ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

“PROPUESTA DE UN MÉTODO PARA EL MANEJO DE INFORMACIÓN DIGITAL SEGURA EN CÁMARAS DE GESELL”

EVELIN MABELL MONAR MONAR

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:

MAGISTER EN SEGURIDAD TELEMÁTICA

RIOBAMBA-ECUADOR

Junio - 2017

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

CERTIFICACIÓN:

EL TRIBUNAL DEL TRABAJO DE INVESTIGACIÓN CERTIFICA QUE:

El Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, titulado "PROPUESTA DE UN MÉTODO PARA EL MANEJO DE INFORMACIÓN DIGITAL SEGURA EN CÁMARAS DE GESELL", de responsabilidad de la Ing. Evelin Mabell Monar Monar, ha sido minuciosamente revisado y se autoriza su presentación.

Tribunal:

Ing. Wilso Zuñiga. MSc. **PRESIDENTE**	**FIRMA**
Ing. Oswaldo Martínez Guashima, M.Sc. **DIRECTOR DE TESIS**	**FIRMA**
Ing. Juan Carlos Díaz, M.Sc. **MIEMBRO DEL TRIBUNAL**	**FIRMA**
Ing. Lady Espinoza Tinoco, M.Sc. **MIEMBRO DEL TRIBUNAL**	**FIRMA**

Riobamba, Junio 2017

DERECHOS INTELECTUALES

Yo, Evelin Mabell Monar Monar, 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 pertenecen exclusivamente a la Escuela Superior Politécnica de Chimborazo.

Evelin Mabell Monar Monar
No. Cédula: 1204288292

DECLARACIÓN DE AUTENTICIDAD

Yo, Evelin Mabell Monar Monar, 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 provienen de otra fuente están debidamente citados y referenciados.

Como autora, asumo la responsabilidad legal y académica de los contenidos de este proyecto de investigación de maestría.

_____

Evelin Mabell Monar Monar

No. Cédula: 1204288292

DEDICATORIA

Dedico este trabajo a Dios por haberme dado la salud y haberme permitido llegar a este punto de mi vida y poder superarme.
A mis padres por su valioso ejemplo y quienes me enseñaron a luchar para alcanzar mis metas.

A mi querido esposo Washington, por su infinito amor, su comprensión y porque siempre ha estado junto a mí brindándome todo su apoyo.

A mis hijas, Arianna, Anahi y Mayte, porque son el motor que me da las fuerzas para continuar y seguir adelante, ya que son las principales impulsoras de mis sueños..

Mabell

AGRADECIMIENTO

Agradezco a la Escuela Superior Politécnica de Chimborazo, Instituto de Posgrado, a mis maestros y compañeros, por brindarme la oportunidad de compartir y recibir nuevos conocimientos.

Un agradecimiento muy especial a toda mi familia, por su comprensión y paciencia durante esta etapa de estudio.

A todas aquellas personas que han colaborado de una u otra manera en la realización del presente trabajo.

Mabell

TABLA DE CONTENIDO

CAPITULO II

CAPITULO III

INDICE DE TABLAS

INDICE DE FIGURAS

INDICE DE GRAFICOS

ÍNDICE DE ANEXOS

RESUMEN

El objetivo fue realizar la propuesta de un método para el manejo de información digital segura en las Cámaras de Gesell, para garantizar la integridad, confidencialidad y disponibilidad de la información. Se ha utilizado como referencia la norma ISO 27001 que tienen características efectivas y completas porque protege la información y otras características importantes para garantizar la seguridad de información. El método identificó los activos de información de la Cámara de Gesell, los cuales fueron sometidos a la matriz de amenazas y vulnerabilidades donde se identificaron los riesgos de seguridad existentes, los cuales fueron mitigados en base a los controles establecidos en el anexo A de la Norma ISO 27001, obteniendo los procedimientos a ser implantados para lograr la seguridad de la información digital en la Cámara de Gesell. Los resultados de la aplicación del método desarrollado, se considera en la fase inicial y post implementación, utilizando el método estadístico de T de Student, donde se obtiene que la diferencia de las medias de los riesgos obtenidos, son significativamente diferentes con un nivel de confianza del 95%, el cual se demuestra que el nivel de seguridad de la información digital mejora luego de aplicado el método para el manejo de información digital segura en Cámaras de Gesell. Se concluye que este método garantiza los principios básicos de la seguridad de la información como son la integridad, disponibilidad y confidencialidad. Se recomienda establecer un sistema de medición, para detectar desviaciones y cambios que deban ser tratados para que el modelo se mantenga operativo

Palabras clave: <TECNOLOGÍA Y CIENCIAS DE LA INGENIERÍA>, <INFORMÁTICA>, <SEGURIDAD TELEMÁTICA>, <CÁMARA DE GESELL>, <INTEGRIDAD>, <CONFIDENCIALIDAD>, <DISPONIBILIDAD>, <ACTIVOS DE INFORMACIÓN>.

ABSTRACT

The objective was to carry out the proposal of a method for the handling of secure digital information in the Chambers of Gesell, to guarantee the integrity, confidentiality and availability of the information. ISO 27001 has was used as a reference, which has effective and complete characteristics because it protects the information and other important characteristics to guarantee the security of information. The method identified the information assets of the Gesell Chamber, which were subjected to the matrix of threats and vulnerabilities where the existing security risks were identified, which were mitigated based on the controls established in Annex A of the Standard ISO 27001, obtaining the procedures to be implemented to achieve the security of digital information in the Chamber of Gesell. The results of the application of the developed method are considered in the initial and post implementation phase, using the statistical method of Student's T, where it was obtained that the difference of the means of the obtained risks, are significantly different with a level of confidence Of 95%, which demonstrates that the level of security of the digital information improves after applying the method for the handling of secure digital information in Chambers of Gesell. It is concluded that this method guarantees the basic principles of information security such as integrity, availability and confidentiality. It is recommended to establish a measurement system, to detect deviations and changes that must be treated in order to keep the model operational

Key words: <ENGINEERING TECHNOLOGY AND SCIENCES>, <COMPUTERS> <TELEMATIC SAFETY>, <CHAMBERS OF GESSEL>, <INTEGRITY> <CONFIDENTIALITY>, <AVAILABILITY> , < INFORMATION ASSETS>.

CAPÍTULO I

1. INTRODUCCIÓN

En los últimos años, con el desarrollo de las tecnologías de información y su relación directa con los objetivos de las instituciones, el universo de amenazas y vulnerabilidades crece, por lo tanto es necesario proteger uno de los activos más importantes de la institución como es la información, garantizando siempre la disponibilidad, confidencialidad e integridad de la misma.

Debido a que existen muchas amenazas que pueden manifestarse en cualquier momento con el fin de obtener la información confidencial de la institución, es necesario contar con una estrategia definida por cada escenario de amenaza.

La estrategia para proteger los activos de información es realizando una correcta gestión de la seguridad de la información, para poder identificar, localizar todos las debilidades y aplicar los controles correspondientes.

Las cámaras de Gesell se han implementado para evitar la revictimización de las víctimas ya que permiten obtener su testimonio grabado digitalmente, el cual será utilizado durante el proceso penal, y al tratarse de una información confidencial esta debe ser protegida y considerarse todas las medidas de seguridad para lograr su integridad.

1.1. Planeamiento del Problema

1.1.1 Situación Problemática

La seguridad ha sido una de las principales preocupaciones para el hombre, los deseos que se tieanexone por proteger la información importante y prescindible con que se cuenta, es indispensable, especialmente porque involucra a la tecnología, las personas, a la organización, sus normas, políticas, y esto hace muy necesario tener un amplio conocimiento sobre cómo realizar la gestión de estos recursos.

Pero para que esta gestión nos ayude a la protección de la información, la institución debe estar preparada para las fallas que son ocasionadas por el hombre, hardware, software, desastres naturales, entre otros.

Por lo cual es fundamental que en todo este proceso, sepamos qué es lo que vamos a proteger, de que lo vamos a proteger y como lo vamos a proteger, para de esta manera poder ejecutar adecuadamente la seguridad de la información.

En la actualidad existen muchas víctimas de delitos, y en alto porcentaje de sexuales, las cuales sufren traumas físicos y psicológicos, lo que no les permiten realizar su testimonio de una forma adecuada y en especial si estas víctimas son niños.

En razón de esta problemática, surge como una alternativa válida, confiable y segura la Cámara de Gesell, para que las víctimas de estos delitos, rindan su versión de los hechos ocurridos teniendo la opción de mantener dicha entrevista en formato electrónico para ser vista cuantas veces sea necesario sin necesidad de que la víctima lo cuente nuevamente y así evitar la revictimizacion.

La falta de una técnica, metodología específica para el manejo de información digital segura en las Cámaras de Gesell, 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 en algunas ocasiones divulgada provocando así la revictimizacion de las víctimas.

Estas declaraciones y/o testimonios por ser información reservada y que servirán como evidencia dentro de un proceso debe tomarse en cuenta todas los procedimientos para que la información digital obtenga la confidencialidad, integridad y disponibilidad.

1.1.2 Formulación del Problema

¿Cómo se asegurará la integridad, confidencialidad y disponibilidad de la información digital en las Cámaras de Gesell.

1.1.3 Sistematización del Problema

- ¿Cuáles son las consecuencias de un mal manejo de la información digital en las cámaras de Gesell?
- ¿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 en las cámaras de Gesell?
- ¿Cuáles son las responsabilidades y controles de cada una de las personas que manejan la información digital?

1.2 Justificación de la Investigación

1.2.1 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 desasociada 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 realizado en las Cámaras de Gesell que servirán para el dictamen en un tribunal.

1.2.2 Justificación Metodológica

Tenemos la “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 (INEN-ISO/IEC, 2012), 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 digital en las Cámaras de Gesell las cuales servirán como evidencia dentro de un proceso penal.

1.3 Objetivos

1.3.1 General

- Realizar la propuesta de un método para el manejo de información digital segura en las Cámaras de Gesell.

1.3.2 Específicos

- Analizar los controles de la norma 27001 con respecto al manejo de la seguridad de la información.
- Determinar los componentes básicos del método para el manejo de información digital segura en las Cámaras de Gesell.
- Implementar el método para el manejo de información digital segura en las Cámaras de Gesell.
- Verificar el nivel de mejora al implementar el método para el manejo de información digital segura en las Cámaras de Gesell, comparando resultados iniciales y post implementación.

1.4 Hipótesis

- El método para el manejo de información digital segura en Cámaras de Gesell permitirá mejorar el nivel de seguridad de la información

CAPITULO II

2 MARCO TEORICO

2.1. Antecedentes del Problema

En la Tesis "**La utilización de la Cámara de Gesell como medida alternativa para evitar la revictimizacion en el proceso penal ecuatoriano**", presentada por María Soledad Romero Moscoso, Universidad Nacional de Loja, Escuela de Derecho, Ecuador, 2012, los objetivos específicos consistieron en "Establecer la necesidad de utilizar la Cámara de Gesell como medida judicial que proteja a las víctimas y los testigos dentro del proceso penal", "Conocer las ventajas que brinda la Cámara de Gesell en la lucha contra la revictimización de la víctimas de delitos", "Presentar una propuesta jurídica de reforma legal al Código de Procedimiento Penal, dirigida a crear un acápite especial para la Cámara de Gesell y su utilización". (Romero, 2012).

La tesis analiza los beneficios, ventajas de utilizar la cámara de Gesell, para evitar la revictimización que sufren las víctimas de delitos especialmente sexuales, teniendo la opción de tener la entrevista en formato electrónico para ser revisada las veces que sea necesaria, donde la victima ya no interviene. (Romero, 2012).

En el papers "**Cámara de Gesell como herramienta investigativa en los abusos sexuales de niños y Niñas**". Caso de Honduras, presentada por Gina Maria Sierra Zelaya, Fiscal del Ministerio Público de Tegucigalpa, Honduras, 2013.(Sierra, 2013).

En este papers se efectúa un análisis de la Cámara de Gesell como herramienta investigativa en el abuso sexual de niñas y niñas, específicamente en el ámbito procesal penal, para evitar que tengan un contacto directo con el acusado o sospechoso al momento de la declaración o identificación, lo cual permite que se pueda indagar, esclarecer los hechos y determinar responsables, asegurando que la víctima pueda participar en proceso, sin ningún temor, como principal testigo de los hechos delictivos, pero no analiza ni considera la integridad que debe tener estas declaraciones. (Sierra, 2013).

Por lo que la presente investigación se diferencia de las descritas en los párrafos anteriores, porque lo que se busca es obtener un método que incluya todos los niveles de seguridad de la información confidencial digital que se genera en la Cámara de Gesell para precautelar la preservación, integridad, confidencialidad de la información obtenida por las declaraciones de las víctimas y que serán una prueba durante el proceso.

