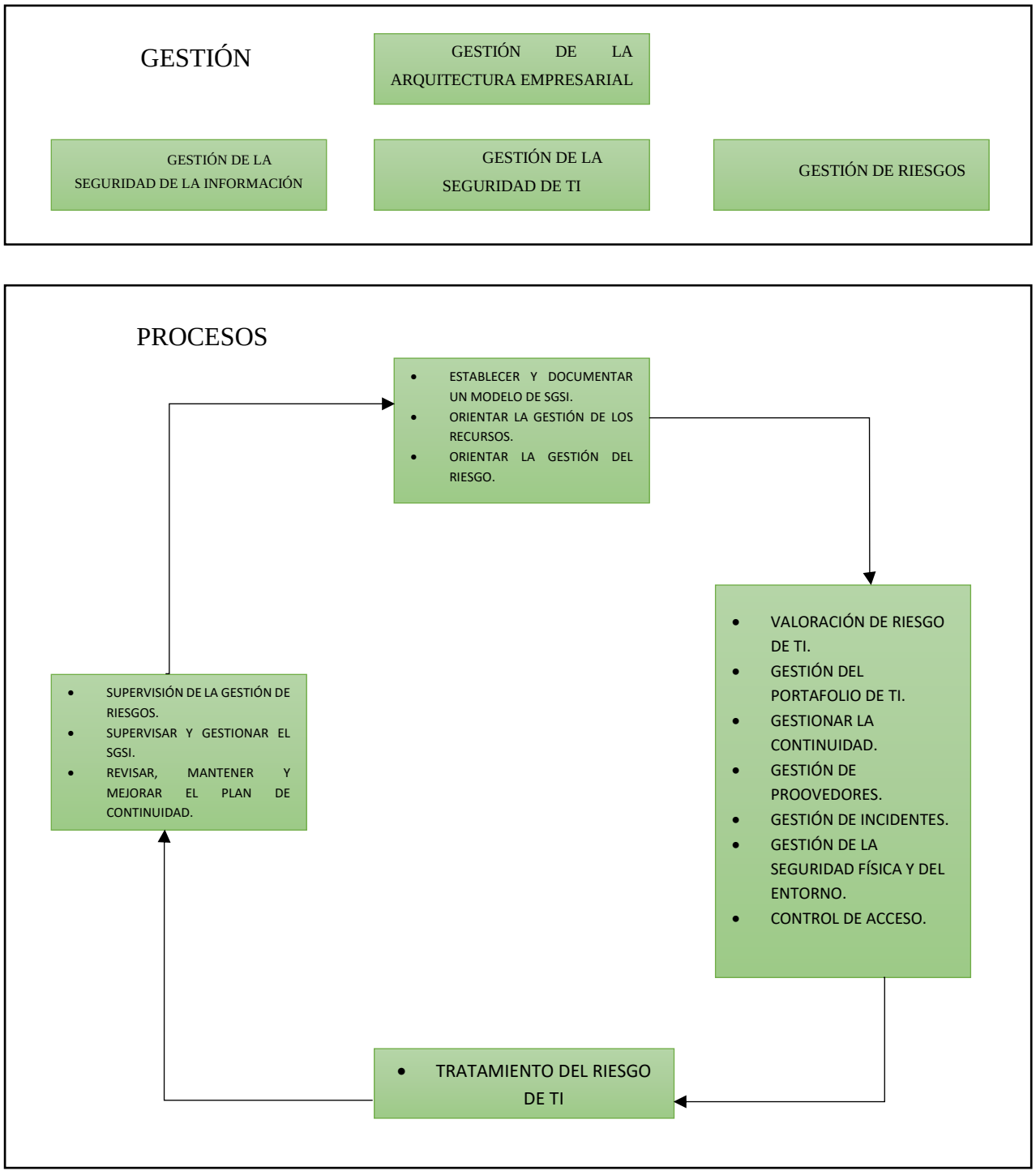
Es significativo que la coordinación de la dirección de la protección de los datos sea miembro y oriente la integración con los procesos de la institución que van a favor con la disposición completa de la administración. (Márquez y Vega, 2017, p. 48).

4.2.3 Integración de estándares en un modelo de gestión TI

4.2.3.1 Diseño del modelo. El plan para la protección de los datos es fundamental para conseguir respaldar la confidencialidad, la lealtad y el medio por el cual los datos, mediante la utilidad de una causa de servicio del peligro, brinda protección a las partes interesadas acerca de que los riesgos forman el plan de carácter adecuado. Es trascendental que el método de asistencia para la seguridad de los datos sea pieza de los procesos y de la organización de servicio integro de los activos se considere en el diseño de procesos, sistemas de información y controles. La posibilidad es que la implementación del procedimiento de gobierno de la protección de los datos será en progreso en correspondencia con todo lo que va utilizar la organización (Márquez y Vega, 2017, p. 46).

En el trabajo realizado (Camargo Barbosa, J., et al., 2020) se establece un modelo de TI para el mundo globalizado que centra su atención en la seguridad de la información y el tratamiento de datos personales. Con el límite de conseguir delimitar un plan de Servicios de TI, conforme con los procesos incorporados de la JEP, se determina una participación organizacional aplicable al área de TI dentro de la institución, en la cual se destaca la misión de la seguridad, los incidentes de riesgos y la infraestructura que soporta TI, como procesos principales que se encuentran encaminados al desarrollo corporativo en los procesos que realiza, como se presentan a continuación:

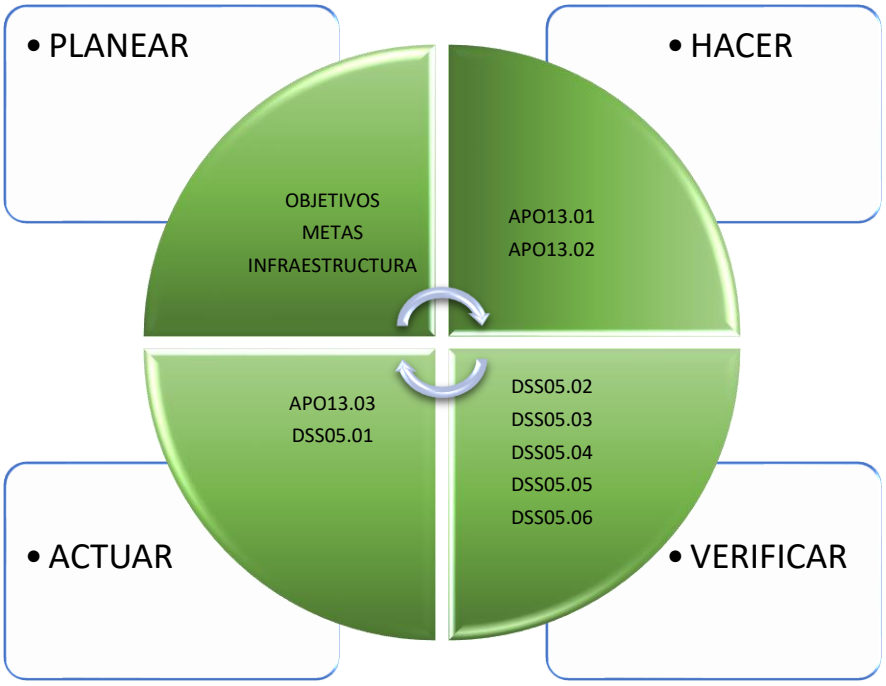
Figura 21. Modelo de Gestión de TI propuesta JEP



Fuente: Autor del proyecto.

Actualmente las entidades públicas del ente nacional están obligadas a implementar esta práctica las cuales están especificadas en la Ley Única Reglamentado 1078 de 2015, en que se regula las TIC. El cual se complementan con el marco de estándares integrales, el cual son una herramienta que vinculan las estrategias y los objetivos que muestran desempeño y resultados a través del núcleo modelo teniendo en cuenta el proceso de COBIT 5.0 APO13 y DSS05. A continuación, se presenta el modelo:

Figura 22. Modelo PHVA procesos de TI



Fuente: Autor del proyecto.

Cabe resaltar que los procesos de gestión de TI propuestos para implementar dentro de la JEP están enfocados a un ciclo de mejora continua, de acuerdo al esquema operativo por procesos que están diseñados por la empresa, en el que se proponen la integración de los procesos de COBIT 5 con el ciclo PHVA, como se expone en la anterior ilustración 22.

- Es de mucha jerarquía que la JEP cuente con políticas de protección de datos en el que actualmente estas guiaran la gestión exclusiva y profesional de todos los funcionarios de la JEP, haciendo que la empresa trabaje en base a las mejores prácticas de protección y acatamiento de los requisitos legales en los que se rige para conseguir su adecuado ejercicio. El plan está trazado con el propósito de utilizarlo en empresas que pretendan:
- Elegir los registros adentro del desarrollo de ejecución para un plan de Servicio de Protección de los datos apoyado en COBIT 5.
- Implementar controles de protección de los datos apoyado en los procesos de APO13 y DSS05.

Por otro lado, proporciona protección de los datos que tienen afinidad, y el cual se encargan de garantizar que, adentro de la organización, que los datos estén protegidos frente a la publicidad por usuarios no autorizados como los son la Confidencialidad, modificación inapropiada de la información, y el acceso ilícito cuando es requerida (Márquez y Vega, 2017, p. 47).

Con el cierre de detallar la guía estándar de servicios de ti, que sirva como informe a las entidades de inspección de entes nacionales en cuestión específica de la JEP, es necesario iniciar reuniendo las principales características de la empresa como lo son las partes interesadas, los requisitos organizacionales y protección de los datos y por último la identificación de oportunidades.

4.2.3.1.1 Intereses para los interesados. En este módulo se comprende el nivel de las partes interesadas de la JEP, el cual se interrelacionan a todas las partes de la empresa ya sean que pasen por dentro o fuera, por el cual se establecen las siguientes partes interesadas:

Tabla 3. Necesidades, Expectativas y Partes interesadas.

PARTES INTERESADAS	NECESIDADES	EXPECTATIVAS
Todos los grupos de interés, entidades concernidas implicadas o titulares de derechos (interno – externo)	Aplicación adecuada de confiabilidad, lealtad y estar disponible.	**Cumplimiento de las exigencias de seguridad en la información establecidos, tales como tratamiento adecuado de la información.**
Instituciones del Estado (Ministerio de Defensa)	Validación de la veracidad de los datos con la recepción en listados recibidos.	**Confirmación de recepción de los datos de los listados de los miembros del ente Público que cumplan con las circunstancias para tomar la autonomía condicionada o para la sustitución de la voluntad intramural por la escasez de la autonomía en la policía.**
Instituciones del Estado (Gobierno Nacional)	Validación de la veracidad de los datos con la recepción en listados recibidos.	**Confirmación de la recepción de los datos por miembro de la oficina de los listados de integrantes de las FARC-EP (para contrastarlos con las personas que efectúen las manifestaciones de rendición).**

Rama Ejecutiva (Presidencia de la República)	Validación de la veracidad de los datos con la recepción en listados recibidos.	**Confirmación de la recepción de los datos de los actos administrativos mediante los cuales se aplica e individualiza a las personas beneficiarias del perdón de iure que no estén privadas de la libertad.**
Organizaciones no gubernamentales (Jurisdicción Indígena)	Validación de la veracidad de los datos con la recepción en listados recibidos.	**Confirmación de los datos referente a los casos de capacidad de la JEP. El estatuto de la JEP debe instaurar los mecanismos de relación con la Autoridad Regional.**
Víctimas y las organizaciones que las agrupan	**Validación de la integridad de la información con la recepción de los listados recibidos**	**Verificación de la admisión de los datos referente a las conductas cometidas en el contienda armada, en colaboración en audiencias públicas, declaración de sanciones y remanente espacios que se definan en el estatuto y en el código de la JEP.**

Fuente: autor del proyecto.

