ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

DESARROLLO DE UN PLAN DE SEGURIDAD INFORMÁTICA QUE PERMITA LA CONFIDENCIALIDAD INTEGRIDAD Y DISPONIBILIDAD DE LA INFORMACIÓN EN EL JUZGADO DE LA NIÑEZ Y ADOLESCENCIA DE LA CIUDAD DE QUITO

CHRISTIAN ALBERTO COSTALES ESPINOZA

Trabajo de Titulación modalidad: Proyectos de Investigación y Desarrollo, presentado ante el Instituto de Posgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del grado de:

MAGÍSTER EN SEGURIDAD TELEMÁTICA

RIOBAMBA-ECUADOR

Julio 2021

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

CERTIFICACIÓN:

EL TRIBUNAL DEL TRABAJO DE INVESTIGACIÓN CERTIFICA QUE:

El **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo,** denominado DESARROLLO DE UN PLAN DE SEGURIDAD INFORMÁTICA QUE PERMITA LA CONFIDENCIALIDAD INTEGRIDAD Y DISPONIBILIDAD DE LA INFORMACIÓN EN EL JUZGADO DE LA NIÑEZ Y ADOLESCENCIA DE LA CIUDAD DE QUITO, de responsabilidad de Christian Costales, ha sido minuciosamente revisado y se autoriza su presentación.

Tribunal:

Ing. Oswaldo Geovanny Martínez Gaushima; Mag.

PRESIDENTE

Firmado digitalmente por OSWALDO GEOVANNY MARTINEZ GUASHIMA

OSWALDO GEOVANNY MARTINEZ GUASHIMA

Ing. Christian Fernando Barragán Quizhpe; Mag.

DIRECTOR

Firmado electrónicamente por: **CHRISTIAN FERNANDO BARRAGAN QUIZHPE**

Ing. Danilo Geovanny Barreno Maranjo; Mag.

MIEMBRO

DANILO GEOVANNY BARRENO NARANJO

Firmado digitalmente por DANILO GEOVANNY BARRENO NARANJO
Fecha: 2021.07.06 14:46:02 -05'00'

Ing. Darwin Paúl Carrión Buenaño; Mag.

MIEMBRO

Firmado electrónicamente por: **DARWIN PAUL CARRION BUENANO**

Riobamba, julio 2021

DERECHOS INTELECTUALES

Yo, Christian Costales, declaro que soy responsable de las ideas, doctrinas y resultados expuestos en el Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo y que el patrimonio intelectual generado por la misma pertenece exclusivamente a la Escuela Superior Politécnica de Chimborazo.

Firmado electrónicamente por:
CHRISTIAN ALBERTO COSTALES ESPINOZA

Christian Alberto Costales Espinoza

No. Cédula: 171959385-5

DECLARACIÓN DE AUTENTICIDAD

Yo, Christian Costales, declaro que el presente proyecto de investigación, es de mi autoría y que los resultados del mismo son auténticos y originales. Los textos constantes en el documento que proviene de otras fuentes están debidamente citados y referenciados.

Como autor, asumo la responsabilidad legal y académica de los contenidos de este Trabajo de Titulación de Maestría.

Firmado electrónicamente por:
CHRISTIAN ALBERTO
COSTALES ESPINOZA

Christian Alberto Costales Espinoza

N.º de Cédula: 171959385-5

DEDICATORIA

La presente tesis la dedico con mucho cariño y devoción a mis padres, amada esposa e hijos.

- Madre querida, madre idolatrada desde muy pequeño sentí tu amor, cariño y devoción, siempre me apoyaste y motivaste a seguir adelante, ayudándome y guiándome en mis actividades diarias, dándome siempre buenos consejos e impartiendo en mí excelentes preceptos de ética y moral; los cuales al final han dado como resultado a un ser humano con principios, agradecido de Dios y con gran deseo de ayudar y seguir adelante como profesional.

Tu dedicación permanente, tus horas de desvelo cuidándome, mimándome, protegiéndome y hasta regañándome cuando me portaba mal; perdón por todos esos malos momentos.

El sacrificio realizado por ti, mi querida madre, tiene ahora sus frutos, gracias por tu entereza y constancia, tu valor para enseñarme a no temer y a superar adversidades, pudiendo así lograr mis metas anheladas.

Gracias mamá por ser la promotora de mis sueños, gracias por los valores que me inculcaste, gracias por confiar en mí, gracias por enseñarme a no temer a las adversidades porque Dios está conmigo siempre.

- Padre amado, siempre has estado presente en mi vida, apoyándome en mi carrera, en mis logros, y sé que estás muy orgulloso de la persona en la que me convertido.

Han pasado muchos años desde que nací, pero mucho antes de eso, ya estabas buscando maneras de ofrecerme lo mejor. Sé que has trabajado duro, y aunque llegabas cansado a casa tenías una sonrisa para nosotros, tu ayuda constante me ha permitido llegar al lugar donde estoy. Muchas gracias papá.

- Esposa abnegada, muy emocionado por tu apoyo y ánimo constante que me brindas día con día para alcanzar nuevas metas, tanto profesionales como personales.

En el camino encuentras personas que iluminan tu vida, una de esas eres tú mi bella esposa, que con tu apoyo alcanzo de mejor manera mis anhelos, por medio de tus consejos, de tu amor, y paciencia que me ayudo a concluir esta meta. Te amo mi vida.

- Queridos hijos, Dios me bendijo al tenerles a mi lado, han sido y serán mi luz, mi motivación permanente para seguir adelante, qué sería de mí sin ellos; son mi mayor tesoro y la fuente más pura de inspiración. Gracias por ser la felicidad de mi vida.

Con amor:

Christian Costales

AGRADECIMIENTO

En el transcurrir de mi vida me veo ahora en el portal final previo a la obtención de mi título como Magister en Seguridad Telemática, ante esta situación es meritorio mencionar a personas que desde mi principio como estudiante, influenciaron en mí, apoyándome, guiándome, incentivándome, motivándome; para así transformar una idea, un sueño, en una hermosa realidad.

A mis padres que son el eje vital de mi vida, sin ellos no hubiera existido ni tampoco estuviera en esta posición si no fuera por ellos, su cariño y dedicación contante, formaron en mi un ser humano a carta cabal, que interactúa correctamente con toda la naturaleza, y que lleva una excelente relación interpersonal con todos los que me rodean.

A toda mi familia que me ha apoyado constantemente, motivándome a seguir siempre adelante.

A mis amigos, muchos de ellos compañeros de estudio, con quienes se pasaron muchos momentos de camaradería, apoyo y colaboración incondicional que nos permitió alcanzar nuestra meta como profesional.

A mis profesores, parte vital de mi formación como profesional, que me permitieron aprender de ellos, su conocimiento y experiencia impartida de todos ellos que he podido palmar en mi conciencia y en mi corazón.

A la Escuela Superior Politécnica del Chimborazo que me permitió estudiar esta maestría.

Quiero terminar estas palabras dando un agradecimiento especial a un ser muy especial: Dios "gracias por permitirme vivir y escribir estas frases" Amén.

Atentamente:

Christian Alberto Costales Espinoza

CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE GRÁFICOS

ÍNDICE DE ANEXOS

ÍNDICE DE ABREVIATURAS

ACRÓNICO	DESCRIPCIÓN
IEC	Comisión Electrotécnica Internacional
ISO	Organización Internacional para la Estandarización
SGSI	Sistema de Gestión de Seguridad de la Información

RESUMEN

Se desarrolló un plan de seguridad informática que permita la confidencialidad integridad y disponibilidad de la información en el Juzgado de la niñez y adolescencia de la ciudad de Quito. Este plan se desarrolló tomando en consideración la legislación actual vigente, además de una comparación entre las Normas ISO 27001 y 27002; este plan ha sido implementado en el Juzgado de la niñez y adolescencia de la ciudad de Quito, con una evaluación efectuada en dos circunstancias; la primera antes de implementar el plan; donde se estableció y ponderó los riesgos a presentarse enfocados a la confidencialidad, integridad y privacidad de la información, estableciéndose los riesgos más críticos; bajo el mismo criterio y metodología, se evaluó luego de la implementación del plan. Del estudio realizado se pudo establecer entre las normas en base a la información recolectada de sus características para proteger los activos de la organización, se ha reducido sustancialmente el promedio de ponderación de probabilidad que los riesgos ocurran frente a la situación inicial, para lo cual se recomienda que el plan implementado en el Juzgado de la niñez y adolescencia de la ciudad de Quito es un proceso que nunca termina, ya que está enfocada en el monitoreo, seguimiento y revisión de manera continua de todos los métodos implementados.

Palabras clave: NORMA ISO 27001, SEGURIDAD DIGITAL, INFORMACIÓN DIGITAL, MITIGACIÓN DE RIESGOS, SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

ABSTRACT

A computer security plan was developed to provide confidentiality, integrity and information availability to the Court of Children and Adolescents of the city of Quito. This plan was developed taking into consideration the current legislation as well as a comparison between the ISO 27001 and 27002 Standards. This plan was implemented in the Court for Children and Adolescents of the city of Quito. Two evaluations were carried out. The first one took place before implementing the plan. Potential risks were found and weighed focusing on the confidentiality, integrity and privacy of the information. As a result, by using this criteria and methodology, critical risks were detected. The second evaluation took place after the implementation of the plan. From the study carried out, it was possible to protect the assets of the organization. The weighted probability average of risks occurring after the plan was implemented significantly decreased. Therefore, it is recommended that the computer security plan in the Court of Children and Adolescents of the city of Quito remains an ongoing process, since it focuses on continuous monitoring and assessment of all the implemented methods.

Keywords: ISO 27001 STANDARD, DIGITAL SECURITY, DIGITAL INFORMATION, RISK MITIGATION, INFORMATION SECURITY MANAGEMENT SYSTEM

CAPÍTULO I

1. MARCO REFERENCIAL

1.1. Introducción

En la actualidad los sistemas de información con los activos más valiosos para las organizaciones empresariales, instituciones públicas y privadas, es importante brindarles una protección apropiada para posibles abusos derivadas de las vulnerabilidades existentes en sus sistemas de seguridad. Para poder descubrir las diferentes vulnerabilidades y amenazas existentes es iniciando los procesos diagnósticos que permitan establecer el estado actual de la seguridad dentro de la organización, instituciones, teniendo en cuenta la normatividad vigente y los procesos de análisis y evaluación de riesgos.

Todos tipo de organizaciones independientemente de sus tamaño o naturaleza, debe ser consciente de las diversas amenazas existentes que pueden atentar contra la seguridad y privacidad de la información, que se convierte en un riesgo económico, sanciónales legales, afectación de la imagen y reputación; para la seguridad de la información se debe realizar medidas preventivas por parte del hombre, organizaciones y sistemas tecnológicos que permitan resguardar y proteger la información (datos); para mantener la integridad de los mismos.

En la actualidad los entornos tecnológicos se van volviendo más complejos en la administración y aseguramiento de la información, la seguridad de la misma forma parte de los objetivos y planes estratégicos de las organizaciones; es indispensable que los responsables de cada organización estén encargados de velar por la protección y seguridad de sus recursos, infraestructura e información, y constantemente estén adoptando, implementando y mejorando medidas de seguridad orientadas a prevenir, detectar los riesgos que pueden llegar a comprometer la disponibilidad, integridad y confidencialidad de los activos de información a través de los cuales se gestiona la información del negocio, independientemente si está es de carácter organizacional o personal, o de tipo pública o privada.

Se puede decir que la característica principal de los sistemas de seguridad es resguardar la integridad de la información de las organizaciones, instituciones, empresas, frente a posibles ataques

cibernéticos, esto se logra con un minucioso análisis de los riegos a los que están expuestos todos los activos de la información como son datos personales, cuentas bancarias, etc.

Se debe implementar estrategias adecuadas para brindar una protección a los activos esto se lo hace mediante la implementación de un sistema de gestión de seguridad de información (SGSI) bajo un marco de trabajo como la ISO/IEC 27001 permitiendo evaluar los riegos de seguridad estructurada, teniendo en cuenta las vulnerabilidades a la que está expuesta las organizaciones, empresas, institutos; permitiendo la correcta selección e implementación de controles, medidas correctivas para el tratamiento de los riesgos que permite tener un proceso de mejora continua y que puede ser adaptable para el resto de organizaciones.

El SGSI es una herramienta que permite a una organización controlar, sistemáticamente, el nivel de seguridad y rendimiento de la información; proporcionando beneficios económicos, disminución del tiempo de investigación, agilizando el tiempo para aprender cosas nuevas, aminorar las disputas, reducir los honorarios legales, la posible reducción de las primas de seguros, la protección de los activos de información, aumentar la conciencia sobre la seguridad de la información, confianza con clientes y otras partes interesadas. {1}

La norma ISO/IEC 27001 ayuda a proteger la confidencialidad de la información de manera que mantenga accesibles al personal autorizado, la norma preserva la integridad, exactitud e integridad de la información y la disponibilidad de información a las entidades autorizadas y la posibilidad de usarlas. Un sistema de gestión que se ha introducido en una organización para la protección de la información. {1}

1.2. Problema de la Investigación

1.2.1. Planteamiento del Problema

Es fundamental en todo este proceso, saber de proteger, de qué proteger, y cómo proteger, esta es la clave para poder direccional adecuadamente la seguridad de la información.

Información. Es uno de los activos más importantes de la empresa contenido en papeles y en sistemas de información. La información que posee la organización debe mantenerse protegida rigurosamente por tal motivo se deben tomar las precauciones necesarias para mantenerla bajo cuidado y preservarla dentro de la entidad y se deben tener en cuenta tres conceptos importantes: Confidencialidad, integridad y disponibilidad.

Confidencialidad. Implica el acceso a la información por parte únicamente de quienes están autorizados.

Integridad. Mantenimiento de la exactitud y cumplimiento de la información y sus métodos de proceso.

Disponibilidad. Es el acceso a la información y a los sistemas de tratamiento de la misma por parte de los usuarios autorizados en el momento que lo requieran.

Amenaza. Evento que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

Impacto. Consecuencia que sobre un activo tiene la materialización de una amenaza.

Riesgo. Posibilidad de que se produzca un impacto determinado en un activo en un dominio o en toda la organización.

Información Digital. "Se trata de información que es almacenada electrónicamente desglosada en dígitos o unidades binarias de unos y ceros que se guardan y se recuperan mediante un conjunto de instrucciones llamados programas o código.

Seguridad. Según algunos autores la seguridad en un sistema de información es un estado que nos indica que ese sistema está libre de peligro, daño o riesgo, entendiendo como peligro todo aquello que puede afectar su funcionamiento directo o los resultados que se obtienen del mismo.
Víctima es "el sujeto pasivo del delito o persona que sufre de manera directa o indirecta los efectos del hecho delictivo".

Víctima es "Persona que individual o colectivamente haya sufrido daños, inclusive lesiones físicas o mentales, sufrimiento emocional, pérdida financiera o menoscabo sustancial de los derechos fundamentales, como consecuencia de acciones u omisiones que violen la legislación penal. El término se aplica a la persona desaparecida o al cadáver hallado producto de ese hecho punible".

Hilda Marchiori en su artículo denominado "**Victimología**: la víctima desde una perspectiva criminológica" p. 266 dice: "Se entiende por segunda victimización, victimización secundaria o revictimización a aquella que tiene lugar no como un resultado directo de la acción delictiva, sino como consecuencia de la respuesta y el trato dado por las instituciones, el entorno social y los medios de prensa que provocan un nuevo daño en la victima".

La falta de una técnica, metodología específica para el manejo de información digital segura, ha ocasionado que exista el incorrecto procedimiento para su preservación, tratamiento y presentación,

provocando que la integridad de la información no sea la ideal, que sea modificada y además al tratarse de información delicada de los testigos en especial niños que han sufrido un abuso sexual y al ser mal utilizada, y en ocasiones ha sido difundida, provocando así la revictimización de los testigos, por ellos es prioritario obtener un método que sea nuestra guía para precautelar esta información.

Por lo que en la presente investigación se diferencia de las anteriores porque lo que se busca es obtener un método que incluya todos los niveles de seguridad de la información para precautelar la preservación, integridad de la información obtenida por las declaraciones de las víctimas.

1.2.2. Formulación del Problema

¿Cómo se manejará la seguridad de la información en el juzgado de la niñez y adolescencia de la ciudad de Quito?

1.2.3. Sistematización del Problema

¿Cuáles son los métodos, normas existentes para el manejo de información digital segura?

¿Cuáles son las ventajas y desventajas de los métodos, normas existentes para el manejo de información digital segura?

¿Cuáles son las consecuencias de un mal manejo de la información digital?

¿Cuáles son los aspectos a considerarse en el nuevo método de los métodos y normas existentes?

¿Cómo afecta para un dictamen el mal manejo información digital?

¿Cuáles son las responsabilidades y controles de cada una de las personas que manejan la información digital?

1.3. Justificación de la Investigación

1.3.1. Justificación Teórica

La Seguridad es un proceso continuo, y como tal, se requiere de un sistema que lo soporte, que requiere además de su definición e implementación, ser mantenido y mejorado acorde a la evolución de las necesidades.

Involucra factores humanos, tecnológicos y procedimentales o de relacionamiento de los anteriores. Por ello, no es suficiente un enfoque meramente técnico, ni exclusivamente humano o conductual.

No bastan decisiones políticas ni reglas estrictas por sí solas, como tampoco es resuelto por la tecnología. Tampoco es suficiente atacar estos aspectos en forma disasociada o disjunta, sino que se requiere de una visión integradora.

Debido al carácter dinámico y necesidad de revisión y mejora continua, se requiere de un enfoque metodológico, de apego a los estándares y a las mejores prácticas.

El uso de las mejores prácticas y estándares internacionales, así como las comparaciones con expertos contribuyen a alcanzar un estado de mayor madurez de la seguridad de la información digital y a su vez obtener un método adecuado para el manejo de información digital segura de los testimonios de las víctimas.

1.3.2. Justificación Metodológica

Las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la Información, en particular, la norma ISO/IEC 27.001, 27.005 si bien define lineamientos genéricos y los requerimientos para un sistema de gestión de seguridad de la información, no se pronuncian en forma concreta sobre algunos aspectos metodológicos que quedan abiertos, como por ejemplo en la elección de un método específico para la seguridad de la información.

1.3.3. Justificación Práctica

Con la aplicación del método de seguridad de la información digital, las pruebas se realizarán en el juzgado de la niñez y adolescencia de la ciudad de Quito, en dos escenarios, en el primero comprobando todas las vulnerabilidades y falta de seguridad de la información digital existentes y en el segundo aplicando el nuevo método y comprobando ambos escenarios para determinar el nivel de seguridad de la información digital existente.

1.4. Objetivos

1.4.1. Objetivo General *No títulos al final de las páginas*

- Realizar una propuesta de un plan de seguridad que permita la confidencialidad integridad y disponibilidad de la información en el juzgado de la niñez y adolescencia de la ciudad de Quito.

1.4.2. Objetivos Específicos

- Analizar los métodos, normas existentes para el manejo de información digital segura.
- Determinar las fortalezas y debilidades de las normas y métodos existentes para el manejo de información digital segura
- Determinar los componentes básicos del método para el manejo de información digital segura en juzgado de la niñez y adolescencia de la ciudad de Quito
- Aplicar el método para el manejo de información digital segura en juzgado de la niñez y adolescencia de la ciudad de Quito
- Verificar el nivel de mejora al implementar el método para el manejo de información.

1.5. Hipótesis

- El Método para el manejo de información digital permitirá mejorar el nivel de seguridad de la información.

CAPÍTULO II

2. MARCO TEÓRICO

2.1. Conceptos Básicos

2.1.1. Seguridad Informática

Se entiende como seguridad informática al conjunto de reglas y normas diseñadas para prevenir, proteger y resguardar la información que está expuesta a daño, robo, perdida de manera personal, grupal o empresarial, se garantiza la confidencialidad, integridad y disponibilidad de la infraestructura tecnológica que abarca hardware y software de diferentes instituciones, empresas u organizaciones públicas y privadas. (Seis Joseph, 2015. pág. 8)

A continuación, se detalla definiciones que se utiliza en Seguridad Informática:

Tabla 1-2: Definiciones que se utilizan en Seguridad Informática

Activo	**Este permite que la organización, empresa o institución funcione correctamente y alcance los objetivos propuestos. Son todas las cosas que tengan valor para la empresa, organización o instituciones.**
Amenaza	Son los eventos que pueden desencadenar grandes incidentes en las empresas, organizaciones e instituciones generando daños materiales o perdidas en sus activos.
Impacto	Resultado de la materialización de una amenaza.
Riesgo	Evento de que se produzca un impacto determinado en un activo en un dominio o en toda la organización.
Vulnerabilidad	Se puede dar la materialización de una amenaza sobre un activo o varios activos de a empresa, organizaciones o instituciones.
Ataque	Son los eventos que se generan de manera exitosa o no, sobre el funcionamiento del sistema

Desastre o Contingencia	Es la interrupción para el acceso de la información mediante las computadoras.