2.2 Bases Teóricas

2.2.1 Seguridad de tecnología de información

- La Unidad de Tecnología de Información, establece mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos, para ello se aplicarán al menos las siguientes medidas: (Registro Oficial N° 78, 2009, p. 92)
- Ubicación adecuada y control de acceso físico a la Unidad de Tecnología de Información y en especial a las áreas de: servidores, desarrollo y bibliotecas.
- Definición de procedimientos de obtención periódica de respaldos en función a un cronograma definido y aprobado.
- En los casos de actualización de tecnologías de soporte se migrará la información a los medios físicos adecuados y con estándares abiertos para garantizar la perpetuidad de los datos y su recuperación.
- Almacenamiento de respaldos con información crítica y/o sensible en lugares externos a la organización.
- Implementación y administración de seguridades a nivel de software y hardware, que se realizará con monitoreo de seguridad, pruebas periódicas y acciones correctivas sobre las vulnerabilidades o incidentes de seguridad identificados.
- Instalaciones físicas adecuadas que incluyan mecanismos, dispositivos y equipo especializado para monitorear y controlar fuego, mantener ambiente con temperatura y humedad relativa del aire controlado, disponer de energía acondicionada, esto es estabilizada y polarizada, entre otros;
- Consideración y disposición de sitios de procesamiento alternativos.

- Definición de procedimientos de seguridad a observarse por parte del personal que trabaja en turnos por la noche o en fin de semana. (Registro Oficial N° 78, 2009, p. 92)

Las disposiciones con respecto a la seguridad de tecnología de la información establecidas en las Normas de Control Interno pueden ser consideradas como un subconjunto de controles de la norma NTE INEN-ISO/IEC 27001:2011, razón por la cual la adopción de esta norma internacional permite cumplir y ampliar las Normas de Control Interno.

2.2.2 Custodia de la Información

Es responsabilidad de las instituciones públicas, personas jurídicas de derecho público y demás entes señalados en el artículo 1 de la presente Ley, crear y mantener registros públicos de manera profesional, para que el derecho a la información se pueda ejercer a plenitud, por lo que, en ningún caso se justificará la ausencia de normas técnicas en el manejo y archivo de la información y documentación para impedir u obstaculizar el ejercicio de acceso a la información pública, peor aún su destrucción. («LEY ORGÁNICA DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA», 2004, p. 7)

Seguridad.- "Toda base informática de datos debe contar con su respectivo archivo de respaldo, cumplir con los estándares técnicos y plan de contingencia que impidan la caída del sistema, robo de datos, modificación o cualquier otra circunstancia que pueda afectar la información pública. («LEY DEL SISTEMA NACIONAL DE REGISTRO DE DATOS PÚBLICOS», s. f., p. 7,8).

Se establecen algunas directivas para la seguridad de la información, tales como la gestión de respaldos, control de accesos, protección contra robo o alteración, como en leyes anteriores, y se las puede considerar como parte de la norma NTE INEN-ISO/IEC 27001:2011.

2.2.3 Descripción de la gestión de seguridad de la información, según la norma NTE INEN-ISO/IEC 27000:2012

La norma NTE INEN-ISO/IEC 27000:2012 la conforman una serie de normas denominadas familia de normas SGSI (Sistema de Gestión de la Seguridad de la Información).

A continuación se analizará de manera breve las principales normas.

2.2.4 Descripción de la norma nte inen-iso/iec 27000:2012

La norma NTE INEN-ISO/IEC 27000:2012 es un marco de trabajo que permite a cualquier tipo de organización ya sea pequeña o grande, pública o privada, desarrollar e implementar un Sistema de Gestión de Seguridad de la Información (SGSI) mediante el uso de la familia de normas SGSI. Un sistema de gestión de seguridad de la información proporciona un modelo para establecer, operar, monitorear, revisar, mantener y mejorar la seguridad de los activos de información (hardware, software, documentación, etc.). (INEN-ISO/IEC, 2012).

2.2.5 Familia de Normas SGSI

La norma NTE INEN-ISO/IEC 27000:2012 la conforman una serie de otras normas denominadas familia de normas SGSI. A continuación se presenta un listado de esta familia de normas (INEN-ISO/IEC, 2012).

- NTE INEN-ISO/IEC 27000, Sistema de gestión de seguridad de la información – Descripción general y vocabulario
- NTE INEN-ISO/IEC 27001, Sistema de gestión de la seguridad de la información –Requisitos
- NTE INEN-ISO/IEC 27002, Código de práctica para la gestión de la seguridad de la información
- NTE INEN-ISO/IEC 27003, Guía de implementación del sistema de gestión de la seguridad dela información

- NTE INEN-ISO/IEC 27004, Gestión de la seguridad de la información –Medición
- NTE INEN-ISO/IEC 27005, Gestión de riesgo de la seguridad de la información
- NTE INEN-ISO/IEC 27006, Requisitos para organizaciones que proveen la auditoria y certificación de los sistemas de gestión de la seguridad de la información
- ISO/IEC 27007, Directrices para auditoria de los sistemas de gestión de la seguridad de la información
- ISO/IEC 27011, Directrices para la gestión de la seguridad de la información para organizaciones de telecomunicaciones, basada en la NTE INEN-ISO/IEC 27002
- NTE INEN-ISO 27799, Informática para la salud – Gestión de la seguridad de la información para la salud utilizando la NTE INEN-ISO/IEC 27002
- ISO/IEC 27037, Directrices para la identificación, recolección, adquisición y preservación de evidencia digital. Estas actividades se establecen como necesarias para la preservación de la integridad de la evidencia digital. (ISO/IEC 27037, 2012)

De todo el conjunto de normas NTE INEN-ISO/IEC 27000:2012, la única certificable es la norma NTE INEN-ISO/IEC 27001, en la cual se especifica los requisitos necesarios para la establecer, implementar, operar, monitorear, revisar, mantener y mejorar los sistemas de gestión de seguridad de la información, todo esto se lo realiza con el apoyo de la familia de normas restantes («NTE INEN - I SO /IEC 2700 1», s. f., p. 6).

A continuación en la Figura se puede visualizar las relaciones entre la familia de normas·

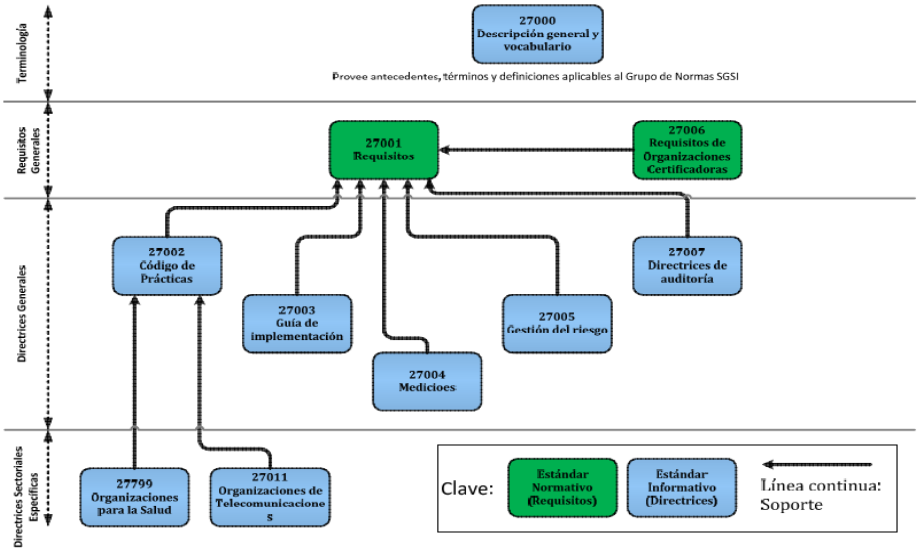

Figura 1-2: Relaciones entre la familia de normas.

Fuente: NTE INEN - I SO /IEC 2700 1, s. f., p.6

Cabe resaltar que aquellas normas que tienen las siglas NTE INEN son aquellas que han sido adoptadas como Normas Técnicas Ecuatorianas según el Instituto Ecuatoriano de Normalización (INEN).

2.2.6 Cámara de Gesell

Para la Dra. Paulina Araujo autora del artículo "Funciones de la Cámara de Gesell, Parte Teórica y Base Legal , "manifiesta que la Cámara de Gesell o Gesell Dome en inglés "consiste en dos habitaciones con una pared divisoria en la que hay un vidrio de gran tamaño que permite ver desde una de las habitaciones lo que ocurre en la otra –donde se realiza la entrevista-, pero no al revés (vidrio de visión unilateral); estas habitaciones cuentan con equipos de audio y de video para la grabación de los diferentes experimentos"(2011). Por lo tanto y para no confundir con un aparato como muchas personas lo han hecho, queda claro que es una habitación o si se quiere dos, divididas por un vidrio de visión unilateral que permita la observación de personas y la práctica de pericias que queda registrada de forma inalterable, gracias a que cuenta con todo un sistema electrónico computarizado que permite lograr estas actividades. («Artículo Funciones de la Cámara de Gesell en la investigación penal», s. f.)

Gesell la creó para observar las conductas de los niños, sin que éstos se sintieran presionados por la mirada de un observador. Es decir, nace como una instrumento de apoyo para estudiar psicológicamente la conducta de los menores, con fines inclusive pediátricos –médicos. Pero que a largo plazo se la vio como un dispositivo utilísimo en la investigación judicial y legal en general. («Artículo Funciones de la Cámara de Gesell en la investigación penal», s. f.)

Otra definición nos dice "Consiste en dos ambientes o habitaciones contiguas y separadas por un vidrio de visión unilateral (una para observadores y otra para observados), que permite una visión unidireccional de un salón hacia el otro y no al contrario, para así promover y facilitar un desarrollo más natural de la actividad observada" (Romero, 2012, p. 48)

2.2.7 Estructura y funcionamiento

La Cámara de Gesell, cuenta con un sistema de Cámaras que con ventana refractiva de 3.9m x 1.9 metros, permite una amplia visibilidad por parte del auditorio, grabando todo lo que sucede en una de las habitaciones como respaldo, pero sin que la persona que está siendo observada note su presencia. Además de micrófonos que permiten escuchar con precisión lo que se habla, es importante mencionar que aún cuando la persona que está siendo observada y analizada dentro del laboratorio de Gesell, no puede observar ni la Cámara ni los micrófonos, ella sabe que afuera están presentes, el Fiscal y otras partes procesales. Por lo que, todo lo que se hable dentro del laboratorio servirá para el proceso· (El Laboratorio de pruebas de producto y usabilidad, s. f)

El sistema de Audio y video es de gran tecnología, todas las habitaciones están plenamente acondicionadas para la finalidad, por ejemplo en el caso de los niños víctimas de abuso sexual, tienen varios instrumentos didácticos para que puedan contar su relato, tales como muñecos para que representen a sus agresores o casitas de juguete, libros para dibujar y colorear, dulces, refrescos, etc. Lo que se busca al implementar todos estos materiales de soporte, es que la víctima se encuentre en perfecta armonía y comodidad con el ambiente y que entre en confianza con el psicólogo, para relatar su versión. (El Laboratorio de pruebas de producto y usabilidad, s. f)

2.2.8 Aplicación.

La Cámara de Gesell aplicada al derecho, tiene como primordial objetivo erradicar las prácticas judiciales abusivas que atentan contra la integridad de las víctimas, tales como la reiteración de las declaraciones que son procedimientos que estimulan por lo general temor, contradicción, negativa a recordar y expresar lo sucedido, ansiedad, falsedad de la realidad, etc.

En este sentido la Cámara de Gesell permite a la víctima relatar los hechos de los cuales ha sido objeto en un ambiente donde se sienta segura aunque esté siendo observado por todos los actores procesales. Por ello, se le otorga absoluta validez a la declaración de los menores de edad, cuyos registros escritos, de video o audio pueden ser reproducidos en juicio; por ende, si lo que se procura es evitar agravar los daños que pueda ocasionar la

declaración de los hechos delictivos por parte de los niños o niñas abusados, se les debe proteger mediante la utilización de la Cámara de Gesell al momento que rindan declaración. Condiciones audiovisuales que además ayudan a nivel probatorio, en los casos de retracción de la víctima cuando ésta es sometida a presiones o manipulaciones para que no narre en las instancias investigativas o judiciales los hechos de que fue objeto por parte del agresor, evitándose así resoluciones judiciales arbitrarias producto de intimidación o amenazas de represalias en perjuicio de la justicia, del interés del niño o niña y en beneficio de la impunidad**.** (Sierra, 2013, p. 10)

Figura 2-2: Cámara de Gesell

Fuente: Sierra, 2013, p. 10

2.2.9 Requisitos para el uso de la Cámara de Gesell

- Consentimiento de las personas que harán uso de la Cámara de Gesell, respecto a ser observadas y grabadas al mismo tiempo, así como deberán ser debidamente informadas sobre la diligencia que se efectuará, antes de iniciarla.
- Las personas que son observadas deberán conocer los propósitos y usos de la información que están proporcionando y contar con la garantía de confidencialidad y protección integral.
- Las diligencias que se practiquen en la Cámara de Gesell deberán ser específicas, programadas y estructuradas con antelación y previsión. (Resolución 117, 2014, p. 5)

2.2.10 Conformación de la Cámara de Gesell

La Cámara de Gesell está conformada por dos ambientes, claramente definidos y estructuralmente separados por un vidrio-espejo de visión unidireccional que constituyen dos áreas:

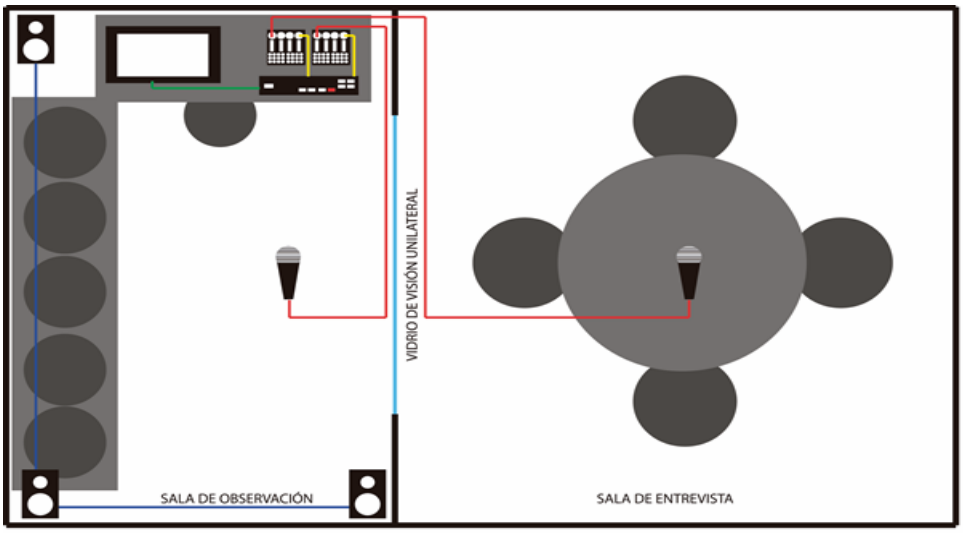

Figura 3-2: Estructura de la Cámara de Gesell

Fuente: Fiscalía General del Estado.

