UNIVERSIDAD DE EL SALVADOR

FACULTAD DE CIENCIAS ECONÓMICAS

ESCUELA DE CONTADURÍA PÚBLICA

MANUAL DE PROCEDIMIENTOS DE AUDITORÍA DE SISTEMAS BASADO EN LA NORMA ISO 27002, ORIENTADO A ORGANIZACIONES NO GUBERNAMENTALES QUE EJECUTAN PROYECTOS DE EDUCACIÓN.

TRABAJO DE INVESTIGACIÓN PRESENTADO POR:

ORELLANA PORTILLO, JULIO CESAR

PARA OPTAR AL GRADO DE:

LICENCIADO EN CONTADURÍA PÚBLICA

OCTUBRE 2018

SAN SALVADOR, EL SALVADOR, CENTROAMÉRICA

UNIVERSIDAD DE EL SALVADOR

AUTORIDADES UNIVERSITARIAS

RECTOR	:Mae. Roger Armando Arias Alvarado
SECRETARIO GENERAL	: Lic. Cristóbal Hernán Ríos Benítez
DECANO DE LA FACULTAD DE CIENCIAS ECONÓMICAS	: Lic. Nixon Rogelio Hernández Vásquez.
SECRETARIA DE LA FACULTAD DE CIENCIAS ECONÓMICAS	: Licda. Vilma Marisol Mejía Trujillo
DIRECTORA DE LA ESCUELA DE CONTADURÍA PÚBLICA	: Licda. María Margarita de Jesús Martínez Mendoza de Hernández
COORDINADOR GENERAL DE PROCESOS DE GRADUACIÓN FACULTAD DE CIENCIASECONÓMICAS	: Lic. Mauricio Ernesto Magaña Menéndez
COORDINADOR DEL SEMINARIO	: Lic. Daniel Nehemías Reyes López
DOCENTE DIRECTOR	: Mae. Mario Hernán Cornejo Pérez
JURADO EXAMINADOR	: Mae. Mario Hernán Cornejo Pérez Licda. María Margarita de Jesús Martínez Mendoza de Hernández. Lic. Daniel Nehemias Reyes Lopez

AGRADECIMIENTOS

Agradecimiento total a Dios por darme las fuerzas de seguir día a día luchando en cada una de las dificultades que pudieron surgir a lo largo del camino, a todas las personas maravillosas que me permitió conocer en este trayecto. A mis padres que me brindaron su apoyo incondicional para salir adelante, mi familia que estuvo apoyando cada paso de mi carrera, a mi hermanita Jenniffer Orellana, al Maestro Mario Hernán Cornejo asesor en éste proyecto de investigación que en todo momento me apoyó y dirigió con sabiduría para culminarlo exitosamente, a la Asociación Jovesolides El Salvador, a mis amigos y amigas que estuvieron conmigo en momentos difíciles, a los docentes de cada una de las materias que curse los cuales me brindaron conocimiento para poder aplicarlo en el diario vivir y a esas personas que me apoyaron en alguna etapa de mi formación profesional y personal.

Julio Cesar Orellana Portillo

ÍNDICE

	RESUMEN EJECUTIVO	i
	INTRODUCCIÓN	iii
1.	**CAPÍTULO 1. PLANTEAMIENTO DEL PROBLEMA**	**1**
1.1.	SITUACIÓN PROBLEMÁTICA	1
1.2.	ENUNCIADO DEL PROBLEMA	3
1.3.	JUSTIFICACIÓN DE LA INVESTIGACIÓN	3
1.4.	OBJETIVOS DE LA INVESTIGACIÓN	5
1.5.	HIPÓTESIS	6
2.	**CAPÍTULO II. MARCO TEÓRICO**	**7**
2.1.	ESTADO ACTUAL DEL HECHO O SITUACIÓN	7
2.2.	PRINCIPALES DEFINICIONES	11
2.3.	LEGISLACIÓN APLICABLE	14
2.4.	NORMATIVA TÉCNICA APLICABLE	17
3.	**CAPITULO III. METODOLOGÍA DE LA INVESTIGACIÓN**	**23**
3.1.	ENFOQUE Y TIPO DE INVESTIGACIÓN	23
3.2.	DELIMITACIÓN ESPACIAL Y TEMPORAL	23
3.2.1.	ESPACIAL	23
3.2.2.	TEMPORAL	24
3.2.3.	SUJETOS Y OBJETO DE ESTUDIO	24
3.3.	TÉCNICAS, MATERIALES E INSTRUMENTOS	28

3.3.1. TÉCNICAS Y PROCEDIMIENTOS PARA LA RECOPILACIÓN DE LA INFORMACIÓN 28

3.3.2. INSTRUMENTOS DE MEDICIÓN 28

3.4. PROCESAMIENTO Y ANÁLISIS DE LA INFORMACIÓN 29

3.5. CRONOGRAMA DE ACTIVIDADES 30

3.6. PRESENTACIÓN DE RESULTADOS 31

3.6.1. TABULACIÓN Y ANÁLISIS DE RESULTADOS 31

3.6.2. DIAGNÓSTICO 41

4. CAPÍTULO IV. PROPUESTA DE SOLUCIÓN 45

4.1. PLANTEAMIENTO DEL CASO 45

4.2. ESTRUCTURA DEL PLAN DE SOLUCIÓN 46

4.3. BENEFICIOS Y LIMITANTES 48

4.4. DESARROLLO DE CASO PRÁCTICO 49

SECCIÓN 1: INTRODUCCIÓN Y ALCANCE DEL MANUAL 51

SECCIÓN 2. REFERENCIAS 53

SECCIÓN 3: TÉRMINOS Y DEFINICIONES 53

SECCIÓN 4.COMPROMISO Y RESPONSABILIDADES DE LA ORGANIZACIÓN 56

SECCIÓN 5: LINEAMIENTOS 59

SECCIÓN 6: PROCEDIMIENTOS DE AUDITORÍA DE SISTEMAS 90

CONCLUSIONES 108

RECOMENDACIONES 110

BIBLIOGRAFÍA 112

ANEXOS 114

ÍNDICE DE TABLAS

Tabla 1 - Existencia de políticas y uso de controles en dispositivos móviles 32

Tabla 2 - Políticas de dispositivos móviles y respaldos 34

Tabla 3- Uso de dispositivos móviles y Criptografía 35

Tabla 4- Registro de eventos y uso de firma electrónica 36

Tabla 5- Uso de software legal y registro de eventos 37

Tabla 6 - Firma electrónica y Criptografía 38

Tabla 7 - Respaldo de seguridad y existencia de área segura 39

Tabla 8 - Registro de actividades y registro de eventos 40

ÍNDICE DE FIGURAS

Ilustración 1- Objetivos de la seguridad de la información 9

Ilustración 2 - Línea de tiempo ataques informáticos 12

Ilustración 3 - Cronograma de actividades 30

Ilustración 4 - Existencia de políticas y uso de dispositivos móviles 33

Ilustración 5 - Políticas de dispositivos móviles y respaldo 34

Ilustración 6- Uso de dispositivos móviles y criptografía 35

Ilustración 7- Registro de eventos y uso de firma electrónica 36

Ilustración 8 - Uso de software y registro de eventos 37

Ilustración 9- Firma electrónica y Criptografía 38

Ilustración 10 - Respaldo de seguridad y existencia de área segura 39

Ilustración 11- Registro de actividades y registro de eventos 40

Ilustración 12- Estructura del plan de solución 47

RESUMEN EJECUTIVO

Dentro de los orígenes que han dado pauta para proponer un manual de procedimientos en las Organizaciones no Gubernamentales se encuentran los niveles de vulnerabilidad a la que se expone la información y los datos sensibles que se manipulan, la falta de propuestas en busca de evitar esta debilidad impulsó a elaborar un manual basado en la NTS ISO/IEC 27002.

La propuesta presentada provee al auditor de sistemas de un manual que contiene procedimientos adecuados, que le ayudarán al desarrollo de una auditoría de sistemas basado en la norma ISO 27002, orientado a Organizaciones no Gubernamentales, para alcanzar esta meta se: Identificó si el auditor de sistemas, poseía una guía especializada para desarrollar su cargo dentro de las ONG´s. Se determinó las deficiencias del auditor de sistemas al momento de ejecutar el cargo por no contar con los procedimientos adecuados de auditoría de sistemas, y por último se procedió a elaborar un manual de procedimientos de auditoría de sistemas basado en la norma ISO/IEC 27002.

Para la elaboración de la investigación la fuente principal que se tomó como base fueron los contadores públicos que están inscritos en el Consejo de vigilancia de la profesión de la contaduría pública y auditoría, los cuales ejercen la auditoría en San Salvador, la recolección de la información se llevó a cabo por medio de cuestionario de preguntas cerradas y de selección múltiple para conocer el nivel de seguridad que posee la información y los datos resguardados en el sistema informático de las ONG´s, así como también los controles que son utilizados por dichas organizaciones para la protección de la información, posteriormente se procedió a realizar el diagnóstico de la información que se recolectó por medio de cruce de variables dependiente e independiente.

Se encontró que en menos del 50% de las ONG´s se mantiene en un lugar seguro el registro de eventos que ocurren dentro del sistema de información, lo que tiene como consecuencia que las acciones ejecutadas por cualquier usuario no se guardan y por lo tanto la evidencia desaparece y ante cualquier litigio no se tendría un responsable.