Realizado por: (Costales Christian, 2020)

El área informática está expuesto a diferentes riegos como: ataque de virus, códigos maliciosos, gusanos, caballos de troya, hackers; en la actualidad el internet es el medio de comunicación y colaboración; estos riesgos han evolucionados y las empresas deben enfrentar un sin número de ataques de negación de servicios y amenazas combinadas, accesos no autorizados, capacidades de identificar y explotar las vulnerabilidades de los sistemas operativos para dañar los recursos informáticos. (Seis Joseph, 2015. pág. 10)

2.1.1.1. Seguridad Física

La seguridad física evita el acceso no autorizado, daños o intromisiones en las instalaciones y que afecte a la información de la organización, por esta razón el procesamiento de la información debe estar ubicado en áreas seguras y protegidas en un perímetro de seguridad definido por barreras y controles de entradas adecuadas. (Cadme Christian, 2012, pág. 25)

2.1.1.2. Seguridad física del Edificio

Se trata de minimizar el riesgo que personas ingresen a algunos recursos informáticos específicos, con el objetivo de asegurar los activos y este a su vez debe estar ubicado en un lugar seguro sin vulnerabilidades de acceso a los mismos. (Cadme Christian, 2012, pág. 25)

Se debe generar políticas de seguridad bien planificadas, diseñadas y desarrolladas que abarquen la mayoría de los aspectos para que exista un verdadero SGSI, que a su vez generen planes de seguridad en la toma de decisiones para cuando se genere un acceso físico sin ninguna autorización en la empresa. (Cadme Christian, 2012, pág. 25)

2.1.1.3. Controles de Acceso

Todos los sitios donde se encuentran sistemas de procesamiento de datos informáticos o de almacenamiento, deben estar protegidos de accesos no autorizados, utilizando tecnologías de autenticación, monitoreo, registro de entrada y salida, guardias de seguridad, detectores metálicos.

2.1.1.4. Seguridad en el acceso a la información

Es de vital importancia que todos os datos de la empresa estén protegidos por tipos de riesgos que constantemente se interceptan en la Organización, poniendo en peligro la información que puede ser divulgada causando graves problemas en todo tipo. Por esta razón se debe implementar herramientas

o estándares como una medida de protección para los problemas que se pueden generar. (Cadme Christian, 2012, pág. 25)

2.1.1.5. Seguridad en las estaciones de trabajo

La estación de trabajo en donde se genera toda la información de la empresa, para ello se restringe varios tipos de entretenimientos, páginas web que no intervienen en el uso de la empresa, para un buen funcionamiento de su trabajo para lo cual se realizara algunas restricciones importantes que se realiza en este tipo de seguridad para no tener problemas en posteriores informaciones del trabajo que se realiza en empresa.

- Las computadoras de trabajo no deben tener instalado ningún otro software como juegos o software de entretenimiento que no sea requerido por el usuario para su trabajo.
- Todos los equipos deben tener instalado un software antivirus, con su última actualización.
- Esta estrictamente prohibido emplear cualquier configuración manual como direcciones IP, DNS, puertas de enlace o default Gateway, rutas estáticas entre otras. En el trabajo se debe obtener direcciones de manera automática.
- Se debe de escanear los discos flexibles y cualquier archivo o medio electrónico de transmisión antes del acceso a la información contenida en ellos.
- Respaldar periódicamente los datos de aplicaciones y configuración, y almacenarlas en lugares seguros.
- Solo el personal autorizado de área de información puede efectuar cambios en l configuración siempre o cuando justifique el por qué.
- Esta estrictamente prohibido que los usuarios cambien equipo del lugar al que han sido asignados.
- Los equipos den estar configurados para que empleen el protocolo TCP/IP y se debe remover cualquier otro protocolo innecesario. (Cadme Christian, 2012, pág. 25)

2.1.2. Seguridad en los Sistemas Informáticos

En la actualidad la gran demanda de los sistemas informáticos ha permitido el aumento de los delitos informáticos para la cual se debe generar un conjunto de soluciones técnicas, métodos y planes con el objetivo que los sistemas informáticos establezcan un plan de seguridad.

La seguridad genera un costo y que la seguridad absoluta es imposible por lo cual se debe generar objetivos con los niveles de seguridad a los que se desee llegar como empresa, institución u organización en este como Juzgado de la niñez y adolescencia de la ciudad de Quito. (Seis Joseph, 2015. pág. 10)

2.1.3. Propiedades de la seguridad Informática

Tabla 2-2: Las propiedades principales deben brindar un sistema de seguridad

Confidencialidad	Se debe contralar quien puede leer la información y que esta información confidencial sea entregada o receptada por personas no autorizadas.
Disponibilidad	Se debe verificar que los sistemas trabajen de manera eficiente, con buen desempeño, garantizar la protección, recuperación del sistema en caso de ataques o desastres.
Integridad	Se debe asegurar que la información recibida sea exactamente igual a la información enviada, con esto se quiere decir que la l información no ha sido dañada en la transmisión o alterada en su contenido o secuencia.
Autenticidad	Se debe garantizar que la información no sea replica de información vieja la cual se haga pasar por información fresca y que esta provenga de fuentes genuinas.
Identificación o Control de Acceso	Se debe verificar, autorizar y controlar la identidad de las personas que accedan a los recursos del sistema.

Realizado por: (Costales Christian, 2020)
Fuente: (Seis Joseph, 2015. pág. 12-13)

2.1.4. Objetivos de la Seguridad

Tabla 3-2: Objetivos de la Seguridad

Identificación de los Usuarios	Se puede aplicar diferentes técnicas como los passwords (contraseñas), reconocimiento facial, huella dactilar o retina del ojo, reconocimiento de habla.
Detección de Intrusos en la red	Se debe detectar cualquier acceso no autorizado en el sistema, esto se aplica en tiempo real para que no cause daños en el sistema.

Análisis de Riesgos	Se debe cuantificar los beneficios obtenidos con la protección contra amenazas, vulnerabilidades. También se debe cuantificar las pérdidas que se produce cuando esto ocurre.
Clasificación Apropiada de los Datos	En la gestión de seguridad llegan gran cantidad de datos provenientes de los últimos programas de control generados a partir de las actuaciones que lleva a cabo los usuarios en el sistema. Se debe tener una buena supervisión de la seguridad para clasificar los datos de tal manera que se ahorre tiempo.
Control de nuevas Aplicaciones	Cuando se instala una nueva aplicación se debe comprobar que no se introduzca nuevas brechas de seguridad especialmente si se ejecuta con permiso de root.
Análisis de los Accesos de los Usuarios	Se debe tener un control para detectar los intentos de accesos no autorizados.

Realizado por: (Costales Christian, 2020)
Fuente: (Seis Joseph, 2015. pág. 13-14)

2.1.5. Términos de Riesgo

Los siguientes términos utilizados para la seguridad de la información:

- **Valorización de Riesgos:** Se analiza las diferentes amenazas, vulnerabilidades y el impacto potencial de un sistema de información.
- **Evaluación de Riegos**: Esto se evalúa según los criterios de seguridad aplicados en la empresa como normas, reglamentos, et.
- **Análisis de Riesgos: Identificación** y evaluación de los niveles de riegos de activos, amenazas y vulnerabilidades.
- **Gestión de Riesgos:** Aquí se determina las estrategias a implementar para el tratamiento de las amenazas como ejemplo:

  1.- Aceptarlo

  2.- Minimizarlo, identificarlo, seleccionarlo e implementar las medidas para la reducción del impacto

  3.- Transferirlos.

2.1.6. Factores de Riesgos

El riesgo es la combinación de una amenaza que aprovecha las vulnerabilidades de los activos para impactarlos y hacer mucho daño. (Seis Joseph, 2015)

2.1.6.1. Activos

Todos los bienes de la empresa necesitan protección a frente posibles situaciones de pérdidas de condiciones como: Confidencialidad, Integridad o Disponibilidad.

Confidencialidad: La información no está disponible y no puede ser divulgada a otras entidades.

Integridad: Es la que salvaguarda todos los activos de la empresa, instituciones u organizaciones públicas o privadas.

Disponibilidad: Es cuando la información esta accesible solo para el personal autorizado.

Los activos de información poseen un valor y por lo tanto la empresa debe protegerlo, esto se clasifica por las categorías siguientes:

- Activos de Información (Datos, manuales de usuarios)
- Documentos de papel (contratos)
- Activos de software (aplicación, software del sistema)
- Activos físicos (computadoras, medios magnéticos)
- Personal (clientes, personal)
- Imagen de la institución y reputación
- Servicios (comunicaciones) (Seis Joseph, 2015)

2.2. Sistema de Gestión de Seguridad de la Información (SGSI)

Las normas **ISO 27001** aportan un **S**istema de **G**estión de la **S**eguridad de la **I**nformación **(SGSI)**, consistente en medidas orientadas a **proteger la información** contra cualquier amenaza, de manera que se garantice la continuidad de las actividades de la empresa o institución.

Figura 1-2: Modelo SGSI
Fuente: https://www.normas-iso.com/wp-content/uploads/2012/02/SGSI.png

El SGSI permite la implementación de controles de seguridad, ayudando a monitorear, revisar, mantener, y mejorar la seguridad de la información.

2.2.1. Familia de las ISO 27000

La serie de las normas ISO 27000 es el conjunto de estándares desarrollados por ISO e IEC (Comisión Electrónica Internacional) que proporciona un marco de seguridad de la información utilizable para cualquier tipo de organización. Las más conocidas son:

- ISO/IEC 27000: Proporciona una visión general de las normas que componen la serie 27000, una introducción a los Sistemas de Gestión de Seguridad de la Información.
- ISO/IEC 27001: Es la norma principal de la serie y contiene los requisitos del Sistema de Gestión de Seguridad de la Información. Se origina en las BS 7799-2:2002 y es la norma con arreglo de la cual se certifica la SGI de las organizaciones.
- ISO/IEC 27002: Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables a seguridad de información. Este contiene 39 objetivos de control y 133 controles agrupados en 11 dominios. (*Guía de Iniciación a Actividad Profesional Implantación de Sistemas de Gestión de la Seguridad de la Información (SGSI) según la norma ISO 27001*, s. f.)

Tabla 4-2: Resumen de la Familia ISO 27000

NORMA	CONTENIDO
27000	Visión general de la serie
27001	Norma principal de la serie Requisitos del SGSI Certificable
27002	Guía de buenas prácticas: 11 dominios, 39 objetivos de control y 133 controles
27003	Aspectos críticos para el diseño e implementación de un SGSI
27004	Guía para el desarrollo y utilización de métricas y técnicas de medida de la eficacia de un SGSI y de los controles o grupos de controles
27005	Directrices para la gestión del riesgo
27006	Requisitos para la acreditación de entidades de auditoria y certificación
27007	Guía de auditoria de un SGSI
27008	Guía de auditoría de los controles seleccionados
27013	Guía de implementación integrada de ISO/IEC 27001 E ISO/IEC 20000-1
27014	Guía de gobierno corporativo de la seguridad de la información
27031	Guía de continuidad de negocio en cuanto a tecnologías de la información y comunicaciones.
27032	Guía relativa a la ciberseguridad
27033	Guía de seguridad en redes (7partes)
27034	Guía de seguridad en aplicaciones informáticas
27035	Guía de gestión de incidentes de seguridad de la información
27036	Guía de seguridad de externalización de servicios
27037	Guía de identificación, recopilación y preservación de evidencias digitales

Fuente: (*Guía de Iniciación a Actividad Profesional Implantación de Sistemas de Gestión de la Seguridad de la Información (SGSI) según la norma ISO 27001*, pág. 11)

2.2.1.1. Términos y Definiciones

Tabla 5-2: Normas ISO 27000 y sus Definiciones

Aceptación del riesgo	**Es la decisión de aceptar un riesgo**
Activos	Cualquier bien que tiene valor para la organización, institución o empresa
Análisis de Riesgos	Utilización sistemática de la Información no se pone a disposición o se revela a individuos, entidades o procesos no autorizados
Declaración de aplicabilidad (SOA) Statement of Applicability	Aquí se describe los objetos de control y los controles que son importantes para la SHSI de la organización y aplicables al mismo.
Disponibilidad	La propiedad de ser accesible y utilizable por una entidad.
Estimación de Riesgos	Es el proceso de comparación del riesgo estimado con los criterios de riesgo, para así determinar la importancia del riesgo.
Evaluación del Riesgo	Es el proceso general de análisis y estimación de riesgos.
Evento de seguridad de la Información	Es la ocurrencia detectada en un estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información, fallo de la salvaguardias o situación desconocida hasta el momento y que puede ser relevante para la seguridad.
Gestión de Riesgos	Actividades coordinadas para dirigir y controlar una organización

(*Guía de Iniciación a Actividad Profesional Implantación de Sistemas de Gestión de la Seguridad de la Información (SGSI) según la norma ISO 27001*, pág. 13).

2.2.1.2. Fases del SGSI

- Análisis y evaluación de riegos
- Implementación de controles
- Definición de un plan de tratamiento de los riesgos o esquema de mejora
- Alcance de la gestión
- Con texto de organización

- Partes interesadas
- Fijación y medición de objetivos
- Proceso documental
- Auditorías internas y externas

2.2.1.3. Modelo PDCA

La norma ISO 27001 sigue el modelo PDCA que le permite estructurar todos los procesos del SGSI de forma que resulta compatible con las normas ISO 9001 e ISO14001.

El modelo PDCA (Plan-Do-Check-Act) es una estrategia de mejora continua de la calidad de 4 pasos, de manera cíclica (también conocida como espiral de Deming) que consta de cuatro fases:

- **PLAN** (Planificar): se establece los objetivos y procesos necesarios para la obtención de resultados de acuerdo con el resultado esperado. Se toma como base el resultado esperado, difiere de otras técnicas en las que el logro o la precisión de la especificación es también parte de la mejora.
- **DO** (Hacer): Se implementa los nuevos procesos en pequeñas escalas.
- **CHECK** (Verificar): Después de un periodo de tiempo previsto de antemano, se vuelve a la recopilación de datos de control y analizarlos, luego se compara con los objetivos y especificaciones iniciales, para la evaluación y verificar se ha producido la mejora esperada. Se debe documentar las conclusiones.
- **ACT** (Actuar): se debe modificar los procesos según las conclusiones obtenidas con anterioridad que permite alcanzar los objetivos planteados con anterioridad. Se debe aplicar nuevas mejoras que permita la detección de errores. Se debe documentar todo el proceso como guía para un futuro.

Tabla 6-2: Modelo PDCA en un caso SGSI

Planificar (Plan) **Crear el SGSI**	Definir la política de seguridad Establecer al alcance del SGSI Realizar el análisis de riesgo Seleccionar los controles Definir competencias Establecer un mapa de procesos Definir autoridades y responsabilidades	Se define las políticas, objetivos, procesos y procedimientos del SGSI que permite la gestión del riesgo para luego mejorar la seguridad de la información, que permita obtener resultados de acuerdo con las políticas y objetivos generales de la organización.
Hacer (DO) **Implementar y Operar**	Implantar el plan de gestión de riesgos Implantar el SGSI Implantar los controles	Implementar y operar la política, controles, procesos y procedimientos del SGSI.
Verificar (Check) **Supervisar y Revisar**	Revisar internamente el SGSI Realizar auditorías internas del SGSI Poner en marcha indicadores y métricas Hacer una revisión por parte de la Dirección	Se debe evaluar y medir el rendimiento del proceso contra la política, los objetivos y la experiencia práctica del SGSI, y se debe informar de los resultados a la dirección para su revisión.
Actuar (Act) **Mantener y Mejorar**	Adoptar acciones correctivas Adoptar acciones de mejora	Se debe adoptar medidas correctivas y preventivas en función de los resultados de la auditoría interna del SGSI y de la revisión por parte de la dirección.

Realizado por: (Costales Christian, 2020)

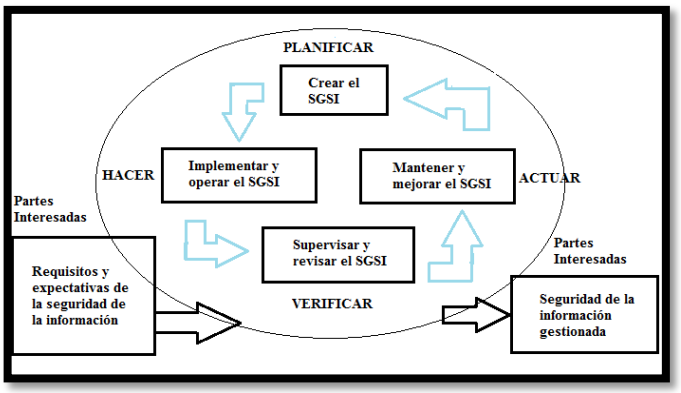

Figura 2-2: Modelo PDCA aplicado al proceso del SGSI

Fuente:(*Guía de Iniciación a Actividad Profesional Implantación de Sistemas de Gestión de la Seguridad de la Información (SGSI) según la norma ISO 27001*, pág.14-15)

2.2.2. Normas ISO/IEC 27001

Es una norma internacional que da a conocer los lineamientos de seguridad de información, los cuales permite implementar en la gestión de seguridad de la información de cualquier empresa, permite mejorar continuamente la seguridad física y loica de la información, ayudando a proteger la información de posibles robos o daños. (Bermúdez Kelly, 2015. pág. 10)

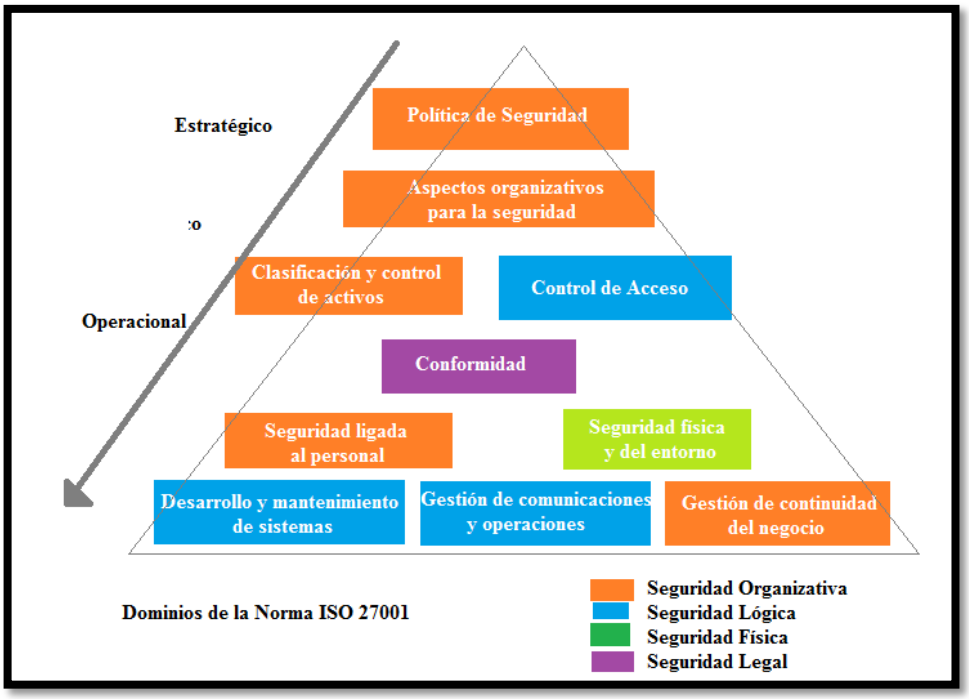

Figura 3-2: Modelo de la Norma ISO 27001
Fuente: Cooperativa Sanfrancisco

2.2.2.1. Funcionamiento de la norma ISO/IEC 27001

Para brindar soporte a los datos que se encuentran registrados de la organización para eso se implementa un SGSI con estándar 27001 para el cuidado de la información brindando confidencialidad, disponibilidad e integridad de los datos para el buen uso de la información y no divulgación en las organizaciones que pueden ser grandes o pequeñas. (Cadme Christian, 2012)

Tabla 7-2: Funcionamiento de las Normas ISO/IEC 27001

Confidencialidad de datos	Es cuando el empleado y usuario de la empresa garantiza la seguridad de la información al momento de ingresarla, no divulgando esta información a personas o empresas ajenas. La seguridad se garantiza con el acceso solo a los administradores y gerentes de la empresa.

Disponibilidad de datos	Es el permiso de acceder a la información de la empresa en tiempos y horas adecuadas en los cuales los usuarios alteran, actualizan, respaldan los datos de mayor importancia para que no ocasionen pérdidas financieras y de personal.
Integridad de datos	Esto se refiere a los datos que no pueden ser alterados por ningún tipo de personal, solo por altos mandos como la dirigencia, para la cual se debe tener un tipo de seguridad que ayude con el manejo correcto de datos.