Área de entrevista.- Es el área donde se ubica a las personas que van a ser observadas, sobre quienes se realizarán, las diligencias de intervención e investigación que sean necesarias, así como el personal experto correspondiente. En los casos que sea estrictamente necesario, se permitirá la presencia de una tercera persona que facilite la comunicación (traductor/ intérprete) y/o de una o un acompañante de confianza, bajo los criterios de la no revictimización. (Resolución 117, 2014, p. 6)

Área de observación.- Es el área donde se ubican las personas que observarán y presenciarán las diligencias que se lleven a cabo en el área de entrevista, sin ser vistas, y donde se graban estas diligencias a través de un equipo de grabación audiovisual. (Resolución 117, 2014, p. 6)

2.2.11 Usos de la Cámara de Gesell

- Como instrumento de Testimonios. En la sala de testimonios se realizarán diligencias tales como: testimonios de la víctima, evaluaciones psicológicas del procesado,

declaraciones testimoniales, entrevistas, denuncias y otras diligencias en que su uso se justifique y que la autoridad competente lo determine.

- Como instrumento de identificación personal. Sala de identificación o reconocimiento del procesado. En esta sala se identificará y reconocerá al procesado. (Resolución 117, 2014, p. 6)

2.2.12 Normas Generales

Normas para el uso de la Cámara de Gesell:

- Ingreso solo de personas autorizadas.
- En ambas áreas, no se podrá hacer uso de cualquier aparato electrónico que ocasione interferencias con los equipos tecnológicos de la Cámara de Gesell.
- Se prohíbe el ingreso de alimentos y bebidas, a excepción de necesidades urgentes que tenga la víctima.
- Se prohíbe el ingreso de armas de fuego u objetos corto punzantes.
- Una vez comenzada la diligencia, ninguna persona, podrán salir hasta culminar la misma, para evitar interrupciones e ingreso de luz que haga visibles a las personas que se encuentran dentro del área de observación.
- Las preguntas deberán formularse, de manera ordenada, una a la vez, y deberán ser calificadas por la autoridad competente, para evitar confusiones y discusiones, cuidando siempre el bienestar psicológico de la persona sobre quien recaiga la diligencia, de conformidad con la Constitución de la República del Ecuador y la ley.
- No se formularán preguntas lesivas, impertinentes, capciosas, sugestivas y tendientes a revictimizar, conforme lo determinado en la Constitución de la República del Ecuador y la ley.
- El operador o técnico de Cámara de Gesell deberá permanecer desde el inicio hasta el final de las diligencias que se lleven a cabo en la Cámara de Gesell.
- Se podrá solicitar el diferimiento de la diligencia justificadamente con 48 horas de anticipación.
- Las diligencias programadas no podrán suspenderse, a menos que sea por caso fortuito o fuerza mayor, debidamente justificado o solicitado por la jueza o el juez; y se señalará nuevo día y hora.

- Cuando de manera simultánea, la Cámara de Gesell es solicitada para dos diligencias, tendrá prioridad aquella que se trate de víctimas de violencia contra la mujer y miembros del núcleo familiar, testigos de violencia, víctimas y testigos que su integridad haya sido amenazada en razón de procesos de familia.
- Se deberá considerar la posibilidad de un equipo de reemplazo (respaldo de equipamiento), para originar la sustitución respectiva en caso de falla del equipo principal, a fin de evitar interrupciones al normal desempeño de la diligencia por temas tecnológicos y de falta de previsión.
- Para toda diligencia, se considerará primero el ingreso de la parte ofendida, luego se procederá a ubicar a las personas en el área respectiva de acuerdo al objeto de la diligencia. (Considerar la infraestructura)
- Solo la autoridad competente podrá autorizar el ingreso de terceras personas, respetando siempre la confidencialidad de la diligencia.
- Los testimonios obtenidos mediante esta herramienta se los recepta en una sola ocasión y únicamente por disposición de la autoridad competente.
- Las partes procesales que deban intervenir en la diligencia, serán notificadas con la debida anticipación.
- La interacción de los testigos dentro de las diligencias, no serán grabadas.
- En caso de tratarse de niñas, niños, adolescentes o personas con discapacidad, estos deberán estar acompañados por su representante legal, curador, funcionario de la DINAPEN o una persona autorizada por la jueza o el juez o el fiscal.
- Las declaraciones proporcionadas por la víctima deberán grabarse siempre, sin perjuicio del secreto profesional y confidencial entre el perito y la víctima, lo que da lugar a que su testimonio se lo escuche por una sola vez, evitando así la revictimización. (Resolución 117, 2014, p. 6-8)

2.3 Estado del Arte

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. (Rodriguez, 2014, p. 21)

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 (Rodriguez, 2014, p. 21)

Disponibilidad. Debe estar disponible cuando se necesita los datos, la información o recursos para el personal adecuado (Rodriguez, 2014, p. 21)

Impacto. medir la consecuencia al materializarse una amenaza (Rodriguez, 2014, p. 21)

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. (Rodriguez, 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" (Rodriguez, 2014, p. 21)

La Cámara de Gesell. (CG), fue creado por el psicólogo estadounidense Arnold Gesell (1880-1961), para estudiar las etapas de conducta de los niños sin que se sientan presionados por quien los observa.

La cámara de Gesell. Consiste en "dos habitaciones con una pared divisoria en la que hay un vidrio de gran tamaño que permite ver desde una de las habitaciones lo que ocurre en la otra –donde se realiza la entrevista-, pero no al revés (vidrio de visión unilateral); estas habitaciones cuentan con equipos de audio y de video para la grabación de los diferentes que le experimentos".(Araujo, 2009).

Las habitaciones de la cámara de Gesell están perfectamente acondicionadas para el efecto, y la persona que realiza las entrevistas en una de las habitaciones es un psicólogo quien tiene un micrófono para receptar las preguntas hacen el fiscal, o los abogados desde

la otra habitación, a fin de que el busque la manera más adecuada para preguntar a la víctima para que esta no se sienta interrogada. (Araujo, 2009).

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"(2004, p. 266).

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.(Contreras, 2004, p. 1).

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 "el sujeto pasivo del delito o persona que sufre de manera directa o indirecta los efectos del hecho delictivo"(Reglamento Sustitutivo del Sistema de Protección a Víctimas, testigos y otros participantes en el proceso penal, 2007).

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"(Zarate. M, 2011, p. 133).

CAPITULO III

3 METODOLOGÍA DE LA INVESTIGACIÓN

3.1 Diseño de la investigación

El diseño de la investigación es del tipo Cuasi-Experimental ya que se escoge la metodología que será utilizada como base para la creación del nuevo método para manejo de información digital segura en Cámaras de Gesell, partimos de la descripción del problema las exigencias y la necesidad son de aplicación inmediata sin necesidad de someterla a pruebas, además los datos de prueba son generados por el autor de esta investigación.

3.2 Tipo de investigación

Para el presente trabajo de investigación se lo realizo mediante una investigación descriptiva y aplicada, ya que se basa en experiencia y conocimientos existentes para realizar un método que ayude a mejorar la seguridad de la información digital que se maneja en Cámaras de Gesell.

3.3 Métodos

En la investigación se utiliza el método científico ya que se refiere a la serie de etapas que hay que recorrer para obtener un conocimiento válido desde el punto de vista científico, utilizando para esto instrumentos que resulten 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

Método Deductivo: analizando los riesgos que puede provocar la manipulación de información por no manejar políticas y procedimientos de seguridad, se tratará de encontrar un método adecuado para mitigar y garantizar su confidencialidad, la integridad y la disponibilidad.

3.4 Técnicas

Las técnicas que serán utilizadas son las proporcionadas por la investigación científica para recolección de datos, siendo:

Encuesta

Esta técnica la aplicamos a funcionarios encargados de las Cámaras de Gesell, la información proporcionada se registra en un formulario de verificación.

Opinión de Expertos

Es una técnica que obtiene el criterio de una persona reconocida como una fuente confiable de un tema, cuya capacidad para juzgar o decidir en forma correcta, y justa le confiere autoridad por sus pares o por el público en una materia especifica.

Bibliográfica

La información se obtiene mediante la lectura científica de los textos, documentos, manuales, revistas, acudiendo a las bibliotecas.

Observación Directa

La información se la obtiene mediante la observación al desarrollo de ciertos procesos especialmente los relacionados al manejo de la información.

3.5 Fuentes de información

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

Primaria

- Pruebas
- Observación de resultados

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

Recursos humanos

Dentro la parte humana intervienen:

- Ejecutor de tesis
- El Tutor
- Los Miembros

Recursos técnicos

Los recursos técnicos que se utilizarán en la investigación son:

Recurso Hardware

Se utilizará el siguiente equipo hardware:

- **Modelo**: ELITEBOOK 8460P
- **Procesador**: Intel® Core™ i7-2,7GHZ

- **Memoria**: 4,00 GB
- **Disco Duro:** 500GB Serial ATA.

Recursos materiales y suministros

Los recursos materiales y suministros que se utilizarán son:

- Resmas de papel
- Empastado de tesis
- Copias
- Flash Memory
- Caja de CD's
- Carpeta colgante
- Carpetas de cartón
- Botellas de tinta para Epson
- Artículos varios de oficina
- Internet
- Transporte
- Energía eléctrica.

3.7 Planteamiento de la hipótesis

El método para el manejo de información digital segura en Cámaras de Gesell permitirá mejorar el nivel de seguridad de la información.

Variable Dependiente:

Mejorar el nivel de seguridad de la información.

Variable Independiente:

Método para el manejo de información digital segura.

3.8 Operacionalización conceptual de variables

Tabla 1-3: Operacionalización de variables.

VARIABLES	TIPO	CONCEPTO
Mejorar el nivel de seguridad de la información	Variable Dependiente	Disminuir la probabilidad de inseguridad de la información digital generada en las cámaras de Gesell.
Método para el manejo de información digital segura.	Variable Independiente	Establecer un Modelo de pasos a seguir y buenas políticas, basadas en la Norma ISO 27001, para el manejo de información segura en cámaras de Gesell.

Realizado por : Mabell Monar Monar, 2017

3.9 Operacionalización metodológica de variables

Tabla 2-3: Operacionalización metodológica de variables.

VARIABLES	TIPO	INDICADORES
Mejorar el nivel de seguridad de la información	Variable Dependiente	Frecuencia de riesgos a los recursos de información
		Incidencias de seguridad por los usuarios
		Prevención de ataques
Método para el manejo de información digital segura.	Variable Independiente	Frecuencia de cumplir con las políticas de seguridad
		Beneficios de usar políticas de seguridad
		Procedimientos adecuados

Fuente: Fiscalía General del Estado

Realizado por: Mabell Monar, 2017

3.10 Población

La población de donde se pudo obtener la información para el desarrollo del proyecto de investigación fue con el personal encargado del manejo y administración de Cámaras de Gesell de la Fiscalía General del estado, que es un total de 19 funcionarios. Por el número de unidades que la integran, resulta accesible en su totalidad, no será necesario extraer una muestra.

3.11 Instrumentos de recolección de datos

Para la recolección de datos en esta investigación se realizará una encuesta, la cual será aplicada antes y después de la implementación del modelo de seguridad basado en la Norma ISO 27001, con la finalidad de buscar información para evaluar los indicadores de las variables planteadas, el modelo del cuestionario se muestra en Anexo A

3.12 Instrumentos para procesar datos recolectados.

El instrumento que se usará para procesar la información obtenida es el software Microsoft Excel.

3.13 Valor práctico de la investigación

El presente trabajo de investigación tiene una gran importancia práctica debido a que la implementación de un método para manejo de información digital segura, ayuda a disminuir los posibles riesgos que se pueda generar en las Cámaras de Gesell, al contar con procedimientos para el manejo de la información que es tan sensible, se asegura que su información cumple con la confidencialidad, integridad y disponibilidad.