En el 88% de las ONG´s se debe poseer autorización previa para el ingreso de datos al sistema de información lo que es importante dado que el permiso es vital para ejecutar alguna acción con un recurso computarizado, constituye un privilegio técnico, por ejemplo, la capacidad de leer, crear, modificar o eliminar un archivo o dato.

Algunas recomendaciones a considerar para las ONG´s son: Mantener requisitos básicos de seguridad para el acceso a las instalaciones y a las oficinas donde se procesa la información, mantener el hábito de hacer respaldos de seguridad al menos cada semana o dependiendo el cómo se establezca el control en la organización, además los respaldos deben protegerse en un lugar seguro y probar su integridad con frecuencia.

Para los contadores que realizan auditorías de sistemas, se recomienda utilizar el presente manual como una guía básica para la ejecución de futuras auditorías en ONG´s para comprobar la aplicabilidad de los requisitos de seguridad que establece la NTS ISO/IEC 27002 como un valor agregado del manejo y resguardo de la información y los datos que son vitales dentro de éstas entidades.

INTRODUCCIÓN

La seguridad de la información es un factor de vital importancia dentro de las Organizaciones no Gubernamentales pues tanto como en el sector privado o en la parte Estatal, dentro de ellas se manipulan datos que son privativos de cada proyecto que se ejecuta, la manera en que se manipule la información puede tener repercusiones financieras negativas si las intenciones van en contra de los fines y objetivos de cada entidad. La Norma Técnica Salvadoreña ISO/IEC 27002 contiene lineamientos y explica una serie de controles estructurados en bloques los cuales pueden ser considerados por las ONG´s para implementar dentro de su estructura organizativa, así mismo los auditores de sistemas pueden tomarla como referencia para realizar sus auditorías cuando aplique.

La presente investigación ha sido estructurada en cuatro capítulos los cuales tienen como objetivo poner a disposición de los auditores un manual de procedimientos de auditoría de sistemas basada en la NTS ISO/IEC 27002.

El capítulo primero, se desarrolla la situación problemática la cual define el origen del problema a investigar, el enunciado del problema, la justificación de la investigación a realizar, además contiene los objetivos trazados para la realización de la investigación, así como también las limitantes de la investigación, incluye también la hipótesis de la investigación y por último la forma en la que se llevara a cabo el diagnóstico de la investigación.

Capítulo II, Se detalla la situación actual del problema de investigación, así como una serie de principales definiciones que enmarcan la investigación, además este capítulo incluye legislación y normativa técnica aplicable al tema a desarrollar.

Capítulo III, desarrolla la metodología a utilizar, el enfoque y el tipo de investigación que se realizará, la delimitación geográfica de la investigación así como también la delimitación temporal, se presenta además los sujetos y el objeto de investigación, así como también se detalla las técnicas y los instrumentos que servirán de ayuda en la recolección de información para la realización de la investigación, además se presenta el procesamiento, el análisis y la interpretación de los datos procesados, para finalizar se desarrolla el diagnóstico de las diferentes áreas que fueron sujetas a investigación.

Capítulo IV, desarrolla la propuesta de solución, a la problemática, estructurado de un manual dividido en 6 secciones dentro de las cuales se incluyen lineamientos a considerar por cada área vulnerable dentro del sistema informático, finalmente se presentan unos procedimientos diseñados a partir de la NTS ISO/IEC 27002 adecuados para ser implementados en las ONG´s.

1. CAPÍTULO 1. PLANTEAMIENTO DEL PROBLEMA

1.1. SITUACIÓN PROBLEMÁTICA

En El salvador, las empresas han invertido un porcentaje de hasta el 10% de sus ingresos, para la compra de software como antivirus para la protección de la información y cuido de sus equipos, mientras a qué nivel mundial se ha destinado entre el 6% y el 18% de los ingresos respectivamente.

Las empresas que para el año 2013 ya poseían un sistema de seguridad, lo enfocaron más en protección de propiedad intelectual. Uno de los proveedores, Columbus Business Solutions (CBS) que ofrecen servicios de conectividad y soluciones de tecnologías de la información, mostró un informe donde señalaba que por cada dólar ingresado a las empresas cierto margen era invertido en sistemas de protección. (Solís, 2013)

En el sector las ONG´s, se han detectado otros detalles en seguridad como los siguientes: la falta de personal que vigile el ingreso a las instalaciones, escasez en el presupuesto, la manipulación de programas no está restringido completamente, ya que cualquiera puede acceder a las computadoras cuando no existe un encargado de su vigilancia.

La seguridad de la información, es de gran importancia dentro del sector de ONG´s, ya que tienen la necesidad de salvaguardar la información, por ello los gerentes tienen que inspeccionar continuamente el cumplimiento apropiado de las políticas de seguridad, las normas y otros requerimientos de seguridad sobre los procedimientos y procesamiento de la información.

Otro detalle a considerar dentro de las ONG´s es que generalmente han existido gran cantidad de voluntarios y personal no permanente y desde el punto de vista de seguridad, se debe tener en cuenta que, normalmente, suelen tener credenciales de acceso (identificadores de usuario y contraseña, tarjetas de acceso e identificación) que les permiten desarrollar sus funciones, la ONG se deben asegurar, de cancelar y anular todas esas credenciales de voluntarios cuando ya no estén brindando la ayuda a la organización.

En el aspecto lógico, han experimentado infiltraciones al sistema operativo, mediante controles remotos, los cuales han hecho posible que terceros tengan acceso a la información sin la debida autorización, es importante resaltar que el ingreso a distancia no es perjudicial si es utilizado para realizar actividades que conlleven al logro del crecimiento de las actividades de la ONG, algunas de las entidades del sector no poseen sistemas operativos o software utilitario de forma legal, por ello son susceptibles de ser vulnerados, por los creadores de éste software o un tercero conocedor de programación el cual habiéndolo modificado deja entradas ocultas las que pueden servir para ingresar sin la debida autorización.

Las organizaciones en su mayoría dependen de lineamientos con empresas propietarias de software, para así facilitarles la adquisición de licencias para ser utilizadas como herramientas informáticas. Los programas de gestión empresarial, en concreto, son muy costosos que algunas ONG deciden copiar los programas, ya sean contables o de otra índole; ambos necesarios para su operatividad.

Por lo anterior, es conclusa la necesidad de estructurar un manual de procedimientos que le permita al auditor de sistemas ejecutar una labor más certera, en el manejo y verificación de controles en el procesamiento de la información dentro de las ONG´s.

1.2. ENUNCIADO DEL PROBLEMA

La formulación del problema tiene el objeto de describir los elementos de la problemática o fenómeno en estudio, que afecta el funcionamiento y desarrollo de las Organizaciones no Gubernamentales, en tal sentido se dará a conocer cómo afecta no tener un manual de procedimientos de auditoría de sistemas, que pueda tomar como marco guía de referencia el auditor de sistema al momento de realizar su cargo, haciendo así, una "verificación más eficaz de controles en el procesamiento de la información, con el objetivo de evaluar su efectividad y presentar recomendaciones a la Gerencia"

Para ello se formula el problema de la siguiente manera:

¿En qué medida afecta, al auditor de sistemas no contar con los procedimientos adecuados para llevar a cabo el desarrollo de una auditoría de sistemas en las Organizaciones no Gubernamentales?

1.3. JUSTIFICACIÓN DE LA INVESTIGACIÓN

A medida que el tiempo transcurre, en el ámbito tecnológico, las entidades están sometidas a un régimen de modernización constante, que implica la realización de cambios drásticos y constantes en su funcionamiento, para la aplicación de nuevos procedimientos.

En lo referente, para el profesional que desempeña la auditoría de sistemas se vuelve conveniente el desarrollo de una guía de procedimientos que incluya diferentes técnicas de recolección de evidencia suficiente y adecuada que faciliten la verificación de controles en el procesamiento de la información, basada en la norma ISO 27002 tecnología de la información - Código de práctica para la gestión de la seguridad de la información.

Es importante debido a la existencia de nuevas tecnologías, las cuales se usan de manera maliciosa en los sistemas informáticos con objeto de sustraer información confidencial y violar la integridad de los datos, siendo esto perjudicial para la institución.

Un manual de procedimientos para el profesional que desempeña la auditoría de sistemas es novedoso, porque a medida que el tiempo avanza; la tecnología mejora y la información almacenada en los equipos informáticos se puede usar para beneficio propio, por ello es necesario el desarrollo de procedimientos de auditoría de sistemas que ayuden a disminuir la problemática.

La falta de aporte de investigaciones que busquen solucionar el problema del auditor de sistemas y no contar con los procedimientos adecuados para llevar a cabo el desarrollo de una auditoría de sistemas siendo prioridad la seguridad de la información en el sector abordado hacen relevante el aporte que se presenta, la seguridad de la información es importante tanto para negocios del sector público, Organizaciones no Gubernamentales y negocios del sector privado, así como otras entidades que requieren este tipo de instrumento para tener un control sobre la información.

La investigación es factible porque que se cuenta con estándares internacionales como la norma ISO 27002, la cual ayuda de forma inmediata y presenta procedimientos a seguir, por las organizaciones para la seguridad de la información. Con la investigación se pretende beneficiar al auditor de sistemas de las Organizaciones no Gubernamentales, siendo auditor de planta o contratado externamente por la ONG para prestar su servicio.