Tabla 4. Partes Interesadas internas, Necesidades y Expectativas

PARTES INTERESADAS	NECESIDADES	EXPECTATIVAS
Comunidad internacional, Sindicatos, Organizaciones no gubernamentales.	Validación de la integridad de la información con la recepción de los listados recibidos	**Verificación del transporte de informes a la JEP referente a conductas cometidas en el cuadro del problema; traslado de datos referente a los procesos de la asociación agraria.**
Víctimas y las organizaciones que las agrupan, Comparecientes ante la JEP	Integridad en las decisiones judiciales y administrativas basado en la confiabilidad, lealtad y tener los recursos de información disponibles.	• **Integridad en las decisiones judiciales y administrativas.** • **Aplicación de las mejores prácticas en cuanto al manejo de la información**
Sociedad en su conjunto	Aplicación de los recursos tecnológicos confiables en cuanto al manejo de la información	**Derecho a alcanzar Compañía ciudadana Informada y con garantías de no frecuencia.**
Todos los grupos de interés, entidades concernidas implicadas o titulares de derechos (interno – externo)	Definir los mecanismos de interrelación, interinstitucional y nacionales al igual que le manejo de los mecanismos de intercambios de información.	**Cumplimiento con los lineamientos y normatividad establecida para el intercambio de información**

Instituciones del Estado (INPEC)	Definir estrategias para asegurar la privacidad, lealtad y recurso de la información que se transfiere en el marco del cumplimiento de la misión.	• **Continuidad de la seguridad de la información en situaciones de contingencia.** • **Dar tratamiento adecuado a los datos personales suministrados a la entidad.** • **Contar con el camino a los datos requeridos en la realización de su misionalidad.** • **Cumplimiento por parte de JEP de cada uno de sus requisitos pertinentes a seguridad de la información.**
Rama Ejecutiva	Disponer de información oportuna, integra y veraz	• **JEP implemente el Modelo de Seguridad y Privacidad de la Información MSPI - de la Estrategia de Gobierno Digital.** • **JEP asigne los recursos necesarios para la protección de los activos.**
Rama Legislativa	Validación de la integridad de la información con la recepción de los listados recibidos	**Reporte de informes a la JEP sobre conductas cometidas en el cuadro de los conflictos.**

Víctimas y las organizaciones que las agrupan	**Validación de la integridad de la información con la recepción de los listados recibidos**	**Información detalla de las Víctimas (Registro Único de Víctimas).**

Fuente: autor del proyecto.

Tabla 5. Partes Interesadas Externas, Necesidades y Expectativas.

PARTES INTERESADAS	NECESIDADES	EXPECTATIVAS
Instituciones del Estado (Justicia Penal Militar)	Validación de los datos con la recepción de los listados recibidos	**Diligencia de los datos enviados a la JEP de reportes de investigaciones y sentencias proferidas por la JPM, con copia de estas últimas.**
Rama Judicial	Validación de la integridad de la información con la recepción de los listados recibidos	**Utilidad de los datos sobre providencias judiciales para contrastarlas con las manifestaciones de acatamiento realizadas por personas vinculadas a la JEP.**
Secretaría Ejecutiva - Misión de Monitoreo y Verificación (MMV)	Validación de la integridad de la información con la recepción de los listados recibidos	**El Funcionario recibe los datos relativos para el abandono efectiva de armas, para incluirla en su reporte a las Salas de la JEP.**

Contratistas	• Retroalimentación de la información de JEP. • Revisión del cumplimiento de los requisitos de seguridad de la información. • Seguimiento y revisión de los servicios para conocer estado de satisfacción.	• **Cumplimiento de los requisitos de seguridad de la información establecidos en los acuerdos con los Proveedores, tales como tratamiento adecuado de la información.** • **Dar tratamiento adecuado a los datos personales suministrados a la entidad.**
Periodistas, columnistas y líderes de opinión.	Disponer de información oportuna, integra y veraz.	**Contar con credenciales para obtener datos en el momento requerido.**
Sociedad en conjunto o público en general	Mecanismos para interponer PQRS. • Establecer mecanismos que faciliten la realización de trámites y la solicitud de los datos.	• **Dar tratamiento adecuado a los datos personales suministrados a la entidad.** • **Contar con el acceso a la información en el momento requerido.**
Servidores, servidoras y contratistas	**Formación y sensibilización en seguridad de la información para el**	• **Establecimiento de lineamientos de protección de los datos que contribuyan en la composición de sus funciones.** • **Aplicar el talento adquirido durante las jornadas de establecimiento y sensibilización en**

	ejercicio de funciones.	**protección de la información.** • **JEP da un procedimiento conveniente a los datos personales suministrados a la entidad.**

Fuente: Autor del Proyecto.

4.2.3.1.2 Objetivos empresariales en la Gestión de TI. La propuesta para la JEP, sirven como base para que el modelo se defina en las diferentes perspectivas de las dependencias, como lo son, financiera, TIC, interna, recursos humanos, el cual establecen cada una de las metas en la gestión, el cual se encuentran organizadas desde la gerencia para su posterior cumplimiento y se basan en los definidos por el marco de referencia de COBIT 5.

Tabla 6. Objetivos Corporativos y Gestión de TI

DEPENDENCIA	OBJETIVOS CORPORATIVOS	OBJETIVOS DE GESTIÓN DE TI
FINANCIERA	1. Riesgos de negocio gestionados (Salvaguardar los activos)	Riesgos de ejercicio interrelacionados con las TI gestionados.
	2. Desempeño de leyes y regulaciones externas	Acatamiento de las normas de TI
	3. Transparencia financiera	Optimización de activos, recursos y capacidades de las TI.
TIC	4. Continuidad y disponibilidad del servicio de negocio	Protección de la infraestructura tecnológica y activos de la información.

	5. Liderazgo basado en los datos adquiridos	Disponibilidad de los activos de la información.
INTERNA	6. Optimización en las funcionalidades en los procesos	Base de las actividades dentro de la JEP compuestas por los recursos tecnológicos y normas de TI.
	7. Procesos de mejora continua	Responsabilidad de la alta gerencia ejecutiva para obtener decisiones relacionadas con TI.
	8. Cumplimiento con las políticas internas	Acatamiento de las normas internas.
RECURSOS HUMANOS	9. Personas preparadas y motivadas	Funcionarios capacitados, competentes y motivados.

Fuente: Autor del Proyecto.

4.2.3.1.3 Dominios para la Gestión de TI basado en los procesos de COBIT 5 (APO13 Y DSS05)

Tabla 7. Dominio de Objetivos

CODIGO	DOMINIO
PDE	PLANEACIÓN Y DIRECCIÓN ESTRATEGICA
GDR	GESTIÓN DE RIESGOS
GSI	GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Fuente: Autor del proyecto.

4.2.3.1.3.1 Planeación y Dirección estratégica de TI. La meta fundamental del mando de Planeación y Orientación estratégica de TI, es instaurar un modelo de Servicios de TI que estructure y direccione el camino de las decisiones adentro del departamento de TI que garantice la composición y la formación con la normatividad actual, las políticas, los procesos y los servicios de la JEP.

Tabla 8. Dominio Plan Estratégico Gestión TI

CODIGO	PROCESO COBIT 5	CODIGO ACTIVIDAD	ACTIVIDAD
PDE01	Alineación de la Gestión de TI	PDE01.A01	Evidenciar el estado real de la JEP, en el curso organizacional y del medio, y reconocer los factores internos y externos, que puedan intervenir en el diseño del trabajo de TI.
PDE02	Esquema de Gestión de TI	PDE02.A01	Delimitar las políticas, lineamientos y directrices que hacen pieza de las habilidades de Trabajo de TI.
		PDE02.A02	Organizar e implementar un marco de causa de servicio de TI que permita direccionar, valorar y monitorear las capacidades de TI.

		PDE02.A03	Delimitar los roles y funciones en la organización de TI, que tienen responsabilidades en la toma de decisiones.
PDE03	Informe a las partes interesadas	PDE03.A01	Inspeccionar lo relacionado con los requisitos de comunicación obligatoria actuales y futuros relacionados con el uso de las TI dentro de la empresa.
		PDE03.A02	Reconocer lo referente a la situación actual y futura de la indagación para otros grupos que se beneficien y estén interconectados con el empleo de las TI adentro de la JEP.
		PDE03.A03	Conservar los principios para la información con los grupos de asociados que son externos e internos, incluyendo los formatos de notificación.
PDE04	Supervisar la comunicación con las partes interesadas	PDE03.A04	Evaluar periódicamente la eficacia de los mecanismos.
		PDE03.A05	Valorar periódicamente la capacidad de los

			mecanismos y las expectativas de la información con las partes interesadas inmediatamente sean externos o internos.
		PDE03.A06	Establecer si se cumplen los requisitos de los diferentes grupos.
PDE05	Evaluación y Mejora continua del sistema de Gestión	PDE01.A01	Fijar las acciones que permitan reformar, optimizar y regular procesos de TI que se encuentren adentro de los detalles de no conformidades realizadas en las auditorías internas y externas.

Fuente: Autor del Proyecto.

4.2.3.1.3.2 Dominio Gestión de Riesgo de TI – GDR. El objetivo del cuidado de Peligro de TI es resguardar los datos de la JEP para conservar admisible la medida de Peligro de protección de los datos en alianza con el manejo de protección. Estableciendo y manteniendo roles de convencimiento y privilegios de entrada de los datos para ejecutar la supervisión de la protección.

Tabla 9. Dominio Gestión de Riesgo TI

CODIGO	PROCESO COBIT 5	CODIGO ACTIVIDAD	ACTIVIDAD

GDR01	Gestionar la seguridad de la Red y las conexiones	GDR01.A01	Análisis de riesgos en los requerimientos de la JEP, manteniendo una política de seguridad para las conexiones.
		GDR02.A02	Establecer mecanismos de confianza para dar soporte a la transmisión y recepción segura de información.
GDR02	Gestionar la seguridad de los puestos de usuario final	GDR02.A01	Cifrar la información almacenada de acuerdo a su clasificación, protegiendo la integridad del usuario final.
		GDR02.A02	Proveer protección física a los dispositivos de usuario final, gestionando el acceso, control y configuración de la red en la JEP.
GDR03	Gestionar la identidad del usuario y el acceso lógico	GDR03.A01	Alinear la gestión de identidades y derechos de acceso a

			los roles y responsabilidades definidos, basándose en los principios de menor privilegio, necesidad de tener y necesidad de conocer.
		GDR03.A02	Autentificar todo acceso a los activos de información basándose en su clasificación de seguridad, coordinando con las unidades de la JEP que gestionan la autenticación.
GDR04	Gestionar el acceso físico a los activos de TI	GDR04.A01	Gestionar las peticiones y concesiones de acceso a las instalaciones de procesamiento. Los formularios deben incluir la identificación específicamente las áreas a las que el usuario tiene acceso concedido.

		GDR04.A02	Restringir el acceso a ubicaciones de TI sensibles estableciendo restricciones.
GDR05	Gestionar documentos sensibles y dispositivos de salida	GDR05.A01	Asignar privilegios de acceso a documentos sensibles y dispositivos de salida basados en el principio del menor privilegio, equilibrando riesgo y requerimiento de la JEP.
		GDR05.A02	Establecer un inventario de documentos sensibles y dispositivos de salida y realizar regularmente conciliaciones.
GDR06	Supervisar la infraestructura para detectar eventos relacionados con la seguridad	GDR06.A01	Definir y comunicar la naturaleza y características de los incidentes potenciales relacionados con la seguridad de forma que sean fácilmente reconocibles y sus impactos

			comprendidos para permitir una respuesta.
		GDR06.A02	Revisar regularmente los registros de eventos para detectar incidentes potenciales.

Fuente: Autor del Proyecto.

4.2.3.1.3.2 Dominio gestión de la seguridad de la información – GSI

Tabla 10. Dominio GSI

CODIGO	PROCESO COBIT 5	CODIGO ACTIVIDAD	ACTIVIDAD
GSI01	Establecer y mantener un SGSI	GSI01.A01	Establecer el alcance y los límites del SGSI en términos de las características de la JEP, su localización, activos y tecnología. Incluyendo detalles para cualquier exclusión.
		GSI01.A02	Definir un SGSI de acuerdo con la política de empresa y alineada con la JEP, su localización, activos y tecnología.