Fuente: (Cadme Christian, 2012, pág. 17)

2.2.2.2. Beneficios de la Norma ISO/IEC 27001

La norma ISO/IEC 27001 permite disminuir los riesgos de vulnerabilidades en los sistemas informáticos y en la información en general de los usuarios que son manejados por personal de la empresa, teniendo una mejor organización de los procesos, aumentando la competitividad de la empresa debido a que se demuestra el interés por salvaguardar la integridad, confiabilidad y disponibilidad de la información de los clientes. (Bermúdez Kelly, 2015, pág. 10)

2.2.2.3. Dominios de Seguridad de la ISO/IEC 27001

- Política de Seguridad
- Organización de la Seguridad
- Gestión de Activos
- Seguridad de los Recursos Humanos
- Seguridad Física y del Entorno
- Gestión de Comunicaciones y Operaciones
- Control de Accesos
- Adquisición, Desarrollo y mantenimiento de la Información
- Gestión de Incidentes de Seguridad de la Información
- Gestión de la continuidad de los negocios
- Cumplimiento

2.2.2.4. Protección de Activos

Los activos que necesitan protección son: información digital, documentos en papel y activos físicos (computadores y redes), para lograr esto se debe elaborar mecanismos de protección personal hasta protección técnica contra fraudes.

- Confidencialidad, permite que acceda a la información solo las personas que están autorizadas.
- Integridad, protege la totalidad de la información y los métodos de procesamiento.
- Disponibilidad, permite que los usuario o personal autorizado tengan acceso a la información. (Guachi Tania, 2012, pág. 27)

2.3. Definiciones utilizadas por el Juzgado

Para el desarrollo de esta tesis se utilizaron los siguientes conceptos básicos:

Amenaza. Evento que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos. («Seguridad de la información y auditoría de sistemas - Monografias.com», s. f.).

Confidencialidad. La información sólo debe ser legible para los autorizados, esto implica el buscar prevenir el acceso no autorizado ya sea en forma intencional o no intencional de la información («Seguridad de la información y auditoría de sistemas - Monografias.com», s. f.).

Disponibilidad. Debe estar disponible cuando se necesita los datos, la información o recursos para el personal adecuado («Seguridad de la información y auditoría de sistemas - Monografias.com», s. f.).

Impacto. medir la consecuencia al materializarse una amenaza («Seguridad de la información y auditoría de sistemas - Monografias.com», s. f.)

Información. Es uno de los activos más importantes de la empresa contenido en papeles y en sistemas de información. La información que posee la organización debe mantenerse protegida rigurosamente por tal motivo se deben tomar las precauciones necesarias para mantenerla bajo cuidado y preservarla dentro de la entidad y se deben tener en cuenta tres conceptos importantes: Confidencialidad, integridad y disponibilidad. (Rodríguez, 2014, p. 21)

Información Digital. "Se trata de información que es almacenada electrónicamente desglosada en dígitos o unidades binarias de unos y ceros que se guardan y se recuperan mediante un conjunto de instrucciones llamados programas o código". (NFSTC, 2012, p.3).

Integridad. "Mantenimiento de la exactitud y cumplimiento de la información y sus métodos de proceso" (Rodríguez, 2014, p. 21)

Revictimización. - Hilda Marchiori en su artículo denominado "**Victimología:** la víctima desde una perspectiva criminológica" p. 266 dice: "Se entiende por segunda victimización, victimización secundaria o revictimización a aquella que tiene lugar no como un resultado directo de la acción delictiva, sino como consecuencia de la respuesta y el trato dado por las instituciones, el entorno social y los medios de prensa que provocan un nuevo daño en la victima".

Seguridad. Es un estado de cualquier tipo de información (informático o no) que indica que ese sistema está libre de peligro, daño o riesgo. Se entiende como peligro o daño todo aquello que pueda afectar su funcionamiento directo o los resultados que se obtienen del mismo. («Seguridad Informática - EcuRed», s. f.).

Seguridad informática, es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinadas a conseguir un sistema de información seguro y confiable. (López, 2010, p. 9)

Víctima es "cualquier persona que ha sufrido menoscabo en sus derechos como consecuencia de un delito"(«Sistema Nacional de Protección y Asistencia a Víctimas y Testigo», 2011, p. 4)

CAPÍTULO III

3. METODOLOGÍA DE LA INVESTIGACIÓN

3.1. Diseño de la Investigación

El siguiente proyecto es de tipo cuasi-Experimental porque permite escoger la metodología que se va a emplear en el desarrollo de la propuesta del nuevo manejo de información digital en el Juzgado de la niñez y adolescencia de la ciudad de Quito, el punto de partida es la descripción del problema, necesidades, exigencias son de manera inmediata sin necesidad de someterle apruebas los datos.

3.2. Tipo de Investigación

La presente investigación es de tipo: De campo, Bibliográfica, Descriptiva y Experimental

- **De campo:** Se empleará este tipo de investigación porque se necesita ir al lugar donde se desarrollan los hechos, obteniendo información veraz de los ocurrido**,** de tal manera que el análisis realizado este acorde con los objetivos planteados.
- **Bibliográfica:** Se va a realizar un estudio de seguridad basadas en las normas ISO/IEC 27000, que proporciona criterios de buenas prácticas y gestión de la información**.**
- **Descriptiva:** Con este tipo de investigación se detallan las actividades que se llevan a cabo en los procesos manejados en el objeto de estudio, permitiendo conocer en forma sistemática las falencias que se puede presentar.
- **Experimental:** esta investigación va a realizar pruebas en laboratorio, en la que se va a observar todos los elementos más relevantes e importantes del objeto de estudio que se está investigando para la obtención de fenómenos a primera vista y no se puede realizar cambios en el objeto de la investigación de manera deliberada.

3.3. Métodos

Se aplicará el método científico en la presente investigación, la que permitirá realizar una serie de actividades para la obtención de un conocimiento valido desde un punto de vista valido científicamente, para lo cual se utilizará instrumentos fiables, el cual consta de las siguientes etapas:

- Planteamiento del problema
- Formulación de la hipótesis
- Levantamiento de la información
- Análisis e interpretación de resultados
- Comprobación de la hipótesis
- Difusión de resultados

3.4. Técnicas

En la presente investigación las técnicas a utilizar son:

- **Búsqueda de información:** permite obtener la información necesaria acerca del objeto de estudio de la investigación para su desarrollo, utilizando las fuentes secundarias disponibles.
- **Pruebas:** permite realizar experimentos en escenarios de laboratorio.
- **Observación:** permite determinar resultados de las pruebas realizadas en los escenarios de laboratorio.
- **Análisis:** se van a determinar los resultados de la investigación.

3.5. Fuentes de Información

Las principales fuentes que serán utilizadas en el estudio de investigación serán:

3.5.1. Primaria

- Pruebas
- Observación de resultados

3.5.2. Secundaria

- Tesis realizadas internacionales y nacionales de cuarto nivel.
- Trabajos de investigaciones internacionales y nacionales.

- Artículos científicos en base de datos de bibliotecas virtuales.
- Libros especializados en la biblioteca y electrónicos.
- Diccionarios especializados.
- Conferencias académicas, congresos, seminarios.
- Revistas indexadas y no indexadas publicadas de prestigio.
- Revistas electrónicas.
- Páginas de internet que brinden información confiable.

3.6. Recursos

3.6.1. Recursos técnicos

Los recursos técnicos que se utilizarán en la investigación son:

3.6.2. Recurso Hardware

Se utilizará el siguiente computador:

- **Modelo**: TOS. S55-B5203SL
- **Procesador: Intel® Core™ i7-4510U**
- **Memoria:** 8,00 GB DDR3L 1600
- **Disco Duro:** 1TB (5400 RPM) Serial ATA

3.7. Población

Las unidades básicas objeto de investigación la conforman 250 empleados de los departamentos del Juzgado de la Niñez y Adolescencia

3.8. Selección de la muestra

Para el estudio y análisis de datos, se realizó un muestreo deliberado donde los criterios para la selección dentro de la población consistieron:

- A los directivos del departamento que posee un amplio conocimiento de las actividades que se realizan por los empleaos del área y se mantengan un rol ejecutor en la toma decisiones.
- Los operarios de cada unidad o departamento que manipulen información para llevar a cabo las actividades que su rol exige.

Es factible que un número mínimo de 25 funcionarios a entrevistar y encuestar se puede lograr una apreciación muy real de la situación actual, ya que el análisis se centra sobre el grupo de personas que cumplan un papel relevante en los procesos del Juzgado.

3.9. Operación de Variables e Indicadores

Tabla 1-3: Matriz de Operaciones de variables

Variable	***Definición Conceptual***	***Dimensiones***	***Indicadores***
Controles de Seguridad	Los controles de seguridad ayudan a controlar las actividades realizadas sobre la información.	Divulgación de las medidas de Seguridad Valoración de las políticas de seguridad	Políticas de seguridad que los usuarios deben conocer y aplicar. Medios determinados para la comunicación de las políticas de seguridad. Periodicidad en la verificación de la efectividad de las medidas de seguridad. Periodos determinados para la evaluación interna.
Nivel de Compromiso	Es el apoyo que s brinda a los sistemas de seguridad de la información.	Inversiones que se debe realizar para la adquisición de recursos que permitan el control y monitoreo continuo de las políticas de seguridad. Cumplimiento de los procedimientos y controles de seguridad establecidos	Adquisición de herramientas tecnológicas y contratación de personal especializado en gestión de seguridad de la información. Revisión de las actividades de manera periódicas que están establecidas de acuerdo al rol del funcionario.
Infraestructura Informática	Es el conjunto de software y hardware que dan soporte al procesamiento y almacenamiento de datos.	Seguridad brindada por los sistemas de procesamiento, transmisión y almacenamiento de información.	Periodos de revisión de la configuración de seguridad de los equipos de almacenamientos de la información. Periodos de evaluación de seguridad de los sistemas informáticos de procesamientos de información.

			Periodos de revisión de la seguridad en los sistemas de comunicaciones.
Madurez de los Procesos	Es la definición, estandarización, automatización y regulación de los procesos	Nivel de los procesos de la empresa.	Evaluación del estado actual del proceso.
Madurez de la seguridad de la información	Es el cumplimiento e implementación de controles establecidos.	Establecimiento de controles de seguridad de la información. Seguridad de la información a nivel de Tecnologías de la información.	Capacitaciones del personal. Incidentes detectados sobre las políticas de seguridad. Auditorías realizadas en las áreas administrativas. Incidentes reportados en las aplicaciones que pueden afectar la información. Incidentes reportados en los equipos de cómputo de los funcionarios. Criterios en las evaluaciones de los sistemas de información.
Vulnerabilidad en los procedimientos	A esto se le considera como las falencias o huecos q pueden ser explotados	Estas se pueden conocer y no han podido ser cubiertas.	Se debe realizar un historial de las vulnerabilidades sobre las cuales se han tomado acciones correctivas. Vulnerabilidades encontradas y reportadas. Hacer un reporte de las amenazas detectadas.
Amenazas	Es el conjunto de vulnerabilidades que se han detectado y significan un riesgo para la seguridad de la información.	Identificación de las amenazas existentes. Gestión sobre las amenazas	Reportes de amenazas detectadas. Procedimientos definidos para la gestión y control de amenazas.

			Seguimiento sobre amenazas criticas gestionadas. Historial de las gestiones de amenazas que se presentan.

Realizado por: (Costales Christian, 2020)

3.10. Plan de Recolección de la Información

Se va a realizar el análisis de seguridad de la información se propondrá los siguientes mecanismos para la recolección de información:

- Entrevistas
- Encuestas
- Reuniones
- Revisión de documentación
- Consultas
- Observación

3.11. Plan de Procesamiento de la Información

Se realizará las siguientes actividades:

- Archivo de la Información
- Análisis de la Información
- Levantamiento de Información
- Verificación de la Información
- Registro de la Información
- Clasificación de la Información

3.12. Análisis del Riesgo

Para saber los riesgos que se pueden presentar se va a considerar lo siguiente: probabilidad, impacto, exposición del riesgo; los que permitirán categorizar a los mismos para luego poder gestionar los riesgos más relevantes y tomar decisiones de manera correcta precautelando la información.

3.12.1. Probabilidad del Riesgo

Es la posibilidad de que ocurra un evento y las consecuencias que puede dejar dicho evento.

La probabilidad de que se presente un riesgo o amenaza debe ser mayor a cero (0), pero debe ser menor a (1).

Tabla 2-3: Valores de Probabilidad de que se genere el riego

Descripción	*Probabilidad de Ocurrencia*	*Puntuación*
Imposible que suceda	Raro	0.0 a 0.24
Ocurre alguna vez	Ocasional	0.25 a 0.39
Probablemente ocurra	Probablemente	0.4 a 0.69
Ocurre la mayoría de veces de manera repetida	Frecuentemente	0.70 a 0.99

Fuente: (Costales Christian, 2020)

3.12.2. Impacto del Riesgo

El impacto es la realización del riesgo y son los efectos adversos de los mismos.

La clasificación del impacto va del 1 a 4 cuan mayor sea el número, mayor será el impacto.

Tabla 3-3: Valores de Impacto (Riesgos)

Impacto	*Valor*
Muy Alto	4
Alto	3
Medio	2
Bajo	1

Realizado por: (Costales Christian; 2020)

3.12.3. Valoración del Riesgo

La valoración del riesgo es el resultado que se obtiene al multiplicar la probabilidad por el impacto. Los riesgos con un nivel de valoración alta son los que necesitan de una administración adecuada y nomas de seguridad adecuadas. Se considera al valor máximo que se obtendrá de la valoración será 4, poniendo como límite que los riesgos superiores a 2,5 serán consideraos como críticos.

3.12.4. Identificación del Riesgo

Después de haber realizado el análisis y la validación de los riesgos en el Juzgado, se puede observar que los riesgos que ocurren con gran frecuencia son los siguientes:

Tabla 4-3: Riesgos que ocurren con mayor frecuencia

Ítem	Amenazas
1	Existencia del Manual de Políticas de Seguridad de la Información
2	Existe el área o responsables de la Seguridad Informática
3	Mecanismos de Autenticación (Contraseñas)
4	Acceso no autorizado a la información o datos
5	Herramientas de Seguridad Implementadas
6	Divulgación de la información
7	Errores de usuarios y operadores
8	Software o Códigos Maliciosos
9	Sustracción o robo de información
10	Existen respaldos de la Información

Realizado por: (Costales Christian, 2020)

CAPÍTULO IV

4. RESULTADOS Y DISCUSIÓN

4.1. Preguntas de la Encuesta

Con respecto al plan de recolección de la información, se realizó una muestra para la encuesta a 25 personas de diferentes áreas del juzgado incluyendo a 3 personas del área de Sistema. Generando los resultados siguientes donde se puede visualizar el nivel de seguridad de la información del Juzgado de la Niñez y Adolescencia de la ciudad de Quito.

Se va a establecer la probabilidad de ocurrencia de un riesgo, en función del promedio de las respuestas obtenidas en la encuesta, a las preguntas realizadas para la evaluación de cada riesgo, el cálculo de la probabilidad de ocurrencia del riesgo es:

$$\text{Probabilidad} = \frac{\text{Promedio de Respuestas negativas}}{\text{Total de la población encuestada}}$$

Total, población encuestada: 25

Dónde se obtienen los siguientes resultados de las preguntas:

Pregunta:

¿Existe Manual de Políticas de Seguridad de la información?

Objetivo:

Identificar si existe el Manual de Políticas de Seguridad de la Información para saber si ellos realizan adecuadamente las actividades sin necesidad de tener una dependencia para su ejecución.

Tabla 1-4: Existe un manual de Políticas de Seguridad de la Información

Detalle	*Encuestados*	*Porcentaje*
Si	8	32%
No	5	20%
Desconoce	12	48%

Realizado por: (Costales Christian, 2020)

Gráfico 1-4: Existe un Manual de Políticas de Seguridad de la información
Realizado por: (Costales Christian, 2020)

De los 25 funcionarios encuestados que corresponde al 100%, el 48 % desconocen que existe este Manual de Políticas de Seguridad de la Informacion, el 20 % no sabe nada acerca de este tema, mientras que el 32% conocen que existe este manual.

Pregunta:

¿Existe en el Juzgado de la Niñez y Adolescencia un responsable o área encargada de la Seguridad de la información o Seguridad Informática?

Objetivo:

Conocer si los funcionarios del Juzgado saben si existe esta área o responsables de la Seguridad de la Información o algo similar.

Tabla 2-4: Existe un área de seguridad Informática

Detalle	*Encuestados*	*Porcentaje*
Si	13	52%
No	7	28%
Desconoce	5	20%

Realizado por: (Costales Christian, 2020)

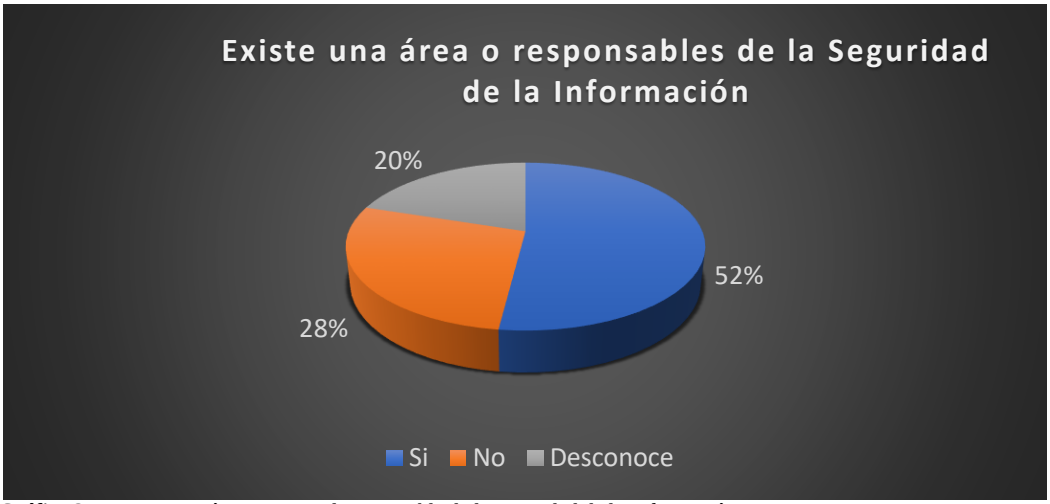

Gráfico 2-4: Existe una área o personal responsable de la seguridad de la Información
Realizado por: (Costales Christian, 2020)

De los 25 funcionarios encuestados que corresponde al 100%, el 52 % conoce que, si existe esta área o responsables de la Seguridad de la Información, el 28 % no sabe nada acerca de los responsables de la Seguridad de la Información, mientras que el 20% desconocen de este tema.

Se puede entender que existe una figura que cumple por partes con el rol de responsable de seguridad de la información, pero no están formalmente establecidas sus funciones.

Pregunta:

¿Las contraseñas que utiliza usted poseen una combinación de números, letras y es más de 8 cárteres?

Objetivo:

Conocer si los funcionarios del Juzgado establecen medidas mínimas de seguridad para la protección de la información.

Seguridad en las contraseñas de los funcionarios

Tabla 3-4: Existen Seguridad en las Contraseñas de los funcionarios

Detalle	*Encuestados*	*Porcentaje*
Solo números y más de 8 caracteres	3	12%
Solo letras y más de 8 caracteres	2	8%
Letras y números con más de 8 caracteres	6	24%
Otras	14	56%

Realizado por: (Costales Christian, 2020)

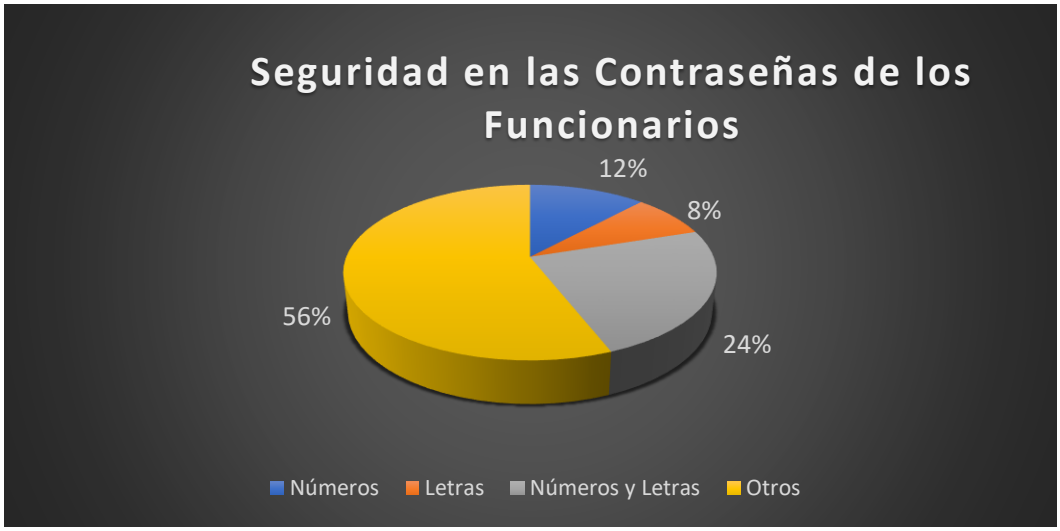

Gráfico 3-4: Existe Seguridad en las contraseñas de los funcionarios
Realizado por: (Costales Christian, 2020)

De los 25 funcionarios encuestados que corresponde al 100%, el 24% utiliza números y letras con más de 8 caracteres, mientras que el 28 % y 12 % utilizan solo letras o números para las contraseñas de sus equipos, y el 56% opta por otra clase de contraseñas como símbolos, letras con longitudes, huellas dactilares entre otras.