1.4. OBJETIVOS DE LA INVESTIGACIÓN

Los objetivos propuestos en esta investigación son los siguientes:

Objetivo General: Proporcionar, al auditor de sistemas un manual que cumpla con los procedimientos adecuados que le ayude al desarrollo de una auditoría de sistemas basado en la norma ISO 27002, orientado a Organizaciones no Gubernamentales.

Objetivos específicos

- Identificar si el auditor de sistemas, cuenta con una guía especializada con la que lleva a cabo el desarrollo de su cargo dentro de las Organizaciones no Gubernamentales.

- Determinar las deficiencias del auditor de sistemas al momento de desarrollar el cargo por no contar con los procedimientos adecuado de auditoría de sistemas.

- Elaborar un manual de procedimientos de auditoría de sistemas basado en la norma ISO/IEC 27002.

1.5. HIPÓTESIS

Hipótesis de trabajo

La implementación de un manual de procedimientos de auditoría de sistemas basado en la norma ISO 27002 contribuirá a que el auditor de sistemas ejecute una revisión adecuada en las Organizaciones no Gubernamentales.

Determinación de las variables

- Variable dependiente: Auditoría de sistemas adecuada, debido a que mientras no se aplique un manual de procedimientos de auditoría de sistemas, menos acertado será el trabajo que ejecute el auditor de sistemas.

- Variable independiente: El manual de procedimientos de auditoría de sistemas, ya que la existencia de éste y la puesta en práctica al momento de ejecutar una auditoría dentro de las ONG´s contribuirá a que el trabajo del auditor sea mas objetivo y efectivo para presentar mejores recomendaciones a la Gerencia.

2. CAPÍTULO II. MARCO TEÓRICO

2.1.ESTADO ACTUAL DEL HECHO O SITUACIÓN

Seguridad de la información

La información, un recurso clave para muchas empresas desde que se genera hasta que se destruye, las TI están avanzando cada vez más y se ha generalizado en las empresas y entornos sociales, públicos y de negocios.

La seguridad de la información es un catalizador de negocios que está básicamente unido a la confianza de las partes interesadas. “En un momento en que la importancia de la información y las tecnologías relacionadas con ella están creciendo en cada aspecto del mundo de los negocios y la vida pública, la necesidad de mitigar el riesgo sobre la información, lo que incluye proteger la información y los activos de TI relacionados con ella de amenazas que cambian continuamente, se está intensificando constantemente.” (ISACA, COBIT 5 Para seguridad de la información, 2012)

La importancia de la gestión de la seguridad de la Información.

El componente más difícil para la protección de la información es el establecimiento de las bases para una gestión efectiva de la seguridad de la información. El inicio del intercambio electrónico por medio de las personas que abastecen de servicio y que lo hacen de forma directa con los clientes, las disminución de barreras por medio de mecanismos en acceso remoto y la exposición al riesgo de seguridad mucho más alto, estas y otras causas han elevado el nivel de inseguridad de la información.

El manual de preparación CISA, establece algunos objetivos de seguridad de la información (ver ilustración 1) para satisfacer los requerimientos del negocio de las organizaciones incluyen los siguientes: (ISACA, Manual de preparacion al examen CISA , 2014)

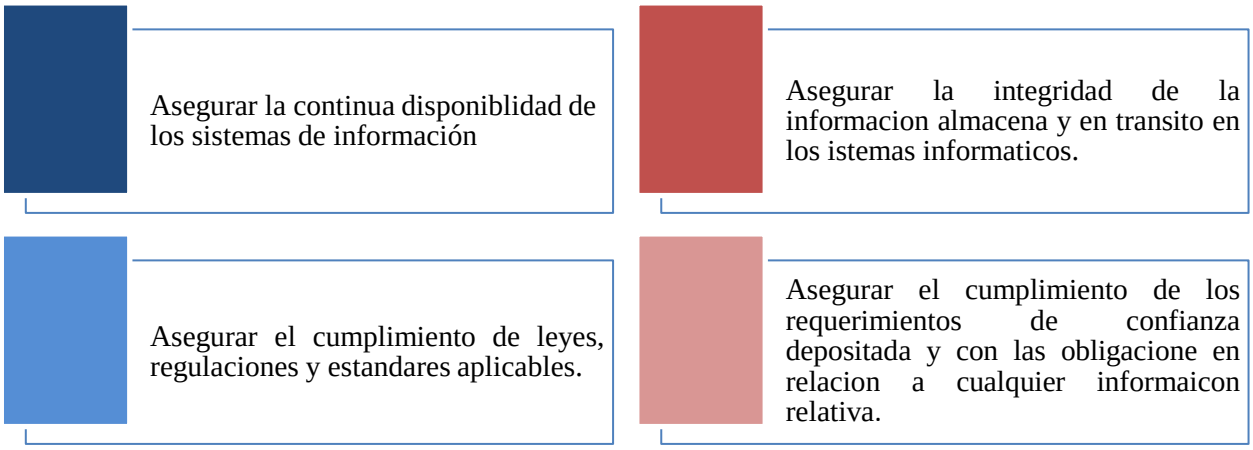
La protección de los datos se logra con la implementación de conjuntos adecuados de controles, tales como: políticas, proceso, procedimientos, estructuras organizacionales y funciones de software y hardware.

Para lograr un alto nivel de seguridad de la información, deben establecerse controles que sean aplicados, monitoreados, revisados y mejorados de acuerdo a la necesidad para asegurar que los objetivos sean cumplidos, un Sistema de Gestión de Seguridad de la Información como el especificado en la NTS ISO/IEC 27001, dicho sistema establece una visión de forma integrada y coordinada de los riesgos de seguridad de la información en las organizaciones para implementar un conjunto amplio de inspecciones.

En la NTS ISO/IEC 27002 en uno de sus apartados establece los requisitos de seguridad de la información la cuales se citan a continuación:

- La valoración de los riesgos para la organización, considerando la estrategia y objetivos de negocio en marcha. A través de una evaluación de riesgos.
- La evaluación de los requisitos legales, estatutarios, reglamentarios y contractuales que una organización, sus socios comerciales, contratistas y proveedores de servicios tienen que satisfacer, asa como su entorno social cultural.

Ilustración 1- Objetivos de la seguridad de la información



- El conjunto de principios, objetivos y requisitos de negocio para el manejo, procesamiento, almacenamiento, comunicación y el archivado de información, que una organización ha desarrollado para apoyar sus operaciones.

Las organizaciones deben identificar los recursos a emplear y los controles implementados, que estarían balanceados contra el probable daño que pueda estar sufriendo la organización, resultante de los incidentes de seguridad por la ausencia de la implementación de controles.

HECHOS DE LOS ÚLTIMOS AÑOS ACERCA DE LA PROBLEMÁTICA

En 2005, con el lanzamiento de la segunda edición del marco normativo ISO 27002, comienza el desafío para las Organizaciones no Gubernamentales de dar cumplimiento con dicho marco, ya que la información es almacenada en equipos informáticos, y estos son susceptibles de sufrir ataques, tanto físicos como lógicos.

En el 2013 el tema con más auge en el “Día de la Tecnología”, fue la seguridad informática. Por lo que muchas empresas que asistieron, entre ellos, CBS, Cisco, Fortinet, ESET, entre otras, concordaron que la seguridad informática es vulnerable por los muchos ataques recibidos a través de la historia. En Latinoamérica el 43% de las empresas que sufren “ataques cibernéticos” provienen de El Salvador, mientras que el 23% de Guatemala, según estudios brindados en el foro ESET de seguridad informática en Río de Janeiro 2016. (Aguilar, 2016)

A nivel nacional se encuentran varios eventos en los cuales se puede comprender lo susceptible que es la información en diferentes entidades, por los ataques informáticos de múltiples maneras, seguido se detallan algunos de ellos.

En 2011, Anonymous realizó un ataque a los sitios web del gobierno salvadoreño como una protesta por el alto índice de criminalidad, según informes además realizaron publicaciones durante las elecciones presidenciales en las cuales resaltaban un candidato para de esa manera hacer mayor popularidad.

En 2012, Yahoo confirmó haber sufrido un hackeo en el cual más de 500 millones de cuentas fueron vulneradas (copiadas con todo y clave de acceso), aunque no se publica a detalle el lugar del cual fue, pero se sabe que fue con intenciones de vender dichas direcciones web para publicidad.

En 2013 un hacker salvadoreño reveló su forma de ataque en la web, la cual consistía básicamente en: “hacer ´phishing´ del correo electrónico. Es decir, usurpando la identidad de una página web, donde se pide que actualice sus datos y el usuario cae y mete sus datos en una página ficticia la cual archiva la contraseña y la deja a disposición del hacker”, expresó Rodrigo. (Página, 2013)

En 2014 un ingeniero de CAESS realizó un desfalco financiero por cerca de $95 mil dólares a la empresa mediante el ingreso de recibos cancelados por los usuarios cobrando en efectivo, pero sin ingresarlo a la caja o banco de la empresa.

En 2015 se publica “Francisco Flores a Juicio por corrupción”, donde se explica la forma en que fue distribuido el dinero. Según el análisis, el fondo había sido depositado en una cuenta y con cargo a esta fueron emitidos varios cheques, lo que falló aquí fue el control en la supervisión de aprobar estas salidas de recurso.