		GSI01.A03	Alinear el SGSI con el enfoque global de la gestión de la seguridad de la empresa.
		GSI01.A04	Definir y comunicar los roles y las responsabilidades de la gestión de la seguridad de la información.
GSI02	Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.	GSI02.A01	Formular y mantener un tratamiento de riesgos de la información alineado con los objetivos estratégicos. Asegurando que el plan identifique las prácticas de gestión y las soluciones de seguridad apropiada.
		GSI02-A02	Implementar el plan de tratamiento de riesgos de seguridad de la información.
		GSI02.A03	Definir la forma de medición de la efectividad de las prácticas de gestión y especificar la forma

			de utilizar estas mediciones para evaluar la efectividad y producir resultados reproducibles y comparables.
		GSI02.A04	Integrar la planificación, el diseño, la implementación y la supervisión de los procedimientos de seguridad de información y otros controles que permitan la prevención y detección temprana de eventos de seguridad, así como la respuesta a incidentes de seguridad.
GSI03	Supervisar y revisar el SGSI.	GSI03.A01	Realizar revisiones periódicas del SGSI, incluyendo aspectos de políticas, objetivos y prácticas de seguridad del SGSI.
		GSI03.A02	Realizar revisiones periódicas del SGSI

		por la dirección para asegurar que el alcance siga siendo adecuado y que se han identificado mejoras en el proceso del SGSI.
	GSI03.A03	Proporcionar información para el mantenimiento de los planes de seguridad para que consideren las incidencias de las actividades de supervisión y revisión periódica.
	GSI03.A04	Registrar las acciones y los eventos que podrían tener un impacto en la efectividad o el desempeño del SGSI.

A partir de estos dominios, se propone recolectar indicadores de resultados más objetivos y cuantificables, logrando combinar estos indicadores de manera equilibrada con los procesos de COBIT 5, lo que define cómo promover acciones futuras y lograr metas. Estos componentes son importantes para el Modelo de Gestión de TI porque permite tener una visión holística, permitiendo definir cada elemento, de esa manera se tiene mayor claridad sobre lo que se busca en la gestión de TI, encontrando un equilibrio entre las partes.

Por otra parte, estos dominios aportan beneficios a los procesos internos, permitiendo conocer en que se debería centrar la JEP para obtener los resultados deseados. El aprendizaje y el crecimiento, serviría para poder alcanzar los objetivos y las metas, desde la innovación y la mejora continua. Por ultimo no menos importantes los usuarios finales, que este caso correspondería a la comunidad en general, desde la gestión de TI vendría siendo el cómo brindar los resultados para demostrar confianza antes de los demás.

4.2.3.1.4 Niveles de Riesgos en Actividades Gestión de TI. Valorar de modo objetivo e autónomo la misión realizada por los procesos de los Servicio de TI, en el plan del tiempo PHVA determinado en la determinación documentada en el Método de Trabajo de Eficacia, con el objetivo de ayudar al mejoramiento permanente y certificar de modo oportuno y efectivo el acatamiento de las metas de los procesos.

Tabla 11. Niveles de Riesgo Actividades

CAUSAS	NIVEL DE RIESGO	PLAN DE ACCIÓN ASOCIADO
Planificación de las actividades.	ALTO	**1. Realizar reunión de apertura.**
Alta carga laboral. **Incapacidad médica.** **Calamidad doméstica.**	MEDIO	**2. Socialización del Programa de Auditoria Interna al proceso a evaluar y presentar el equipo auditor, resaltando la importancia de su cumplimiento y los efectos positivos en los resultados de este.**
Problemas de orden público (Protestas, manifestaciones, transporte, etc.). **Desastres naturales.**	MEDIO	
Inadecuada Planificación de la auditoria asignada	**MEDIO**	**3. Motivación a los auditores internos con formación complementaria que les permita mejorar sus competencias y**

	habilidades, cuando estos sean requeridos.

Fuente: Autor del proyecto.

4.2.3.1.4.1 Caracterización del proceso "Gestión de las Tecnologías" basado en el proceso APO13.01. En el cual se elabora la caracterización en el Sistema de Gestión de Calidad mediante el cual se establece el ciclo PHVA de las actividades a desarrollar por el proceso. En el marco de la gestión realizada por el proceso se propone las siguientes actividades, el cual sirven como mecanismos de apoyo tecnológicos para la seguridad y gestión de TI.

Con el propósito de dar soporte a las operaciones de la JEP, se definió una arquitectura de aplicaciones y/o soluciones informáticas, cuya vista de alto nivel se observa en la siguiente ilustración.

Figura 23. Arquitectura soluciones TI.

Fuente: Autor del Proyecto.

4.2.3.1.4.1 Gestión de soluciones tecnológicas. La Dirección de TI se encarga de la gestión de TI, en realizar articulaciones con las diferentes dependencias para la adquisición de soluciones tecnológicas que apoyen la ejecución de la gestión en la JEP en el marco de los objetivos institucionales, así:

- Formulario de solicitud de acreditación de víctimas y gestión en el despacho
- Herramienta tecnológica para la gestión de los Casos.
- Actualización e implementación del control de cambios para la herramienta YACHAY, la cual se encuentra en operación.
- Implementación del Sistema de Gestión Documental para la JEP, incluyendo la consultoría, licenciamiento y prestación del servicio durante 24 meses, posteriores a la salida en producción, el cual se encuentra en ejecución el contrato.
- Implementación del Sistema de Gestión Judicial, que permite el manejo del ciclo de vida del proceso de juzgamiento desde la apertura del caso hasta su fallo, cierre y archivo.
- Adquisición Software Nvivo (Software Especializado en análisis cualitativo), Software ArcGIS (Software especializado en el análisis geográfico y cartográfico), Adquisición Software Abbyy (Software de OCR), Adquisición Software de Transcripción (Dragon y Adobe Audition), Adquisición Software Nitro (Software especializado en manejo de archivos en formato PDF), Adquisición Software IBM i2 (Software Especializado en análisis criminal), Adquisición Software Stata (Software especializado en análisis estadístico), los cuales se encuentra instalado.

Así mismo, se requiere que la dependencia logre brindar soluciones informáticas que definan lograr mantener en el tiempo previsto, respuestas a los servicio o adquisiciones, tales como:

- Portal WEB.
- Sistema CRM
- Sistema de Planeación y Gestión.
- Por otra parte, como medida de contingencia, mediante el Sistema de Gestión Judicial Transitorio INDI – "SOL". Herramienta que permita el reparto y gestión de los trámites judiciales.

Seguidamente, se permite realizar soluciones "in house" que sean desarrolladas por la Dirección de TI, como soluciones temporales a las necesidades prioritarias de las dependencias, así:

- Requerimientos Seguridad (formularios con procesos automatizados para la solicitud de diferentes servicios, son formularios y flujos de proceso en SharePoint),
- Formularios de consecutivos, registro de actividades cobro (formularios y flujos de proceso en SharePoint),
- Formato de órdenes de pago y cuenta de cobro (formularios y flujos de proceso en SharePoint).

4.2.3.2 Política basada en el proceso APO13.02. Preservar la confidencialidad, integridad y disponibilidad de su información, mediante la formulación de objetivos, definición de lineamientos, procedimientos, protocolos y controles con el propósito de gestionar de manera efectiva los activos de información y sus riesgos en el marco de su misión institucional. Igualmente, fomentará la formación de una cultura de seguridad y privacidad de la información, el cumplimiento del marco normativo vigente en esta materia y velará por la asignación de los recursos necesarios para la implementación de la política y mejora continua del Sistema de Gestión de Seguridad y Privacidad de la Información.

4.2.3.3 Alcance y privacidad basado en APO13.03. Según la Política, el alcance y la privacidad de los activos tecnológicos, son los activos requeridos para el adecuado funcionamiento en los procesos en la JEP, en la sede central, grupos territoriales y en las demás que en el futuro se establezcan.

4.2.3.4 Objetivos de seguridad de la información. Para lograr cumplir con los objetivos propuestos dentro de la JEP, se incluyen unos puntos claros que se deben cumplir, el cual sirve de apoyo para los procesos dentro de la empresa.

- Asegurar la confidencialidad, integridad y disponibilidad de los activos de información, mediante la gestión de los riesgos de Seguridad de la Información.
- Promover una cultura de Seguridad de la Información a los usuarios internos y demás personas vinculadas, a través de la implementación de programas de capacitación y sensibilización.
- Asegurar el mejoramiento continuo de la Privacidad de los datos mediante la implementación de acciones correctivas, de mejora y planes de acción.
- Reducir las debilidades en los incidentes presentados enfocados a la protección de los activos tecnológicos.

4.2.3.5 Contexto de la organización. El contexto de la Jurisdicción Especial para la Paz - JEP, considera las expectativas y necesidades de sus partes interesadas, identificando en qué medida los aspectos internos y externos podrían afectar el propósito de la entidad y su capacidad para lograr los resultados requeridos por el Sistema de Gestión de Seguridad y Privacidad de la Información, con base en los procesos de COBIT 5.

4.2.3.6 Comunicación. En consecuencia, la seguridad en la información, de la JEP, manejará las comunicaciones internas y externas manteniendo los registros necesarios, tales

como: asistencia a capacitaciones, actas de reunión, publicaciones en página web, redes sociales o evidencia del envío formal de la comunicación o publicación.

Resultados esperados de la comunicación:

- Que los grupos de interés conozcan y entiendan las políticas y objetivos de seguridad de la información, así como la importancia del cumplimiento y logro de los mismos.
- Que los usuarios internos conozcan los documentos del Sistema de Gestión de Seguridad y Privacidad de la Información - SGSPI, así como los medios de acceso a ellos y las responsabilidades de su utilización.
- Que la alta dirección conozca los resultados del desempeño y privacidad de la de los datos en el SGSPI.
- Que todos los usuarios internos tengan conocimiento sobre la eficacia de las acciones correctivas y de mejora continua.
- Que los usuarios internos conozcan sus responsabilidades.

4.2.3.7 Sanciones en caso de infracción. Toda falta por parte de un usuario interno, de cualquiera de las políticas establecidas en este manual, acarreará las sanciones a las que haya lugar, según la Ley 734 de 2002 por la cual se expide el Código Disciplinario Único, y las respectivas acciones penales de la Ley 599 de 2000 por la cual se expide el Código Penal y la Ley 906 de 2004 por la cual se expide el Código de Procedimiento Penal.

4.2.3.8 Organización de la seguridad Basado en el proceso DSS05

Roles y responsabilidades basado en el proceso DSS05.04

Los roles y responsabilidades del Sistema de Gestión de Seguridad y Privacidad de la Información - SGSPI, estarán definidos en el plan estratégico de la Jurisdicción Especial para la Paz – JEP, el cual se encargará de gestionar las identidades y derechos de acceso.

4.2.3.9 Lineamientos generales. Los lineamientos estipulados para la JEP, deben ser cumplidos por las partes interesadas ya sean externos o internos, para lograr el buen manejo y efectividad dentro de los procesos, el cual se deben cumplir de la siguiente manera:

- Todo usuario interno contará con equipo de cómputo de escritorio o portátil de acuerdo con la asignación de la Dirección de Tecnologías de la Información - DTI.
- El intercambio de información digital dentro de la JEP, se realiza a través del uso de carpetas compartidas en el servidor de archivos ("file server") y de los servicios de Office 365.
- Todos los equipos de cómputo de escritorio y portátiles, deberán contar con software y antivirus autorizado, los cuales serán instalados exclusivamente por personal de la DTI.
- Para evitar que el usuario interno instale software no autorizado en su equipo de cómputo de escritorio o portátil se restringirá el uso del usuario administrador.
- El usuario Administrador de todos los equipos de cómputo de escritorio y portátiles que son de la Jurisdicción Especial para la Paz - JEP será de uso exclusivo del personal de la DTI.
- Todos los equipos de cómputo de escritorio y portátiles que son de la Jurisdicción Especial para la Paz - JEP, deberán tener activado el cifrado del disco duro, actividad realizada por la Mesa de Ayuda.
- La Jurisdicción Especial para la Paz - JEP no tendrá ninguna responsabilidad sobre la seguridad física de los dispositivos móviles, equipos de cómputo de escritorio y portátiles de terceros.