3.14 Análisis e Identificación del Riesgo

Para determinar cuáles son los riesgos relevantes que serán considerados para la toma de decisiones, se considera la probabilidad, el impacto, la exposición del riesgo, los que permitirán categorizar los riesgos, para poder administrar los riesgos más relevantes.

3.14.1 Probabilidad del Riesgo

Es la probabilidad de ocurrencia de un evento y las consecuencias ocasionadas al presentarse dicho evento.

Para que la probabilidad del riesgo sea una amenaza debe ser superior a cero (0), de igual forma la probabilidad debe ser menor que (1) o el riesgo será una certeza.

Tabla 3-3: Valores de Probabilidad de ocurrencia

PROBALIDAD DE OCURRENCIA	DESCRIPCION	VALOR
Frecuente	Ocurre en la mayoría de los casos repetidos	0.75 a 0.99
Probable	Probablemente ocurrirá	0.5 a 0.74
Ocasional	Puede ocurrir alguna vez	0.25 a 0.4
Raro	Improbable que suceda	0.0 a 0.24

Fuente: Norma ISO 27005

Realizado por: Mabell Monar , 2017

3.14.2 Impacto del Riesgo materialización del riesgo

El impacto es la materialización del riesgo, es la gravedad de los efectos adversos, causados por la consecuencia.

Se clasifica el impacto para nuestro caso en la escala del 1 al 4, según la norma ISO 27005, de Gestión de Riesgos, y según varias investigaciones de tesis ya realizadas, cuan mayor sea el número, mayor será el impacto.

Tabla 4-3: Valores de Impacto del riesgo

IMPACTO	VALOR
Bajo	1
Medio	2
Alto	3
Muy Alto	4

Fuente: Iso 27005, Tesis desarrolladas

Realizado por: Mabell Monar

3.14.3 Ponderación del Riesgo.

La ponderación del riesgo es el resultado que se obtiene al multiplicar la probabilidad por el impacto. Los riesgos con un nivel de ponderación alta son los que necesitan de una administración adecuada. Considerando que el valor máximo que se obtendrá de la ponderación será 4, se establece que los riesgos superiores a 2,5 se les consideran como críticos.

3.14.4 Identificación de Riesgos

Luego de haber analizado y validado las probabilidades de ocurrencia de los riesgos en la Cámara de Gesell, se observa que los siguientes riesgos mostrados en la tabla son los de mayor frecuencia.

Tabla 5-3: Valores de Impacto del riesgo

Ítem	Amenazas
1	Divulgación de la información
2	Errores de usuarios y operadores
3	Acceso no autorizado a Datos
4	Acceso no autorizado a la red
5	Código Malicioso
6	No existen respaldos de información
7	Sustracción o robo de información
8	Ausencia de personal clave

Realizado por: Mabell Monar, 2017

CAPITULO IV

4 RESULTADOS Y DISCUSIÓN

4.1 Análisis de la situación actual.

En la encuesta se han realizado las siguientes preguntas basadas en las principales amenazas.

Tabla 1-4: Preguntas de la Encuesta.

Preguntas realizadas en base a las amenazas
Divulgación de la información
En la Institución existen acuerdos documentados de confidencialidad de la información
Existe una política que establezca que no se debe suministrar información a terceros hasta no verificar la identidad y autoridad del solicitante
Errores de usuarios y operadores
Se le capacita regularmente en temas de seguridad de la información
Existen procedimientos documentados de uso y operación para la Cámara de Gesell.
Acceso no autorizado a Datos
Conoce sobre los procedimientos de seguridad para accesos y los mecanismos de identificación / autenticación confiables
Existe documentado un procedimiento de registro y autorización de salida de equipos de la Cámara de Gesell
Acceso no autorizado a la red
Existen documentados procedimientos para acceso remoto a la Cámara de Gesell
Es consciente de los temas de ingeniería social y cómo tales tácticas pueden crear vulnerabilidad en el acceso
Código Malicioso
Existen políticas para el uso de medios removibles de almacenamiento y de uso de email en la Cámara de Gesell
Existen documentados procedimientos o mecanismos de actualización del software antivirus
No existen respaldos de información
Existen procedimientos documentados para la realización de respaldos de información de la Cámara de Gesell.
Existen disponibilidad de backups de información digital de las diligencias de la Cámara de Gesell
Sustracción o robo de información
Existen controles para los accesos a funcionarios a las instalaciones de la Cámara de Gesell

Existe procedimientos documentados sobre la acción disciplinaria en caso de incumplimiento de las políticas en la Cámara de Gesell
Ausencia de personal clave
Existen procedimientos documentados de la cámara de Gesell
Existen acuerdos definidos para el reemplazo de empleados

Realizado por: Mabell Monar, 2017

De donde se han obtenido los siguientes resultados.

Tabla 2-4: Respuestas de las Encuestas

Número	PREGUNTAS	RESPUESTA	
		SI	NO
1	En la Institución existen acuerdos documentados de confidencialidad de la información	0	19
2	Existe una política que establezca que no se debe suministrar información a terceros hasta no verificar la identidad y autoridad del solicitante	0	19
3	Se le capacita regularmente en temas de seguridad de la información	0	19
4	Existen procedimientos documentados de uso y operación para la Cámara de Gesell.	4	15
5	Conoce sobre los procedimientos de seguridad para accesos y los mecanismos de identificación / autenticación confiables	11	8
6	Existe documentado un procedimiento de registro y autorización de salida de equipos de la Cámara de Gesell	0	19
7	Existen documentados procedimientos para acceso remoto a la Cámara de Gesell	2	17
8	Es consciente de los temas de ingeniería social y cómo tales tácticas pueden crear vulnerabilidad en el acceso	19	0
9	Existen políticas para el uso de medios removibles de almacenamiento y de uso de email en la Cámara de Gesell	4	15
10	Existen documentados procedimientos o mecanismos de actualización del software antivirus	16	3
11	Existen procedimientos documentados para la realización de respaldos de información de la Cámara de Gesell.	1	18
12	Existen disponibilidad de backups de información digital de las diligencias de la cámara de Gesell	0	19
13	Existen controles para los accesos a funcionarios a las instalaciones de la Cámara de Gesell	11	8
14	Existe procedimientos documentados sobre la acción disciplinaria en caso de incumplimiento de las políticas en la Cámara de Gesell	16	3

15	Existen procedimientos documentados de la cámara de Gesell	2	17
16	Existen acuerdos definidos para el reemplazo de empleados.	6	13

Realizado por: Mabell Monar, 2017.

En la encuesta que se va aplicar, se establece la probabilidad de ocurrencia de un riesgo, determinado en función del promedio de las respuestas obtenidas de 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: 19

Donde se obtienen los siguientes resultados de las preguntas, agrupadas por las amenazas:

Tabla 3-4: Probabilidad de ocurrencia de los riesgos.

ID	AMENAZAS	PROMEDIOS		PROBABILIDAD
		SI	NO	
1	Divulgación de la información	0,0	19,0	1,0
2	Errores de usuarios y operadores	2,0	17,0	0,9
3	Acceso no autorizado a Datos	5,5	13,5	0,7
4	Acceso no autorizado a la red	10,5	8,5	0,4
5	Código Malicioso	10,0	9,0	0,5
6	No existen respaldos de información	0,5	18,5	1,0
7	Sustracción o robo de información	13,5	5,5	0,3
8	Ausencia de personal clave	4,0	15	0,8

Realizado por: Mabell Monar , 2017

Se procede a obtener la ponderación 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 4-4: Ponderación de ocurrencia de los riesgos

ID	AMENAZAS	PROBABILIDAD	IMPACTO	PONDERANCIA
1	Divulgación de la información	1,0	4	4,00
2	Errores de usuarios y operadores	0,9	3	2,68
3	Acceso no autorizado a Datos	0,7	4	2,84
4	Acceso no autorizado a la red	0,4	4	1,79
5	Código Malicioso	0,5	2	0,95
6	No existen respaldos de información	1,0	4	3,89
7	Sustracción o robo de información	0,3	4	1,16
8	Ausencia de personal clave	0,8	4	3,16

Realizado por: Mabell Monar, 2017

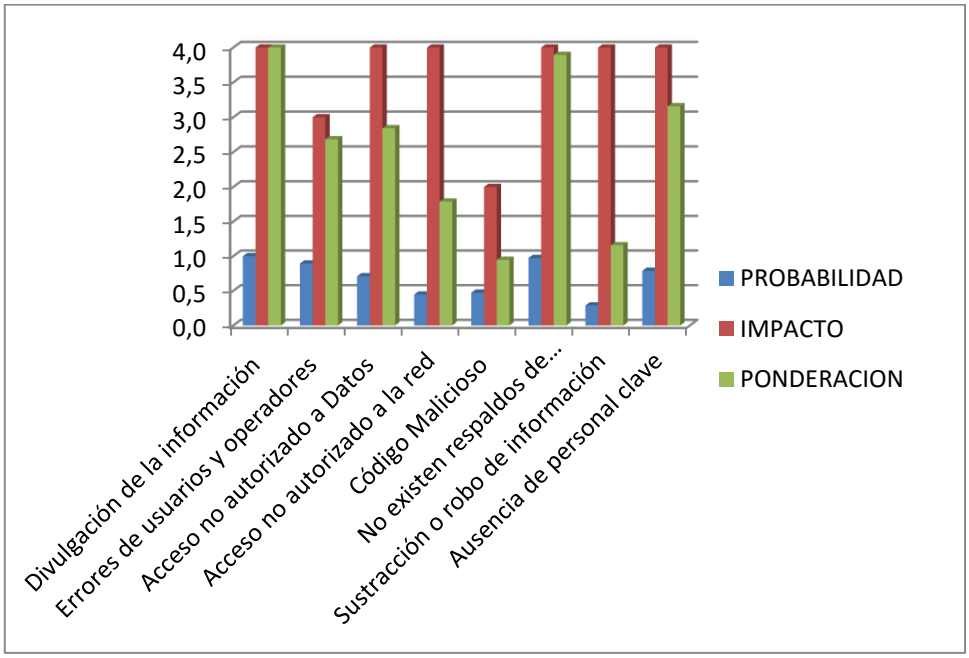

Gráfico 1-4: Ponderación de riesgos

Realizado por: Mabell Monar, 2017

En base al análisis debemos establecer que los riesgos de ponderación superior a los 2.5 son los más críticos, que es a los que se debe prestar mayor atención.

Tabla 5-4: Riesgos de mayor ponderación

ID	AMENAZAS	PROBABILIDAD	IMPACTO	PONDERACION
1	Divulgación de la información	1,0	4	4,00
6	No existen respaldos de información	1,0	4	3,89
8	Ausencia de personal clave	0,8	4	3,16
3	Acceso no autorizado a Datos	0,7	4	2,84
2	Errores de usuarios y operadores	0,9	3	2,68

Realizado por: Mabell Monar, 2017

Como se puede observar se está afectando directamente a la Confidencialidad, Privacidad, Integridad, de la información digital que se generan de las diligencias realizadas en la Cámara de Gesell, por la falta de procedimientos adecuados que permitan asegurar dicha información.

4.2 Análisis de la situación Post-Implementación.

Una vez implementados los procedimientos obtenidos del método realizado en base a la norma ISO 27001 se aplicó nuevamente la misma encuesta que se hizo el análisis inicial, siguiendo la misma metodología de análisis, de lo cual se obtuvo los siguientes resultados:

Donde se han obtenido los siguientes resultados:

Tabla 6-4: Datos de respuestas Post-Implementación.

Número	PREGUNTAS	RESPUESTA	
		SI	NO
1	En la Institución existen acuerdos documentados de confidencialidad de la información	18	1
2	Existe una política que establezca que no se debe suministrar información a terceros hasta no verificar la identidad y autoridad del solicitante	16	3
3	Se le capacita regularmente en temas de seguridad de la información	0	19
4	Existen procedimientos documentados de uso y operación para la Cámara de Gesell.	17	2
5	Conoce sobre los procedimientos de seguridad para accesos y los mecanismos de identificación / autenticación confiables	18	1
6	Existe documentado un procedimiento de registro y autorización de salida de equipos de la Cámara de Gesell	19	0
7	Existen documentados procedimientos para acceso remoto a la Cámara de Gesell	16	3
8	Es consciente de los temas de ingeniería social y cómo tales tácticas pueden crear vulnerabilidad en el acceso	19	0
9	Existen políticas para el uso de medios removibles de almacenamiento y de uso de email en la Cámara de Gesell	19	0
10	Existen documentados procedimientos o mecanismos de actualización del software antivirus	17	2
11	Existen procedimientos documentados para la realización de respaldos de información de la Cámara de Gesell.	19	0
12	Existen disponibilidad de backups de información digital de las diligencias de la cámara de Gesell	16	3
13	Existen controles para los accesos a funcionarios a las instalaciones de la Cámara de Gesell	14	5
14	Existe procedimientos documentados sobre la acción disciplinaria en caso de incumplimiento de las políticas en la Cámara de Gesell	16	3
15	Existen procedimientos documentados de la cámara de Gesell	14	5
16	Existen acuerdos definidos para el reemplazo de empleados.	16	3

Realizado por: Mabell Monar, 2017

Tabla 7-4: Probabilidad de ocurrencia de los riesgos Post-Implementación.