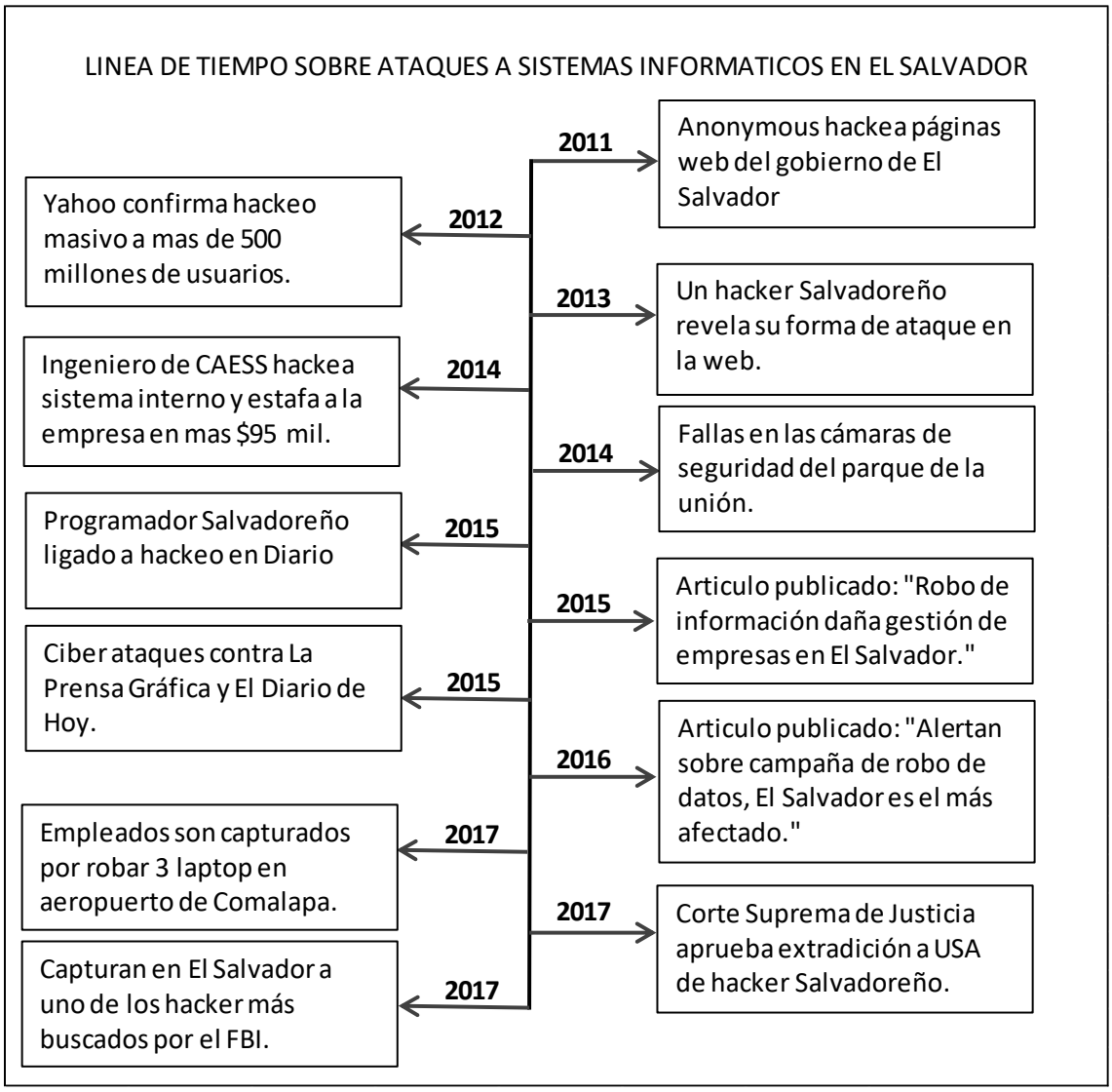
En febrero 2017, envían a juicio a implicados en ciberataque al Diario de Hoy y la Prensa Gráfica por los delitos de violación de derechos de autor y derechos conexos, violación de distintivos comerciales y falsedad material. (López, 2017)

A continuación, se muestra (ver Ilustración 2) una línea de tiempo con algunos de los sucesos ocurridos a partir de 2011 en El Salvador donde se evidencia la vulnerabilidad de la información en distintas Entidades.

2.2.PRINCIPALES DEFINICIONES

Seguridad lógica: consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y solo se permita acceder a ellos a las personas autorizadas para ello, a fin de reducir el riesgo de transferencia, modificación, pérdida o divulgación accidental o intencional de éstos. (Cornejo, 2017)

Ilustración 2 - Línea de tiempo ataques informáticos



Fuente: Equipo de investigación del presente trabajo a partir de varias publicaciones en noticieros de la web.

Seguridad de la información: ISACA define a la seguridad de la información como algo que: Asegura que dentro de la empresa, la información está protegida contra su divulgación a usuarios no autorizados (confidencialidad), modificación inadecuada (integridad) y su falta de acceso cuando se la necesita (disponibilidad), La seguridad de la información es un catalizador de negocio que está intrínsecamente unido a la confianza de las partes interesadas, ya sea tratando los riesgos de negocio o creando valor para la empresa como una ventaja competitiva. (ISACA, COBIT 5 Para seguridad de la información, 2012)

Identificación y autenticación: La I&A en el software de control de acceso lógico, es el proceso de establecer y probar la identidad de alguien. Es el proceso por el cual se obtiene de un usuario su identidad y las credenciales necesarias para autenticar esta identidad y valida ambas piezas de identificación. Es la primera línea de defensa (una medida técnica) que impide que personas no autorizadas (o procesos no autorizados) entren a un sistema informático. (Cornejo, 2017)

Auditoría de sistemas: este proceso recolecta y evalúa la evidencia para determinar si los sistemas de información y los recursos relacionados protegen adecuadamente los activos, mantienen la integridad y disponibilidad de los datos del sistema, proveen información relevante y confiable, logran de forma efectiva las metas organizacionales, usan eficientemente los recursos y tiene en efecto controles internos que proveen una certeza razonable de que los objetivos de negocio, operacionales y de control serán alcanzados y que los eventos no deseados serán evitados o detectados y corregidos de forma oportuna. (ISACA, Manual de preparacion al examen CISA , 2014)

2.3. LEGISLACIÓN APLICABLE

Ley de asociaciones y fundaciones sin fines de lucro: Cuando una asociación o fundación se constituye deberá hacerlo a través del Ministerio de Gobernación, siguiendo un proceso de constitución, donde debe presentar los siguientes documentos: Escritura de Constitución, Registro de miembros, certificación de punto de acta de elección de Junta Directiva, y los libros de actas, y libros contables. En cuanto a la contabilidad, dicha ley establece, la presentación de Estados Financieros en base a las normativas vigentes en el país. (Legislativa A. , 1996)

Ley reguladora del ejercicio de la Contaduría: regula el ejercicio de la profesión de la contaduría pública, de la auditoría y los derechos y obligaciones de las personas que la ejercen. Establece las personas que pueden ejercer la Contaduría Pública y por consiguiente de los requisitos en el artículo 2, en su apartado requisitos para ser autorizado como contador público, la autorización del contador público está a cargo del Consejo de Vigilancia de la Profesión de contaduría Pública y Auditoría.

"Para los efectos de esta Ley, si un contador público una vez autorizado, dejare de reunir los requisitos del artículo 2, no podrá continuar ejerciendo su función. El Consejo, de oficio, o a petición de cualquier persona, lo suspenderá de conformidad a esta Ley". (Legislativa A. , 2000) Cabe mencionar las atribuciones del contador público dentro del artículo 17, como las prohibiciones en el artículo 22. Entre otras situaciones que son de importancia para la aplicación de la investigación.

Ley especial contra delitos informáticos y conexos: posesión de equipos o prestación de servicios para la vulneración de la seguridad, artículo 8 el que utilizando las tecnologías de la información y la comunicación posea, produzca, facilite, venda equipos, dispositivos, programas informáticos, contraseñas o códigos de acceso; con el propósito de vulnerar, eliminar ilegítimamente la seguridad de cualquier sistema informático, ofrezca o preste servicios destinados a cumplir los mismos fines para cometer cualquiera de los delitos establecidos en la presente ley, será sancionado con prisión de tres a cinco años.

Violación de la seguridad del sistema, en el artículo 9 establece que la persona que sin poseer la autorización correspondiente transgreda la seguridad de un sistema informático restringido o protegido con mecanismo de seguridad específico, será sancionada con prisión de tres a seis años.

Alteración, daño a la integridad y disponibilidad de los datos, el artículo 19 claramente trata de la sanción para cualquiera que violando la seguridad de un sistema informático destruya, altere, duplique, inutilice o dañe la información, datos o procesos, en cuanto a su integridad, disponibilidad y confidencialidad en cualquiera de sus estados de ingreso, procesamiento, transmisión o almacenamiento, será sancionado con prisión de tres a seis años. (Legislativa A. , Ley especial contra delitos informáticos y conexos, 2015)

Ley de propiedad intelectual, en el artículo 85 establece que se entiende por medida tecnológica efectiva, cualquier tecnología, en el curso normal de su operación, controla el acceso a una obra, fonograma u otra materia protegida, o que protege cualquier derecho de autor o cualquier derecho conexo al derecho de autor, en su último apartado de igual forma constituyen excepciones a cualquiera de las medidas que implementen las prohibiciones establecidas en los literales a) y b) (Legislativa A. , Ley de propiedad intelectual, 2017)

Ley de firma electrónica, en el artículo 4 hace referencia a las actividades que se regirán bajo los siguientes principios: en su literal b) menciona lo siguiente seguridad, la certeza y legalidad que la persona firmante y acreditada, ha sido debidamente identificada, garantizando la disponibilidad, integridad, confidencialidad, autenticación, no repudio y buen uso de la información que reside en un sistema informático.