4.2.4 Políticas complementarias de seguridad de la información basado en el proceso DSS05

4.2.4.1 Política para dispositivos móviles basado en el proceso DSS05.01. Con el término de minimizar los riesgos de protección de los datos que implican el empleo de dispositivos móviles, la DTI permite el acceso a las redes institucionales de dispositivos móviles personales tales como: teléfonos inteligentes, equipos de cómputo portátiles, tabletas, entre otros, siempre y cuando se dé cumplimiento a los mecanismos de seguridad establecidos por la DTI para tal fin. Para efectos de lo anterior, se dispone de las siguientes redes inalámbricas y servicios:

Redes inalámbricas: Basado en el proceso DSS05.02

Con el fin de lograr preservar la seguridad de las redes WLAN se debe implementar una serie de reglamentos el cual sirvan de apoyo para la oficina de las TIC, en el cumplimiento y uso adecuado de la siguiente manera:

- **Red inalámbrica de "visitantes JEP":** Para servicio de dispositivos móviles de usuarios externos, se permite el acceso a Internet con las restricciones que establece la Entidad, no debe permitir conexión a las redes corporativas.
- **Red inalámbrica de "usuarios internos JEP":** Para el servicio de usuarios internos cuyos dispositivos móviles no son de la Jurisdicción Especial para la Paz - JEP. Esta red permite el acceso a internet con las restricciones que establece la Entidad.
- **Red inalámbrica de "servidores VIP JEP":** Para el servicio de Magistrados, Fiscales y Directivos de la Secretaría Ejecutiva cuyos dispositivos móviles no están dentro de la red permite el acceso a internet con las restricciones que establece la Entidad.
- **Red inalámbrica de "Computadores JEP":** Para el servicio de equipos de cómputo que son, de los mismos niveles de acceso que provee la red LAN.

- **La Jurisdicción Especial para la Paz - JEP** se reserva el derecho de monitorear y revisar el cumplimiento de la política para dispositivos móviles conectados a las redes inalámbricas, cuando lo estime conveniente.

La transferencia o manejo de la información de la Entidad por medio de aplicaciones de mensajería instantánea, puede realizarse siempre y cuando se dé cumplimiento a los mecanismos de seguridad establecidos por la DTI para tal fin. Todas las excepciones deben quedar debidamente documentadas y aprobadas.

4.2.4.2 Política de trabajo en casa basado en los procesos DSS05.02. Esta política hace referencia al conjunto de controles y medidas para garantizar la protección de los datos.

- Desde cualquier punto de vista tecnológico y de protección de datos, toda sesión de trabajo en casa requerida por un usuario que previamente sea autorizado se realiza a través de una VPN (Red Privad Virtual) o cualquier solución definida por la DTI, que debe proveer conexión segura con la Entidad. La VPN o solución definida por la DTI debe solicitarse siguiendo el procedimiento establecido por la DTI a través de la Mesa de Ayuda.
- En el caso de los usuarios internos de la DTI, que por labores de soporte técnico requieran acceso en horarios hábiles o no hábiles, debe solicitar, el acceso por VPN requerido, siguiendo el procedimiento establecido por la DTI a través de la Mesa de Ayuda.

En los casos en que las credenciales y el procesamiento de los datos de la JEP sea mediante la circunstancia de compromiso en residencia, los responsables de estas actividades deben proporcionar obediencia a las situaciones y restricciones definidas con el ambiente a la protección de los datos, tales como:

- Tener configurado el cifrado de disco duro.
- Toda sesión de trabajo en casa debe realizarse con un equipo propietario de la Entidad.

- Se prohíbe cualquier otro tipo de acceso remoto y el uso de sistemas de información que no estén autorizados por la DTI.

4.2.4.3 Políticas de acceso basado en el proceso - DSS05.03. La DTI gestiona el control de acceso lógico a la información en la JEP, establecido con los roles, en compromiso con las principales normas que debe conocer:

- **Lo que necesita saber:** únicamente se concede credenciales a los datos que el beneficiario responsable en la empresa requiera para la realización de sus tareas (diferentes tareas/roles significan diferentes cosas que se necesita estar al corriente y, en efecto, tener diferentes perfiles para lograr acceder).
- **Lo que necesita utilizar:** únicamente se concede credenciales a los servicios (equipos de TI, aplicaciones, procedimientos, recintos) que el interesado internamente necesita para la ejecución de su tarea/trabajo/rol.
- La Oficina Asesora de Seguridad y Protección define la estrategia de la seguridad física de la Entidad.

4.2.4.4 Servicios de internet basado en el proceso - DSS05.02. Se deben seguir las siguientes indicaciones para lograr una mejora continua en los procesos técnicos dentro de las instalaciones de la JEP, en cuanto a los puntos de red que se establezcan, el cual evitara futuras amenazas dentro de la empresa:

- Los puntos de red que no estén en uso deben ser deshabilitados, con el fin de evitar conexiones no autorizadas en la red en la JEP. Adicionalmente, los puntos de red activos se controlan de forma segura como PORT SECURITY, característica de los switches que permiten retener las direcciones Media Access Control - MAC (identificador único de cada equipo en la red), con el fin de evitar la conexión de equipos no autorizadas.

- La DTI es la responsable de autorizar o de realizar la instalación de dispositivos adicionales de red. En caso de que alguna área o usuario necesite puntos adicionales o accesos a la red, se comunica con soporte técnico.
- La DTI asigna los roles, permisos y controla el acceso de usuarios a cada sistema de información de acuerdo con la solicitud realizada por los Magistrados, Fiscales y Directivos de la Secretaría Ejecutiva, siguiendo el procedimiento establecido a través de la Mesa de Ayuda.
- Los privilegios del Usuario Administrador de cualquier solución tecnológica o componentes en la empresa como lo son (equipos de cómputo, recursos de conectividad, equipos de seguridad perimetral, etc.) son de administración y uso exclusivo de la DTI. Ningún otro usuario interno está autorizado.
- El intercambio de información digital entre los usuarios internos de la Entidad se realiza a través del uso de las carpetas compartidas en el servidor de archivos ("file server") y de los servicios de Office 365, ofrecidos por la DTI. La gestión de las carpetas compartidas se realiza a través de la Mesa de Ayuda.

La Jurisdicción Especial para la Paz - JEP brinda recursos tecnológicos a los usuarios internos y usuarios externos para navegar en la Web. Esta conexión es controlada mediante perfiles de navegación que la DTI defina. Sin embargo, se deben bloquear las siguientes categorías para todos los usuarios:

- Alcohol, drogas y tabaco, entretenimiento, radio y televisión, descargas y transmisión de multimedia, apuestas en línea, blogs, mensajería instantánea, redes sociales, almacenamiento personal y en red, accesos remotos, recursos compartidos, juegos, dibujos animados, contenido grotesco, palabras soeces, violencia, armas, desnudez, pornografía, materiales sexuales, compras en línea, bienes raíces, anonimizadores, vulnerabilidades de los navegadores, discriminación,

descargas maliciosas, intercambio de archivos/P2P, suplantación de identidad, posibles actividades delictivas, posible crimen informático, posible software ilegal, código malicioso.

- Los proveedores que requieran acceso remoto a la infraestructura tecnológica de la Jurisdicción Especial para la Paz - JEP deben hacerlo a través de una conexión VPN o solución definida por la DTI para tal fin. Esta solicitud se realiza siguiendo el procedimiento de la Mesa de Ayuda.

4.2.4.5 Credenciales para las partes interesadas basado en el proceso DSS05.04. Toda solicitud dentro de la JEP, debe cumplir unos parámetros el cual servirán de apoyo para lograr realizar los procesos de asignación de usuario de la manera más rápida y efectiva de la siguiente manera:

- La solicitud de creación de usuarios, la asignación de privilegios y todas las novedades asociadas al usuario deben realizarse a través del procedimiento Gestión de usuarios definido por la Entidad.
- La DTI debe inspeccionar cuatrimestralmente el registro de usuarios con credenciales a los sistemas, y lo confrontará con el registro de usuarios internos suministrado por la Subdirección y el registro de contratistas suministrado por la Subdirección de Contrato.

4.2.4.5.1 Responsabilidades de los Usuarios basado en el proceso DSS05.03. Todos los usuarios deben seguir y poner en práctica las políticas de la empresa para el uso adecuado de sus cuentas, de manera que sean seguras.

- Salvaguardar las claves para el acceso a los diferentes activos de información a los cuales esté autorizado.
- Si requiere de mecanismos seguros para guardar sus claves, el personal de la DTI podrá indicarle la mejor forma de hacerlo.

- La Jurisdicción Especial para la Paz - JEP, establece el cambio obligatorio de las contraseñas según la periodicidad establecida por la DTI.
- Las claves de acceso para los activos tecnológicos de la JEP deben cumplir con lo siguiente:
- Ser distinto para toda práctica o procedimiento de búsqueda con rareza de aquellos sistemas que se autentiquen automáticamente.
- Omitir datos de familiares.
- Estructurar una clave de longitud entre ocho (8) y doce (12) dígitos.
- Actualizar las claves cada 6 meses en las aplicaciones y sistemas de información son controladas mediante el directorio activo y este exige el cambio automático de las mismas.
- Para el desbloqueo de la clave se debe seguir el procedimiento de Mesa de Ayuda definido para tal fin.

4.2.4.6 Acceso a sistemas y aplicaciones basado en el proceso DSS05.05. Está basado en una serie de pasos y lineamientos establecidos por la JEP, para lograr la efectividad en los procesos de la siguiente manera:

- Las aplicaciones WEB públicas críticas en la JEP deben mantener su certificado de seguridad SSL vigente, de forma tal que su acceso se realice mediante el protocolo HTTPS.
- Las aplicaciones WEB públicas críticas en la JEP deben implementar mecanismos de seguridad hacia los intentos de entrada mediante influencia bruta, como, lo son, los recaptcha y/o interrupción de cuentas por un lapso posteriormente de múltiples intentos.
- Con el fin de controlar el acceso no autorizado a la administración de soluciones tecnológicas o componentes de la infraestructura tecnológica de la Entidad, las contraseñas de

usuario administrador (ROOT, SYS, SYSADMIN, cuenta de administrador de Windows, entre otras) deben ser mantenidas bajo condiciones máximas de seguridad.

La contraseña debe estar compuesta de dos partes:

- La primera parte a cargo del administrador técnico del componente.
- La segunda parte a cargo del Oficial de Seguridad de la Información.
- Cada una de las partes de la contraseña se debe depositar en sobre sellado y lacrado y ser guardada en un sitio seguro dentro de las instalaciones de la Entidad.
- Proveedores y contratistas solo deberán cumplir con sus obligaciones contractuales, con un perfil y un rol específico en los respectivos sistemas de información. Estos accesos se otorgan siguiendo el procedimiento Gestión de usuarios.

4.2.4.7 Política sobre el uso de controles criptográficos basado en el proceso DSS05.06. La DTI debe establecer los algoritmos en clave y protocolos autorizados para práctica para la JEP, y establecer los sistemas para acceder solamente aquellos algoritmos autorizados, teniendo los datos de los grupos, con el resultado de separar algoritmos de en clave débiles. Se debe contemplar la práctica de algoritmos robustos y/o los protocolos SSL/TLS y nuevos controles criptográficos que posteriormente estén disponibles.

4.2.4.8 Política de gestión de llaves criptográficas basado en el proceso DSS05.06. Se deben cumplir las políticas sobre las llaves criptográficas para lograr proteger y aumentar la confidencialidad de información valiosa para la JEP y para los usuarios, una vez se inicie algún proceso de la siguiente manera:

- El periodo de vigencia de las llaves criptográficas gestionadas por la Jurisdicción Especial para la Paz - JEP será definido por la DTI.

- El periodo de vigencia de las llaves criptográficas gestionadas por terceros y utilizadas por la Jurisdicción Especial para la Paz - JEP, lo define el tercero que las gestiona.
- La administración de llaves criptográficas y certificados digitales gestionados por la Jurisdicción Especial para la Paz - JEP, deben estar a cargo de la DTI. Asimismo, la administración de llaves criptográficas y certificados digitales gestionados por terceros y utilizados por la Jurisdicción Especial para la Paz - JEP, están a cargo de la unidad usuaria.
- Los usuarios internos a quienes les sean asignados llaves criptográficas y certificados digitales, deben almacenarlos de manera segura cuando no los estén utilizando o cuando se ausenten de sus puestos de trabajo.