ID	AMENAZAS	PROMEDIOS		PROBABILIDAD
		SI	NO	
1	Divulgación de la información	18	1	0,05
2	Errores de usuarios y operadores	8,5	10,5	0,55
3	Acceso no autorizado a Datos	18,5	0,5	0,03
4	Acceso no autorizado a la red	17,5	1,5	0,08
5	Código Malicioso	18	1	0,05
6	No existen respaldos de información	18	1	0,05
7	Sustracción o robo de información	15	4	0,21
8	Ausencia de personal clave	15	4	0,21

Realizado por: Mabell Monar, 2017

Se procede a obtener la ponderación de ocurrencia.

Tabla 8-4: Ponderación de ocurrencia de los riesgos Post- Implementación

ID	AMENAZAS	PROBABILIDAD	IMPACTO	PONDERACION
1	Divulgación de la información	0,05	4	0,21
2	Errores de usuarios y operadores	0,55	3	1,66
3	Acceso no autorizado a Datos	0,03	4	0,11
4	Acceso no autorizado a la red	0,08	4	0,32
5	Código Malicioso	0,05	2	0,11
6	No existen respaldos de información	0,05	4	0,21
7	Sustracción o robo de información	0,21	4	0,84
8	Ausencia de personal clave	0,21	4	0,84

Realizado por: Mabell Monar, 2017

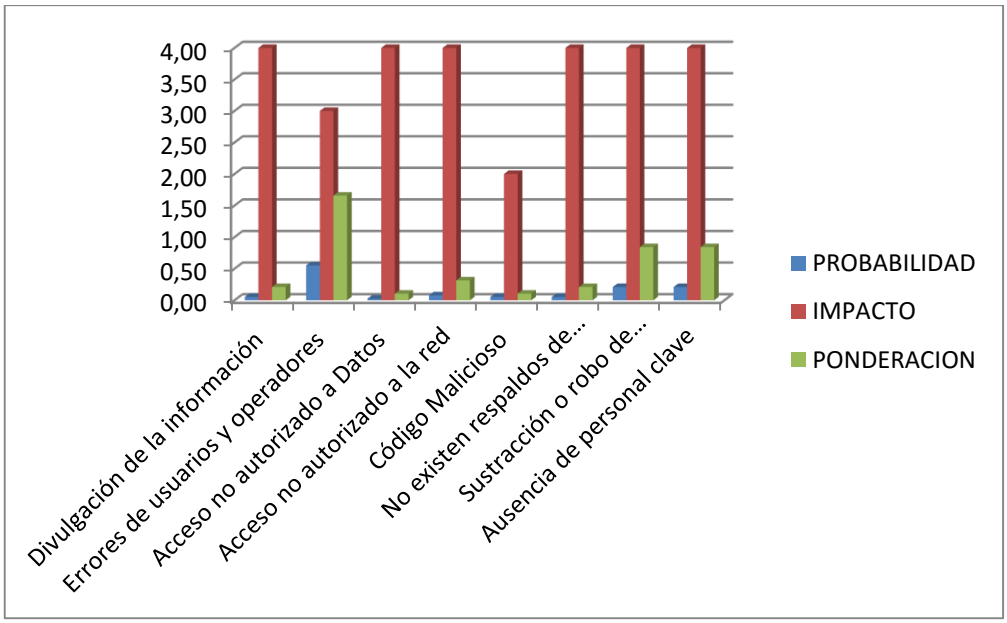

Gráfico 2-4: Ponderación de riesgos Post-Implementación

Realizado por: Mabell Monar

Como podemos observar se puede establecer que los riesgos de ponderación superior a los 2.5 que se establecieron en la situación inicial han disminuido notablemente:

Tabla 9-4: Riesgos de Ponderación Inicial - Post-Implementación

ID	AMENAZAS	PONDERACION INICIAL	PONDERACION POST-IMPLEMENTACION
1	Divulgación de la información	4,00	0,21
6	No existen respaldos de información	3,89	0,21
8	Ausencia de personal clave	3,16	0,84
3	Acceso no autorizado a Datos	2,84	0,11
2	Errores de usuarios y operadores	2,68	1,66

Realizado por: Mabell Monar, 2017

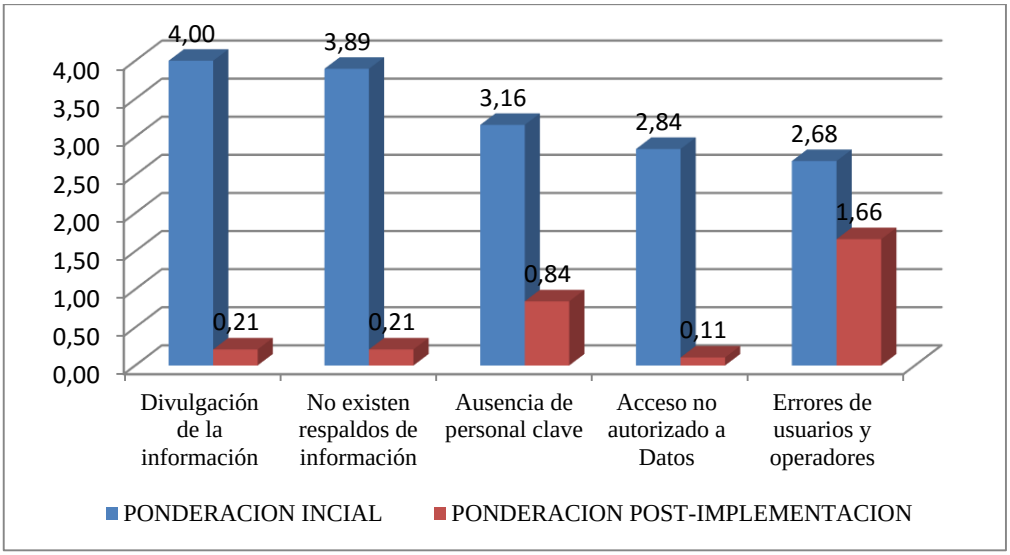

Gráfico 3-4: Ponderación de riesgos Inicial y Post-Implementación

Realizado por: Mabell Monar, 2017

Expresamos la tabla en función de porcentaje.

Tabla 10-4: Porcentaje de la reducción de riesgo

ID	AMENAZAS	PONDERACION INCIAL	PONDERACION POST-IMPLEMENTACION	PORCENTAJE DE REDUCCION DE RIESGO
1	Divulgación de la información	100,00 %	5,26%	94,74%
6	No existen respaldos de información	97,37%	5,26%	92,11%
8	Ausencia de personal clave	78,95%	21,05%	57,90%
3	Acceso no autorizado a Datos	71,05%	2,63%	68,42%
2	Errores de usuarios y operadores	67,10%	41,45%	25,65%

Realizado por: Mabell Monar, 2017

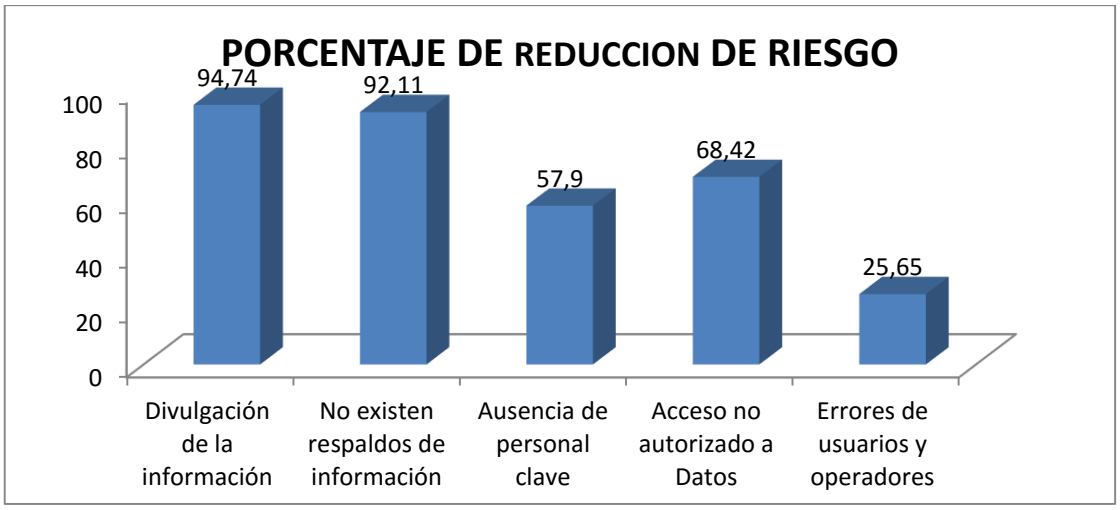

Gráfico 4-4: Porcentaje de reducción de riesgo

Realizado por: Mabell Monar, 2017

Como podemos observar en la ilustración, 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 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 segura en Cámaras de Gesell permitirá mejorar el nivel de seguridad de la información.

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

$$H_0: \mu_{\bar{d}} = 0$$

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

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

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

4.3.2 Nivel de significancia

Se debe elegir un nivel de significancia para la prueba que permite juzgar si 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 Estadístico de prueba

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

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

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

Donde:

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 decisión

Caso 1.

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

Caso 2.

$$Valor\ p < \alpha, se\ rechaza\ la\ hipotesis\ nula\ H_0$$

4.3.5 Conclusiones

La data fue evaluada en la herramienta Análisis de Datos, con la función Prueba t para medias de dos muestras empararejadas, 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 11-4: Datos Iniciales y de Post-Implantación

ID	AMENAZAS	INICIAL	POST-IMPLEMENTACION
1	Divulgación de la información	4,00	0,21
6	No existen respaldos de información	3,89	0,21
8	Ausencia de personal clave	3,16	0,84
3	Acceso no autorizado a Datos	2,84	0,11
2	Errores de usuarios y operadores	2,68	1,66

Realizado por: Mabell Monar, 2017

Tabla 12-4: 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	

Realizado por: Mabell Monar, 2017

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 el manejo de información digital segura en cámaras de Gesell para el de la Fiscalía General del Estado.

Una vez que se cuenta con el método para el manejo de información segura 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 Identificar el Proceso sobre el cual se desea aplicar el Método.

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

En el siguiente documento se muestra el proceso obtenido (Ver Anexo B).

4.4.2 Identificar los activos de información del proceso a ser analizado

Luego de haber realizado el proceso del funcionamiento de la Cámara de Gesell, se procede a identificar y seleccionar cada uno de los activos de información que intervienen en el proceso, los cuales son los que dan mayor valor a la institución y los que genera, procesan o almacenan información y permiten alcanzar los objetivos del proceso que estamos obteniendo.

Para poder clasificar loa activos de información se ha considerado identificarlos por en sus diversos tipos, los cuales pueden ser: Software, Documentos Físicos, Documentos Electrónicos, Hardware y Recurso Humano. Además de Identificar el responsable y una descripción del Activo de Información, los cuales son listados en la tabla 13-4.

Tabla 13-4: Inventario de Activos de Información

ID	ACTIVO DE INFORMACION IDENTIFICADO	DESCRIPCION	TIPO	RESPONSABLE
1	Sala de Observación	Es el lugar donde se ubican las autoridades y permite ver el desarrollo de la diligencia que se está llevando a cabo en la sala de Entrevista, esta sala dispone de un vidrio de visión unilateral; esta habitación cuenta con equipos de audio y de video para la grabación de las diferentes diligencias.	Físico	Técnico de la Cámara de Gesell
2	Sala de Entrevista	Es el lugar donde se desarrollan las diligencias; esta habitación cuenta con todo	Físico	Técnico de la Cámara de Gesell

		los equipos de audio y video para su grabación.		
3	Sistema de Documentación	Sistema informático de la FGE, el cual permite registrar y generar automaticamente la numeración de oficios, memos internos y externos	Software	Técnicos del sistema de Documentación de la FGE
4	Bitácora de registro física	Documento que permite registrar la reservación para la diligencia a llevarse a cabo en la Cámara de Gesell.	Físico	Técnico de la Cámara de Gesell
5	Aplicativo para Video Conferencias	Software que permite realizar Video Conferencias para la ejecución de las diligencias, el cuál debe ser instalado y validado.	Software	Técnico de la Cámara de Gesell
6	Internet	Servicio proporcionado por terceros, para poder realizar las diligencias mediante el sistema de Video Conferencia	Software	Técnicos de Infraestructura de la FGE y Técnico de la cámara de Gesell
7	Técnico de la Cámara de Gesell	Funcionario responsable de la instalación, mantenimiento y optimización de que los equipos informáticos en la SALA DE ENTREVISTA y la SALA DE OBSERVACION, los cuales deben funcionar correctamente al momento de la diligencia.	Recurso Humano	Técnico de la Cámara de Gesell
8	Asistente de la Cámara de Gesell	Funcionario responsable de la instalación, mantenimiento y optimización de los equipos informáticos adicionales, para la realización de la diligencia mediante Video Conferencia en la SALA DE ENTREVISTA.	Recurso Humano	Asistente de la Cámara de Gesell
9	Formulario de registro de diligencia	Documento donde se registra todos los datos y firmas pertinentes a la realización de la diligencia.	Físico	Técnico de la Cámara de Gesell
10	Hardware para la grabación	Dispositivo que permite almacenar el desarrollo de la diligencia, respaldando el contenido en un medio magnético.	Físico	Técnico de la Cámara de Gesell
11	Acta de la diligencia	Documento que es firmado por todos los participantes de la diligencia para registrar la constancia de la diligencia realizada en la Cámara de Gesell.	Físico	Secretaria del Juzgado
12	Formulario de entrega de la grabación de la diligencia.	Documento que se emite como constancia de la entrega de la grabación de la diligencia en un medio magnético.	Físico	Técnico de la Cámara de Gesell

Realizado por: Mabell Monar, 2017

4.4.3 Agrupar los Activos de Información en Grano Grueso.

Después de obtener los resultados de la información de los 12 activos de Información identificados, procedo a realizar la agrupación de los activos para reducir en el menor número de activos de información. Se considera agruparlos de acuerdo al Tipo de Activo de Información, haciendo el respectivo análisis del Activo de información y dando un nuevo nombre que englobe los activos de información agrupados.