Dentro del artículo 15 se establece que toda persona jurídica que realice el almacenamiento de documentos electrónicos para terceros, redactará una declaración de prácticas de almacenamiento, en la que detallará, dentro del marco de esta ley y de su reglamento, la siguiente información: literal c) Las medidas de seguridad técnica, física y organizativa; cabe mencionar que cuenta con obligación de los proveedores de los servicios de certificación Art.- 48 en su literal h) Garantizar la autenticidad, integridad y confidencialidad de la información, y documentos relacionados con los servicios que proporcione. A tales efectos, deberán mantener un sistema de seguridad informática y respaldos confiables y seguros de dicha información, de conformidad a lo establecido en la presente ley, su reglamento, normas y reglamentos técnicos. (Legislativa A. , 2015)

2.4. NORMATIVA TÉCNICA APLICABLE

NTS ISO/IEC 27001; 2013 Tecnología de Información, es un estándar internacional preparado con el objetivo de proporcionar un modelo para el establecimiento, implementación, operación, monitoreo, revisión y mantenimiento de un sistema de gestión de seguridad de la información, la adopción de este sistema debe ser por decisiones estratégicas por parte de la gerencia de la organización al igual que el diseño y la implementación.

En las organizaciones debe implementarse dependiendo las necesidades y objetivos propuestos a futuro, requerimientos de seguridad, los procesos empleados. (NTS ISO/IEC 27002; 2013; Organismo Salvadoreño de Normalización, 2013) Este estándar internacional puede ser utilizado por entidades internas y externas para evaluar la conformidad.

La implementación de un sistema de procesos dentro de una organización junto con la identificación de las áreas y las interacciones de estos procesos, la gestión puede considerarse un enfoque del proceso para el cumplimiento de los objetivos de las organizaciones.

Permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan. El estándar ISO 27001; 2013 permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlo. Esta norma está estructurada en 10 capítulos los cuales brindan la guía necesaria para la adopción de un SGSI.

NTS ISO/IEC 27002:2013 TECNOLOGÍA DE LA INFORMACIÓN. CÓDIGO DE PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.

La información va más allá de ser unas simples palabras de intercambio, números e imágenes; conocimiento conceptos, ideas y marcas en general, los anteriores son algunos ejemplos de formas intangibles de información las cuales pueden ser objeto de hurto.

Todos los procesos relacionados entre sí, y los relacionados, sistemas, redes y personal involucrados directa o indirectamente en su operación, manejo y protección, son activos que al igual que otros son importantes para las organizaciones y necesitan de protección contra diversas amenazas. (ISO 27002, 2013)

Al igual que la ISO 27001; 2013 Tecnología de Información; este estándar trata los puntos más detallados, ha sido diseñado para las organizaciones que utilizan como referencia para la selección de los controles dentro del proceso de implementación de un Sistema de Gestión de Seguridad de la Información.

Cabe destacar que fue diseñado como un documento para que sirva a las organizaciones como una guía para la implementación de controles de seguridad de la información; además tiene el propósito de ser utilizada en el desarrollo de procedimientos de gestión de seguridad de la información.

En tal sentido la ayuda o la participación de personas externas es fundamental en la implementación de este tipo de estándares para el asesoramiento especializado. Los profesionales de la contaduría pública debidamente autorizados por el Consejo de Vigilancia para la Contaduría Pública y la Auditoría (CVCPA), que desempeñan el rol de auditor externo deben

contar con una guía para la implementación de este estándar NTS ISO/IEC 27002; 2013 en las organizaciones no gubernamentales.

COBIT 5 PARA SEGURIDAD DE LA INFORMACIÓN

Proporciona un marco de trabajo completo que ayuda a las entidades a lograr sus metas para el gobierno y la gestión de las tecnologías de información corporativas. Dicho de una manera sencilla, colabora con las empresas para crear el valor óptimo desde la tecnología de la información (TI) manteniendo el equilibrio entre la generación de beneficios, la optimización de los niveles de riesgo y la utilización de recursos. COBIT 5 permite que las tecnologías de la información se gobiernen y gestionen de un modo holístico para toda la empresa, abarcando al negocio completo de principio a fin y las áreas funcionales de responsabilidad de estas, considerando los intereses relacionados con las mismas de los grupos de interés internos y externos. (ISACA, 2012).

Incluye los cinco principios que permiten a la organización construir un marco efectivo de gobierno y administración basado en una serie holística de siete habilitadores, que optimizan la inversión en tecnología e información, así como su uso en beneficio de las partes interesadas.

COBIT 5 para Seguridad de la Información incluyen:

La necesidad de puntualizar la seguridad de la información en el contexto de una empresa incluyendo así:

- Las responsabilidades que pueden ser funcionales desde un inicio a fin para seguridad de la información en el negocio.

- Todos los aspectos que llevan a un gobierno y gestión efectivos de la seguridad de la información, tales como estructuras organizativas, políticas y cultura.
- La relación y enlace de la seguridad de la información con los objetivos de la empresa. (ISACA, 2012)

Una necesidad creciente de la empresa de:

- Mantener el riesgo de información a un nivel aceptable y proteger la información contra divulgaciones no autorizadas, modificaciones involuntarias o no autorizadas y posibles intrusiones.
- Asegurar que los servicios y sistemas de información se encuentran disponibles continuamente para los grupos de interés internos y externos, con el objetivo de satisfacer a los usuarios en relación con el compromiso y los servicios proporcionados por TI.

IEPS 2 TECNOLOGÍA DE LA INFORMACIÓN PARA CONTADORES

El IES 2, Contenido de los Programas de Formación en Contaduría profesionales, señala el contenido de conocimiento de los programas de educación contables profesionales que los candidatos necesitan adquirir para calificar como contadores profesionales. Proporciona orientación para los organismos miembros de la IFAC y otros educadores en la aplicación sobre tecnologías de la información para contadores en relación con el componente de conocimientos informáticos de los programas de educación de contabilidad profesional.

Esta IEPS también proporciona una guía para los organismos miembros de la Federación Internacional de Contadores, en la implementación de IES 7, Desarrollo profesional continuo: un programa de aprendizaje permanente y desarrollo continuo de la competencia profesional, Y las Normas Internacionales de Formación 8, Requisitos de competencia para los profesionales de la auditoría, En relación con el futuro desarrollo de los conocimientos de TI y competencias post-calificación. (IFAC, 2008)

En los alcances que pretende esta norma se espera que a todos los profesionales en contaduría pública proporcionarles un conocimiento y comprensión de por lo menos una de las tres funciones establecidas en las Normas Internacionales de Formación 2 (gerente, evaluador y diseñador de sistemas de información), o una combinación de estos roles. Sección 1 de este IEPS ofrece orientación sobre buenas prácticas en estos roles, con el apoyo de los Anexos 4, 5 y 6 Estos contienen elementos de competencia que los organismos miembros de la IFAC pueden incluir en el componente de conocimientos informáticos de los programas de educación de contabilidad profesional de precalificación. (IFAC, 2008)

IES 2 CONTENIDO DE LOS PROGRAMAS DE EDUCACIÓN PROFESIONAL CONTABLE

El objetivo de esta Norma Internacional de Formación es que los aspirantes a participar en un organismo miembro de la Federación Internacional de Contadores posean conocimientos contables avanzados suficientes para poder actuar como contadores profesionales competentes en un entorno cada vez más complejo y cambiante.

El conocimiento principal en los programas profesionales de formación en contaduría puede dividirse en tres aspectos importantes:

a) Contaduría, finanzas y conocimientos relacionados;

b) Conocimiento organizacional y de negocios; y

c) Conocimiento de tecnología de la información y competencias.

Las habilidades profesionales requeridas y el contenido de la formación general, los valores, ética y actitud profesionales y los requisitos relacionados con la experiencia práctica se exponen en la IES 3, Habilidades profesionales y formación general, IES 4, Valores, ética y actitud profesionales e IES 5, Requisitos de experiencia práctica. (IFAC, 2008)

NORMAS INTERNACIONALES PARA EL EJERCICIO PROFESIONAL DE LA AUDITORÍA INTERNA (NIEPAI)

Los auditores deben poseer conocimientos sobre los riesgos y controles claves con respecto a las tecnologías de la información, basados en normativa aplicable a buenas prácticas para llevar a cabo la auditorías interna en las empresas, las NIEPAI establecen una serie de lineamientos aplicables, dentro de los cuales establece tanto el uso de tecnologías de información que permitan desempeñar el trabajo asignado, como la evaluación de si el gobierno de tecnología de la información apoya las estrategias y objetivos de la organización; las obligaciones de los auditores al realizar una auditoría es dejar constancia de cada uno de los procesos que se lleven a cabo, incluyendo alcance, objetivos, tiempo y asignación de recursos, todo esto como las buenas prácticas establecidas.