4.2.4.9 Normas puesto de trabajo limpios basado en el proceso - DSS05.05

- Principalmente, se establece un control tecnológico de solicitud de contraseña para la impresión y digitalización, con el objetivo de no dejar información sensible expuesta en las impresoras o scanners.
- Todos los usuarios internos deben proteger sus datos con contraseñas y apagar los equipos al finalizar la utilización de cada uno de los recursos tecnológicos dentro de la empresa.
- La DTI configura el bloqueo de sesión automático, después de la inactividad del usuario de cinco (5) minutos, de acuerdo con los requerimientos de seguridad de la información.
- Los usuarios internos de la Jurisdicción Especial para la Paz - JEP, cada vez que se ausenten de sus puestos de trabajo, deben bloquear el equipo de cómputo que es de su responsabilidad, para evitar que se pueda ver, tomar o copiar por terceros no autorizados.
- Los usuarios internos deben reducir el daño causado en equipos de cómputo por acciones inadecuadas (consumo de alimentos y/o bebidas, obstrucción de ventilación, ubicación inadecuada, entre otros). En caso de presentarse algún daño, será responsabilidad del custodio.

- Los equipos de cómputo cargarán por defecto el fondo de pantalla configurado por la DTI, el cual no puede ser modificado y debe permanecer activo.

4.2.4.10 Política de respaldo de información basado en el proceso DSS05.06. Dentro de la JEP, siempre se debe contar con lineamientos que nos lleven a obtener un bakcup, dentro de un rango determino el cual pueda servir de ayuda, al momento de estar en medio de un riesgo inminente de perdida de información, cumpliéndolo de la siguiente manera:

- La JEP, periódicamente debe realizar backups en los procedimientos de Gestión.
- Los datos sensibles de tipo institucional, que utilicen los usuarios internos, debe ser almacenada en el servidor de archivos de la red ("file server") identificado con la letra "X: Nombre_de_usuario:", el cual cuenta con el servicio de copia de respaldo diario. La información no sensible de tipo institucional, que utilicen los usuarios internos, debe ser almacenada en el servidor de archivos de la red ("file server") identificado con la letra "X: Nombre_de_usuario:" o OneDrive, teniendo en cuenta que, la copia de respaldo de la información almacenada en los servicios de Office 365, está sujeta a los lineamientos de respaldo de Microsoft.
- Los discos duros de los equipos de cómputo de escritorio y portátiles no deben contener información institucional, ya que a éstos no se les realiza copias de respaldo.
- La DTI no es responsable del respaldo de la información personal almacenada en los equipos de cómputo de escritorio o portátiles en caso de pérdida.
- Se debe conservar el registro de la ejecución de las copias de respaldo realizadas a los servidores de producción (archivos, sistemas operativos, bases de datos, aplicaciones, unidades de almacenamiento presentadas a los servidores) empleando el software destinado para tal fin.
- Registrar las fallas presentadas, con el fin de asegurar el correcto funcionamiento de estas en caso de restauración.

- Las copias de respaldo se deben probar cada seis meses, con el fin de asegurar que se puede depender de ellas en caso de contingencia.
- Las restauraciones de copias de respaldo solicitadas se deben realizar de acuerdo con el procedimiento de Copias de Respaldo y se podrán documentar como pruebas.
- Los datos contenidos en las copias de respaldo se deben realizar de acuerdo a las normas de la dirección estratégica.
- Las copias de respaldo se guardan únicamente con el objetivo de restaurar información en caso de situaciones como borrado de datos, incidente de seguridad de la información, defectos en los discos de almacenamiento, problemas de los servidores o equipos de cómputo, o que, por requisitos legales sea necesario recuperarla.
- Los usuarios internos son los responsables de almacenar la información que requiera copias de respaldo en el destino o recurso asignado por DTI, o solicitar formalmente la realización de copias de seguridad a información almacenada por fuera de estas.

4.2.4.11 Políticas y procedimientos de transferencia de información basado en el proceso DSS05.02

Para la solicitud de información de interés dentro de la JEP, los usuarios deben cumplir con una serie de condiciones para preservar la seguridad de la información que se le va brindar, de la siguiente manera:

- Los usuarios internos que requieren transferir interna o externamente información sensible (pública clasificada o publica reservada), deben firmar el “Acuerdo de confidencialidad”. Adicionalmente, se debe contar con la autorización previa de su jefe inmediato y se deben utilizar los medios aprobados por DTI para tal fin.

- Los usuarios internos deben seguir las indicaciones del procedimiento Transferencia de información, el cual contiene las directrices para tener en cuenta al momento de intercambiar información catalogada como pública clasificada o pública reservada.
- La transferencia o intercambio de información con entes de control y autoridades de supervisión, se rige por las directrices y mecanismos que dispongan dichos entes de control.
- Toda solicitud de transferencia o intercambio de información debe ser autorizada por el dueño del activo de información respectivo.
- La herramienta de cifrado de información es definida por la DTI.

4.2.4.12 Política de desarrollo seguro Basado en el proceso DSS05. El desarrollo de software dentro de la JEP, se realiza de forma excepcional, siempre y cuando no exista una solución en el mercado para cubrir la necesidad.

Etapas:

- Requerimiento con especificaciones funcionales detalladas por parte del usuario solicitante.
- Reunión de validación y entendimiento del requerimiento entre la DTI y el usuario solicitante.
- Estimación del cronograma de desarrollo y entrega para pruebas del requerimiento.
- Construcción de software.
- Pruebas unitarias por parte de la DTI.
- Pruebas integrales por parte del usuario.
- Aceptación del desarrollo por parte del usuario.
- Presentación del paso a producción a las partes interesadas.
- Puesta en producción del desarrollo.

- Seguimiento y ajustes.

4.2.4.13 Requisitos de seguridad de los sistemas de información basado en el proceso DSS05. La DTI debe puntualizar los requisitos de protección de los datos para los sistemas nuevos o mejoras a los sistemas existentes, contratados externamente o desarrollados al interno de la Jurisdicción Especial para la Paz - JEP.

Para ello, se deben tener en cuenta:

- Los requisitos de autenticación de colaboración con los privilegios que dan las credenciales para acceder a la información, un caso en particular, la implementación de segundos factores de autenticación, el uso de contraseñas fuertes, cambio habitual de contraseñas y que guarde una relación de contraseñas para impedir su reúso.
- El proceso de gestión para obtener credenciales y lograr acceder a los datos, para todos los interesados internos de acuerdo con los roles y/o privilegios establecidos.
- Áreas de trabajo que requieran contar con software desarrollado a la medida o soluciones de mercado deben solicitarlo a la DTI, dependencia que definirá los requisitos de seguridad de la información.

4.2.4.13.1 Seguridad en los procesos de desarrollo y soporte Control de cambios en sistemas

Todo proceso que este dentro del marco de desarrollo y de soporte para realizar algún procedimiento de modificación debe cumplir con los siguientes requisitos:

- Las mejoras continuas en los recursos tecnológicos de la empresa, se deben realizar de acuerdo a lo establecido en el modelo de gestión.

Principio de construcción de los sistemas seguros:

- La DTI define los manuales de seguridad para la construcción de sistemas de información, los cuales se deben aplicar a los desarrollos realizados por la JEP y a los contratados externamente.

Ambiente de desarrollo seguro:

- La DTI aplica los mismos controles del círculo de elaboración en el círculo de progreso, tales como, inspección de las credenciales, backups, reportes de eventos.
- La DTI debe implementar los controles necesarios para garantizar que las migraciones entre los ambientes de progreso y elaboración han sido aprobadas, de compromiso con la forma de cambios.
- La DTI debe tener sistemas de vigilancia de versiones para dirigir los cambios en los sistemas desarrollados dentro de la JEP.

Desarrollo contratado externamente:

- La DTI debe certificar que los sistemas adquiridos o desarrollados por terceros cuenten con un convenio de licencias en el cual se especifique el contexto de práctica del software y los derechos de posesión.
- La DTI debe pedir muestras de que se realizaron pruebas de protección al software desarrollado por terceros.
- • La DTI cuando contrate desarrollos externos debe garantizar que se realicen pruebas de aprobación del software, con la finalidad de comprobar el desempeño de los requisitos de protección acordados.
- La DTI debe contener en los acuerdos contractuales: la privación de que el software cumpla con las leyes y regulaciones aplicables, para ejecutar auditorías mientras el progreso de la contratación.

- La documentación de uso de los sistemas de información y aplicaciones deberá estar disponible para los usuarios internos y usuarios externos.

- Los reportes de los informes son de uso exclusivo de la DTI.

4.2.4.13.2 Ejecución de pruebas. Se debe requerir la realización de pruebas funcionales que incluyan la valoración de los requisitos de protección de los datos y la seguridad enfrente vulnerabilidades conocidas, como parte de los desarrollos o mejoras al software.

4.2.4.13.3 Pruebas de aceptación de sistemas, Antes de colocar a funcionar cualquier proceso en los sistemas de la JEP, se deben ejecutar pruebas previas para lograr un óptimo rendimiento, de la siguiente manera:

- Se deben ejecutar pruebas de aprobación del software desarrollado o renovado, con la finalidad de aprobar los requisitos de Protección de los datos y la adhesión a prácticas de perfeccionamiento de sistemas seguros (adonde sea aplicable). En estas pruebas se puede crear una rutina para utilizar herramientas automatizadas, tales como herramientas de estudio de códigos o escáneres de vulnerabilidad, y se debe comprobar que se han reformado los defectos conectados con la protección.

- De ser viable, las pruebas de aprobación se deben realizar en un círculo de pruebas objetivo, para afirmar que la técnica no introducirá vulnerabilidades al sistema de la JEP, y que las pruebas han sido confiables.

4.2.4.13.4 Datos de prueba. La DTI debe aprobar que los datos entregados a los desarrolladores para la realización de pruebas se enmascaran o que los datos sensibles están totalmente eliminados con la finalidad de no destapar los datos confidenciales de los ambientes de elaboración y, por ende, proporcionar desempeño bajo la Ley 1581 de 2012 (Ley de Protección de Datos Personales) y a la Ley 1712 de 2014 (Ley de Transparencia y Acceso a la Información pública).

4.2.4.14 Políticas para los proveedores. Ante cualquier evento de negociación con los proveedores, se debe tener en cuenta el control de la información y la confidencialidad de ella de la siguiente manera:

- Establecer mecanismos de control en las relaciones con sus proveedores o contratistas, con el objetivo de asegurar que la información a la que tengan acceso o los servicios que sean provistos por los mismos, cumplan con las políticas y procedimientos de seguridad de la información.
- Los Supervisores de contratos, deben asegurar la divulgación, aceptación y acatamiento de las políticas y operaciones de protección de los datos por parte de los proveedores o contratistas a su cargo.
- Sin privilegio, todos los proveedores o contratistas que manejen datos en progreso de su obligación contractual deben sellar el "Acuerdo de Confidencialidad de la Información", con el cual se comprometen a no publicar, utilizar o aprovechar los datos Íntimo a los que puedan acceder, en convenio con los niveles establecidos para la categorización de los datos.
- Sin excepción todos los proveedores o contratistas de la Entidad, que manejen datos personales deben realizar su tratamiento, la cual debe ser revisada por el proveedor o contratista para su entendimiento y aceptación.
- Los cambios en el suministro de servicios por parte de los proveedores o contratistas de la JEP, están gestionados a través del procedimiento Gestión de cambios, establecido por la DTI.
- Los proveedores o contratistas, que por razón de sus obligaciones contractuales deben tener acceso a los recursos tecnológicos de la organización, se le otorgará acceso a la red de datos institucional siguiendo los procedimientos establecidos por la DTI para tal fin.

- Todo mecanismo o sistema externo utilizado por los proveedores o contratistas para acceder a la plataforma tecnológica, debe ser autorizado por la DTI.
- Todos los proveedores o contratistas deben dar cumplimiento a las políticas de seguridad de la información y el Supervisor del contrato puede validar su cumplimiento cuando lo estime conveniente.
- La Supervisión de los contratos debe gestionar los riesgos de seguridad de la información y el plan de tratamiento de riesgos asociados con la cadena de suministro.
- Todos los proveedores o contratistas deben darle cumplimiento a la Política de Seguridad y Privacidad de la Información y las Políticas Complementarias de Seguridad de la Información incorporadas en este manual.
- Todo sistema externo utilizado por los proveedores o contratistas para acceder a la información, debe ser autorizado por la DTI.
- El software utilizado por los Proveedores o Contratistas debe ser legal y contar con la respectiva licencia que acredita su uso.

4.2.4.14.1 Política de no repudio. Para los procesos que se consideren críticos, se deben implementar mecanismos en los que no exista la oportunidad de retar la eficacia de un ejercicio el cual un responsable del proceso generó. Estos mecanismos deben garantizar la participación de las partes en el envío de la información, de tal manera que sea posible demostrar la identidad del emisor y se deben cumplir los siguientes requisitos:

- Los mecanismos a implementar deben contar con un tercero confiable y quien permita garantizar la plenitud y principio de los datos.