En la tabla 14-4 , podemos observar cómo fueron agrupados los activos de Información de acuerdo al Tipo .

Tabla 14-4: Activos de Información de acuerdo al tipo

ID	ACTIVO DE INFORMACION GRANO GRUESO	ACTIVO DE INFORMACION	TIPO
1	CAMARA DE GESELL	Sala de Observación	Físico
		Sala de Entrevista	
2	FORMULARIOS Y DOCUMENTOS DE REGISTRO	Bitácora de registro física	Físico
		Formulario de registro de diligencia	
		Acta de la diligencia	
		Formulario de entrega de la grabación de la diligencia.	
3	PERSONAL TECNICO	Técnico de la Cámara de Gesell	Recurso Humano
		Asistente de la Cámara de Gesell	
4	SOFTWARE y SERVICIOS	Aplicativo para Video Conferencias	Software
		Sistema de Documentación	
		Internet	
5	HARDWARE	Hardware para la grabación	Físico

Realizado por: Mabell Monar, 2017

En la tabla 15-4 tenemos el resultado de haber agrupado los activos de información a grano grueso, obteniendo un total de 5 activos de información, donde se realiza una descripción de cada uno.y su tipo.

Tabla 15-4: Inventario de Activos de Información en Grano Grueso

ID	ACTIVO DE INFORMACION	DESCRIPCION	TIPO
1	CAMARA DE GESELL	Area que consta de dos habitaciones con una pared divisoria en la que hay un vidrio de gran tamaño que permite ver desde una de las habitaciones lo que ocurre en la otra –donde se realiza la entrevista-, (vidrio de visión unilateral); estas habitaciones cuentan con equipos de audio y de video para la grabación de las diferentes diligencias. Las habitaciones de la cámara de Gesell están perfectamente acondicionadas para el efecto	Físico
2	FORMULARIOS Y DOCUMENTOS DE REGISTRO	Documento Físico que permite el registro y verificación de todos los procesos consernientes a la Cámara de Gesell	Físico
3	PERSONAL TECNICO	Funcionarios encargados del buen funcionamiento de la Cámara de Gesell para la optima realización de las diligencias.	Recurso Humano
4	SOFTWARE y SERVICIOS	Software y servicios utilizados para la realización de las diligencias en la Cámara de Gesell	Software
5	HARDWARE	Equipos y dispositivos utilizados para la generación, procesamiento, almacenamiento y distribución de la información obtenida del resultado de la diligencia.	Físico

Realizado por: Mabell Monar, 2017

4.4.4 Someter los Activos de Información a la Matriz de Vulnerabilidades y Amenazas.

En las Instituciones, los activos de información están sometidos a que les ocurran las distintas formas de amenazas. Una amenaza puede causar un incidente no deseado que puede generar mucho daño a los activos de la institución

Las amenazas se pueden originar de diferentes fuentes o eventos accidentales. Para que una amenaza cause daño a algún activo de información tiene que explotar una o varias vulnerabilidades.

Al definir las vulnerabilidades, nos enfocamos en las debilidades del sistema de seguridad. Las vulnerabilidades no son la causa de un daño, son las condiciones que se pueden dar para que una amenaza afecte a un activo de información.

Se procede a determinar las Amenazas y Vulnerabilidades que afectan a la seguridad de la información digital en la Cámara de Gesell, de acuerdo al análisis realizado de la fuente Norma ISO27001, basado en la experiencia adquirida y en asesoramiento de un experto en Seguridad de la Información.

En la tabla 15-4 se muestran todos los activos de información identificados con sus Amenazas y Vulnerabilidades detectadas.

Tabla 16-4: Amenazas y Vulnerabilidades en la Cámara de Gesell.

ID	Activo de Información	Amenazas	Vulnerabilidades
1	CAMARA DE GESELL	Errores de usuarios y operadores	Entrenamiento insuficiente en seguridad
		Errores de usuarios y operadores	Falta de conciencia en seguridad de la información
		Errores de usuarios y operadores	Falta de documentación de procedimientos (uso y operación)
		Errores del personal y acciones equivocadas	Falta de conocimiento y oportuno entrenamiento

		Manipulación de la información	Falta de conocimiento y oportuno entrenamiento
		Pérdida o ausencia de personal clave	Procedimientos no documentados
		Contaminación	Falta de mantenimiento y protección de equipos e instalaciones
		Destrucción, robo, fraude, sabotaje de instalaciones y equipos	Falta de seguridad física
		Falla y fluctuaciones en suministro eléctrico	No existen sistemas UPS
		Robo y Fraude	Falta de conciencia en seguridad de la información
		Robo y Fraude	Inadecuada revisión de antecedentes
		Sabotaje	Falta de un procedimiento de administración de privilegios de acceso
		Sabotaje	Falta de incentivos al personal y oportunidades de crecimiento
		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.
2	**Formularios y documentos de registro**	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
		Divulgación de la información	Falta de acuerdos de confidencialidad
		Divulgación de la información	Falta de incentivos al personal y oportunidades de crecimiento
		Errores de usuarios y operadores	Falta de conciencia en seguridad de la información

		Errores del personal y acciones equivocadas	Falta de conocimiento y oportuno entrenamiento
		Manipulación de la información	Falta de conocimiento y oportuno entrenamiento
		Acceso no autorizado a datos	Falta de mecanismos de identificación / autenticación confiables
		Destrucción, robo, fraude, sabotaje de instalaciones y equipos	Falta de seguridad física
		Ingeniería Social	Falta de una política que establezca y prohiba que no se debe suministrar información a terceros hasta no verificar la identidad y autoridad del solicitante
		Robo y Fraude	Falta de mecanismos de identificación / autenticación confiables
		Robo y Fraude	Falta de conciencia en seguridad de la información
		Robo y Fraude	Inadecuada revisión de antecedentes
		Sabotaje	Falta de incentivos al personal y oportunidades de crecimiento
		Sabotaje	Falta de conciencia en seguridad de la información
		Amenazas Externas o Medioambientales (incendio, inundación, terremoto, maremoto, explosión, desordenes civiles)	Las instalaciones y equipos son susceptibles a desastres.
3	**Personal Técnico**	Divulgación de la información	Falta de incentivos al personal y oportunidades de crecimiento
		Errores de usuarios y operadores	Falta de conciencia en seguridad de la información
		Extorsión / Corrupción	Desconocimiento de estándares y reglas establecidas por la empresa
		Falla en la elección del personal	Falta de especificaciones con respecto a la selección de personal
		Incapacidad y restauración	No está definido un plan de de recuperación de información o de activos de información
		Pérdida o ausencia de personal clave	Procedimientos no documentados

		Pérdida o ausencia de personal clave	Falta de acuerdos definidos para reemplazo de empleados
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
		Errores de usuarios y operadores	Falta de conciencia ó entrenamiento insuficiente en seguridad de la información
		Errores de usuarios y operadores	Falta de procedimientos del uso, operación y control de cambios
		Manipulación de la información	Falta de conocimiento y oportuno entrenamiento
		Pérdida o ausencia de personal clave	Procedimientos no documentados
		Acceso no autorizado a datos	Falta de seguridad física de los dispositivos de comunicaciones y cableado
		Acceso remoto no autorizado a la red	Despliegue de información que pueda facilitar una conexión remota no autorizada
		Acceso remoto no autorizado a la red	Falta de esquema de firewall
		Acceso remoto no autorizado	Falta de mecanismos de identificación / autenticación confiables
		Acceso remoto no autorizado a la red	Falta de restricciones para acceso remoto
		Acceso remoto no autorizado	Falta de logs de auditoria
		Acceso remoto no autorizado	Falta de mecanismos para la detección de intrusos
		Acceso remoto no autorizado	Uso de módems sin restricción al interior de la red
		Cambios no autorizados a datos	Indisponibilidad de backups de información electrónica o sistemas de backup
		Cambios no autorizados a datos	Reporte y manejo inadecuado de fallas en la funcionalidad del sistema
		Código malicioso	Falta de políticas de uso de e-mail

		Código malicioso	Falta de políticas en el uso de medios removibles de almacenamiento
		Código malicioso	Indisponibilidad de backups de información electrónica o sistemas de backup
		Código malicioso	No hay procedimientos o mecanismos de actualización del software antivirus
		Código malicioso	No hay software de detección de virus instalado en los equipos
		Contaminación	Indisponibilidad de backups de información electrónica o sistemas de backup
		Destrucción, robo, fraude, sabotaje de instalaciones y equipos	Falta de seguridad física
		Falla en servicios de comunicación	Administración inadecuada de la seguridad de la red
		Falla en servicios de comunicación	Falta de planeación en capacidad o cambios en la red
		Falla en servicios de comunicación	No existen canales redundantes
		Falla y Fluctuaciones en suministro eléctrico	Indisponibilidad de backups de información electrónica o sistemas de backup
		Falla en suministro eléctrico	No existen sistemas UPS
		ID spoofing	Falta de controles de identificación y autenticación
		ID spoofing	Passwords no protegidos (lógica o físicamente)
		Ingeniería Social	Falta de una política que establezca que no se debe suministrar información a terceros hasta no verificar la identidad y autoridad del solicitante
		Ingeniería Social	Falta de una política que prohíba el suministro de información telefónicamente
		Robo y Fraude	Copias no controladas de datos y software
		Robo y Fraude	Falta de logs de auditoría

		Robo y Fraude	Falta de mecanismos de identificación / autenticación confiables
		Robo y Fraude	Falta de políticas y procedimientos de control de cambios
		Robo y Fraude	Inadecuada segregación de funciones del personal
		Robo y Fraude	Falta de conciencia en seguridad de la información
		Robo y Fraude	Inadecuada revisión de antecedentes
		Sabotaje	Falta de un procedimiento de administración de privilegios de acceso
		Sabotaje	Falta de incentivos al personal y oportunidades de crecimiento
		Sabotaje	Falta de conciencia en seguridad de la información
		Uso de software pirata	No esta 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.
5	**Hardware**	Errores de usuarios y operadores	Entrenamiento insuficiente en seguridad
		Errores de usuarios y operadores	Falta de conciencia en seguridad de la información
		Errores de usuarios y operadores	Falta de documentación de procedimientos (uso y operación)
		Errores del personal y acciones equivocadas	Falta de conocimiento y oportuno entrenamiento
		Manipulación de la información	Falta de conocimiento y oportuno entrenamiento
		Pérdida o ausencia de personal clave	Procedimientos no documentados
		Acceso no autorizado a datos	Falta de logs de auditoría
		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	Administración inadecuada de la seguridad de la red
		Falla en servicios de comunicación	Falta de planeación en capacidad o cambios en la red
		Falla en servicios de comunicación	No existen canales redundantes
		Falla en suministro eléctrico	No existen sistemas UPS
		Fallas técnicas – Hardware	Falta de instalaciones, equipos o procesos de respaldo
		Fallas técnicas – Hardware	Falta de mantenimiento de equipos e instalaciones
		Fallas técnicas – Hardware	Falta de procedimientos de monitoreo de hardware
		Fallas técnicas – Hardware	Falta de procedimientos de planeación de la capacidad del hardware
		Fluctuaciones de potencia eléctrica	No existen sistemas de regulación
		Destrucción, robo, fraude, sabotaje de instalaciones y equipos	Falta de seguridad física
		Robo y Fraude	Falta de conciencia en seguridad de la información
		Robo y Fraude	Inadecuada revisión de antecedentes
		Sabotaje	Falta de un procedimiento de administración de privilegios de acceso
		Sabotaje	Falta de incentivos al personal y oportunidades de crecimiento
		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: Mabell Monar, 2017**.**

4.4.5 Identificación y evaluación de opciones de tratamiento de riesgos de la Matriz

Luego de obtener las Amenazas y Vulnerabilidades de la seguridad de la Cámara, de Gesell por cada uno de los activos de información del proceso, se escoge la alternativa más adecuada de acuerdo a las necesidades y requerimientos de la institución.

En la tabla 16-4, se muestra la alternativa de tratamiento escogida, para cada una de las amenazas y vulnerabilidades de los activos de información.