3. CAPITULO III. METODOLOGÍA DE LA INVESTIGACIÓN

3.1.ENFOQUE Y TIPO DE INVESTIGACIÓN

A través del estudio de tipo analítico descriptivo, se pretende analizar la problemática respecto a la vulnerabilidad que presenta la información, en el sector de las Organizaciones no Gubernamentales, y la necesidad de un manual de procedimientos de auditoría de sistemas basado en NTS ISO/IEC 27002:2013 Tecnología de la información. Código de prácticas para la gestión de la seguridad de la información aplicando el método hipotético-deductivo:

a) Hipotético, porque permitirá estudiar los aspectos que han dado origen a ese fenómeno y elaborar la hipótesis que será de guía para el resultado de la investigación.
b) Deductivo, pues por medio de ello se determinarán las deficiencias existentes en los procedimientos o técnicas utilizadas por el área de informática o tecnologías de información en las ONG´s. que permitirán plantear una alternativa de solución.

3.2.DELIMITACIÓN ESPACIAL Y TEMPORAL

3.2.1. ESPACIAL

La investigación fue aplicada tomando como referencia los contadores públicos del municipio de San Salvador registrados en el Consejo de Vigilancia de la profesión de Contaduría Pública y Auditoría. La selección de dicho sector fue por la factibilidad para acceder a la información y la necesidad que presentan de aplicar un manual de procedimientos de auditoría,

por su razón de ser, existe mayor sentido de colaboración para ser sujetos objeto de estudio en investigaciones llevadas a cabo por estudiantes.

3.2.2. TEMPORAL

La investigación sobre la vulnerabilidad de la información en las Organizaciones no Gubernamentales ONG´s se basó en el periodo del 2005 hasta la actualidad, pues desde el 2005 que es emitida la segunda edición del marco normativo NTS ISO/IEC 27002:2013 Tecnología de la información. Código de prácticas para la gestión de la seguridad de la información, naciendo la oportunidad para cumplir este requerimiento para la protección de la información por los riesgos a que están expuestos cuando el control informático es débil o inexistente, así mismo, por la existencia de tecnología que permite la intervención y alteración perjudicial de los sistemas informáticos cada vez, se hace necesario la mejora e innovación en la implementación de mecanismos para la seguridad y protección.

3.2.3. SUJETOS Y OBJETO DE ESTUDIO

3.2.3.1.UNIDADES DE ANÁLISIS

Las unidades de análisis a considerar en la investigación fueron los contadores públicos registrados en el Consejo de Vigilancia de la profesión de la Contaduría Pública y Auditoría, que ejercen la función de auditoría en las Organizaciones no Gubernamentales ubicadas en el municipio de San Salvador.

3.2.3.2.POBLACIÓN Y MARCO MUESTRAL

Población, La población de los contadores del municipio de San Salvador que están inscritos en el Consejo de Vigilancia de la profesión de Contaduría Pública y Auditoría son 1399 , listado proporcionado por un miembro debidamente inscrito CVPCPA que conforma el universo de elementos de los cuales se extraerá la muestra para la investigación de campo.

Muestra, Una vez se determinó el universo, se procedió a realizar el cálculo de la muestra debido a la dificultad en tiempo y recursos económicos para analizar el total de los contadores públicos del municipio de San Salvador inscritos en el Consejo de vigilancia de la profesión de Contaduría y Auditoría. El cuestionario como instrumento para la obtención de la información, se utilizó para recopilar la información suficiente acerca del problema en estudio y así abordar un análisis mediante datos cuantificables; el cálculo de la muestra se determinó mediante una fórmula estadística utilizada para una población finita.

La fórmula es la siguiente:

$$n = \frac{N.P.Q.\ Z^2}{(N-1)\ e^2 + P.Q.\ Z^2}$$

Dónde:

n =Tamaño de la muestra.

N= Población

Z = Coeficiente de confianza

e = Margen de error

P =Probabilidad de éxitos de que la problemática exista.

Q = Probabilidad de fracaso.

Entonces:

n =?	e = 0.10
N= 1399	P =0.90
Z = 1.96	Q = 0.10

$$n = \frac{(1399)(0.90)(0.10)(1.96)^2}{(1399-1)\,(0.10)^2 + (0.90)\,(0.10)\,(1.96)^2}$$

$$n = \frac{(1399)(0.90)(0.10)(3.8416)}{(1399-1)\,(0.01) + (0.90)\,(0.10)\,(3.8416)}$$

$$n = \frac{483.695856}{13.98 + 0.345744}$$

$$n = \frac{483.695856}{14.325744}$$

n = 33.7641 n= 34 **Contadores Públicos.**

Es por este resultado que 34 Contadores Públicos inscritos en el Consejo de Vigilancia de la Profesión de Contaduría Pública y Auditoría conformaron la muestra, los que fueron seleccionados mediante el muestreo aleatorio simple, donde cada uno tuvo la misma probabilidad de ser escogido.

3.2.3.3.VARIABLES E INDICADORES

Variables

- Variable dependiente: auditoría de sistema adecuada, debido a que mientras no se aplique un manual de procedimientos de auditoría de sistema, menos acertado será el trabajo que ejecute el auditor de sistema.
- Variable independiente: el manual de procedimientos de auditoría de sistema, ya que la existencia de este y la puesta en práctica al momento de ejecutar una auditoría dentro de la ONG´s contribuirá a que el trabajo del auditor sea más objetivo y efectivo para prestar mejores recomendaciones a la gerencia.

Variable dependiente: auditoría de sistema adecuada.

- Medidas de resguardo de la información contable administrativa que poseen
- Revisión de los niveles de ingreso a los diferentes programas que utilizan.
- Procedimientos de ingreso a las instalaciones.
- Eficacia de la etapa de desechar información obsoleta.
- La existencia de usuarios en estructura de escala según nivel de confianza y responsabilidad.
- Autenticidad del software utilizado en la manipulación de la información

Variable independiente: el manual de procedimientos de auditoría de sistema.

- Grado de preparación del encargado del área contable e informática, respecto a procedimientos de auditoría de sistemas.
- Riesgo que presenta las diferentes áreas del sistema informático.
- Efecto que genera en la información de la institución la falta de aplicación de un manual de procedimientos auditoría
- Los procedimientos adecuados para llevar a cabo una auditoría de sistemas en las ONG´s los cuales contribuyen a disminuir la vulnerabilidad de la información.
- La aplicación continúa del manual de procedimientos de auditoría de sistemas.

3.3.TÉCNICAS, MATERIALES E INSTRUMENTOS

3.3.1. TÉCNICAS Y PROCEDIMIENTOS PARA LA RECOPILACIÓN DE LA INFORMACIÓN

Para la obtención de la información sobre el problema que se investigó, se usó la técnica de la entrevista, porque de esa forma se pudo tener acceso a información veraz en cuanto a los aspectos por los cuales la información es vulnerable en las ONG´s.

3.3.2. INSTRUMENTOS DE MEDICIÓN

El instrumento que se usó para la recolección de datos fue el cuestionario dirigido a los profesionales que ejercen la Contaduría Pública y que pueden desempeñar la función especializada de auditoría de sistemas en las ONG´s del municipio de San Salvador, que

ejecutan proyectos de educación, el cual fue formulado con una serie de preguntas enfocadas a conocer y brindar una solución al problema en estudio, indagando sobre la necesidad de un manual de procedimientos de auditoría en sistemas basado en la normativa NTS ISO/IEC 27002:2013 Tecnología de la información. Código de prácticas para la gestión de la seguridad de la información.

3.4. PROCESAMIENTO Y ANÁLISIS DE LA INFORMACIÓN

La información, recopilada por medio del cuestionario, se tabuló en Microsoft Excel, herramienta que facilitó el diseño de gráficos para mayor comprensión de los resultados, y para el cálculo de variables, como el cruce de preguntas, se utilizó además el programa estadístico SPSS.

3.5.CRONOGRAMA DE ACTIVIDADES

Ilustración 3 - Cronograma de actividades

PERIODO / ACTIVIDADES	2017																															
	MARZO				ABRIL				MAYO				JUNIO				JULIO				AGOSTO				SEPTIEMBRE				OCTUBRE			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Introducción al trabajo de graduación																																
Planificación de la investigación																																
Planteamiento del problema																																
Definición del problema																																
Estructuración del anteproyecto																																
Primer entrega de anteproyecto																																
Devolución de anteproyecto para mejorar																																
Segunda entrega de anteproyecto																																
Capítulo I Planteamiento del problema																																
Elaboración del capítulo I																																
Entrega de capítulo I																																
Revisión del capítulo I																																
Capítulo II Marco teórico																																
Elaboración del capítulo II																																
Entrega del capítulo II																																
Revisión del capítulo II																																
Capítulo III Metodología de investigación																																
Elaboración del cuestionario																																
Revisión del cuestionario																																
Mejora del cuestionario																																
Aprobación del cuestionario																																
Recolección de la información																																
Procesamiento de la información																																
Entrega de capítulo III																																
Capítulo IV Propuesta de solución																																
Elaboración de capítulo IV																																
Entrega de capítulo IV																																
Elaboración de trabajo final																																
Entrega de trabajo final																																
Revisión de trabajo final																																
Segunda entrega de trabajo final																																

3.6.PRESENTACIÓN DE RESULTADOS

3.6.1. TABULACIÓN Y ANÁLISIS DE RESULTADOS

Una vez tabulada la información recolectada mediante los cuestionarios, se procedió con la interpretación de la misma, el análisis se ejecutó de la siguiente forma:

Se inició colocando la pregunta, se tabuló destacando la frecuencia en términos absolutos y porcentuales, estas frecuencias fueron presentadas mediante gráficos de pastel y de barra en 3D del programa Excel. Se concluyó a la interrogante destacando la mayor de las frecuencias de las opciones de respuesta; además, se tabularon, presentaron y analizaron varios cruces de variables e interrogantes del cuestionario (ver anexo 3) para mostrar la existencia de la problemática planteada, así como también la necesidad de la propuesta de solución presentada en esta investigación.