Se puede entender que la gestión de autenticación de los usuarios o funcionarios de los sistemas de procesamiento de la información no es homogénea según los datos obtenidos de las encuestas.

Pregunta:

¿Se ha generado alguna clase de incidente en la seguridad en su puesto de trabajo en el último año como por ejemplo (pérdida de documentos, daño en la computadora, bloqueo, entre otros)?

Objetivo:

Identificar los incidentes de seguridad que han reportados los usuarios o funcionarios

Tabla 4-4: Incidentes de Seguridad

Detalle	*Encuestados*	*Porcentaje*
Si	11	44%
No	10	40%
Desconoce	4	16%

Realizado por: (Costales Christian, 2020)

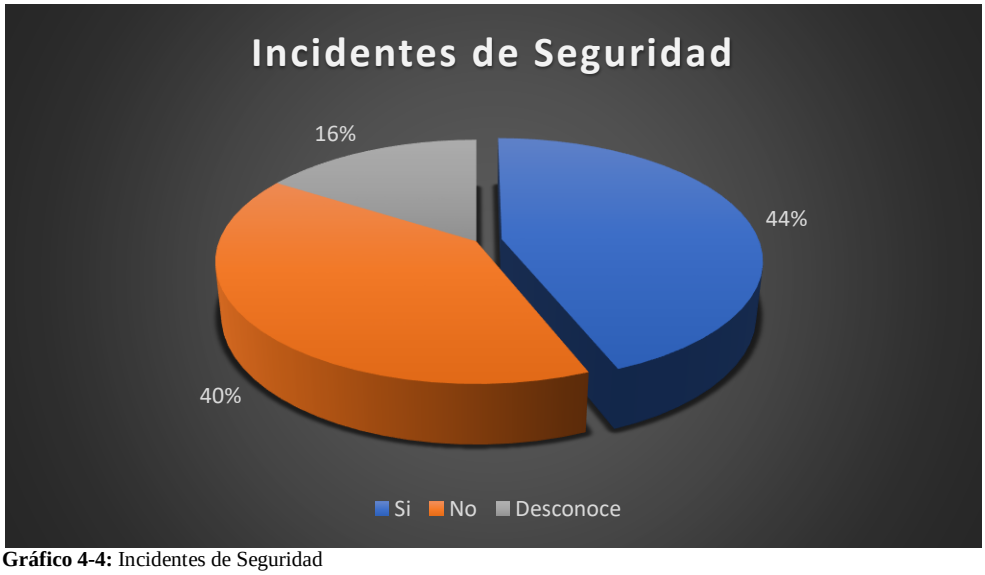

Gráfico 4-4: Incidentes de Seguridad
Realizado por: (Costales Christian, 2020)

De los 25 funcionarios encuestados que corresponde al 100%, el 44% de los funcionarios han experimentado un problema de seguridad, mientras que el 40% no ha reportado ninguna clase de problema en la seguridad de sus equipos, y el 16% desconocen si han tenido algún incidente con la seguridad de sus equipos.

Se puede entender que casi la mitad de los funcionarios has estado expuestos a los problemas de seguridad de cualquier nivel para la obtención de la información.

Pregunta:

¿Su computadora o equipo de trabajo se bloquea automáticamente cuando no la está utilizando?

Objetivo:

Identificar el mecanismo de seguridad instalada en la computadora o equipos de trabajos de los funcionarios del Juzgado para evitar la pérdida de información.

Bloqueo automático del equipo de trabajo

Tabla 5-4: Bloqueo automático del equipo de trabajo

Detalle	*Encuestados*	*Porcentaje*
Si	5	20%
No	18	72%
Desconoce	2	8%

Realizado por: (Costales Christian, 2020)

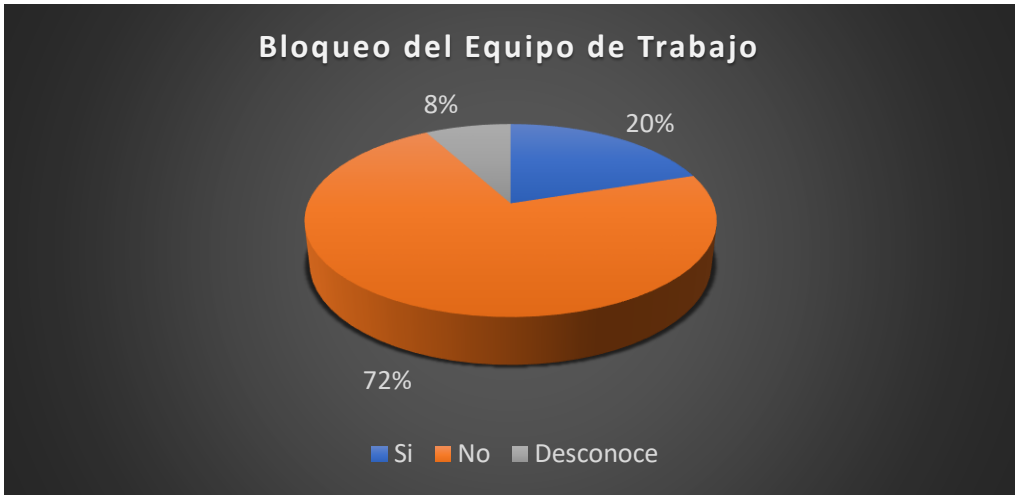

Gráfico 5-4: Bloqueo del Equipo de trabajo
Realizado por: (Costales Christian, 2020)

De los 25 funcionarios encuestados que corresponde al 100%, el 20% de los funcionarios dicen que sus equipos de trabajos cuentas con un mecanismo de seguridad, mientras que el 72% menciona que no poseen ninguna clase de mecanismos para la seguridad de sus equipos y el 8% desconocen de alguna clase de seguridad para sus equipos de trabajo.

Se puede decir que existe una grave falla de seguridad en los equipos de trabajos de los funcionarios, dada que cualquier persona puede ingresar para poder obtener la información que ahí se encuentra y hacer mal uso de esta.

Pregunta:

¿En la Institución (Juzgado) existen acuerdos documentados de Confidencialidad de la Información?

Objetivo:

Identificar si existen acuerdos firmados por los funcionarios para que no haya divulgación de la información hacia terceros.

Tabla 6-4: Divulgación de la Información

Detalle	*Encuestados*	*Porcentaje*
Si	7	28%
No	9	36%
Desconoce	9	36%

Realizado por: (Costales Christian, 2020)

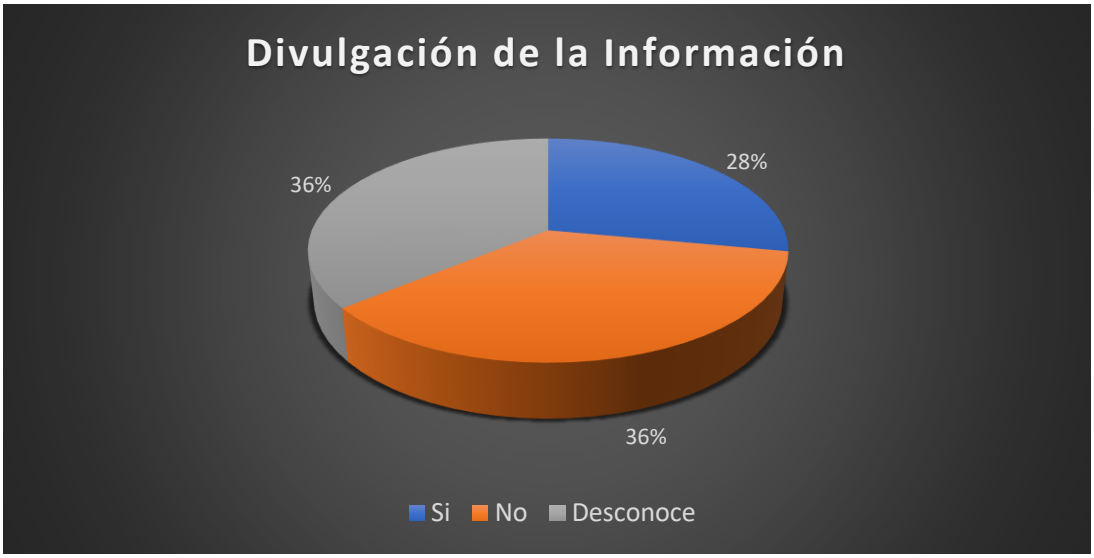

Gráfico 6-4: Divulgación de la Información
Realizado por: (Costales Christian, 2020)

De los 25 funcionarios encuestados que corresponde al 100%, el 28% de los funcionarios dicen que si existen documentos que les impide divulgar la información hacia terceros, mientras que el 36 % menciona que no poseen acuerdos de confidencialidad y el 36% desconocen de esto tipos de acuerdos confidenciales sobre la divulgación de la información que se maneja en la Institución.

Se puede decir que existe una grave falla de seguridad en cuanto a la divulgación de la información dentro y fuera de la Institución (Juzgado); para lo cual deben existir estos tipos de acuerdos de confidencialidad

Pregunta:

¿Se les capacita regularmente en temas de seguridad de la información?

Objetivo:

Identificar si existen capacitaciones de manera frecuente para mejorar la seguridad de la información dentro de la Institución (Juzgado)

Tabla 7-4: Capacitaciones sobre temas de Seguridad

Detalle	*Encuestados*	*Porcentaje*
Si	4	16%
No	12	48%
Desconoce	9	36%

Realizado por: (Costales Costales, 2020)

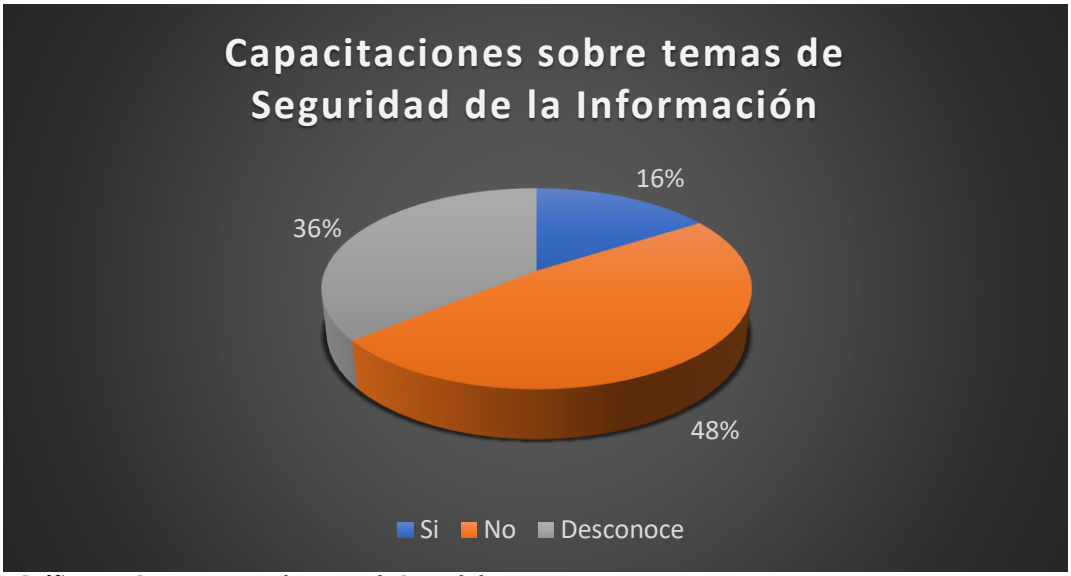

Gráfico 7-4: Capacitaciones sobre temas de Seguridad
Realizado por: (Costales Christian, 2020)

De los 25 funcionarios encuestados que corresponde al 100%, el 48% de los funcionarios dicen que no existen capacitaciones de manera constante sobre la seguridad de la información, mientras que el 36 % menciona que desconocen sobre las capacitaciones relacionadas con este tema y el 16% si tienen este tipo de capacitaciones sobre seguridad de la información de manera continua dentro de la Institución (Juzgado).

Se puede decir que no existen capacitaciones de manera continua dentro de la institución sobre el tema de seguridad de la información.

Pregunta:

¿Existen documentados, procedimientos o mecanismos de actualización del software antivirus?

Objetivo:

Identificar si existen mecanismos o procedimientos para la actualización de software de antivirus para evitar la pérdida o eliminación de información dentro de la Institución (Juzgado)

Tabla 8-4: Actualización del Software Antivirus

Detalle	*Encuestados*	*Porcentaje*
Si	11	44%
No	6	24%
Desconoce	8	32%

Realizado por: (Costales Christian, 2020)

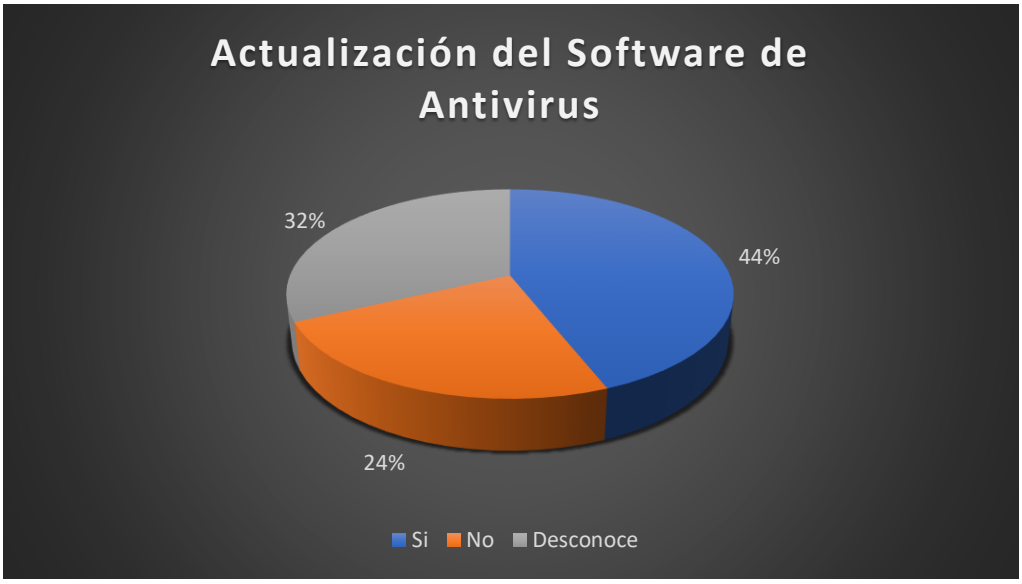

Gráfico 8-4: Actualización del Software de Antivirus
Realizado por: (Costales Christian, 2020)

De los 25 funcionarios encuestados que corresponde al 100%, el 44% de los funcionarios dicen que, si existen actualizaciones del Software antivirus de manera periódica, mientras que el 24 % menciona que desconocen sobre estas actualizaciones del software antivirus y el 32% no tienen estas actualizaciones del software de antivirus dentro de la Institución (Juzgado).

Pregunta:

¿Existen controles de acceso a las instalaciones para los funcionarios de la Institución (Juzgados)?

Objetivo:

Identificar si existen controles de accesos como (huella dactilar, firma de ingreso, gafetes, entre otros) a las instalaciones por los funcionarios del (Juzgado).

Tabla 9-4: Existen Respaldos de la Información

Detalle	*Encuestados*	*Porcentaje*
Si	19	76%
No	3	12%
Desconoce	3	12%

Realizado por: (Costales Christian, 2020)

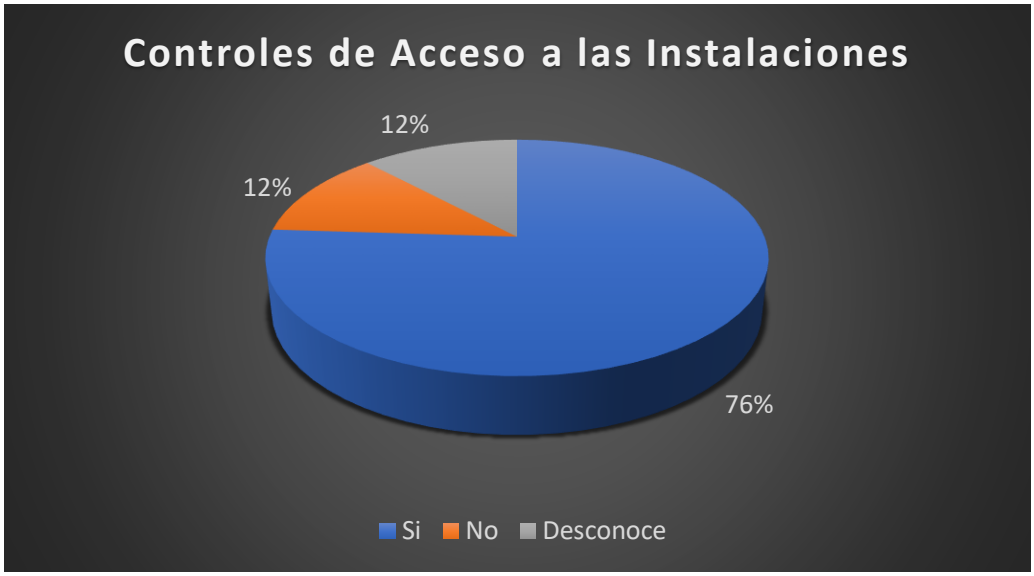

Gráfico 9-4: Controles de acceso a las instalaciones
Realizado por: (Costales Christian, 2020)

De los 25 funcionarios encuestados que corresponde al 100%, el 76% de los funcionarios dicen que, si existen controles para el ingreso del personal a las instalaciones, mientras que el 12 % menciona que desconocen sobre los controles de seguridad para el ingreso a las instalaciones y el 12% no poseen controles para el ingreso a las instalaciones de la Institución (Juzgado).

Pregunta:

¿Existen procedimientos documentados y disponibilidad de backups para la realización de respaldos de la información?

Objetivo:

Identificar si existen procedimientos y backups para hacer los respaldos de la información dentro de la Institución (Juzgado)

Tabla 10-4: Existe respaldos de la información

Detalle	*Encuestados*	*Porcentaje*
Si	22	88%
No	2	8%
Desconoce	1	4%

Realizados por: (Costales Christian, 2020)

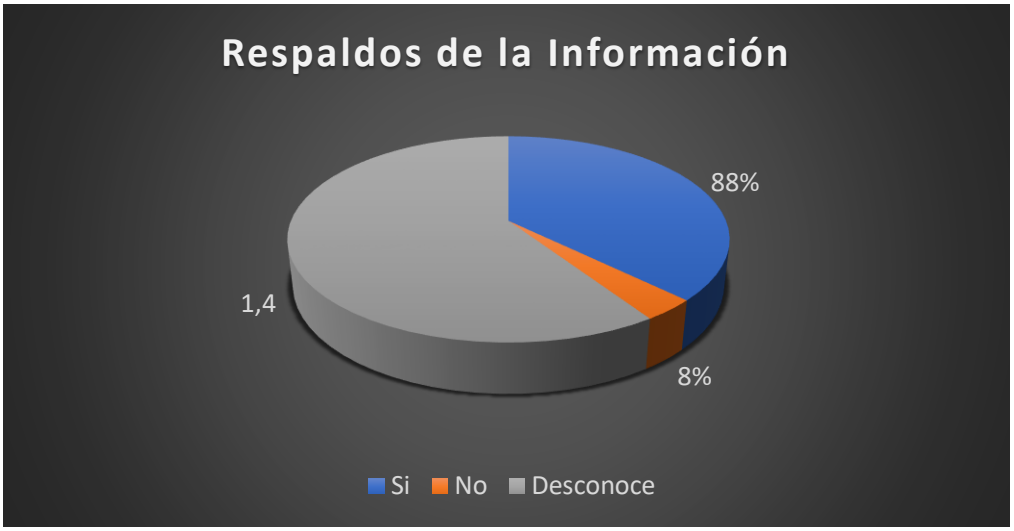

Gráfico 10-4: Respaldos de la Información
Realizado por: (Costales Christian, 2020)

De los 25 funcionarios encuestados que corresponde al 100%, el 88% de los funcionarios dicen que, si existen procedimientos para sacar respaldos de la información de manera periódica, mientras que el 4 % menciona que desconocen sobre los procedimientos para sacar respaldos de la información y el 8% no realizan respaldos de la información de manera periódica dentro de la Institución (Juzgado).