Tabla 17-4: Alternativa de Tratamiento del Riesgo

ID	Activo de Información	Amenazas	Vulnerabilidades	Alternativa de Tratamiento
	CAMARA DE GESELL	Errores de usuarios y operadores	Entrenamiento insuficiente en seguridad	Mitigar
		Errores de usuarios y operadores	Falta de conciencia en seguridad de la información	Mitigar
		Errores de usuarios y operadores	Falta de documentación de procedimientos (uso y operación)	Mitigar
		Errores del personal y acciones equivocadas	Falta de conocimiento y oportuno entrenamiento	Mitigar
		Manipulación de la información	Falta de conocimiento y oportuno entrenamiento	Mitigar
		Pérdida o ausencia de personal clave	Procedimientos no documentados	Mitigar
		Contaminación	Falta de mantenimiento y protección de equipos e instalaciones	Mitigar
		Destrucción, robo, fraude, sabotaje de instalaciones y equipos	Falta de seguridad física	Mitigar
		Falla y fluctuaciones en suministro eléctrico	No existen sistemas UPS	Mitigar, Aceptar
		Robo y Fraude	Falta de conciencia en seguridad de la información	Mitigar

		Robo y Fraude	Inadecuada revisión de antecedentes	Mitigar
		Sabotaje	Falta de un procedimiento de administración de privilegios de acceso	Mitigar
		Sabotaje	Falta de incentivos al personal y oportunidades de crecimiento	Mitigar
		Sabotaje	Falta de conciencia en seguridad de la información	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.	Mitigar
2	**Formularios y documentos de registro**	Destrucción de la información	Falta de un debido control de acceso a usuarios y de una protección física	Mitigar
		Divulgación de la información	Almacenamiento no protegido	Mitigar
		Divulgación de la información	Falta de acuerdos de confidencialidad	Mitigar
		Divulgación de la información	Falta de incentivos al personal y oportunidades de crecimiento	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
		Manipulación de la información	Falta de conocimiento y oportuno entrenamiento	Mitigar
		Acceso no autorizado a datos	Falta de mecanismos de identificación / autenticación confiables	Mitigar
		Destrucción, robo, fraude, sabotaje de instalaciones y equipos	Falta de seguridad física	Mitigar

		Ingeniería Social	Falta de una política que establezca y prohiba que no se debe suministrar información a terceros hasta no verificar la identidad y autoridad del solicitante	Mitigar
		Robo y Fraude	Falta de mecanismos de identificación / autenticación confiables	Mitigar
		Robo y Fraude	Falta de conciencia en seguridad de la información	Mitigar
		Robo y Fraude	Inadecuada revisión de antecedentes	Mitigar
		Sabotaje	Falta de incentivos al personal y oportunidades de crecimiento	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
3	**Personal Técnico**	Divulgación de la información	Falta de incentivos al personal y oportunidades de crecimiento	Mitigar
		Errores de usuarios y operadores	Falta de conciencia en seguridad de la información	Mitigar
		Extorsión / Corrupción	Desconocimiento de estándares y reglas establecidas por la empresa	Mitigar
		Falla en la elección del personal	Falta de especificaciones con respecto a la selección de personal	Mitigar
		Incapacidad y restauración	No está definido un plan de 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
4	**Software y Servicios**	Acceso no autorizado a datos	Inadecuada segregación de funciones del personal	Mitigar
		Destrucción de la información	Falta de un debido control de acceso a usuarios y de una protección física	Mitigar
		Divulgación de la información	Almacenamiento no protegido	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
		Manipulación de la información	Falta de conocimiento y oportuno entrenamiento	Mitigar
		Pérdida o ausencia de personal clave	Procedimientos no documentados	Mitigar
		Acceso no autorizado a datos	Falta de seguridad física de los dispositivos de comunicaciones y cableado	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 esquema de firewall	Mitigar
		Acceso remoto no autorizado	Falta de mecanismos de identificación / autenticación confiables	Mitigar
		Acceso remoto no autorizado a la red	Falta de restricciones para acceso remoto	Mitigar
		Acceso remoto no autorizado	Falta de logs de auditoria	Mitigar
		Acceso remoto no autorizado	Falta de mecanismos para la detección de intrusos	Mitigar
		Acceso remoto no autorizado	Uso de módems sin restricción al interior de la red	Mitigar

		Cambios no autorizados a datos	Indisponibilidad de backups de información electrónica o sistemas de backup	Mitigar
		Cambios no autorizados a datos	Reporte y manejo inadecuado de fallas en la funcionalidad del sistema	Mitigar
		Código malicioso	Falta de políticas de uso de e-mail	Mitigar
		Código malicioso	Falta de políticas en el uso de medios removibles de almacenamiento	Mitigar
		Código malicioso	Indisponibilidad de backups de información electrónica o sistemas de backup	Mitigar
		Código malicioso	No hay procedimientos o mecanismos de actualización del software antivirus	Mitigar
		Código malicioso	No hay software de detección de virus instalado en los equipos	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
		Falla en servicios de comunicación	Administración inadecuada de la seguridad de la red	Mitigar
		Falla en servicios de comunicación	Falta de planeación en capacidad o cambios en la red	Mitigar
		Falla en servicios de comunicación	No existen canales redundantes	Mitigar
		Falla y Fluctuaciones en suministro eléctrico	Indisponibilidad de backups de información electrónica o sistemas de backup	Mitigar
		Falla en suministro eléctrico	No existen sistemas UPS	Mitigar

		ID spoofing	Falta de controles de identificación y autenticación	Mitigar
		ID spoofing	Passwords no protegidos (lógica o físicamente)	Mitigar
		Ingeniería Social	Falta de una política que establezca que no se debe suministrar información a terceros hasta no verificar la identidad y autoridad del solicitante	Mitigar
		Ingeniería Social	Falta de una política que prohíba el suministro de información telefónicamente	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 / autenticación confiables	Mitigar
		Robo y Fraude	Falta de políticas y procedimientos de control de cambios	Mitigar
		Robo y Fraude	Inadecuada segregación de funciones del personal	Mitigar
		Robo y Fraude	Falta de conciencia en seguridad de la información	Mitigar
		Robo y Fraude	Inadecuada revisión de antecedentes	Mitigar
		Sabotaje	Falta de un procedimiento de administración de privilegios de acceso	Mitigar
		Sabotaje	Falta de incentivos al personal y oportunidades de crecimiento	Mitigar
		Sabotaje	Falta de conciencia en seguridad de la información	Mitigar
		Uso de software pirata	No esta 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
5	**Hardware**	Errores de usuarios y operadores	Entrenamiento insuficiente en seguridad	Mitigar
		Errores de usuarios y operadores	Falta de conciencia en seguridad de la información	Mitigar
		Errores de usuarios y operadores	Falta de documentación de procedimientos (uso y operación)	Mitigar
		Errores del personal y acciones equivocadas	Falta de conocimiento y oportuno entrenamiento	Mitigar
		Manipulación de la información	Falta de conocimiento y oportuno entrenamiento	Mitigar
		Pérdida o ausencia de personal clave	Procedimientos no documentados	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
		Contaminación	Falta de mantenimiento de equipos e instalaciones	Mitigar
		Falla en servicios de comunicación	Administración inadecuada de la seguridad de la red	Mitigar
		Falla en servicios de comunicación	Falta de planeación en capacidad o cambios en la red	Mitigar
		Falla en servicios de comunicación	No existen canales redundantes	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 mantenimiento de equipos e instalaciones	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
		Robo y Fraude	Falta de conciencia en seguridad de la información	Mitigar
		Robo y Fraude	Inadecuada revisión de antecedentes	Mitigar
		Sabotaje	Falta de un procedimiento de administración de privilegios de acceso	Mitigar
		Sabotaje	Falta de incentivos al personal y oportunidades de crecimiento	Mitigar
		Sabotaje	Falta de conciencia en seguridad de la información	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: Mabell Monar, 2017.

4.4.6 Identificación de controles a implementar.

Luego de identificar y haber evaluado las opciones de tratamiento del riesgo, se debe decidir cuales controles se debe escoger para el tratamiento.

Los objetivos de control y los controles, se lo ha seleccionado del 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 18-4, se muestra el plan de tratamiento para los activos de información y sus controles relacionados.

Tabla 18-4: Controles Relacionados

ID	Activo de Información	Amenazas	Vulnerabilidades	Alternativa de Tratamiento	Controles 27001 relacionados
1	CAMARA DE GESELL	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 A13.1.2
		Errores del personal y acciones equivocadas	Falta de conocimiento y oportuno entrenamiento	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
		Manipulación de la información	Falta de conocimiento y oportuno entrenamiento	Mitigar	A.8.2.2
		Pérdida o ausencia de personal clave	Procedimientos no documentados	Mitigar	A.8.1.1 A.8.1.2 A.8.1.3 A.8.2.1 A.8.2.3 A.8.3.1 A.8.3.2 A.8.3.3
		Contaminación	Falta de mantenimiento y protección de equipos e instalaciones	Mitigar	A.9.2.1 A.9.2.4

		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
		Falla y fluctuaciones en suministro eléctrico	No existen sistemas UPS	Mitigar, Aceptar	A.9.2.2
		Robo y Fraude	Falta de conciencia en seguridad de la información	Mitigar	A.8.2.2 A.8.2.3 A.15.2.1
		Robo y Fraude	Inadecuada revisión de antecedentes	Mitigar	A.8.1.2
		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
		Sabotaje	Falta de incentivos al personal y oportunidades de crecimiento	Mitigar	A.8.1.3 A.8.2.1
		Sabotaje	Falta de conciencia en seguridad de la información	Mitigar	A.8.2.2 A.8.2.3 A.15.2.1
		Sniffing	Falta de seguridad física de los dispositivos de comunicaciones y cableado	Mitigar	A.9.2.3
		Amenazas Externas o Medioambientales (incendio, inundación, terremoto, maremoto,	Las instalaciones y equipos son susceptibles a desastres.	Mitigar	A.9.1.4 A.9.2.1

		explosión, desordenes civiles)			
2	**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	Almacenamiento no protegido	Mitigar	A.7.2.1 A.7.2.2 A.9.1.1 A.9.1.2 A.15.1.3
		Divulgación de la información	Falta de acuerdos de confidencialidad	Mitigar	A.5.1.5 A.8.1.3
		Divulgación de la información	Falta de incentivos al personal y oportunidades de crecimiento	Mitigar	A.8.1.3 A.8.2.1
		Errores de usuarios y operadores	Falta de conciencia en seguridad de la información	Mitigar	A.8.2.2
		Errores del personal y acciones equivocadas	Falta de conocimiento y oportuno entrenamiento	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
		Manipulación de la información	Falta de conocimiento y oportuno entrenamiento	Mitigar	A.8.2.2
		Acceso no autorizado a datos	Falta de mecanismos de identificación / autenticación 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
		Ingeniería Social	Falta de una política que establezca y prohiba que no se debe suministrar información a terceros hasta no verificar la identidad y autoridad del solicitante	Mitigar	A.5.1.1 A.5.1.2 A.6.1.1 A.6.1.5 A.7.1.2 A.7.1.3 A.7.2.1 A.7.2.2 A.10.8.1
		Robo y Fraude	Falta de mecanismos de identificación / autenticación 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 conciencia en seguridad de la información	Mitigar	A.8.2.2 A.8.2.3 A.15.2.1
		Robo y Fraude	Inadecuada revisión de antecedentes	Mitigar	A.8.1.2
		Sabotaje	Falta de incentivos al personal y oportunidades de crecimiento	Mitigar	A.8.1.3 A.8.2.1
		Sabotaje	Falta de conciencia en seguridad de la información	Mitigar	A.8.2.2 A.8.2.3 A.15.2.1
		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
3	**Personal Técnico**	Divulgación de la información	Falta de incentivos al personal y oportunidades de crecimiento	Mitigar	A.8.1.3 A.8.2.1
		Errores de usuarios y operadores	Falta de conciencia en seguridad de la información	Mitigar	A.8.2.2

		Extorsión / Corrupción	Desconocimiento de estándares y reglas establecidas por la empresa	Mitigar	A.8.2.2
		Falla en la elección del personal	Falta de especificaciones con respecto a la selección de personal	Mitigar	A.8.1.2 A.8.1.3
		Incapacidad y restauración	No está definido un plan de de recuperación de información o de activos de información	Mitigar	A.10.5.1 A.14.1.3
		Pérdida o ausencia de personal clave	Procedimientos no documentados	Mitigar	A.8.1.1 A.8.1.2 A.8.1.3 A.8.2.1 A.8.2.3 A.8.3.1 A.8.3.2 A.8.3.3
		Pérdida o ausencia de personal clave	Falta de acuerdos definidos para reemplazo de empleados	Mitigar	A.8.2.1
4	**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
		Errores de usuarios y operadores	Falta de conciencia ó entrenamiento insuficiente en seguridad de la información	Mitigar	A.8.2.2
		Errores de usuarios y operadores	Falta de procedimientos del uso, operación y control de cambios	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

					A.10.3.2 A.12.4.1 A.12.5.1 A.12.5.2 A.12.5.3 A.12.5.4 A.12.5.5
		Manipulación de la información	Falta de conocimiento y oportuno entrenamiento	Mitigar	A.8.2.2
		Pérdida o ausencia de personal clave	Procedimientos no documentados	Mitigar	A.8.1.1 A.8.1.2 A.8.1.3 A.8.2.1 A.8.2.3 A.8.3.1 A.8.3.2 A.8.3.3
		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 a la red	Falta de esquema de firewall	Mitigar	A.10.6.1 A.10.6.2 A.10.9.3
		Acceso remoto no autorizado	Falta de mecanismos de identificación / autenticación 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 logs de auditoria	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