Un análisis más claro se ha realizado mediante el cruce de variables mostradas a continuación.

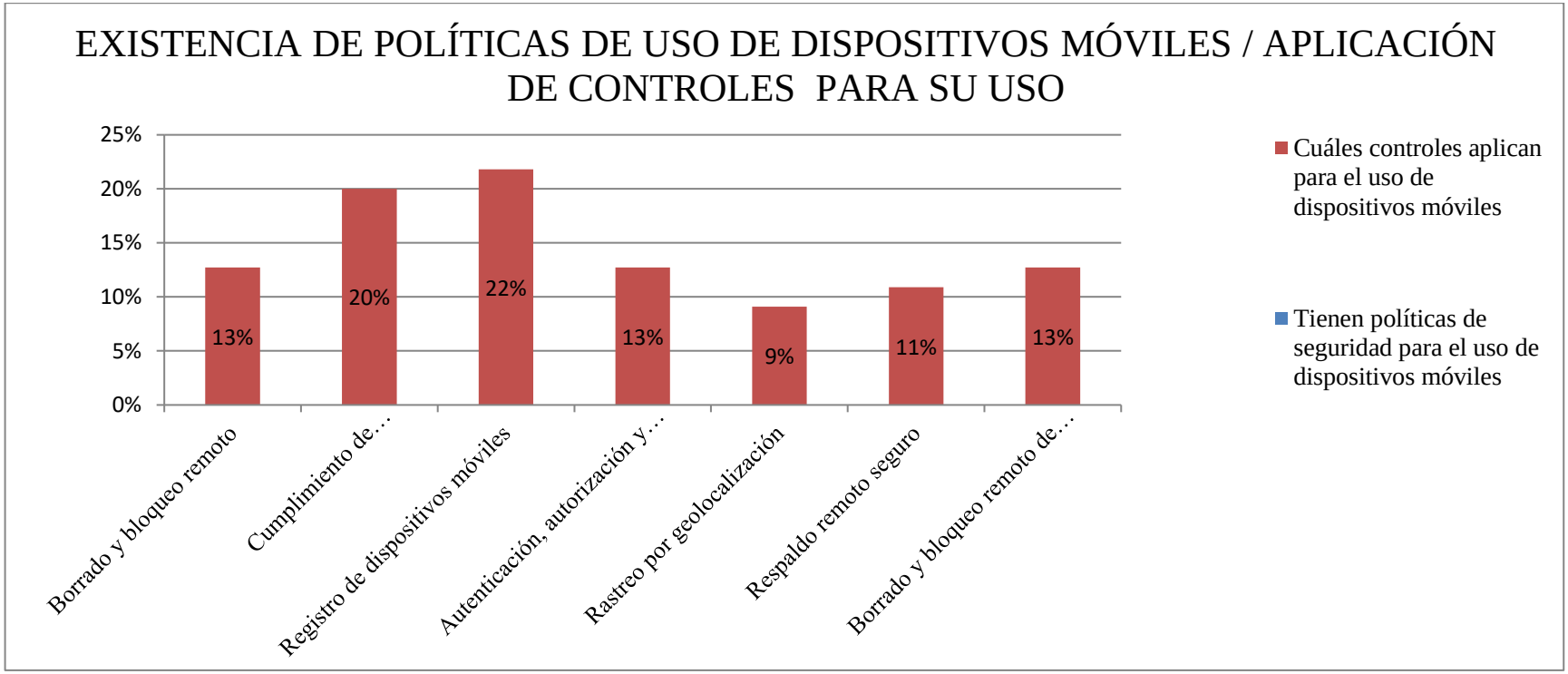
La investigación se llevó a cabo por cruce de variables y se dividió por las siguientes áreas:

Cruce 1

Tabla 1 - Existencia de políticas y uso de controles en dispositivos móviles

		Cuáles controles aplican para el uso de dispositivos móviles							
		Borrado y bloqueo remoto	Cumplimiento de requerimientos de seguridad	Registro de dispositivos móviles	Autenticación, autorización y responsabilidad en la red	Rastreo por geolocalización	Respaldo remoto seguro	Borrado y bloqueo remoto de acceso a dispositivos móviles	TOTAL
Tienen políticas de seguridad para el uso de dispositivos móviles	Si	13%	20%	22%	13%	9%	11%	13%	**100%**
	No	0%	0%	0%	0%	0%	0%	0%	**0%**
TOTAL									**100%**

Ilustración 4 - Existencia de políticas y uso de dispositivos móviles



Análisis**,** del total de auditores encuestados en un 56% se han encontrado la existencia de políticas de seguridad para el uso de dispositivos móviles en conexiones de acceso remoto en las ONG; de ellos un 22% aplican como medida de control para su uso el "registro de dispositivos móviles", un 20% el "cumplimiento de requerimientos de seguridad", un 13% aplica "borrado y bloqueo remoto", otro 13% la "autenticación, autorización y responsabilidad en la red" , un 11% aplica el "respaldo remoto seguro" y finalmente un 9% utiliza el "rastreo por geolocalización"

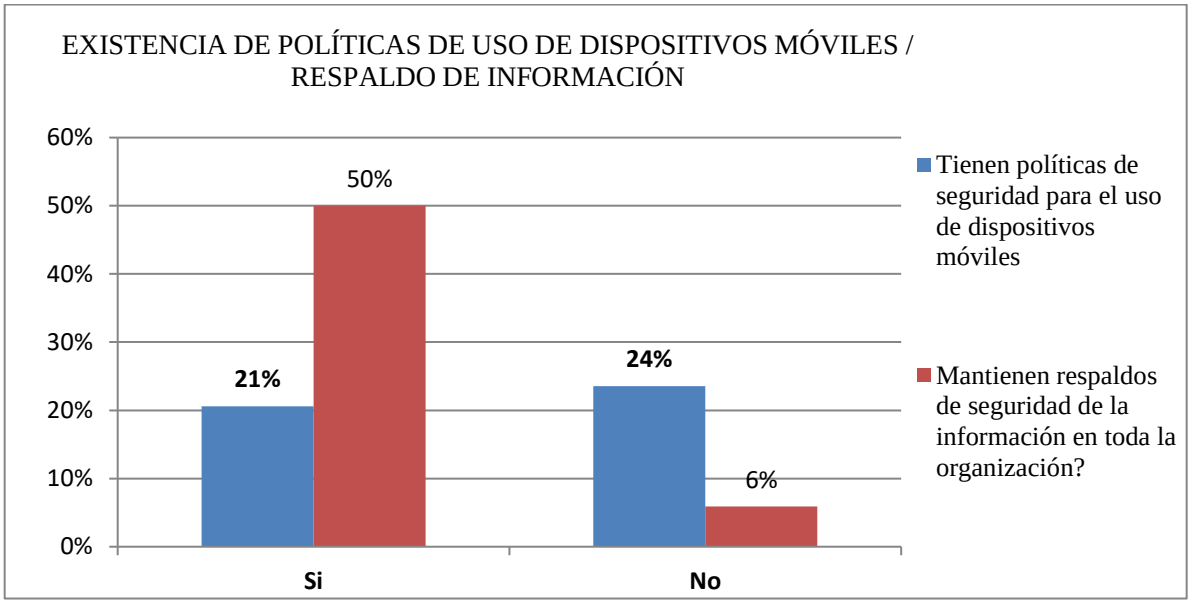
Cruce 2

Tabla 2 - Políticas de dispositivos móviles y respaldos

		Mantienen respaldos de seguridad de la información en toda la organización		TOTAL
		Si	No	
Tienen políticas de seguridad para el uso de dispositivos móviles	Si	50%	6%	56%
	No	21%	24%	44%
TOTAL				100%

Grafico del cruce

Ilustración 5 - Políticas de dispositivos móviles y respaldo



Análisis**,** Del total de auditores encuestados un 56% han encontrado la existencia de políticas de seguridad para el uso de dispositivos móviles en conexiones de acceso remoto en las ONG; de ellos un 50% mantienen respaldos de seguridad de la información, mientras que un 6% no cuenta con respaldo, aunque si tengan políticas de seguridad. Dentro del 44% complementario, que no han encontrado la existencia de políticas de seguridad para el uso de dispositivos móviles en conexiones de acceso remoto en las ONG, el 21% si mantienen respaldos de seguridad mientras que el 24% no mantienen este respaldo.