- Se debe disponer de registros que permitan evidenciar la trazabilidad de las acciones de formación, principio, admisión, transferencia de datos y otros, que sirven de seguridad para lograr autenticar el no repudio.
- Estos registros se deben salvaguardar frente al daño o alteración de tal modo que se garantice su medio y su compromiso.
- Se deben ejecutar auditorías continuas a los mecanismos de inspección y a los procesos, para poseer reportes cuando las partes implicadas posiblemente nieguen tener relación con un ejercicio específico.
- Cuando la DTI evidencie algún tipo de evento o incidente relacionado a la ejecución de acciones que eviten dejar trazabilidad de lo realizado, deben informarlo de manera oportuna al administrador o propietario del activo de información para que se tomen las medidas pertinentes.

4.2.4.15 Política de gestión de incidentes de seguridad de la información. Adentro de la JEP se establece responsabilidades a todos los usuarios internos y a las partes involucradas para la comunicación de eventos o incidentes de Protección de los datos en colaboración con la forma en la que se manejan los incidentes, señalados por la DTI, el cual permite garantizar una refutación rápida, efectiva y ordenada poniendo en marcha los siguientes puntos:

- Todas las fallas o anomalías que afecten la disponibilidad, integridad y disponibilidad de los activos de información (hardware, software, servicios, recursos humanos, información física y digital) deben ser reportadas oportunamente, como un evento o incidente de Seguridad de la Información y deben ser atendidos de acuerdo con el procedimiento Gestión de incidentes, establecido por la DTI.
- En los casos que el análisis del incidente requiera el descubrimiento, recaudación, caracterización, rotulado, transportación y custodia de testimonio de calidad digitalizada, se

deben utilizar los procedimientos para esta práctica, preservando las características de responsabilidad, confidencialidad, recurso, no abandono, innovación y realidad, logrando asimismo conservar su esfuerzo demostrativo para formar los procesos disciplinarios, judiciales y/o administrativos si tuviera parte obligatorio.

4.2.4.16 Política de gestión de activos de información basado en el proceso DSS05.07

4.2.4.16.1 Inventario de activos. Los propietarios de los activos de información que en el caso son los Lideres de Proceso, anualmente deben actualizar y documentar los activos de información de los cuales son responsables, siguiendo el procedimiento Gestión de activos de información, con el acompañamiento del Oficial de Seguridad de los datos en caso que se requiera.

4.2.4.16.2 Uso aceptable de los activos. Los activos de información tales como: información (física y digital), software, servicios y hardware propiedad, son proporcionados a los usuarios internos, para el desarrollo de sus funciones en la Entidad. Es responsabilidad del propietario y custodio de los activos de información, dar uso adecuado a los mismos, cumpliendo las políticas:

- Todos los usuarios internos son responsables de etiquetar la información, y darle una administración conveniente según su categorización, siguiendo las directrices de Encargo Evidente y el Explicativo de Activos tecnológicos.
- Los usuarios internos deben generar un informe sobre los eventos de protección de los datos identificados, relacionados con los recursos de incidentes, determinado por la DTI.

Prácticas en equipos de tratamiento de la información único de escritorio y portátiles:

- La DTI es la única unidad autorizada para la adquisición, asignación e instalación de equipos de computación personal, requeridos para soportar la operación de los usuarios internos
- La instalación y administración de todo componente de software y hardware a cargo de la DTI es de su responsabilidad y, por tanto, se debe realizar una solicitud siguiendo el procedimiento de Mesa de Ayuda definido para tal fin.
- Todos los cambios sobre la infraestructura tecnológica son responsabilidad de la DTI, y debe ser tramitado por los usuarios internos, siguiendo el procedimiento de Mesa de Ayuda definido para tal fin.
- Cualquier traslado de hardware dentro o fuera de las instalaciones, debe solicitar los procedimientos de Mesa de Ayuda definido para tal fin, y sólo el personal de la DTI coordinará el traslado de equipos de cómputo.
- La DTI junto con la Subdirección de Recursos Físicos e Infraestructura son los encargados para dar de baja cualquier elemento de hardware de propiedad de la JEP, en relación a los criterios y protocolos de seguridad previamente definidos y el procedimiento Borrado seguro de la información, con el fin de garantizar la no divulgación de datos confidenciales.
- Los equipos de cómputo portátiles asignados a los usuarios internos no podrán sacarse de las instalaciones, salvo autorización documentada del Jefe Inmediato y la Subdirección de Recursos Físicos e Infraestructura.
- Se debe respetar y no modificar la configuración de ningún programa dentro de la empresa. Si se presenta algún requerimiento de cambio de configuración se debe seguir el procedimiento de Mesa de Ayuda definido para tal fin.
- Se prohíbe sustraer información por ningún medio, con excepción de aquellos usuarios internos que, por sus funciones, sean autorizados por la DTI, de forma temporal o permanente.

- Toda diligencia informática (escaneos de protección, ataques de autenticación o de desaprobación de asistencia, etc.) no autorizada que afecte en proporción las redes corporativas como los sistemas, está prohibida y dará término a los procesos disciplinarios o legales según corresponda.
- Es responsabilidad de todos los usuarios internos apagar o hibernar los equipos que no estén prestando servicio.
- Los equipos de tratamiento de la información, servidores, teléfonos IP y equipos de comunicación, deben conectarse a los puntos de frecuentes eléctricas identificados como regulados establecidos dentro de la empresa, excepto las impresoras que pueden conectarse a las tomas blancas.
- Los puntos eléctricos de los equipos de procesamiento de datos personales deben hacerse por medio de los puntos eléctricos no regulados. No se responsabiliza por daños que no puedan resistir estos dispositivos.
- Los equipos que ingresen dentro de la JEP y que no son de su propiedad, son responsabilidad única y exclusiva de sus propietarios. La Jurisdicción Especial para la Paz - JEP, no es responsable por estos equipos en ningún caso.

4.2.4.16.3 Uso de la Intranet y de Internet. Los usuarios internos son responsables del acceso a la Intranet y a sus contenidos. El servicio de la intranet y de Internet es exclusivo para el perfeccionamiento de sus oficios, el cual le corresponden desempeñar con los siguientes lineamientos propuestos a la JEP:

- La DTI debe implementar las herramientas tecnológicas y los controles necesarios para mitigar los riesgos de la navegación en internet. Asimismo, debe promover entre los usuarios

internos, el uso responsable del servicio de navegación en Internet, mediante actividades de sensibilización desarrolladas con el apoyo de las áreas encargadas (Subdirecciones de Comunicaciones, Talento Humano, Fortalecimiento Institucional, entre otras.

- Está prohibido el uso de la infraestructura tecnológica para fines comerciales, o algún tipo de acoso, difamación o calumnia.
- Está prohibido, establecer cualquier instrumento para ejecutar el monitoreo de puertos o examen de intercambio de puntos, por personas diferentes a la DTI. Los usuarios internos no deben pretender hostigar los sistemas de protección y de comprobación de las credenciales; acciones de esta particularidad se consideran violatorias de las políticas de la Jurisdicción Especial para la Paz - JEP y de la ley y serán sancionadas de acuerdo con la Ley 734 de 2002 (Código Único Disciplinario).
- Está prohibido enlazar módems o cualquier aparato celular (en forma Access Point) para permitir a internet, adentro de la malla de la Jurisdicción Especial para la Paz - JEP.
- La DTI cuando lo considere necesario puede monitorear la infraestructura (Software y Hardware).

4.2.4.16.4 Uso del correo electrónico. Se provee a todos los usuarios internos un correo electrónico institucional en el dominio jep.gov.co para el ejercicio de sus labores, el cual deben utilizar solo de manera institucional, cumpliendo con las políticas expuestas a continuación:

- El e-mail corporativo es propio y personal y, por ende, los usuarios internos están completamente responsabilizados de todas las actividades realizadas con sus credenciales.
- El e-mail corporativo se debe emplear estrictamente como instrumento de información, que solo va ser utilizado para transferir datos relacionados única y solamente con el progreso de las funciones misionales y de soporte asignadas.

- Toda información enviada o publicada a través del correo o el sitio web de la JEP, debe llevar un texto que prevenga sobre la posibilidad de ser información confidencial y al tratamiento permitido cuando es recibida por alguien que no es su destinatario.
- Los correos electrónicos sospechosos deben tratarse con extremo cuidado, por lo tanto, no está permitido abrir sus archivos adjuntos y se debe reportar el evento Comité de Gestión de acuerdo con el procedimiento Gestión de incidentes.

4.2.4.16.5 Devolución de activos. La devolución de activos por terminación o cambio de empleo se controla siguiendo las directrices del procedimiento Gestión de activos de información.

4.2.4.16.6 Clasificación de la información. La JEP clasifica, etiqueta y maneja la información y sus activos asociados de acuerdo con el procedimiento e instructivo de Gestión de Activos de Información y los lineamientos de Gestión Documental.

4.2.4.16.7 Gestión de medios removibles (unidades de almacenamiento). Toda información institucional debe ser enviada a los correos de los administrativos o usuario final, con el fin de mantener la confidencialidad de la información, sin ninguna excepción como se expone a continuación:

- Se prohíbe el uso de medios extraíbles (USB, celulares, discos externos, CD, DVD, entre otros) para almacenamiento de información institucional, con excepción de aquellos usuarios internos que, por sus funciones, sean autorizados por la DTI, de forma temporal o permanente. Para lo anterior el usuario interno debe tener en cuenta el procedimiento Gestión de medios removibles.
- La ejecución de sistemas operativos desde medios removibles en las estaciones de trabajo está bloqueada desde el BIOS del sistema y el acceso a la misma está protegido por contraseña.

- El almacenamiento, etiquetado y eliminación de la información contenida en los medios removibles, debe ser acorde con el esquema de clasificación de la entidad y debe seguir el procedimiento Gestión de medios removibles.
- Las unidades de medios removibles de las estaciones de trabajo y equipos de cómputo portátiles pertenecientes a la Jurisdicción Especial para la Paz - JEP están bloqueadas para booteo, desde el BIOS (Sistema básico de entrada y salida, la cual hace referencia a la utilidad que se ejecuta al momento de encender el equipo de cómputo) y el acceso a esta funcionalidad requiere contraseña.
- La Oficina Asesora de Seguridad y Protección controla el ingreso y salida de los equipos de cómputo y medios extraíbles de almacenamiento de información de las instalaciones de la Jurisdicción Especial para la Paz - JEP, de acuerdo con los lineamientos establecidos por esta oficina.
- Los medios removibles en los que se almacene información catalogada como información pública clasificada e información pública reservada deben estar cifrada.

4.2.5 Disposición de los medios. La disposición de los medios cuando ya no se requieran se realiza de acuerdo con el procedimiento seguro de la información.

4.2.6 Transferencia de medios físicos. La Jurisdicción Especial para la Paz - JEP realiza actividades de inducción y reinducción a los usuarios internos, con el fin de asegurar que se conozcan, entiendan y cumplan las responsabilidades de seguridad de la información, de la siguiente manera:

- La transferencia de medios físicos se realiza siguiendo los lineamientos de la DTI.
- Política de capacitación y sensibilización en seguridad de la información.

- La Jurisdicción Especial para la Paz - JEP debe asegurar que todos los usuarios internos que tengan definidas responsabilidades de seguridad de la información sean competentes (en cuanto a capacitación formal y no formal) para desempeñar sus funciones. Para ello, la Subdirección de Fortalecimiento elabora anualmente el Plan Anual de Capacitación, en donde se incluyen los temas sugeridos por la DTI en cabeza del Oficial de Seguridad de la Información.

4.2.7 Separación de deberes. Todo aquel que tenga acceso a la información de la Jurisdicción Especial para la Paz - JEP, debe tener claramente definidas sus funciones y actividades, con el fin de reducir el uso no autorizado, indebido o accidental de los activos de información.

Todos los sistemas de información de la Jurisdicción Especial para la Paz - JEP deben implementar reglas de acceso, de tal forma que haya segregación de funciones entre quien administre, opere, mantenga, audite y, en general, tenga la posibilidad de acceder a los sistemas de información, así como entre quien otorga los privilegios y quien lo utiliza.