		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	Indisponibilidad de backups de información electrónica o sistemas de backup	Mitigar	A.9.1.3 A.9.1.4 A.10.5.1 A.10.8.3 A.15.1.3
		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 de uso de e-mail	Mitigar	A.10.8.1 A.10.8.2 A.10.8.4 A.10.8.5
		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	Mitigar	A.10.4.1
		Código malicioso	No hay software de detección de virus instalado en los equipos	Mitigar	A.10.4.1
		Contaminación	Indisponibilidad de backups de información electrónica o sistemas de backup	Mitigar	A.10.5.1
		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.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 servicios de comunicación	No existen canales redundantes	Mitigar	A.9.2.2
		Falla y Fluctuaciones en suministro eléctrico	Indisponibilidad de backups de información electrónica o sistemas de backup	Mitigar	A.10.5.1
		Falla en suministro eléctrico	No existen sistemas UPS	Mitigar	A.9.2.2
		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
		Ingeniería Social	Falta de una política que establezca que no se debe suministrar información a terceros hasta no verificar la identidad y autoridad del solicitante	Mitigar	A.5.1.1 A.5.1.2 A.6.1.1 A.7.1.2 A.7.1.3 A.7.2.1 A.7.2.2 A.10.8.1

		Ingeniería Social	Falta de una política que prohíba el suministro de información telefónicamente	Mitigar	A.5.1.1 A.5.1.2 A.6.1.1 A.6.1.5 A.7.1.2 A.7.1.3 A.7.2.1 A.7.2.2 A.10.8.1
		Robo y Fraude	Copias no controladas de datos y software	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.11.3.2 A.11.3.3 A.12.4.2 A.12.5.4 A.12.5.5 A.15.1.2
		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 / autenticación 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
		Robo y Fraude	Inadecuada segregación de funciones del personal	Mitigar	A.10.1.3
		Robo y Fraude	Falta de conciencia en seguridad de la información	Mitigar	A.8.2.2 A.8.2.3 A.15.2.1
		Robo y Fraude	Inadecuada revisión de antecedentes	Mitigar	A.8.1.2
		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
		Sabotaje	Falta de incentivos al personal y oportunidades de crecimiento	Mitigar	A.8.1.3 A.8.2.1
		Sabotaje	Falta de conciencia en seguridad de la información	Mitigar	A.8.2.2 A.8.2.3 A.15.2.1
		Uso de software pirata	No esta 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
5	**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
		Errores del personal y acciones equivocadas	Falta de conocimiento y oportuno entrenamiento	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
		Manipulación de la información	Falta de conocimiento y oportuno entrenamiento	Mitigar	A.8.2.2
		Pérdida o ausencia de personal clave	Procedimientos no documentados	Mitigar	A.8.1.1 A.8.1.2 A.8.1.3 A.8.2.1 A.8.2.3 A.8.3.1 A.8.3.2 A.8.3.3
		Acceso no autorizado a datos	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

		Acceso no autorizado a datos	Falta de seguridad física de los dispositivos de comunicaciones y cableado	Mitigar	A.9.2.3
		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 servicios de comunicación	No existen canales redundantes	Mitigar	A.9.2.2
		Falla en suministro eléctrico	No existen sistemas UPS	Mitigar	A.9.2.2
		Fallas técnicas – Hardware	Falta de instalaciones, equipos o procesos de respaldo	Mitigar	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
		Fallas técnicas – Hardware	Falta de procedimientos de monitoreo de hardware	Mitigar	A.10.10.1 A.10.10.2 A.10.10.5 A.10.10.6
		Fallas técnicas – Hardware	Falta de procedimientos de planeación de la capacidad del hardware	Mitigar	A.6.1.4 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

		Robo y Fraude	Falta de conciencia en seguridad de la información	Mitigar	A.8.2.2 A.8.2.3 A.15.2.1
		Robo y Fraude	Inadecuada revisión de antecedentes	Mitigar	A.8.1.2
		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
		Sabotaje	Falta de incentivos al personal y oportunidades de crecimiento	Mitigar	A.8.1.3 A.8.2.1
		Sabotaje	Falta de conciencia en seguridad de la información	Mitigar	A.8.2.2 A.8.2.3 A.15.2.1
		Sniffing	Falta de seguridad física de los dispositivos de comunicaciones y cableado	Mitigar	A.9.2.3
		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: Mabell Monar, 2017

4.4.7 Selección de controles a implementar

Después de incluir todos los objetivos de control escogidos del Anexo A de la norma de cada uno de los activos de información procedo a seleccionar los controles a implementar para tratar los riesgos que afecten a la Cámara de Gesell, analizando cada uno de los activos de información.(Ver Anexo C).

4.4.8 Implementar los Procedimientos Obtenidos.

De acuerdo a los controles seleccionados para el tratamiento del riesgo, se realiza el análisis de cada uno de los Activos de información y se crean los procedimientos que son implementados para obtener la seguridad de la información digital en Cámaras de Gesell

Los Procedimientos Obtenidos son los siguientes:

Tabla 19-4: Procedimientos

1	Política de seguridad de la Información
2	Procedimiento de Etiquetamiento de Activos de la Información
3	Procedimiento de capacitación en seguridad de la información
4	Procedimiento para acceso, uso y procesamiento de la información
5	Procedimiento de funciones, obligaciones y responsabilidades de la seguridad de la información.
6	Procedimiento para el mantenimiento de los equipos
7	Procedimiento para la seguridad física de instalaciones, equipos e información
8	Procedimiento para la protección en fallas de suministro de energía y otras anomalías eléctricas.
9	Procedimiento para respaldo de información
10	Procedimiento para la selección idónea del personal
11	Procedimiento para la gestión de activos de información frente a desastres.
12	Procedimiento de confidencialidad de la información
13	Procedimiento para monitorear, gestionar los accesos a la red
14	Procedimientos para el intercambio de información
15	Procedimientos para el uso de medios removibles
16	Procedimiento para manejo de software malicioso
17	Procedimiento para uso e instalación de software

Realizado por: Mabell Monar, 2017

. Cada uno de los procedimientos se encuentra descritos en el Anexo D

CAPITULO V

5 PROPUESTA

5.1 Identificar el Proceso sobre el cual se desea aplicar el Método.

Es la representación de la secuencia de pasos que se tiene que realizar para obtener el funcionamiento de la Cámara de Gesell. Para elaborarlo se debe: identificar los requisitos, las actividades, las personas, los documentos que permiten la presentación y resolución de su funcionamiento.

5.2 Identificar los activos de información del proceso a ser analizado

El inventario de activos de información es la base para la gestión de riesgo de los mismos y debe incluir toda la información más importante de la institución para mantenerlos operativos. Para ello es necesario que la Institución previamente haya definido el mapa de procesos sobre el cual se implementará el Sistema de Gestión de Seguridad de la Información. Para la elección del proceso se deberá tomar en cuenta cuál de ellos se constituye en 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 de información debe recoger los activos que realmente tengan un peso específico y sean significativos para la Institución.

La información obtenida y los activos de información identificados serán documentados como se muestra a continuación.

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

- Tipo de Activo de Información.
- Responsable.

5.3 Agrupar los Activos de Información en Grano Grueso.

Luego de tener identificado todos los Activos de Información, estos deben agruparse de acuerdo al Tipo de Activo y de información, para reducirlos y poder procesarlos de mejor manera, los cuales son documentados en una tabla con el siguiente contenido.

Tabla 1-5: Activo de información en Grano Grueso

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

Realizado por: Mabell Monar, 2017.

5.4 Someter los Activos de Información a la Matriz de Vulnerabilidades y Amenazas.

Una vez que conocemos los activos de información que debemos proteger, tenemos que determinar las Vulnerabilidades y Amenazas que se apliquen contra ellos.

A cada uno de los activos de Información Identificados en grano grueso se les somete a la Matriz de Vulnerabilidades y Amenazas y se procede a dimensionar los peligros a los cuales están expuestos y definir las medidas de seguridad para su corrección según el tipo de activo de información.

Por lo expuesto, 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 de Información
- Amenazas
- Vulnerabilidades

5.5 Identificación y evaluación de opciones de tratamiento de riesgos de la Matriz

Cuando las Amenazas y Vulnerabilidades han sido identificadas y evaluadas, la próxima tarea es identificar y evaluar la acción más apropiada de cómo tratar los riesgos, se debe realizar con las siguientes opciones:

- **Asumir el Riesgo.-** Se acepta el riesgo, la perdida probable de la información y continua operando normalmente.
- **Evitar el Riesgo**.- Tomar las medidas encaminadas a prevenir su materialización, mediante la eliminación de su causa...
- **Transferir el Riesgo.-** Permite Reducir su efecto a través del traspaso de las pérdidas a terceros ó contratos de seguros
- **Mitigar el Riesgo.-** Implica en optimizar los procedimientos e implementar los controles que permitan reducir la posibilidad de que la amenaza explote una vulnerabilidad.

5.6 Identificación de controles a implementar.

Cuando la opción seleccionada del tratamiento del riesgo sea "Mitigar ", en esta etapa se identifican los posibles controles de la norma ISO27001 a implementar que podrían mitigar los riesgos identificados para los activos de información de la Cámara de Gesell, con el objetivo de reducir el nivel de riesgo.

5.7 Selección de controles a implementar

Esta etapa consiste en analizar los posibles controles que minimizan la probabilidad de que una amenaza explote una vulnerabilidad, y escoger los controles a ser implementados.

Los resultados de las actividades y selección de los controles se van a registrar como se muestra a continuación.

Tabla 2-5: Controles para el tratamiento de Riesgo.

ID	Activo de Información	Amenazas	Vulnerabilidades	Alternativa de Tratamiento	Controles 27001 relacionados	Alternativa de Tratamiento Seleccionada	Procedimiento a Implementar
1	Cámara de Gesell	Errores de usuarios y operadores	Falta de concienciа en seguridad de la informaci ón	Mitigar	A.8.2.2	Mitigar	Procedimie nto de capacitació n en seguridad de la informació n

Realizado por: Mabell Monar, 2017

5.8 Implementar los Procedimientos Obtenidos.

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

CONCLUSIONES

- Luego de haber analizado las Normas 27001 y haber establecido sus ventajas y desventajas se pudo generar el método de seguridad de información digital para Cámaras de Gesell, objeto de esta investigación, que permite reducir la probabilidad de ocurrencia de riesgos de seguridad de la información, modelo que se implementó en la FGE.

- El Método elaborado garantiza los principios básicos de la seguridad de la información como son la integridad, disponibilidad y confidencialidad.

- El Sistema de Gestión de Seguridad de Información bajo la norma ISO 27001, se fundamentan en la prevención, por lo cual es muy importante identificar los riesgos a los que están expuestos los activos de información, para de esta manera evitar pérdidas importantes de información.

- La implementación del método fue evaluada en dos fases consideradas como inicial y post implementación, obteniendo datos que indican que se mejora y se cumple con las características de integridad de la información que está presente en la norma ISO 27001 pero con un enfoque más directo para la información digital segura en Cámaras de Gesell.

- La implementación del método en las cámaras de Gesell, garantizará la integridad, confidencialidad de la información obtenida por las declaraciones de las víctimas y que serán una prueba durante el proceso.

RECOMENDACIONES

- Se recomienda que el nivel de seguridad que se ha podido alcanzar durante la implementación de este modelo para la seguridad de la información digital en Cámaras de Gesell, deba ser administrado por un Oficial de Seguridad de la Información.

- En la Institución donde se vaya implementar la metodología, se debe extender el sistema de gestión de seguridad de la información a fin de que cubra todos los procesos de la institución.

- Es importante que se establezca un sistema de medición, el cual permita valorar la aplicación del Método para el manejo de información digital segura en Cámara de Gesell, detectando desviaciones y cambios en la institución que deban ser tratados para que el modelo se mantenga operativo.

- Se recomienda asociar la gestión del plan de continuidad del negocio de la institución, con el método para el manejo de la información digital segura, con el objetivo de realizar una implementación integral para lograr un mejor nivel de seguridad de la información.
-

BIBLIOGRAFIA

ARAUJOASOCIADOS. (s. f.). Funciones de la Cámara de Gesell en la investigación penal. Recuperado 22 de febrero de 2017, a partir de http://www.araujoasociados.net/index.php/articulos/101-camara-de-gesell-en-ecuador

LEY DEL SISTEMA NACIONAL DE REGISTRO DE DATOS PÚBLICOS. (s. f.). Recuperado a partir de https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2012/11/LEY-DEL-SISTEMA-NACIONAL-DE-REGISTRO-DE-DATOS-PUBLICOS.pdf

LEY ORGÁNICA DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA. (2004). Recuperado a partir de http://www.wipo.int/edocs/lexdocs/laws/es/ec/ec052es.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

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

RESOLUCIÓN 117. **(2014)**. Protocolo para el uso de la camara de gesell. Recuperado a partir de http://www.funcionjudicial.gob.ec/www/pdf/resoluciones/2014cj/117-2014.pdf

RODRIGUEZ. (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

ROMERO. **(2012).** *La utilización de la Cámara de Gesell como medida alternativa para evitar la revictimizacion en el proceso penal ecuatoriano*. NACIONAL DE LOJA. Recuperado a partir de https://dspace.unl.edu.ec/jspui/bitstream/123456789/2762/1/ROMERO%20MOSCOSO%20MAR%C3%8DA.pdf

SIERRA. (2013). Cámara de Gesell como herramienta investigativa en los abusos sexuales de niños y niñas . c aso de honduras. Recuperado a partir de http://www.uv.es/gicf/4A3_Sierra_GICF_07.pdf