Tabla 11-4: Probabilidad de Ocurrencia del riesgo

ITEM	AMENAZAS	PROMEDIOS		PROBABILIDAD
		SI	**NO**	
1	Existencia del Manual de Políticas de Seguridad de la Información	8	5	0,2
2	Existe el área o responsables de la Seguridad Informática	13	7	0,28
3	Mecanismos de Autenticación (Contraseñas)	6	14	0,56
4	Acceso no autorizado a la información o datos	11	10	0,4
5	Herramientas de Seguridad Implementadas	5	18	0,72
6	Divulgación de la información	7	9	0,36
7	Errores de usuarios y operadores	4	12	0,48
8	Software o Código Malicioso	11	6	0,24
9	Sustracción o robo de información	19	3	0,12
10	Existen respaldos de información	22	2	0,08

Realizado por: (Costales Christian, 2020**)**

A continuación, se procede a obtener la valoración de ocurrencia, para lo cual evaluamos el impacto sobre el riesgo evaluado de acuerdo a la escala definida anteriormente, donde se obtienen los siguientes resultados.

Tabla 12-4: Valoración de ocurrencia

ITEM	AMENAZAS	PROBABILIDAD	IMPACTO	VALORACIÓN
1	Existencia del Manual de Políticas de Seguridad de la Información	0,2	3	0,6
2	Existe el área o responsables de la Seguridad Informática	0,28	4	1,12
3	Mecanismos de Autenticación (Contraseñas)	0,56	3	1,68
4	Acceso no autorizado a la información o datos	0,4	3	1,2
5	Herramientas de Seguridad Implementadas	0,72	4	2,88
6	Divulgación de la información	0,36	3	1,08
7	Errores de usuarios y operadores	0,48	3	1,44
8	Software o Código Malicioso	0,24	2	0,48
9	Sustracción o robo de información	0,12	3	0,36
10	Existen respaldos de información	0,08	4	0,32

Realizado por: (Costales Christian, 2020**)**

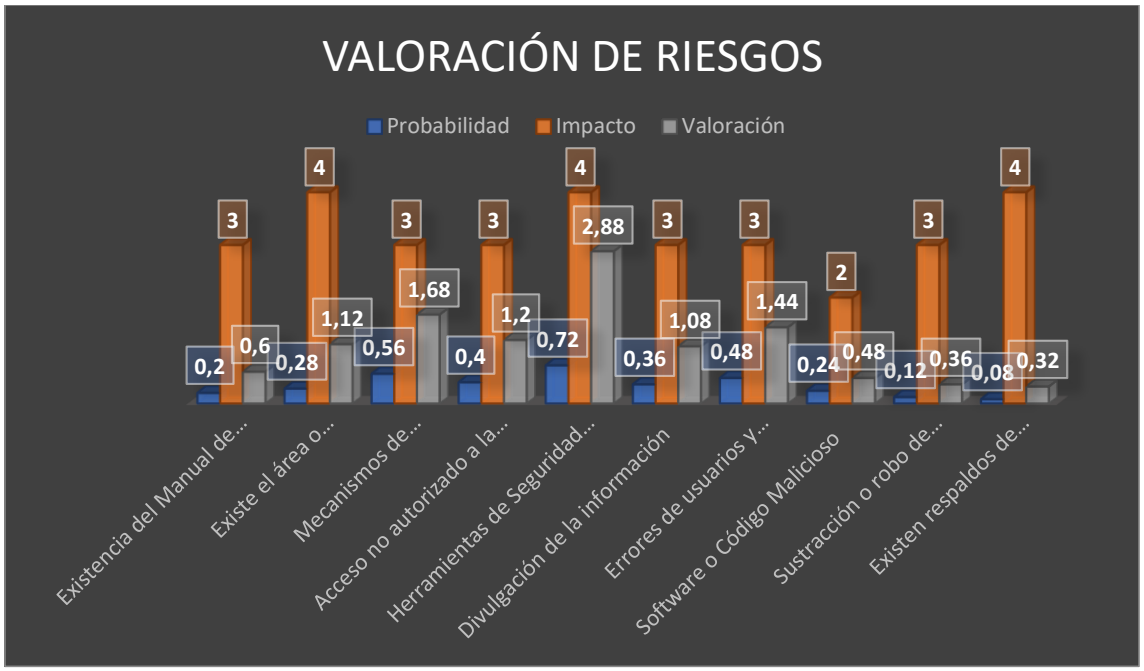

Gráfico 11-4: Valoración de Riegos
Realizado por: (Costales Christian, 2020)

De acuerdo al análisis de la valoración de riesgos los valores superiores 1,2 son las más críticos y a los cuales se les debe prestar mayor atención.

Tabla 13-4: Riesgos con Mayor Valoración

ITEM	AMENAZAS	PROBABILIDAD	IMPACTO	VALORACIÓN
1	Mecanismos de Autenticación (Contraseñas)	0,56	3	1,68
2	Acceso no autorizado a la información o datos	0,4	3	1,2
3	Herramientas de Seguridad Implementadas	0,72	4	2,88
4	Errores de usuarios y operadores	0,48	3	1,44

Realizado por: (Costales Christian, 2020)

En la tabla anterior se muestra directamente como se está afectando la Confidencialidad, Privacidad, Integridad, de la información digital que se generan dentro de la Institución (Juzgados), por la falta de procedimientos adecuados que permitan asegurar dicha información.

4.2. Análisis de la situación Post-Implementación

Después de haber implementado los procedimientos obtenidos del método basados en la norma ISO 27001 se aplicó nuevamente la misma encuesta que se hizo el análisis inicial, siguiendo la misma metodología, de lo cual se obtuvo los siguientes resultados:

Pregunta:

¿Existe Manual de Políticas de Seguridad de la información?

Objetivo:

Identificar si existe el Manual de Políticas de Seguridad de la Información para saber si ellos realizan adecuadamente las actividades sin necesidad de tener una dependencia para su ejecución.

Existencia de un Manual de Políticas de Seguridad de la información

Tabla 14-4: Existencia de un Manual de Políticas de Seguridad de la información

Detalle	*Encuestados*	*Porcentaje*
Si	20	80%
No	3	12%
Desconoce	2	8%

Realizado por: (Costales Christian, 2020)

Gráfico 12-4: Existe un Manual de Políticas de Seguridad de la información
Realizado por: (Costales Christian, 2020)

De los 25 funcionarios encuestados que corresponde al 100%, el 8 % desconocen que existe este Manual de Políticas de Seguridad de la Informacion, el 12 % no sabe nada acerca de este tema, mientras que el 80% conocen que existe este manual.

Pregunta:

¿Existe en la Institución (Juzgado) un responsable o área encargada de la Seguridad de la información o Seguridad Informática?

Objetivo:

Conocer si los funcionarios del Juzgado saben si existe esta área o responsables de la Seguridad de la Información o algo similar.

Tabla 15-4: Existe un área de la Seguridad Informática

Detalle	*Encuestados*	*Porcentaje*
Si	18	72%
No	4	16%
Desconoce	3	12%

Realizado por: (Costales Christian, 2020)

Gráfico 13-4: Existe un área de la Seguridad Informática
Realizado por: (Costales Christian, 2020)

De los 25 funcionarios encuestados que corresponde al 100%, el 72 % conoce que, si existe esta área o responsables de la Seguridad de la Información, el 16 % no sabe nada acerca de los responsables de la Seguridad de la Información, mientras que el 12% desconocen de este tema.

Se puede entender que existe una figura que cumple por partes con el rol de responsable de seguridad de la información, pero no están formalmente establecidas sus funciones.

Pregunta:

¿Las contraseñas que utiliza usted poseen una combinación de números, letras y es más de 8 cárteres?

Objetivo:

Conocer si los funcionarios del Juzgado establecen medidas mínimas de seguridad para la protección de la información.

Seguridad en las contraseñas de los funcionarios

Tabla 16-4: Seguridad en las contraseñas de los funcionarios

Detalle	*Encuestados*	*Porcentaje*
Solo números y más de 8 caracteres	1	4%
Solo letras y más de 8 caracteres	0	-
Letras y números con más de 8 caracteres	7	28%
Otras	17	68%

Realizado por: (Costales Christian, 2020)

Gráfico 14-4: Seguridad en las Contraseñas de los funcionarios
Realizado por: (Costales Christian, 2020)

De los 25 funcionarios encuestados que corresponde al 100%, el 28% utiliza números y letras con más de 8 caracteres, mientras que el 4 % utilizan solo letras o números para las contraseñas de sus equipos, y el 68% opta por otra clase de contraseñas como símbolos, letras con longitudes, huellas dactilares entre otras.

Se puede entender que la gestión de autenticación de los usuarios o funcionarios de los sistemas de procesamiento de la información no es homogénea según los datos obtenidos de las encuestas.

Pregunta:

¿Se ha generado alguna clase de incidente en la seguridad en su puesto de trabajo en el último año como por ejemplo (pérdida de documentos, daño en la computadora, bloqueo, entre otros)?

Objetivo:

Identificar los incidentes de seguridad que han reportados los usuarios o funcionarios

Tabla 17-4: Incidentes de Seguridad

Detalle	*Encuestados*	*Porcentaje*
Si	8	32%
No	15	60%
Desconoce	2	8%

Realizados por: (Costales Christian, 2020)

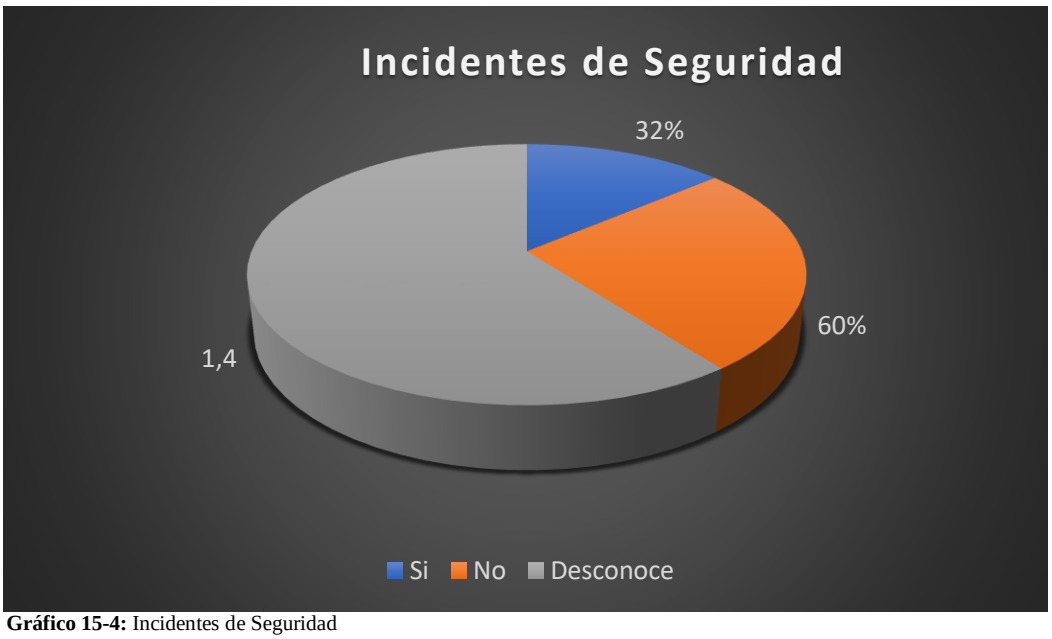

Gráfico 15-4: Incidentes de Seguridad
Realizado por: (Costales Christian, 2020)

De los 25 funcionarios encuestados que corresponde al 100%, el 32% de los funcionarios han experimentado un problema de seguridad, mientras que el 60% no ha reportado ninguna clase de problema en la seguridad de sus equipos, y el 8% desconocen si han tenido algún incidente con la seguridad de sus equipos.

Se puede entender que casi la mitad de los funcionarios has estado expuestos a los problemas de seguridad de cualquier nivel para la obtención de la información.

Pregunta:

¿Su computadora o equipo de trabajo se bloquea automáticamente cuando no la está utilizando?

Objetivo:

Identificar el mecanismo de seguridad instalada en la computadora o equipos de trabajos de los funcionarios del Juzgado para evitar la pérdida de información.

Bloqueo automático del equipo de trabajo

Tabla 18-4: Bloqueo automático del equipo de trabajo

Detalle	*Encuestados*	*Porcentaje*
Si	14	56%
No	7	28%
Desconoce	4	16%

Realizado por: (Costales Christian, 2020)

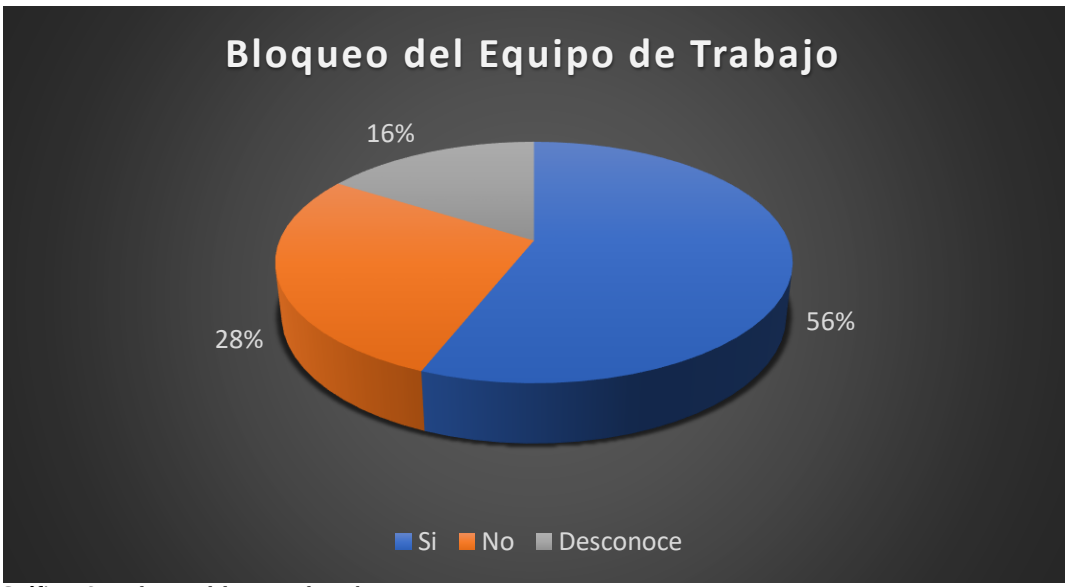

Gráfico 16-4: Bloqueo del Equipo de Trabajo
Realizado por: (Costales Christian, 2020)

De los 25 funcionarios encuestados que corresponde al 100%, el 56% de los funcionarios dicen que sus equipos de trabajos cuentas con un mecanismo de seguridad, mientras que el 28% menciona que

no poseen ninguna clase de mecanismos para la seguridad de sus equipos y el 16% desconocen de alguna clase de seguridad para sus equipos de trabajo.

Se puede decir que existe una grave falla de seguridad en los equipos de trabajos de los funcionarios, dada que cualquier persona puede ingresar para poder obtener la información que ahí se encuentra y hacer mal uso de esta.

Pregunta:

¿En la Institución (Juzgado) existen acuerdos documentados de Confidencialidad de la Información?

Objetivo:

Identificar si existen acuerdos firmados por los funcionarios para que no haya divulgación de la información hacia terceros.

Tabla 19-4: Divulgación de la Informacion

Detalle	*Encuestados*	*Porcentaje*
Si	15	60%
No	4	16%
Desconoce	6	24%

Realizado por: (Costales Christian, 2020)

Gráfico 17-4: Divulgación de la Información
Realizado por: (Costales Christian, 2020)

De los 25 funcionarios encuestados que corresponde al 100%, el 60% de los funcionarios dicen que si existen documentos que les impide divulgar la información hacia terceros, mientras que el 16 % menciona que no poseen acuerdos de confidencialidad y el 24% desconocen de esto tipos de acuerdos confidenciales sobre la divulgación de la información que se maneja en la Institución.

Se puede decir que existe una grave falla de seguridad en cuanto a la divulgación de la información dentro y fuera de la Institución (Juzgado); para lo cual deben existir estos tipos de acuerdos de confidencialidad

Pregunta:

¿Se les capacita regularmente en temas de seguridad de la información?

Objetivo:

Identificar si existen capacitaciones de manera frecuente para mejorar la seguridad de la información dentro de la Institución (Juzgado)

Tabla 20-4: Capacitaciones sobre temas de Seguridad de la Información

Detalle	*Encuestados*	*Porcentaje*
Si	11	44%
No	5	20%
Desconoce	9	36%

Realizado por: (Costales Christian, 2020)

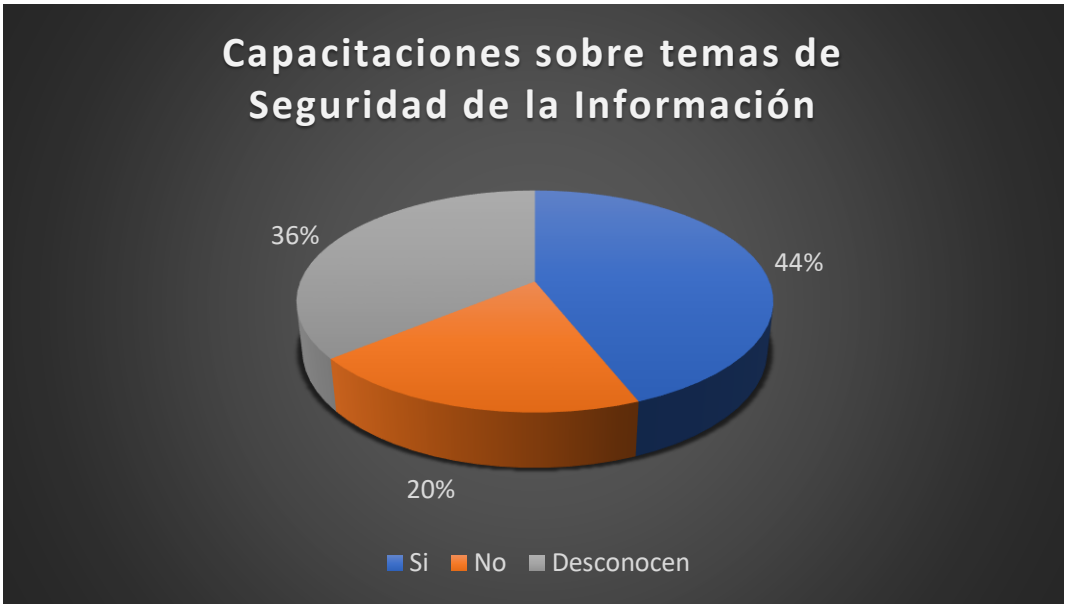

Gráfico 18-4: Capacitaciones sobre temas de Seguridad de la Información
Realizado por: (Costales Christian, 2020)

De los 25 funcionarios encuestados que corresponde al 100%, el 20% de los funcionarios dicen que no existen capacitaciones de manera constante sobre la seguridad de la información, mientras que el 36 % menciona que desconocen sobre las capacitaciones relacionadas con este tema y el 44% si tienen este tipo de capacitaciones sobre seguridad de la información de manera continua dentro de la Institución (Juzgado).

Se puede decir que no existen capacitaciones de manera continua dentro de la institución sobre el tema de seguridad de la información.

Pregunta:

¿Existen documentados, procedimientos o mecanismos de actualización del software antivirus?