4.3.1 Revisión de las políticas para la seguridad de la información basado en el proceso DSS05.07. La Política de Seguridad y Privacidad de la Información, y el Manual del Sistema de Gestión de Seguridad y Privacidad de la Información – SGSPI deben ser revisados y actualizados (en caso de ser necesario) a intervalos planificados o cuando se presenten cambios relevantes en el contexto estratégico de la Jurisdicción Especial para la Paz - JEP, con el fin de asegurar que sigan siendo adecuados a su estrategia y necesidades.

Según el Artículo 10 del Acuerdo AOG No. 045 de 10 septiembre de 2019, la Política de Seguridad y Privacidad de la Información debe ser aprobada por el Órgano de Gobierno y el

Manual del Sistema de Gestión y Privacidad de la Información – SGSPI por el Comité de Gestión para la Administración de Justicia de la Jurisdicción Especial para la Paz - JEP.

4.3.1.1 Controles adicionales

4.3.1.1.1 Seguridad física y del entorno basado en el proceso DSS05.05

4.3.1.1.1.2 Áreas seguras. Dentro de la JEP, se deben crear áreas que solo sean destinadas a cumplir con un proceso especifico, el cual sirva para cumplir con la gestión de la seguridad de la información, protegiendo y especificando de qué tipo de sensibilidad es la información:

- Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido (incluido los activos albergados en los Proveedores). En consecuencia, deben contar con medidas de control de acceso físico en el perímetro tales que puedan ser auditadas, así como con procedimientos de seguridad operacionales que permitan proteger la información, el software y el hardware de daños intencionales o accidentales.
- Los controles para prevenir el acceso físico no autorizado a las instalaciones de la Jurisdicción Especial para la Paz - JEP, son descritos en el procedimiento Trabajo en áreas seguras.
- El acceso de visitantes a las áreas restringidas de la DTI, como son Datacenters, cuartos de control, de cableado, de comunicaciones, telefónicos etc., debe contar con un procedimiento o protocolo de acceso físico aprobado por la DTI, independientemente de su ubicación física, ya sea en las instalaciones de la Jurisdicción Especial para la Paz - JEP o en las instalaciones del proveedor.

- La DTI debe asegurar que las áreas de acceso restringido como son Datacenters, cuartos de control, de cableado, de comunicaciones, telefónicos etc., cuenten con el equipamiento mínimo requerido para asegurar el cumplimiento de los requisitos. ambientales, físicos y de energía necesarios para soportar su operación. Independientemente de la ubicación física, ya sea en las instalaciones de la Jurisdicción Especial para la Paz - JEP o en las instalaciones del proveedor.

4.3.1.1.2 Mantenimiento de equipos. La DTI coordina las labores de mantenimiento correctivo y preventivo a los equipos de propiedad de la Jurisdicción Especial para la Paz - JEP, las cuales están subcontratadas, y realiza seguimiento a la ejecución de los planes anuales de mantenimiento.

El mantenimiento de los equipos de la Jurisdicción Especial para la Paz - JEP se debe realizar aplicando las políticas y controles de seguridad de la información descritos en el presente documento y de acuerdo con el procedimiento Mantenimiento de software y hardware.

4.3.1.1.3 Seguridad de equipos y activos fuera de las instalaciones. La salida de equipos de cómputo de propiedad de la Jurisdicción Especial para la Paz - JEP es controlada por la Oficina Asesora de Seguridad, se debe cumplir con los siguientes lineamientos:

- Los equipos de cómputo portátiles y medios removibles de propiedad de la Jurisdicción Especial para la Paz – JEP y que requieran ser retirados de las instalaciones, debe ser protegidos cifrando la información contenida en ellos, a través de la herramienta definida por la DTI.
- Los usuarios internos que retiren equipos de cómputo o medios removibles de las instalaciones de la Jurisdicción Especial para la Paz - JEP deben seguir las siguientes directrices:

- En ninguna circunstancia los equipos de cómputo portátiles pueden ser dejados desatendidos en lugares públicos o a la vista, en el caso que esté siendo transportado en un vehículo.
- Los equipos de cómputo portátiles siempre deben ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a fuertes campos electromagnéticos, vibraciones o golpes.
- En caso de pérdida o robo de un equipo de cómputo portátil de propiedad de la JEP, se debe adelantar la denuncia ante la autoridad competente e informar inmediatamente al jefe de la Dependencia/Área y a la DTI para que se inicie el trámite interno correspondiente.

4.3.1.1.4 Protección contra códigos maliciosos. La DTI debe seleccionar, adquirir, instalar y mantener un software antivirus apropiado para salvaguardar la información, equipos de cómputo de escritorio o portátiles y servidores que son propiedad la Jurisdicción Especial para la Paz - JEP.

Se deben reportar todos los eventos relacionados con el software antivirus (desactualización, aviso de expiración, alertas de virus), y seguir el procedimiento Gestión de incidentes.

4.3.1.1.5 Registro y supervisión

4.3.1.1.6 Registro de eventos. Los sistemas operativos, servicios y sistemas de información que forman parte de la infraestructura para el procesamiento de información y comunicaciones de la Jurisdicción Especial para la Paz - JEP, deben generar archivos de registro de eventos (logs) definidos en conjunto por los responsables de su administración.

La DTI debe identificar el nivel de monitoreo requerido para las aplicaciones y dispositivos tecnológicos, e implementar los controles necesarios para llevar a cabo dichas

actividades. Además, debe monitorear el rendimiento de la infraestructura tecnológica prestando especial atención a los servicios en red a través del procedimiento Gestión de la capacidad.

4.3.1.1.5.2 Protección de la información de registro. Se debe tener en cuenta la siguiente información para lograr un registro eficiente dentro de la JEP:

- Las cuentas de usuario (del sistema operativo) de los usuarios internos son administradas mediante directorio activo, a través del cual se limita el acceso de estos a herramientas administrativas y, en este caso, a la manipulación de los registros de eventos (logs).
- La DTI con el fin de proteger la información de registro de modificación por parte de usuarios no autorizados, administradores u operadores de los sistemas de información, implementa mecanismos de copiado de logs a un sistema por fuera del control de administradores y operadores de los sistemas.

4.3.1.1.5.3 Sincronización de relojes. Con el fin de obtener un control apropiado para la relación adecuada de eventos no deseados en la infraestructura o para la investigación efectiva de incidentes, los relojes de los diferentes equipos de cómputo, servidores y sistemas de información utilizados por la Jurisdicción Especial para la Paz - JEP, deben estar sincronizados con la hora legal colombiana.

4.3.1.1.6 Control de software operacional

4.3.1.1.6.1 Instalación de software en sistemas operativos

- Controlar la instalación de software en sistemas operativos por medio del procedimiento Instalación de software.
- Todo software debe contar con un soporte técnico para garantizar su funcionamiento.

- Se debe suministrar aprendizaje adecuada a los usuarios y a los de recursos humanos en los aspectos de maniobra y funcionalidad de los nuevos sistemas o mejoras a sistemas existentes, precedentemente de su postura en marcha.
- Todos los sistemas nuevos y mejorados deben quedar completamente soportados por un expediente suficientemente amplia y actualizada, y no deben estar puestos en el círculo de elaboración a excepción de tener en cuenta el expediente disponible.

4.3.1.1.6.2 Gestión de la vulnerabilidad técnica. La DTI debe crear y elaborar reportes de los incidentes presentados anteriormente para su posterior estudio de las debilidades y/o hacking ético para las plataformas críticas.

Cuando se requiera realizar un cambio en las plataformas tecnológicas a fin de corregir dichas vulnerabilidades, se debe seguir las directrices del procedimiento Gestión de cambios.

4.3.1.1.7 Seguridad en las comunicaciones

4.3.1.1.7.1 Gestión de la seguridad en las redes

Se debe cumplir con los siguientes protocolos de Red, para lograr instalar y mantener los puntos de red dentro de la JEP, de la siguiente manera:

Red cableada:

- La DTI debe instalar y mantener, con personal calificado y debidamente autorizado, la red de voz y datos, con el fin de garantizar la operación, seguridad e integridad.
- Cualquier equipo o elemento activo o pasivo de la red que no se utilice debe ser desactivado y controlado. No está autorizada la instalación de ningún equipo de red, diferente a los equipos que pertenecen a la Jurisdicción Especial para la Paz - JEP.
- No está permitido realizar seguimiento o monitoreo de puertos o tráfico de red, por parte de personas diferentes a las autorizadas por la DTI.

- Cumplimiento de requisitos legales y contractuales
- Identificación de la legislación aplicable y de los requisitos contractuales
- El oficial de seguridad de la información junto con el área responsable de la actualización del Normograma.

4.3.1.2.1 Derechos de propiedad intelectual. La DTI realiza revisiones periódicas (al menos semestralmente), con la finalidad de garantizar que cualquiera software que se ejecute esté privilegiado por derechos de productor y requiera estar licenciado para posteriormente utilizarlo, se debe verificar su información de la siguiente manera:

- Los Supervisores de contratos deben asegurarse de que se hayan incluido.
- El uso de firmas escaneadas por parte de los usuarios internos de la JEP está prohibido. Por el cual, de ser requerido, el único mecanismo autorizado para firmar virtualmente documentos digitales es la firma digital. Es importante resaltar que las firmas digitales deben ser adquiridas por la Jurisdicción Especial para la Paz - JEP en entidades de certificación digital avaladas, previa autorización del Jefe Inmediato.

4.3.1.2.2 Protección de registros. Se tiene la obligación de proteger los reportes realizados en contra la pérdida, destrucción o falsificación, de acuerdo con lo establecido por Gestión Documental y por este manual.

4.3.1.2.3 Revisiones de Seguridad de la Información

4.3.1.2.3.1 Revisión independiente de la Seguridad de la Información

La Subdirección de Control Interno realiza auditorías internas al menos una vez al año, siguiendo las directrices para el desarrollo de auditorías internas.

Los jefes de dependencia deben revisar con regularidad (al menos semestralmente) el cumplimiento de las políticas y procedimientos del Sistema de Gestión de Seguridad y Privacidad de la Información - SGSPI dentro de su área de responsabilidad.

4.3.1.2.3.2 Revisión del cumplimiento técnico. La DTI debe coordinar la revisión técnica periódica (al menos semestralmente) de los sistemas de información utilizados en la Jurisdicción Especial para la Paz - JEP, para determinar el cumplimiento con las políticas y procedimientos del Sistema de Gestión de Seguridad y Privacidad de la Información - SGSPI.

4.3.1.2.4 Seguridad de la información en la gestión de contratación. La seguridad de la información se debe integrar en la gestión de la contratación, para asegurar que los riesgos de seguridad de la información se identifiquen y traten como parte de los proyectos. Lo anterior aplica a cualquier contrato, independientemente de su naturaleza. Por lo tanto, es responsabilidad de los directores, subdirectores / jefes de dependencia, asegurar que se sigan las siguientes directrices:

- Incluir objetivos de seguridad de la información en las obligaciones generales del contrato.
- Realizar identificación y valoración de los riesgos de seguridad de la información en los documentos justificativos de la contratación, para identificar los controles necesarios.
- Realizar seguimiento a los riesgos de seguridad de la información identificados y a los controles aplicados para tratar los mismos, durante las diferentes etapas de la contratación.

Capitulo 5. Conclusión

Considerando los estándares aplicables a la seguridad de la información en el contexto de la JEP, se identificaron previamente la administración de los datos de los usuario que se manejan por fuera y por dentro de la empresa, al realizar el diagnóstico por medio de la encuesta a los funcionarios de la JEP donde se muestra como el flujo de información no mantiene una línea auditable, el cual es un riesgo dentro de la empresa, el no saber cómo están los procesos dentro de la misma, teniendo como debilidad principal el no saber que cuentan con un departamento de TI; algo contradictorio ya que tienen como principal objetivo fortalecer la infraestructura tecnológica que tienen dentro de la JEP; así mismo se plantean las buenas prácticas y las legislaciones y modelos adecuados para las organizaciones públicas, como son la ISO27000, los lineamientos de la MINTIC y el COBIT 5, con el cual se propone un repositorio único de información, el cual nos brinda una seguridad de la información, acorde a lo determinado en los planes tecnológicos en la JEP.