Objetivo:

Identificar si existen mecanismos o procedimientos para la actualización de software de antivirus para evitar la pérdida o eliminación de información dentro de la Institución (Juzgado)

Tabla 21-4: Actualización del Software Antivirus

Detalle	*Encuestados*	*Porcentaje*
Si	17	68%
No	5	20%
Desconoce	3	12%

Realizado por: (Costales Christian, 2020)

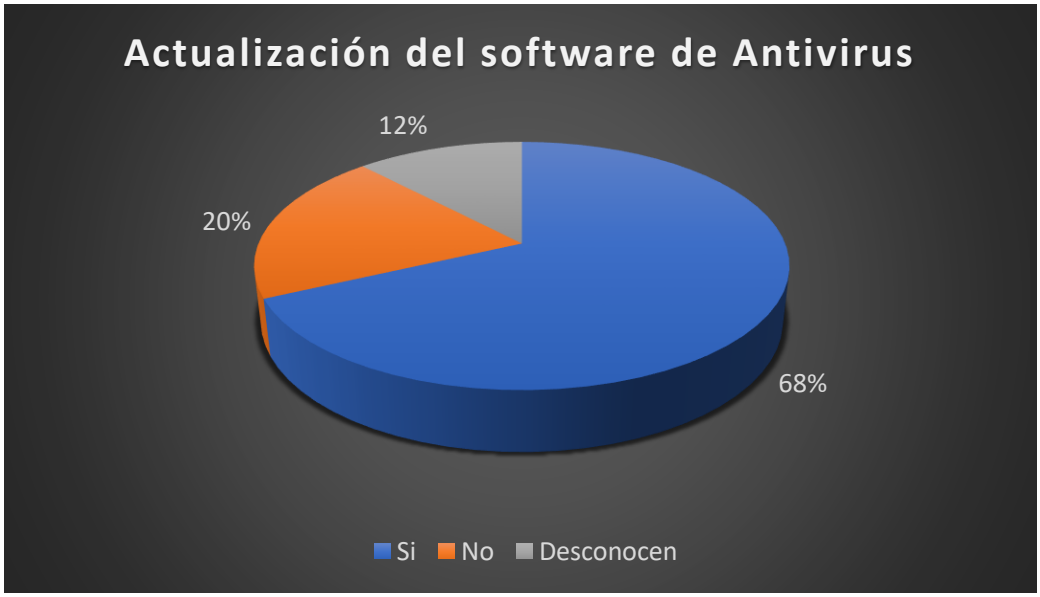

Gráfico 19-4: Actualización del software de Antivirus
Fuente: (Costales Christian, 2020)

De los 25 funcionarios encuestados que corresponde al 100%, el 68% de los funcionarios dicen que, si existen actualizaciones del Software antivirus de manera periódica, mientras que el 12 % menciona que desconocen sobre estas actualizaciones del software antivirus y el 20% no tienen estas actualizaciones del software de antivirus.

Pregunta:

¿Existen controles de acceso a las instalaciones para los funcionarios de la Institución (Juzgados)?

Objetivo:

Identificar si existen controles de accesos como (huella dactilar, firma de ingreso, gafetes, entre otros) a las instalaciones por los funcionarios del (Juzgado).

Existen respaldos de la información

Tabla 22-4: Existe respaldos de la información

Detalle	*Encuestados*	*Porcentaje*
Si	22	88%
No	1	4%
Desconoce	2	8%

Realizado por: (Costales Christian, 2020)

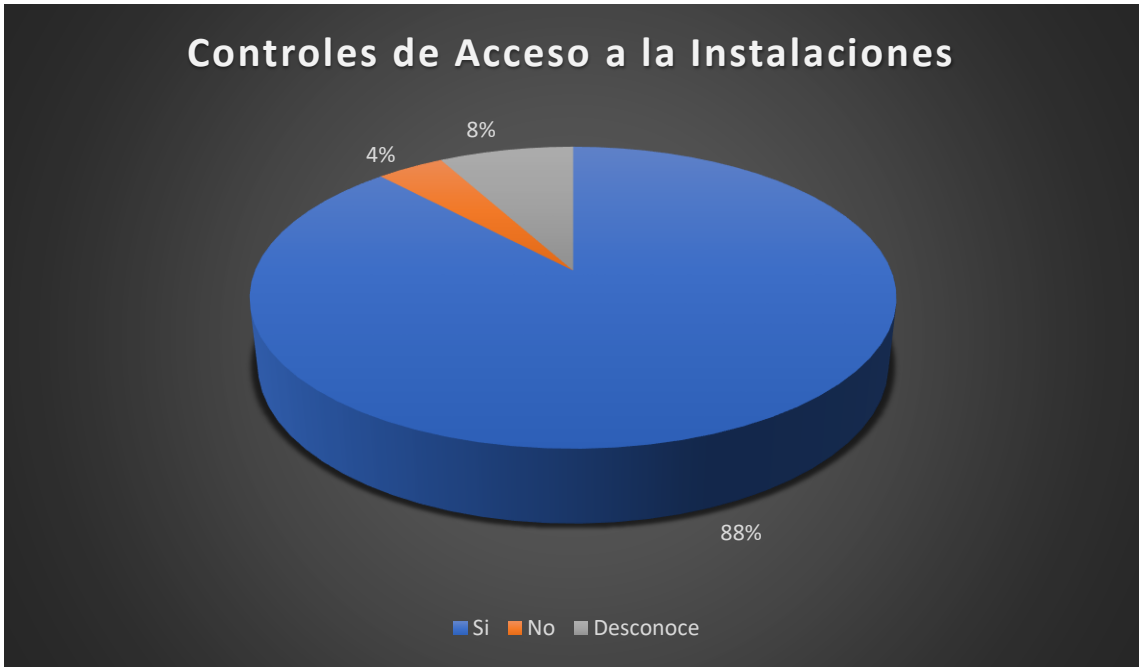

Gráfico 20-4: Controles de Acceso a la Información
Fuente: (Costales Christian, 2020)

De los 25 funcionarios encuestados que corresponde al 100%, el 88% de los funcionarios dicen que, si existen controles para el ingreso del personal a las instalaciones, mientras que el 8 % menciona que desconocen sobre los controles de seguridad para el ingreso a las instalaciones y el 4% no poseen controles para el ingreso a las instalaciones de la Institución (Juzgado).

Pregunta:

¿Existen procedimientos documentados y disponibilidad de backups para la realización de respaldos de la información?

Objetivo:

Identificar si existen procedimientos y backups para hacer los respaldos de la información dentro de la Institución (Juzgado)

Existen respaldos de la información

Tabla 23-4: Existen respaldos de la información

Detalle	*Encuestados*	*Porcentaje*
Si	25	100%
No	0	0%
Desconoce	0	0%

Realizado por: (Costales Christian, 2020)

Gráfico 21-4: Respaldos de la Información
Fuente: (Costales Christian, 2020)

De los 25 funcionarios encuestados que corresponde al 100%, el 100% de los funcionarios dicen que, si existen procedimientos para sacar respaldos de la información de manera periódica, mientras que el 0 % menciona que desconocen sobre los procedimientos para sacar respaldos de la información y el 0% no realizan respaldos de la información de manera periódica dentro de la Institución (Juzgado).

Tabla 24-4: Probabilidad de Ocurrencia del riesgo Post-Implementación

ITEM	AMENAZAS	PROMEDIOS		PROBABILIDAD
		SI	**NO**	
1	Existencia del Manual de Políticas de Seguridad de la Información	20	3	0,12
2	Existe el área o responsables de la Seguridad Informática	18	4	0,16
3	Mecanismos de Autenticación (Contraseñas)	17	1	0,04
4	Acceso no autorizado a la información o datos	8	15	0,6
5	Herramientas de Seguridad Implementadas	14	7	0,28
6	Divulgación de la información	15	4	0,16
7	Errores de usuarios y operadores	11	5	0,20
8	Software o Código Malicioso	17	5	0,20
9	Sustracción o robo de información	22	1	0,04
10	Existen respaldos de información	25	0	0

Realizado por: (Costales Christian, 2020**)**

A continuación, se procede a obtener la valoración de ocurrencia, para lo cual evaluamos el impacto sobre el riesgo evaluado de acuerdo a la escala definida anteriormente, donde se obtienen los siguientes resultados.

Tabla 25-4: Valoración de ocurrencia Post-Implementación

ITEM	AMENAZAS	PROBABILIDAD	IMPACTO	VALORACIÓN
1	Existencia del Manual de Políticas de Seguridad de la Información	0,12	4	0,48
2	Existe el área o responsables de la Seguridad Informática	0,16	4	0,64
3	Mecanismos de Autenticación (Contraseñas)	0,04	3	0,12
4	Acceso no autorizado a la información o datos	0,6	3	1,8
5	Herramientas de Seguridad Implementadas	0,28	3	0,84
6	Divulgación de la información	0,16	4	0,64
7	Errores de usuarios y operadores	0,20	3	0,60
8	Software o Código Malicioso	0,20	4	0,80
9	Sustracción o robo de información	0,04	4	0,12
10	Existen respaldos de información	0	4	0

Realizado por: (Costales Christian, 2020**)**

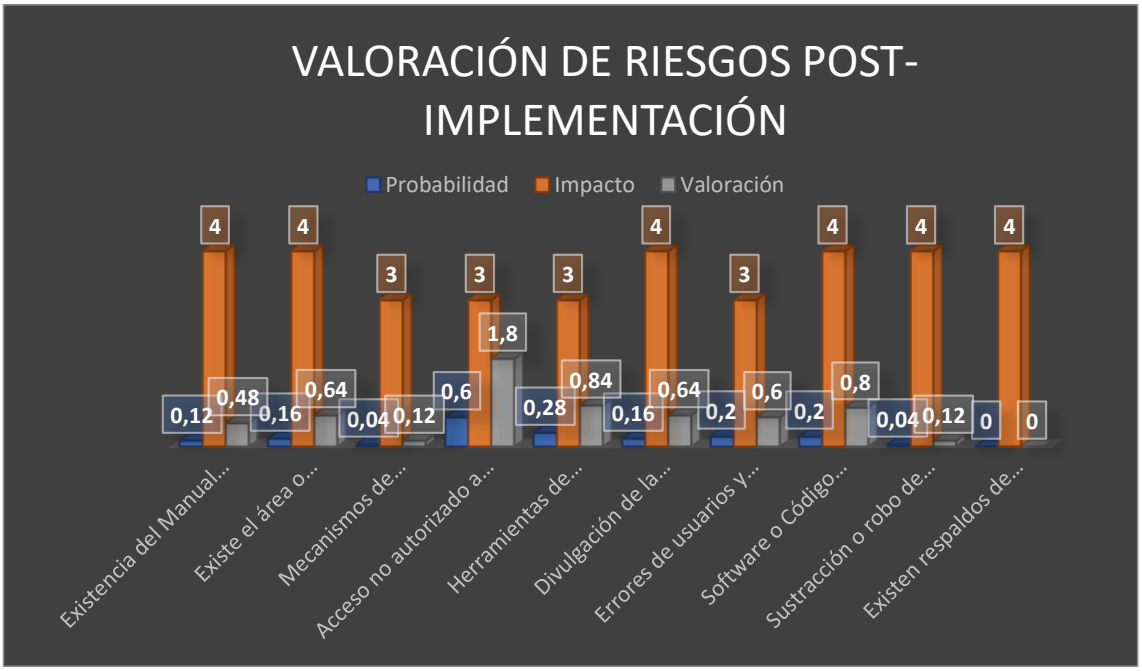

Gráfico 22-4: Valoración de Riesgos Post-Implementación
Fuente: (Costales Christian, 2020)

Como se puede observar en la gráfica anterior se puede establecer que los riesgos de ponderación superior a los 1.2 que se establecieron en la situación inicial han disminuido notablemente:

Tabla 26-4: Riesgos de Valoración Inicial – Post- Implementación

ITEM	AMENAZAS	Valoración Inicial	Valoración Post- Implementación
1	Mecanismos de Autenticación (Contraseñas)	1,68	0,12
2	Acceso no autorizado a la información o datos	1,2	1,8
3	Herramientas de Seguridad Implementadas	2,88	0,84
4	Errores de usuarios y operadores	1,44	0,60

Realizado por: (Costales Christian, 2020)

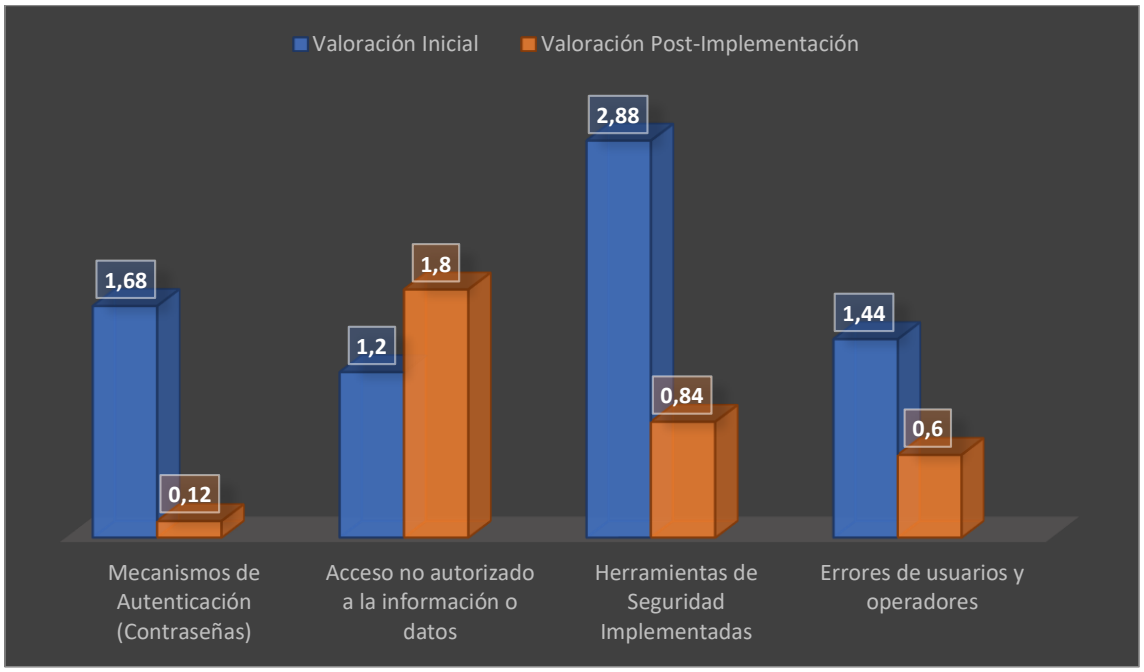

Gráfico 23-4: Riesgos de Valoración Inicial y Post-Implementación
Realizado por: (Costales Costales, 2020)

Como podemos observar en la figura anterior, luego de haber aplicado el modelo generado con los procedimientos, se ha reducido sustancialmente la ponderación de la probabilidad de que los riesgos frente a la situación inicial.

4.3. Comprobación de la Hipótesis

Una de las pruebas estadísticas es la prueba T de Student, que es cualquier prueba en la que el estadístico utilizado tiene una distribución T de Student si la hipótesis nula es cierta.

Se aplica cuando la población estudiada sigue una distribución normal pero el tamaño de la muestra es demasiado pequeño como para que el estadístico en el que está basada la inferencia esté normalmente distribuido, utilizándose una estimación de la desviación típica en lugar del valor real.

4.3.1. Planteamiento de la Hipótesis

Hipótesis de investigación Hi: El Método para el manejo de información digital permitirá mejorar el nivel de seguridad de la información

Hipótesis de Nula H_0: El Método para el manejo de información digital no permitirá mejorar el nivel de seguridad de la información

5. $H_o: \mu_{\bar{d}} = 0$

Hipótesis Alternativa H_1: El Método para el manejo de información digital permitirá mejorar el nivel de seguridad de la información

6. $H1: \mu_{\bar{d}} \neq 0$

Dónde$\mu_{\bar{d}}$ es la media de las medidas.

4.3.2. Nivel de Significancia

Se debe elegir un nivel de significancia para la prueba que permite analizar los resultados de la prueba son estadísticamente significativos y también determina la probabilidad de error que es inherente a la prueba.

Para nuestra investigación se establece un nivel de significancia (denotado como α o alfa) de 0.05. Un nivel de significancia de 0.05 indica un riesgo de 5% de concluir que existe una diferencia cuando no hay una diferencia real.

$$\alpha = 0.05$$

4.3.3. Prueba Estadística

En función de los datos obtenidos utilizamos la distribución T de Student, donde se establece que:

$$t_c = \frac{\bar{d}}{\frac{S_d}{\sqrt{n}}}$$

$$S_d = \sqrt{\frac{\sum_{i=1}^{n}(d-\bar{d})^2}{n-1}}$$

Dónde:

t_c = valor estadístico del procedimiento calculado.

$\bar{d}$ = Valor promedio o media aritmética de las diferencias entre los momentos antes y después.

S_d = desviación estándar de las diferencias entre los momentos antes y después.

n = tamaño de la muestra.

4.3.4. *Regla de Decisiones*

Caso 1.

$$t_c > t_\alpha, rechaza\ la\ hipotesis\ nula\ H_0$$

Caso 2.

$$Valor\ p < \alpha, se\ rechaza\ la\ hipotesis\ nula \quad {}_0$$

4.3.5. Conclusiones

La data fue evaluada en la herramienta Análisis de Datos, con la función Prueba t para medias de dos muestras emparejadas, de Microsoft Excel.

Normalidad

Para la prueba de Normalidad en la que se debe aceptar la hipótesis nula y se consideran todas las categorías de riesgos ponderadas según la siguiente tabla:

Tabla 27-4: Datos Iniciales y de Post-Implementación

ITEM	AMENAZAS	Valoración Inicial	Valoración Post- Implementación
1	Mecanismos de Autenticación (Contraseñas)	1,68	0,12
2	Acceso no autorizado a la información o datos	1,2	1,8
3	Herramientas de Seguridad Implementadas	2,88	0,84
4	Errores de usuarios y operadores	1,44	0,60

Realizado por: (Costales Christian, 2020)

Resultados de la prueba t Student

	Variable 1	*Variable 2*
Media	3,3140	0,606
Varianza	0,3632	0,43133
Observaciones	5,0000	5
Coeficiente de correlación de Pearson	-0,6120	
Diferencia hipotética de las medias	0,0000	
Grados de libertad	4,0000	
Estadístico t	5,3543	
P(T<=t) una cola	0,0029	
Valor crítico de t (una cola)	2,1318	
P(T<=t) dos colas	0,005869	
Valor crítico de t (dos colas)	2,7764	

Fuente: Herramienta Análisis de Datos, con la función Prueba t para medias de dos muestras emparejadas

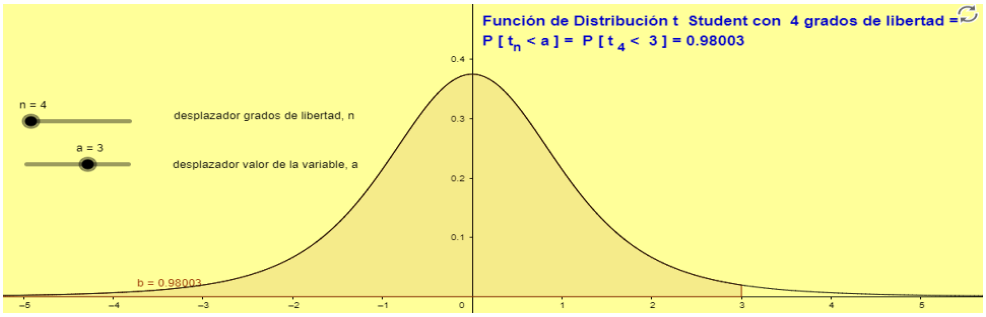

Gráfico 24-4: Curva Normal T de student
Realizado por: (Costales Costales, 2020)

En promedio de los riesgos de amenazas inicial es 3,3140 mayor que los riesgos de amenaza post implementación igual 0,606, hay una diferencia significativa

El valor de P, que es el nivel de significancia cuya valor es 0,005869, es menor que el valor determinado para α = 0,05 por lo que nos lleva a rechazar la hipótesis nula H0 y aceptar la alternativa H1.

Con esto concluimos que la diferencia de las medias de los riesgos obtenidos con amenaza inicial y post-Implementación, son significativamente diferentes con un nivel de confianza del 95%.

4.4. Definición del método para mejorar la seguridad Informática en el Juzgado

Una vez que se cuenta con el método para mejorar la seguridad de la información basado en la norma ISO 27001, se presentan los resultados de la aplicación del método desarrollado, partiendo de los antecedentes y necesidades específicas para este proceso.

4.4.1. Proceso donde se va aplicar el Método

En el diagrama de procesos se procedió a identificar todas las actividades que intervienen para cumplir una diligencia realizada en la seguridad de la información, se ha procedido a identificar, personas, documentos, sistemas, hardware etc. que intervienen en el proceso.

4.4.2. Planteamiento de la Hipótesis

Se procede a identificar y seleccionar cada uno de los activos de información que intervienen en el proceso que generan, procesan o almacenan información y permiten alcanzar los objetivos del proceso que se está planteando.

Para la clasificación de los activos se ha considerado identificarlos en sus diversos tipos, los cuales pueden ser: Software, Documentos Físicos, Documentos Electrónicos, Hardware y Recurso Humano. Los cuales son listados en la tabla siguiente.

Tabla 28-4: **Inventario de Activos de Información**

ID	**ACTIVO DE INFORMACION IDENTIFICADO**	**DESCRIPCION**	**TIPO**	**RESPONSABLE**
1	Sistema de Documentación	Sistema informático en el cual se registran y se generar automáticamente la numeración de oficios, memos internos y externos.	Software	Técnicos del sistema de Documentación.
2	Bitácora de registro física	Documento que permite registrar el ingreso y salida de los funcionarios.	Físico	Técnico o Persona Encargada
3	Internet	Servicio proporcionado por empresas privadas o públicas, para poder realizar las diferentes actividades en línea.	Software	Técnicos de Infraestructura
4	Formulario de registro de diligencia	Documento donde se registra todos los datos y firmas pertinentes de las personas no autorizadas.	Físico	Técnico o secretaria
5	Hardware para la grabación	Dispositivo o cámaras que permite almacenar el desarrollo de la actividad, respaldando el contenido en un medio magnético.	Físico	Técnico de Vigilancia

Fuente: (Costales Christian, 2020)

4.4.3. Agrupación de los Activos

Se generó los resultados de los activos que son 5 se procede a realizar la agrupación de los activos para reducir en el menor número de activos, la agrupación se lo realiza por el tipo de Activo de Información, haciendo el respectivo análisis y dando una nueva etiqueta que englobe todos los activos.

En la tabla siguiente se puede observar cómo son agrupados los activos de Información de acuerdo al Tipo.

Tabla 29-4: Activos de Información de acuerdo al tipo

ID	ACTIVO DE INFORMACIÓN GENERAL	ACTIVO DE INFORMACIÓN	TIPO
1	FORMULARIOS Y DOCUMENTOS DE REGISTRO	Bitácora de registro física	Físico
		Formulario de registro	
		Firma	
		Formulario de entrega	
2	PERSONAL TÉCNICO	Técnico del Área de Sistemas	Recurso Humano
		Guardia Privada	
3	SOFTWARE y SERVICIOS	Consulta en Línea	Software
		Sistema de Documentación	
		Internet	
4	HARDWARE	Hardware	Físico

Fuente: (Costales Christian, 2020)

En la tabla anterior se observan los resultados de haber agrupado los activos de información general, obteniendo un total de 5 activos de información, donde se realiza una descripción de cada uno y su tipo.

Tabla 30-4: Inventario de Activos de Información en General

ID	ACTIVO DE INFORMACIÓN	DESCRIPCIÓN	TIPO
1	FORMULARIOS Y DOCUMENTOS DE REGISTRO	Documento Físico que permite el registro y verificación de datos de los funcionarios y personal que ingresa al Juzgado	Físico
2	PERSONAL TÉCNICO	Funcionarios o personal encargado del buen funcionamiento del sistema para las diferentes actividades.	Recurso Humano
3	SOFTWARE y SERVICIOS	Software y servicios utilizados para la realización de las diferentes actividades físicas o en línea.	Software
5	HARDWARE	Son todos los equipos y dispositivos utilizados para la generación, procesamiento, almacenamiento y distribución de la información.	Físico

Fuente: (Costales Christian, 2020)

4.4.4. Activos sometidos a la Matriz de Vulnerabilidad y Amenazas

En las Instituciones todos los activos de información están sometidos a distintas formas de amenazas, esas pueden causar daños a los activos, estas se pueden manifestar de diferentes formas o provenir de diferentes fuentes; para que estas causen daños deben violar una o varias vulnerabilidades antes mencionadas. Estas vulnerabilidades están enfocadas en las debilidades del sistema de seguridad.

Las amenazas y vulnerabilidades que afectan a la seguridad de la información digital en la Institución, se basan en el análisis realizado de las Norma ISO27001, y de la experiencia adquirida y con asesoramiento de un experto en Seguridad Informática.

En la tabla siguiente se puede observar todos los activos sometidos a las amenazas y vulnerabilidades que se pueden presentar en un determinado tiempo.

Tabla 31-4: Amenazas y Vulnerabilidades de los Activos

ID	Activo de Información	Amenazas	Vulnerabilidades
1	**Formularios y documentos de registro**	Manual de políticas de Seguridad de la Información	Falta de conocimiento de estos manuales por los funcionarios.
		Área o Responsables de la Seguridad Informática.	Que no existe un personal capacitado en este tema.
		Herramientas de Seguridad Implantados	No poseen contraseñas adecuadas en sus equipos de trabajos.
		Divulgación de la información	Falta de acuerdos de confidencialidad
		Destrucción de la información	Falta de un debido control de acceso a usuarios y de una protección física
		Errores de usuarios y operadores	Falta de conciencia en seguridad de la información
		Acceso no autorizado a datos	Falta de módulos de identificación / autenticaciones confiables para los funcionarios.
		Errores del personal y acciones equivocadas	Falta de conocimiento y oportuno entrenamiento
		Mecanismos de Autenticación	Falta de una política o manuales que establezca reglas que prohíba que no se debe suministrar información a terceros cuando no están debidamente identificados.
		Destrucción, robo, fraude, sabotaje de instalaciones y equipos	Falta de seguridad física

		Robo y Fraude	Falta de mecanismos de identificación / autenticaciones confiables
		Amenazas Externas o Medioambientales (incendio, inundación, terremoto, maremoto, explosión, desordenes civiles)	Las instalaciones y equipos son susceptibles a desastres por lo cual se debe sacar respaldos de toda la información.
2	**Personal Técnico**	Divulgación de la información	Debe existir políticas o reglamentos que prohíba suministrar información a terceras personas.
		Errores de usuarios y operadores	Contraseñas inadecuadas.
		Incapacidad y restauración	No está definido un plan de recuperación de información.
		Falla en la elección del personal	Falta de especificaciones con respecto a la selección de personal
		Pérdida o ausencia de personal clave	Falta de personal capacitado para reemplazo de empleados en esta área.
3	**Software y Servicios**		
		Acceso no autorizado a datos	Inadecuada segregación de funciones del personal.
		Destrucción de la información	Falta de un debido control de acceso a usuarios y de una protección física
		Divulgación de la información	Almacenamiento no protegido
		Acceso remoto no autorizado	Falta de mecanismos de identificación / autenticaciones confiables
		Acceso remoto no autorizado	Falta de mecanismos para la detección de intrusos
		Acceso remoto no autorizado a la red	Despliegue de información que pueda facilitar una conexión remota no autorizada
		Código malicioso	Indisponibilidad de backups de información electrónica o sistemas de backup
		Código malicioso	No hay procedimientos o mecanismos de actualización del software antivirus
		Destrucción, robo, fraude, sabotaje de instalaciones y equipos	Falta de seguridad física
		Falla en servicios de comunicación	Falta de planeación en capacidad o cambios en la red
		Robo y Fraude	Falta de logs de auditoría
		Robo y Fraude	Falta de políticas y procedimientos de control de cambios

		Robo y Fraude	Copias no controladas de datos y software
		Sabotaje	Falta de un procedimiento de administración de privilegios de acceso
		Uso de software pirata	No está definido el uso, control, instalación de software pirata.
		Amenazas Externas o Medioambientales (incendio, inundación, terremoto, maremoto, explosión, desordenes civiles)	Las instalaciones y equipos son susceptibles a desastres.
4	**Hardware**	Errores de usuarios y operadores	Entrenamiento insuficiente en seguridad
		Errores del personal y acciones equivocadas	Falta de conocimiento, entrenamiento o capacitaciones
		Pérdida o ausencia de personal clave	No existe personal capacitado en el área de seguridad de la información
		Acceso no autorizado a datos	Falta de seguridad física de los dispositivos de comunicaciones y cableado
		Acceso no autorizado a datos	Falta de un procedimiento de registro y autorización de salida de equipos
		Contaminación	Falta de mantenimiento de equipos e instalaciones
		Falla en servicios de comunicación	Falta de planeación en capacidad o cambios en la red
		Fallas técnicas – Hardware	Falta de mantenimiento de equipos e instalaciones
		Fallas técnicas – Hardware	Falta de procedimientos de monitoreo de hardware
		Fluctuaciones de potencia eléctrica	No existen sistemas de regulación
		Destrucción, robo, fraude, sabotaje de instalaciones y equipos	Falta de seguridad física
		Sabotaje	Falta de conciencia en seguridad de la información
		Sniffing	Falta de seguridad física de los dispositivos de comunicaciones y cableado
		Amenazas Externas o Medioambientales (incendio, inundación, terremoto, maremoto, explosión, desordenes civiles)	Las instalaciones y equipos son susceptibles a desastres.

Realizado por: (Costales Christian, 2020)

4.4.5. Evaluación del tratamiento de Riesgo

Luego de obtener las Amenazas y Vulnerabilidades de la seguridad de la Información o seguridad Informática por cada uno de los activos se pretende seleccionar las alternativas más adecuada de acuerdo a las necesidades y requerimientos de la institución (Juzgado).

En la tabla siguiente se muestra las diferentes alternativas para el tratamiento para cada una de las amenazas y vulnerabilidades de los activos de información.

Tabla 32-4: **Alternativa de Tratamiento del Riesgo**

ID	Activo de Información	Amenazas	Vulnerabilidades	Alternativa de Tratamiento
1	**Formularios y documentos de registro**	Manual de políticas de Seguridad de la Información	Falta de conocimiento de estos manuales por los funcionarios.	Crear
		Área o Responsables de la Seguridad Informática.	Que no existe un personal capacitado en este tema.	Crear
		Herramientas de Seguridad Implantados	No poseen contraseñas adecuadas en sus equipos de trabajos.	Mitigar
		Divulgación de la información	Falta de acuerdos de confidencialidad	Mitigar
		Errores de usuarios y operadores	Falta de conciencia en seguridad de la información	Mitigar
		Errores del personal y acciones equivocadas	Falta de conocimiento y oportuno entrenamiento	Mitigar
		Acceso no autorizado a datos	Falta de mecanismos de identificación / autenticaciones confiables	Mitigar
		Robo y Fraude	Falta de mecanismos de identificación / autenticaciones confiables	Mitigar
		Sabotaje	Falta de conciencia en seguridad de la información	Mitigar
		Amenazas Externas o Medioambientales (incendio, inundación, terremoto, maremoto, explosión, desordenes civiles)	Las instalaciones y equipos son susceptibles a desastres.	Transferir, aceptar
2	**Personal Técnico**	Divulgación de la información	Falta de incentivos al personal y oportunidades de crecimiento	Mitigar
		Manual de políticas de Seguridad de la Información	Falta de conocimiento de estos manuales por los funcionarios.	Crear
		Herramientas de Seguridad Implantados	No poseen contraseñas adecuadas en sus equipos de trabajos.	Mitigar
		Extorsión / Corrupción	Desconocimiento de estándares y reglas establecidas por la empresa	Mitigar
		Incapacidad y restauración	No está definido un plan de recuperación de información o de activos de información	Mitigar
		Pérdida o ausencia de personal clave	Procedimientos no documentados	Mitigar
		Pérdida o ausencia de personal clave	Falta de acuerdos definidos para reemplazo de empleados	Mitigar
3	**Software y Servicios**	Manual de políticas de Seguridad de la Información	Falta de conocimiento de estos manuales por los funcionarios.	Crear

		Herramientas de Seguridad Implantados	No poseen contraseñas adecuadas en sus equipos de trabajos.	Mitigar
		Acceso no autorizado a datos	Inadecuada segregación de funciones del personal	Mitigar
		Errores de usuarios y operadores	Falta de conciencia ó entrenamiento insuficiente en seguridad de la información	Mitigar
		Errores de usuarios y operadores	Falta de procedimientos del uso, operación y control de cambios	Mitigar
		Pérdida o ausencia de personal clave	Procedimientos no documentados	Mitigar
		Acceso remoto no autorizado a la red	Despliegue de información que pueda facilitar una conexión remota no autorizada	Mitigar
		Acceso remoto no autorizado a la red	Falta de restricciones para acceso remoto	Mitigar
		Cambios no autorizados a datos	Reporte y manejo inadecuado de fallas en la funcionalidad del sistema	Mitigar
		Código malicioso	Falta de políticas en el uso de medios removibles de almacenamiento	Mitigar
		Contaminación	Indisponibilidad de backups de información electrónica o sistemas de backup	Mitigar
		Destrucción, robo, fraude, sabotaje de instalaciones y equipos	Falta de seguridad física	Mitigar
		Robo y Fraude	Copias no controladas de datos y software	Mitigar
		Robo y Fraude	Falta de logs de auditoría	Mitigar
		Robo y Fraude	Falta de mecanismos de identificación / autenticaciones confiables	Mitigar
		Sabotaje	Falta de un procedimiento de administración de privilegios de acceso	Mitigar
		Uso de software pirata	No está definido el uso, control, instalación de software pirata.	Mitigar
		Amenazas Externas o Medioambientales (incendio, inundación, terremoto, maremoto, explosión, desordenes civiles)	Las instalaciones y equipos son susceptibles a desastres.	Transferir, aceptar
4	**Hardware**	Manual de políticas de Seguridad de la Información	Falta de conocimiento de estos manuales por los funcionarios.	Crear
		Herramientas de Seguridad Implantados	No poseen contraseñas adecuadas en sus equipos de trabajos.	Mitigar
		Errores de usuarios y operadores	Entrenamiento insuficiente en seguridad	Mitigar
		Acceso no autorizado a datos	Falta de logs de auditoría	Mitigar

		Acceso no autorizado a datos	Falta de seguridad física de los dispositivos de comunicaciones y cableado	Mitigar
		Acceso no autorizado a datos	Falta de un procedimiento de registro y autorización de salida de equipos	Mitigar
		Falla en servicios de comunicación	Administración inadecuada de la seguridad de la red	Mitigar
		Falla en suministro eléctrico	No existen sistemas UPS	Mitigar
		Fallas técnicas – Hardware	Falta de instalaciones, equipos o procesos de respaldo	Mitigar
		Fallas técnicas – Hardware	Falta de procedimientos de monitoreo de hardware	Mitigar
		Fallas técnicas – Hardware	Falta de procedimientos de planeación de la capacidad del hardware	Mitigar
		Fluctuaciones de potencia eléctrica	No existen sistemas de regulación	Mitigar
		Destrucción, robo, fraude, sabotaje de instalaciones y equipos	Falta de seguridad física	Mitigar
		Sniffing	Falta de seguridad física de los dispositivos de comunicaciones y cableado	Mitigar
		Amenazas Externas o Medioambientales (incendio, inundación, terremoto, maremoto, explosión, desordenes civiles)	Las instalaciones y equipos son susceptibles a desastres.	Transferir, aceptar

Realizado por: (Costales Christian, 2020)

4.4.6. Controles a Implementar

Después de haber evaluado las opciones para el tratamiento del riesgo, se debe decidir cuales controles se debe aplicar para el tratamiento de los mismos, la selección está definida en el Anexo **A** de la Norma 27001, de acuerdo a lo que estipula la norma en la cláusula 4.2.1. para establecer un sistema de gestión segura de la información.

En la tabla siguiente, se muestra el plan de tratamiento para los activos y sus controles.

Tabla 33-4: **Controles Relacionados**

ID	Activo de Información	Amenazas	Vulnerabilidades	Alternativa de Tratamiento	Controles 27001 relacionados
1	**Formularios y documentos de registro**	Destrucción de la información	Falta de un debido control de acceso a usuarios y de una protección física	Mitigar	A.9.1.1 A.9.1.2 A.9.1.3 A.11.1.1

					A.11.3.1 A.11.3.2
		Divulgación de la información	Falta de acuerdos o políticas de confidencialidad	Mitigar	A.5.1.5 A.8.1.3
		Errores del personal y acciones equivocadas	Falta de conocimiento y oportuna capacitación	Mitigar	A.8.1.1 A.8.1.2 A.8.2.1 A.8.2.2 A.8.2.3 A.13.2.1
		Acceso no autorizado a datos	Falta de mecanismos de identificación / autenticaciones confiables	Mitigar	A.11.2.3 A.11.3.1 A.11.4.2 A.11.4.3 A.11.5.1 A.11.5.2 A.11.5.3
		Destrucción, robo, fraude, sabotaje de instalaciones y equipos	Falta de seguridad física	Mitigar	A.9.2.5 A.9.1.1 A.9.1.2 A.9.1.3 A.9.1.5 A.9.1.6 A.9.2.1 A.9.2.3 A.9.2.5 A.9.2.7 A.11.3.3 A.11.6.2
		Amenazas Externas o Medioambientales (incendio, inundación, terremoto, maremoto, explosión, desordenes civiles)	Las instalaciones y equipos son susceptibles a desastres.	Transferir, aceptar	A.9.1.4 A.9.2.1
2	**Personal Técnico**	Divulgación de la información	Falta de acuerdos o políticas de confidencialidad	Mitigar	A.8.1.3 A.8.2.1
		Errores de usuarios y operadores	Falta de conciencia en la seguridad de la información	Mitigar	A.8.2.2
		Extorsión / Corrupción	Desconocimiento de estándares y reglas establecidas por la empresa, instituciones, etc.	Mitigar	A.8.2.2
		Pérdida o ausencia de personal clave	Falta de acuerdos definidos para reemplazo de empleados	Mitigar	A.8.2.1
3	**Software y Servicios**	Acceso no autorizado a datos	Inadecuada segregación de funciones del personal	Mitigar	A.10.1.3
		Destrucción de la información	Falta de un debido control de acceso a usuarios y de una protección física	Mitigar	A.9.1.1 A.9.1.2 A.9.1.3 A.11.1.1 A.11.3.1 A.11.3.2
		Divulgación de la información	Almacenamiento no protegido	Mitigar	A.7.2.1 A.7.2.2 A.9.1.1 A.9.1.2 A.15.1.3

		Acceso no autorizado a datos	Falta de seguridad física de los dispositivos de comunicaciones y cableado	Mitigar	A.9.2.3
		Acceso remoto no autorizado a la red	Despliegue de información que pueda facilitar una conexión remota no autorizada	Mitigar	A.11.4.2
		Acceso remoto no autorizado	Falta de mecanismos de identificación / autenticaciones confiables	Mitigar	A.11.2.3 A.11.3.1 A.11.4.2 A.11.4.3 A.11.5.1 A.11.5.2 A.11.5.3
		Acceso remoto no autorizado a la red	Falta de restricciones para acceso remoto	Mitigar	A.6.2.2 A.11.4.2
		Acceso remoto no autorizado	Falta de mecanismos para la detección de intrusos	Mitigar	A.11.4.3
		Acceso remoto no autorizado	Uso de módems sin restricción al interior de la red	Mitigar	A.11.4.2
		Cambios no autorizados a datos	Reporte y manejo inadecuado de fallas en la funcionalidad del sistema	Mitigar	A.13.1.1 A.13.1.2 A.12.5.1 A.12.5.2 A.12.5.3
		Código malicioso	Falta de políticas en el uso de medios removibles de almacenamiento	Mitigar	A.9.2.5 A.9.2.6 A.10.8.3 A.10.7.1 A.10.7.2
		Código malicioso	Indisponibilidad de backups de información electrónica o sistemas de backup	Mitigar	A.10.5.1
		Código malicioso	No hay procedimientos o mecanismos de actualización del software antivirus No hay software de detección de virus instalado en los equipos	Mitigar	A.10.4.1
		Destrucción, robo, fraude, sabotaje de instalaciones y equipos	Falta de seguridad física	Mitigar	A.9.2.5 A.9.1.1 A.9.1.2 A.9.1.3 A.9.1.5 A.9.1.6 A.9.2.1 A.11.3.3 A.11.6.2
		Falla en servicios de comunicación	Administración inadecuada de la seguridad de la red	Mitigar	A.6.1.4 A.10.3.1 A.10.6.1 A.10.6.2 A.11.4.3 A.11.4.4 A.11.4.6 A.11.4.7
		ID spoofing	Falta de controles de identificación y autenticación	Mitigar	A.11.2.3 A.11.3.1 A.11.4.2 A.11.4.3 A.11.5.1

					A.11.5.2 A.11.5.3 --- A.10.8.1 A.10.8.2 A.10.8.4
		ID spoofing	Passwords no protegidos (lógica o físicamente)	Mitigar	A.8.2.1 A.8.2.2 A.11.2.3 A.11.3.1 A.11.5.3
		Robo y Fraude	Falta de logs de auditoría	Mitigar	A.10.6.1 A.10.10.1 A.10.10.2 A.10.10.3 A.10.10.4 A.10.10.5 A.11.5.4 A.10.10.6
		Robo y Fraude	Falta de mecanismos de identificación / autenticaciones confiables	Mitigar	A.11.2.3 A.11.3.1 A.11.4.2 A.11.4.3 A.11.5.1 A.11.5.2 A.11.5.3
		Robo y Fraude	Falta de políticas y procedimientos de control de cambios	Mitigar	A.10.1.1 A.10.1.2 A.10.1.3 A.10.1.4 A.10.3.2 A.12.4.1 A.12.4.2 A.12.5.1 A.12.5.2 A.12.5.3 A.12.5.4 A.12.5.5
		Sabotaje	Falta de un procedimiento de administración de privilegios de acceso	Mitigar	A.6.1.2 A.6.2.1 A.6.2.3 A.8.1.1 A.8.1.2 A.8.3.3 A.11.1.1 A.11.2.1 A.11.2.2 A.11.2.4 A.11.4.1 A.11.6.1
		Uso de software pirata	No está definido el uso, control, instalación de software pirata.	Mitigar	A.6.1.5 A.7.1.1 A.7.1.3 A.9.2.6 A.10.7.1 A.10.7.2 A.10.7.3 A.10.10.1 A.10.10.2 A.10.10.4 A.11.3.2 A.11.3.3 A.12.4.2 A.12.5.4 A.12.5.5 A.15.1.2 A.15.1.5