Una vez realizado el diagnóstico basado en el instrumento planteado, con el objetivo de solventar las debilidades y riesgos que se presentan dentro de la JEP, el cual sirve para tomar como referentes la protección de datos, estándares asociados para el Modelo de Gestión el cual ayudan a fortalecer los procesos dentro de la empresa, asociándolos con los Procesos y Subprocesos de APO13 y DSS05, el cual fueron seleccionados por que se enfocan en la manera de realizar los procesos organizados y eficiente, cumpliendo con una serie de requisitos, el cual apoyan cada uno de los procesos expuestos anteriormente.

Se dio consecución al objetivo presentado para la comprobación, estudio y valoración del trabajo realizado por el desarrollo en el cuadro del modelo PHVA decidido en la determinación de los procesos y los procedimientos determinados en los criterios de implementación de los procesos de COBIT 5, integrándolos al modelo de manera que cada actividad propuesta sea cumplida y puesta en práctica de acuerdo en lo establecido por APO13 que se encarga específicamente de gestionar la seguridad cumpliendo como meta la gestión de riesgo del negocio y DSS05 que se encarga de gestionar los servicios de seguridad complementándose así cada proceso para una excelente aplicación del Modelo en la JEP.

Capitulo 6. Recomendaciones

- Se necesita tener en cuenta el ciclo PHVA dentro del modelo de Gestión de TI, ya que lo que puede ser crítico hoy para la empresa puede dejar de tener importancia con el tiempo.
- Se recomienda que la JEP elabore planes que permitan realizar un seguimiento constante a los roles diseñados y del cumplimiento de las responsabilidades de cada encargado de las dependencias dentro de la JEP.
- Generar planes de capacitación y controles basados en los procesos de COBIT 5 y la Norma ISO 27001:2013, que involucren a las partes externas e internas, las cuales deben garantizar la confiabilidad, integridad y disponibilidad de la información, por medio del cumplimiento de la normatividad y leyes vigentes que rigen a la JEP.
- De igual manera este modelo también puede ser replicado en otras instituciones de acuerdo a sus necesidades, pero para ello primordialmente es de suma importancia realizar un diagnóstico que permita determinar con certeza cuales son los vacíos de la empresa.

Referencias

Aroni Córdova, N., & Barrios Elías, R. (2018). Análisis de los principales factores financieros, operacionales y de reputación empresarial que vienen siendo impactados por el incremento de los delitos informáticos en los principales bancos del Perú como son Banco de crédito del Perú. Lima: Universidad Peruana de ciencias aplicadas.

Baquerizo Anastasio, M. (2014). Modelo de seguridad para sistemas E-Gobierno mediante satisfacibilidad Booleana. Madrid: Universidad Complutense de Madrid.

Camargo Barbosa, J. A., Velásquez Pérez, T., & Castro Silva, H. F. (2020). Modelo gobierno de TI en el mundo globalizado análisis en la industria Colombiana. Ecoe Ediciones.

Cano, J. (2016). Fraude informático: viejos trucos, nuevos entornos. Medellín: ACIS.

Castro Márquez, D., Velásquez Pérez, T., & Castro Silva, H. F. (2020). Estándares y buenas prácticas de tecnologías de la información en empresas colombianas del sector asegurador. Ecoe Ediciones.

Colprensa. (19 de Julio de 2019). Vanguardia. Obtenido de Más del 55% de los crímenes cibernéticos en Colombia son a cuentas bancarias: https://www.vanguardia.com/colombia/mas-del-55-de-los-crimenes-ciberneticos-en-colombia-son-a-cuentas-bancarias-BX1213056

Congreso de la Republica. (1999). LEY 527 de 1999. 1-19.

Congreso de la Republica. (2000). LEY 594 DE 2000. Bogotá.

Congreso de la Republica. (2008). Ley Estatutaria 1266 de 2008. 1-17.

Congreso de la Republica. (2009). LEY 1273 DE 2009. Bogotá.

Congreso de la Republica. (2012). LEY 1581 DE 2012. Bogotá.

García Velásquez, D. (2014). Metodología basada en el cómputo forense para la investigación de delitos informáticos. México: Universidad Nacional Autónoma de México.

Gómez, R., Pérez, D., Donoso, Y., & Herrera, A. (2010). Metodología y gobierno de la gestión de riesgos de tecnologías de la información. Revista de Ingeniería, 11.

Gómez González, E. (2015). Gobernanza Corporativa de la Tecnología de la información (T.I) (Auditoría y control según la norma UNE-ISO/IEC 38500:2013). Leganés: Universidad Carlos III de Madrid.

JEP. (abril de 2018). Jurisdicción Especial para la Paz. Obtenido de JEP: https://www.jep.gov.co/JEP/Paginas/Mision-vision-objetivos.aspx

Levet Rivera, C., Espinoza Maza, J., Macgluff Issasi, A., & Fragozo Teran, J. (2019). La inconclusa reforma al Código Penal Federal en materia de delitos informáticos. Interconectando Saberes, 12.

López Quilumbanco, C. (2019). Gobierno de TI basado en el esquema Gubernamental de seguridad de la información EGSI en el Hospital. Ibarra - Ecuador: Universidad Técnica del Norte.

Loredo González, J., & Ramírez Granados, A. (2013). Delitos informáticos: su clasificación y una visión general de las medidas de acción para combatirlo. Celernet, 8.

Montañez Parraga, A. (2017). Análisis de los delitos informáticos en el actual sistema penal colombiano. Bogotá: Universidad Libre.

Narváez Figueroa, H. (2016). Modelo de gobierno de TI para la gestión de la empresa SAITEL Matriz Ibarra. Ambato: Universidad Regional Autónoma de los Andes.

Navarro Asencio, E., Jiménez García, E., Rappoport Redondo, S., & Thoilliez Ruano, B. (2017). Fundamentos de la investigación y la innovación educativa. Universidad internacional de la Rioja, 1-61.

Novoa Gutiérrez, E. (2018). Ingeniería Social como delito informático en las grandes empresas colombianas. Bello Antioquia: Universidad Nacional Abierta y a Distancia UNAD.

Ojeda Pérez, J., Rincón Rodríguez, F., Arias Flórez, M., & Daza Martínez, L. (2010). Delitos informáticos y entorno jurídico vigente en Colombia. Bogotá.

Parada, R., & Errecaborde, J. (2018). Cibercrimen y Delitos Informáticos. Buenos Aires: ERREIUS.

Parra Calderón, J. (2019). Delitos informáticos y Marco Normativo en Colombia. Pitalito - Huila: Universidad Nacional Abierta y a Distancia UNAD.

Peñaranda Suarez, J. (2017). Diagnóstico de seguridad al sistema informático de gestión de contratos de prestación de servicios (CPS) de la universidad del rosario. Ocaña: Universidad Francisco de Paula Santander Ocaña.

Pillo-Guanoluisa, D., & Enríquez Reyez, R. (2017). Gobierno de TI con énfasis en seguridad de la información para hospitales públicos. 1-15.

Pulido Barreto, A., & Mantilla Rodríguez, J. (2016). Modelo para la implementación del sistema general de seguridad informática y protocolos de seguridad informática en la oficina TIC de la alcaldía municipal de Fusagasugá basados en la gestión del riesgo informático. Fusagasugá: Universidad Nacional Abierta y a Distancia.

Pulido, J., & Bohada, J. (2013). Risk Analysis in security of information. Revista ciencia, innovación y tecnología, 15.

Ramos, M., Solares, P., & Romero, E. (2014). Gobierno y Riesgo de TI. ECORFAN, 16.

Rincón López, C. (2016). Diseño de un framework para el gobierno de información con base en COBIT. Medellín: Universidad Nacional de Colombia - sede Medellín.

Rodríguez, D., Erazo, J., & Narváez, C. (2019). Técnicas cuantitativas de investigación de mercados aplicadas al consumo de carne en la generación millenial de la Ciudad de Cuenca (Ecuador). Revista Espacios, 1-12.

Rubio, I. (24 de octubre de 2019). El PAIS. Obtenido de "Antes debía entrar en tu casa. Ahora puedo conseguir toda tu información desde un ordenador": https://elpais.com/tecnologia/2019/10/17/actualidad/1571331272_536501.html

UNODC. (2013). Estudio exhaustivo sobre el delito cibernético. Nueva York: Naciones Unidas.

Valdivieso Suarez, X. (2019). Metodología de investigación cuantitativa en trabajos de graduación de la modalidad de titulación de la carrera de contabilidad y auditoría. Universidad Técnica de Machala, 1-22.

Vásquez Zarate, K., & Cárdenas Rodríguez, M. (2016). Propuesta de Buenas prácticas para fortalecer los controles de Prevención y Detección temprana del Cibercrimen en las Empresas Colombianas. Bogotá: Pontificia Universidad Javeriana.

Velásquez, T. Establecimiento De Criterios De Gobernabilidad De TI En Las Empresas Colombianas. Universidad de los Andes. Mérida. Venezuela. 2010.

Apéndices

Apéndice A.

PROPÓSITO	CONCEPTUALIZACIÓN	DIMENSIONES	SUBDIMENSIONES	INDICADORES
Diagnosticar los riesgos inherentes a la jurisdicción especial para la paz.	**Gestión de TI** **Seguridad de la Información**	Catalizador personas, habilidades y competencias. **DSS05** Gestionar Servicios de Seguridad	Métricas para el logro de objetivos. Métricas para la aplicación de prácticas. **DSS05.01** Proteger contra software malicioso (Malware) **DSS05.02** Gestionar la seguridad de la Red y las conexiones. **DSS05.03** Gestionar la seguridad de los puestos de usuario final. **DSS05.04** Gestionar la identidad del usuario y el acceso lógico.	Partes interesadas. Objetivos Ciclo de Vida Buenas prácticas. Metas de TI Métricas de TI Elementos claves

		DSS05.05 Gestionar el acceso físico a los activos de TI.	
		DSS05.06 Gestionar documentos sensibles y dispositivos de salida.	
		DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad.	
		APO13.01 Establecer y mantener un SGSI	Metas de TI Métricas de TI Elementos claves
	APO13 Gestionar la Seguridad	**APO13.02** Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.	
		APO13.03 Supervisar y revisar el SGSI.	
JEP			

	Entidades públicas	Procesos	Actividades Resultados Indicadores

Apéndice B.

ENCUESTA ADMINISTRATIVOS JEP

1. ¿La JEP cuenta con un Departamento de TI?

Si

No

Desconoce

2. ¿La JEP cuenta con una División de Seguridad de la información?

Si

No

Desconoce

3. ¿Cómo considera la cantidad de inversión en infraestructura y equipo en TI dentro de la JEP?

Muy Buena

Buena

Media

Baja

Muy Baja

Desconoce

4. La JEP prioriza los gastos de TI en:

Adquirir o actualizar Hardware

Adquirir o actualizar Software

Mejorar la Seguridad de la Información

Protección de los activos de la empresa

5. ¿Todos los usuarios están identificados de manera única y tienen derechos de acceso de acuerdo con sus roles en la JEP?

Si

No

Desconoce

6. ¿Se han implementado medidas físicas para proteger la información de accesos no autorizados, daños e interferencias dentro de la JEP?

Si

No

Desconoce

7. Dentro de la JEP ¿La información se clasifica según su tipo de confidencialidad (Confidencial, privada y pública)?

Si

No

Desconoce

8. Indique cual es la principal amenaza en proteger dentro de la infraestructura tecnológica de la JEP:

Cyber ataques

Desastres naturales

Espionaje

Virus, caballos de troya, gusanos

Otro

9. ¿Se revisan regularmente los registros de eventos para detectar incidentes potenciales?

Si

No

Desconoce

10. ¿Se realizan capacitaciones de concienciación de seguridad física?

Si

No

Desconoce

11. ¿Cree usted que se logrará un cambio positivo con la aplicación de este Modelo de Gestión de seguridad de la información dentro de la JEP?

Si

No

Desconoce

12. ¿Se revisa y evalúa regularmente la información sobre nuevas posibles amenazas?

Si

No

Desconoce

13. ¿Dentro de la JEP se gestiona un plan de tratamiento del Riesgo de la Seguridad de la información?

Si

No

Desconoce

14. ¿Dentro de la JEP se define un portafolio de acciones para la gestión del Riesgo?

Si

No

Desconoce

15. ¿La información dentro de la JEP, procesada, almacenada y transmitida a los usuarios final está protegida?

Si

No

Desconoce