		Amenazas Externas o Medioambientales (incendio, inundación, terremoto, maremoto, explosión, desordenes civiles)	Las instalaciones y equipos son susceptibles a desastres.	Transferir, aceptar	A.9.1.4 A.9.2.1
4	**Hardware**	Errores de usuarios y operadores	Entrenamiento insuficiente en seguridad	Mitigar	A.8.2.2
		Errores de usuarios y operadores	Falta de conciencia en seguridad de la información	Mitigar	A.8.2.2
		Errores de usuarios y operadores	Falta de documentación de procedimientos (uso y operación)	Mitigar	A.10.1.1 A.11.3.1 A.11.3.2 A.11.3.3 A.13.1.1 A.13.1.2
		Manipulación de la información	Falta de conocimiento y oportuno entrenamiento	Mitigar	A.8.2.2
		Acceso no autorizado a datos	Falta de un procedimiento de registro y autorización de salida de equipos	Mitigar	A.9.2.7
		Contaminación	Falta de mantenimiento de equipos e instalaciones	Mitigar	A.9.2.4
		Falla en servicios de comunicación	Administración inadecuada de la seguridad de la red	Mitigar	A.11.4.3 A.11.4.4 A.11.4.6 A.11.4.7
		Falla en servicios de comunicación	Falta de planeación en capacidad o cambios en la red	Mitigar	A.6.1.4 A.10.3.1 A.10.6.1 A.10.6.2
		Falla en suministro eléctrico	No existen sistemas UPS Falta de instalaciones, equipos o procesos de respaldo	Mitigar	A.9.2.2 A.9.1.4 A.10.5.1
		Fallas técnicas – Hardware	Falta de mantenimiento de equipos e instalaciones	Mitigar	A.9.2.4 A.10.3.1 A.10.3.2
		Fluctuaciones de potencia eléctrica	No existen sistemas de regulación	Mitigar	A.9.2.2
		Destrucción, robo, fraude, sabotaje de instalaciones y equipos	Falta de seguridad física	Mitigar	A.9.1.1 A.9.1.2 A.9.1.3 A.9.1.5 A.9.1.6 A.9.2.1 A.9.2.3 A.11.3.3 A.11.6.2
		Sabotaje	Falta de un procedimiento de administración de privilegios de acceso	Mitigar	A.6.1.2 A.6.2.1 A.6.2.3 A.8.1.1 A.8.1.2 A.8.3.3 A.11.1.1 A.11.2.1 A.11.2.2 A.11.2.4 A.11.4.1 A.11.6.1
		Sniffing	Falta de seguridad física de los dispositivos de	Mitigar	A.9.2.3

			comunicaciones y cableado		
		Amenazas Externas o Medioambientales (incendio, inundación, terremoto, maremoto, explosión, desordenes civiles)	Las instalaciones y equipos son susceptibles a desastres.	Transferir, aceptar	A.9.1.4 A.9.2.1

Realizado por: (Costales Christian, 2020)

4.4.7. Selección de los controles a Implementar

Luego de hacer un análisis de los controles establecidos en el **Anexo A** de cada uno de los activos se procede a la selección de los controles a implementar para tratar los riesgos que afecten a la Seguridad de la Información.

4.4.8. Implementación de los Procedimientos

Los controles seleccionados para el tratamiento de los diferentes riesgos permiten hacer un análisis de cada uno de los Activos para la creación de los procedimientos que luego son implementados son implementados para mejorar la seguridad de la información de la empresa o instituciones.

Los Procedimientos Obtenidos son los siguientes:

Tabla 34-4: Procedimientos

1	**Creación de los manuales de Políticas de Seguridad para la Información.**
2	Creación del Área o Responsables de la Seguridad de la Información.
3	Política de seguridad de la Información
4	Capacitación en seguridad de la información
5	Funciones, obligaciones y responsabilidades de la seguridad de la información.
6	Procedimiento para acceso, uso y procesamiento de la información por parte de los funcionarios de la institución.
7	Procedimiento para la seguridad física de instalaciones, equipos e información
8	Procedimiento para la Autenticación de los funcionarios y usuarios
9	Procedimiento para el mantenimiento y protección de los equipos
10	Procedimiento de Etiquetamiento de Activos de la Información
11	Procedimiento para respaldo de información
12	Procedimiento para la creación de políticas de confidencialidad de la información

13	Procedimiento para la gestión de activos de información frente a desastres.
14	Procedimientos para el uso de servicios que permiten el intercambio de información
15	Procedimiento para monitorear y controlar, gestionar los accesos a la red
16	Procedimiento para la selección del personal
17	Procedimiento de Etiquetamiento de Activos de la Información
18	Procedimiento para manejo de software malicioso
19	Procedimiento para el mantenimiento y actualización de hardware

Realizado por: (Costales Christian, 2020)

CAPÍTULO V

5. PROPUESTA

5.1. Identificar los activos del proceso a ser analizado

Para identificar los activos se basa en la gestión de riegos y se debe incluir toda la información mas relevante de la empresa o institución para lo cual se debe definir el mapa de procesos sobre el cual se implementará las Políticas para la Seguridad de la Información; para lo cual se realiza la elección de procesos la cual constituye un generador de valor para la Institución, una vez que el proceso analizado concluya con el ciclo de Demming correspondiente al Sistema de Gestión de Seguridad de la Información, se podrá anexar un nuevo proceso al análisis de riesgo.

El inventario de activos debe tener realmente un peso específico y que sean significativos para la Institución o empresa.

La información obtenida de los activos será documentada como se muestra a continuación.

- Identificador
- Activo de Información Identificado
- Breve descripción del Activo de Información Identificado.
- Tipo de Activo de Información.
- Responsable.

5.2. Agrupar los Activos de manera General

En primer lugar, se debe identificar todos los Activos y luego se deben agrupar de acuerdo al Tipo de Activo y de información, para hacer una reducción y poderlos procesar de mejor manera y documentarlos como se puede mostrar en l tabla siguiente.

Tabla 1-5: Activo de manera General

#	Activo	Descripción	Tipo
1	Documentos de Registro	Documentos donde se registra las acciones, tareas y actividades que se llevan a cabo.	Físico

Realizado por: (Christian Costales, 2020)

5.3. Someter los Activos a la Matriz de Vulnerabilidades y Amenazas.

Una vez identificados los activos que se debe proteger, se determina las Vulnerabilidades y Amenazas a los que pueden ser sometidos; cada uno de estos activos identificados de manera general se procede a verificar los peligros a los cuales están expuestos y definir las medidas de seguridad para su corrección según el tipo de activo. Se elabora un documento con las posibles amenazas y vulnerabilidades de la seguridad de información, basadas en el estándar ISO27001, el documento contendrá:

- Identificador
- Activo
- Amenazas
- Vulnerabilidades

5.4. Identificación y evaluación del tratamiento de riesgos

Luego de que las Amenazas y Vulnerabilidades han sido identificadas y evaluadas, el siguiente punto es identificar y evaluar la acción más apropiada para tratar los riesgos, para la cual se aplicara las siguientes opciones:

- **Asumir el Riesgo. -** Se acepta el riesgo, la perdida de información y continúa operando de manera normal.
- **Evitar el Riesgo**. - Tomar las medidas para prevenir su materialización, mediante la eliminación de su causa...
- **Transferir el Riesgo. –** Se reduce el efecto mediante el traspaso de las pérdidas hacia terceros.
- **Mitigar el Riesgo. -** Se realiza la implementación y optimización de controles permitiendo la reducción de la amenaza y que esta se desencadene en una vulnerabilidad.

5.5. Identificación de controles a implementar.

El tratamiento que se va aplicar es “Mitigar”, en esta etapa se procede a la identificación de los posibles controles establecidos por la norma ISO27001 para que luego se realice la mitigación de los riesgos identificados en los activos con el objetivo de reducir el nivel de riesgo.

5.6. Selección de controles a implementar

Aquí se analizan los posibles controles que minimizan la probabilidad de que una amenaza se desencadene en vulnerabilidad para luego seleccionar los controles que van hacer ser implementados, luego se registra como se muestra a continuación.

Tabla 2-5: Controles para el tratamiento de Riesgo

#	Activo	Amenazas	Vulnerabilidades	Alternativa de Tratamiento	Controles 27001 relacionados	Alternativa de Tratamiento Seleccionada	Procedimiento a Implementar
1	Seguridad de la Información	Fallas en las contraseñas	Pérdida de la Información	Mitigar	A.8.2.2	Mitigar	Procedimiento de capacitación en seguridad de la información

Realizado por: (Costales Christian, 2020)

5.7. Implementar los Procedimientos Obtenidos.

Se procede a desarrollar los Procedimientos obtenidos en base a los controles escogidos de la Norma ISO27001.

CONCLUSIONES

- El análisis realizado da a conocer que los activos de las áreas consideradas críticas de la Institución (Juzgado) con respecto a la seguridad de la información, refleja los índices de riesgos los mismos que exponen la información a daños, robo, modificaciones, divulgaciones, perdidas causando un gran impacto de manera negativa dentro de las actividades del Juzgado.

- Después de haber hecho un análisis profundo sobre las normas 27001 y poder establecer sus ventajas y desventajas, se pudo generar una propuesta para la seguridad de la información que fue objeto de esta investigación, y permite reducir la ocurrencia de riesgos y este modelo se implementó en el Juzgado de la Niñez y Adolescencia de la ciudad de Quito.

- La seguridad Informática se basada en las normas ISO 27001 su punto más importante es la prevención para lo cual se deben identificar los riesgos a los que están expuestos los activos de información y de esta manera evitar pérdidas de información.

- La evaluación del método se lo realizo en dos fases: inicial y post implementación de la cual se obtuvo datos importantes que indican la mejora en la integridad y manejo de la información que está basada en las normas ISO, permitiendo asegurar la información mas valiosa no solo de la institución si no de los usuarios.

- El Método propuesto garantiza la seguridad de la información en su integridad, disponibilidad y confidencialidad si se lo ejecuta de manera correcta.

.

RECOMENDACIONES

- Para tratar temas de la seguridad informática es importante el trabajo de implementación y cumplimiento de controles de seguridad esto se lo realiza en equipos e involucra a todos los funcionarios de la institución.

- Como primer punto se debe planificar y analizar la implementación de los controles de seguridad; no se debe dar mayor importancia a controles que causen inestabilidad en la seguridad proporcionada por los sistemas de procesamiento de la información, lo que se busca es garantizar la confidencialidad, integridad y disponibilidad de la información.

- Se recomienda que se establezca un sistema de medición o ponderación para las amenazas, riesgos y vulnerabilidades que se pueden presentar en la institución ya que no todas tienen la misma infraestructura tecnológica ni las mismas necesidades.

- Para mejorar la gestión se debe realizar un Plan Estratégico basado en la seguridad informática el cual debe generar proyectos pequeños que van hacer llevados a la implementación de cada uno y están basados en las normas ISO/IEC 27001 de manera ordenada y que estos deben estar acorde a las necesidades de cada empresa o institución.

- La seguridad informática implementada dentro de la institución, empresa, locales es un proceso que nunca termina, ya que esta enfocada en el monitoreo, seguimiento y revisión de manera continua de todos los métodos implementados.

BIBLIOGRAFIA

Bermúdez Molina Kelly Gabriela, Bailón Sánchez Edber Rafael. (2015). *Análisis en Seguridad Informática y Seguridad de la Información basadas en la Norma ISO/IEC 27001 Sistemas de Gestión de Seguridad de la Información dirigido a una empresa de Seguridad Financiera*. Guayaquil, Ecuador: Universidad Politécnica Salesiana sede Guayaquil. Carrera de Ingeniería en Sistemas. Recuperado de https://dspace.ups.edu.ec/bitstream/123456789/10372/1/UPS-GT001514.pdf

Cadme Ruiz Christian Miguel, Duque Pozo Diego Fabian. (2012). *Auditoria De Seguridad Informática ISO 27001 Para La Empresa De Alimentos «ITALIMENTOS CIA. LTDA»*. Cuenca, Ecuador: Universidad Politécnica Salesiana sede Cuenca. Carrera de Ingeniería en Sistemas. Recuperado de https://dspace.ups.edu.ec/bitstream/123456789/2644/16/UPS-CT002441.pdf

Guachi Aucapiña Tania Verónica. (2012). *Normas de Seguridad Informática ISO 27001 para mejorar la Confidencialidad, Integridad y Disponibilidad de los Sistemas de Información y Comunicación en el departamento de Sistemas de la Cooperativa de Ahorro y Crédito SAN FRANCISCO LTDA*. Universidad Técnica de Ambato. Facultad de Ingeniería, Electrónica e Industrial. Carrera de Ingeniería en Sistemas Computacionales e Informáticas. Sistemas Recuperado de https://repositorio.uta.edu.ec/bitstream/123456789/2361/1/Tesis_t715si.pdf

Guía de Iniciación a Actividad Profesional Implantación de Sistemas de Gestión de la Seguridad de la Información (SGSI) según la norma ISO 27001. (s. f.). Colegio Oficial Ingenieros de telecomunicaciones. Recuperado de https://www.coit.es/sites/default/files/informes/pdf/implantacion_de_sistemas_de_gestion_de_la_seguridad_de_la_informacion_sgsi_segun_la_norma_iso_27001.pdf

López, P. A. (2010). *Seguridad informática*. Editex. NTE INEN - I SO /IEC 2700 1. (s. f.). Recuperado a partir de http://www.normalizacion.gob.ec/wp-content/uploads/downloads/2016/05/nte_inen_iso_iec_27001.pdf

NTE INEN - I SO /IEC 2700 1. (s. f.). Recuperado a partir de http://www.normalizacion.gob.ec/wp-content/uploads/downloads/2016/05/nte_inen_iso_iec_27001.pdf

Registro Oficial N° 78. (2009). Normas De Control Interno Para Las Entidades, Organismos Del Sector Público Y Personas Jurídicas De Derecho Privado Que Dispongan De Recursos PÚBLICOS. Recuperado a partir de http://www.azuay.gob.ec/imagenes/uploads/File/BANCO%20DE%20LEYES/12.-%20NORMAS%20DE%20CONTROL%20INTERNO%20DE%20LA%20CONTRALORIA%20GENERAL%20DEL%20ESTADO.pdf

Rodríguez. (2014). *Diseño De Un Sistema De Gestión De Seguridad De La Información Para El Laboratorio Clínico Cofesalud Ips Ltda De La Ciudad De Ocaña. Fr A N Cisco De Paula Santander* Ocaña. Recuperado a partir de http://repositorio.ufpso.edu.co:8080/dspaceufpso/bitstream/123456789/392/1/25766.pdf

Seguridad de la información y auditoría de sistemas - Monografias.com. (s. f.). Recuperado 22 de febrero de 2017, a partir de http://www.monografias.com/trabajos61/seguridad-informacion-auditoria-sistemas/seguridad-informacion-auditoria-sistemas.shtml

Seis Guamán Joseph Alexander. (2015). *Diseño de un Sistema de Gestión de Seguridad de la Información para Instituciones Militares*. Quito, Ecuador: Escuela Politécnica Nacional. Facultad de Ingeniería en Sistemas Recuperado de https://bibdigital.epn.edu.ec/bitstream/15000/10439/3/CD-6187.pdf

Sistema Nacional de Protección y Asistencia a Víctimas y Testigo. (2011). Recuperado de http://www.mpfn.gob.pe/escuela/contenido/actividades/docs/2133_diapositiva03.pdf

NTE INEN - I SO /IEC 2700 1. (s. f.). Recuperado a partir de http://www.normalizacion.gob.ec/wp-content/uploads/downloads/2016/05/nte_inen_iso_iec_27001.pdf

Registro Oficial N° 78. (2009). Normas De Control Interno Para Las Entidades, Organismos Del Sector Público Y Personas Jurídicas De Derecho Privado Que Dispongan De Recursos PÚBLICOS. Recuperado a partir de http://www.azuay.gob.ec/imagenes/uploads/File/BANCO%20DE%20LEYES/12.-%20NORMAS%20DE%20CONTROL%20INTERNO%20DE%20LA%20CONTRALORIA%20GENERAL%20DEL%20ESTADO.pdf

Rodríguez. (2014). *Diseño De Un Sistema De Gestión De Seguridad De La Información Para El Laboratorio Clínico Cofesalud Ips Ltda De La Ciudad De Ocaña. Fr A N Cisco De Paula Santander* Ocaña. Recuperado a partir de http://repositorio.ufpso.edu.co:8080/dspaceufpso/bitstream/123456789/392/1/25766.pdf

Seguridad de la información y auditoría de sistemas - Monografias.com. (s. f.). Recuperado 22 de febrero de 2017, a partir de http://www.monografias.com/trabajos61/seguridad-informacion-auditoria-sistemas/seguridad-informacion-auditoria-sistemas.shtml

Seis Guamán Joseph Alexander. (2015). *Diseño de un Sistema de Gestión de Seguridad de la Información para Instituciones Militares*. Quito, Ecuador: Escuela Politécnica Nacional. Facultad de Ingeniería en Sistemas Recuperado de https://bibdigital.epn.edu.ec/bitstream/15000/10439/3/CD-6187.pdf

Sistema Nacional de Protección y Asistencia a Víctimas y Testigo. (2011). Recuperado de http://www.mpfn.gob.pe/escuela/contenido/actividades/docs/2133_diapositiva03.pdf

ANEXOS

Anexo A: Encuesta

ENCUESTA ACERCA DE SEGURIDAD INFORMÁTICA DIRIGIDA AL PERSONAL DE LA INSTITUCIÓN (JUZGADO)

Nota: Marque con una X sus respuestas

1. ¿*Existe Manual de Políticas de Seguridad de la información*?

SI	NO	DESCONOCE

2. *¿Existe en el Juzgado de la Niñez y Adolescencia un responsable o área encargada de la Seguridad de la información o Seguridad Informática?*

SI	NO	DESCONOCE

3. *¿Las contraseñas que utiliza usted poseen una combinación de números, letras y es más de 8 cárteres?*

Solo Números y más de 8 caracteres	Solo Letras y más de 8 caracteres	Números y Letras más de 8 caracteres	¿Otra, Describa?

4. *¿Se ha generado alguna clase de incidente en la seguridad en su puesto de trabajo en el último año como por ejemplo (pérdida de documentos, daño en la computadora, bloqueo, entre otros)?*

SI	NO	DESCONOCE

5. *¿Su computadora o equipo de trabajo se bloquea automáticamente cuando no la está utilizando?*

SI	NO	DESCONOCE

6. *¿En la Institución (Juzgado) existen acuerdos documentados de Confidencialidad de la Información?*

SI	NO	DESCONOCE

7. *¿Se les capacita regularmente en temas de seguridad de la información?*

SI	NO	DESCONOCE

8. *¿Existen documentados, procedimientos o mecanismos de actualización del software antivirus?*

SI	NO	DESCONOCE

9. *¿Existen controles de acceso a las instalaciones para los funcionarios de la Institución (Juzgados)?*

SI	NO	DESCONOCE

10. ¿Existen procedimientos documentados y disponibilidad de Backus para la realización de respaldos de la información?

SI	NO	DESCONOCE

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

DIRECCIÓN DE BIBLIOTECAS Y RECURSOS DEL APRENDIZAJE
UNIDAD DE PROCESOS TÉCNICOS Y ANÁLISIS BIBLIOGRÁFICO Y DOCUMENTAL

REVISIÓN DE NORMAS TÉCNICAS, RESUMEN Y BIBLIOGRAFÍA

Fecha de entrega: *14 / 06 / 2021*

INFORMACIÓN DEL AUTOR/A (S)
Nombres – Apellidos: *Christian Alberto Costales Espinoza*
INFORMACION INSTITUCIONAL
Instituto de Posgrado y Educación Continua
Título a optar: *Magíster en Sistemas de Telecomunicaciones*
f. Analista de Biblioteca responsable: Lic. Luis Caminos Vargas Mgs.

LUIS ALBERTO CAMINOS VARGAS

Firmado digitalmente por LUIS ALBERTO CAMINOS VARGAS
Nombre de reconocimiento (DN): c=EC, l=RIOBAMBA, serialNumber=0602376974, cn=LUIS ALBERTO CAMINOS VARGAS
Fecha: 2021.06.14 12:45:06 -05'00'

0053-DBRAI-UPT-IPEC-2021