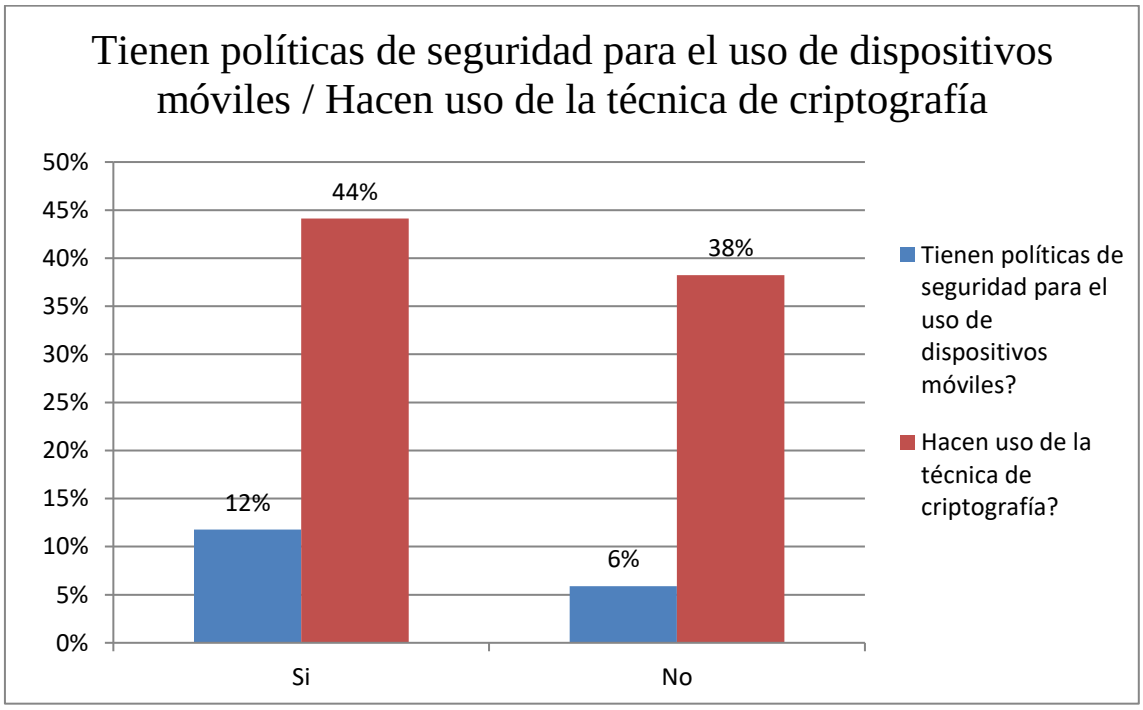
Cruce 3

Tabla 3- Uso de dispositivos móviles y Criptografía

		Hacen uso de la técnica de criptografía		TOTAL
		Si	No	
Tienen políticas de seguridad para el uso de dispositivos móviles	Si	12%	44%	56%
	No	6%	38%	44%
TOTAL				100%

Gráfico del cruce

Ilustración 6- Uso de dispositivos móviles y criptografía



Análisis, del total de auditores encuestados un 56% han encontrado la existencia de políticas de seguridad para el uso de dispositivos móviles en conexiones de acceso remoto en las ONG; de ellos un 12% hacen uso de la técnica de criptografía para la protección de los datos que transfieren, mientras que un 44% no la aplican; mientras que del 44% de los que no tienen políticas de seguridad, un 6% hacen uso de la técnica criptográfica mientras que un 38% no la utilizan.

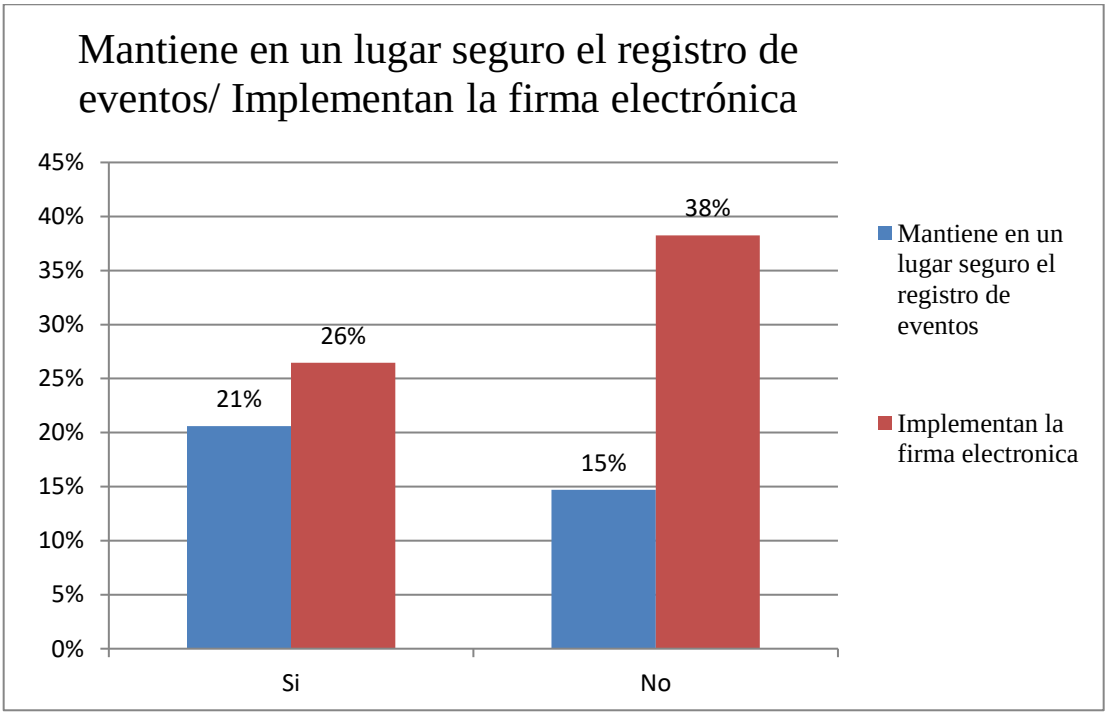
Cruce 4

Tabla 4- Registro de eventos y uso de firma electrónica

		Implementan la firma electrónica		TOTAL
		Si	No	
Mantiene en un lugar seguro el registro de eventos	Si	21%	26%	47%
	No	15%	38%	53%
TOTAL				100%

Grafico del cruce

Ilustración 7- Registro de eventos y uso de firma electrónica



Análisis, Del total de auditores encuestados un 47% han encontrado que en las ONG´s mantienen en un lugar seguro el registro de eventos de los usuarios y de ellos un 21% implementan la firma electrónica en la transferencia de información mientras que un 26% no lo hacen; un 53% no mantienen en un lugar seguro el registro de eventos de los usuarios y de ellos un 15% implementan la firma electrónica mientras que un 38% no lo hacen.

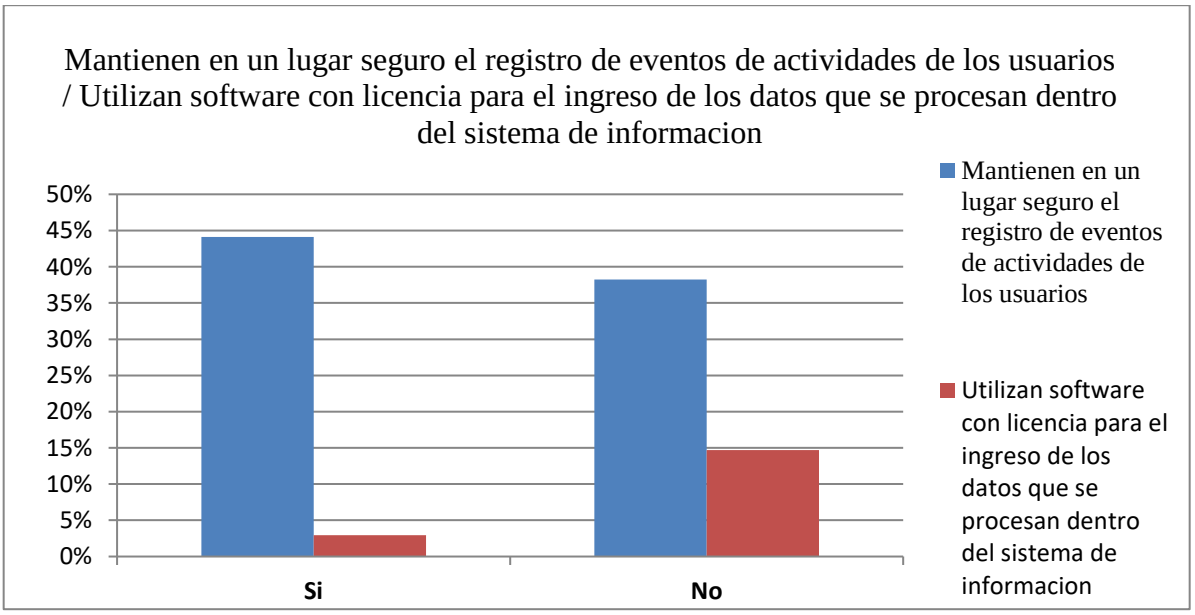
Cruce 5

Tabla 5- Uso de software legal y registro de eventos

		Utilizan software con licencia para el ingreso de los datos que se procesan dentro del sistema de información		TOTAL
		Si	No	
Mantienen en un lugar seguro el registro de eventos de actividades de los usuarios	Si	44%	3%	47%
	No	38%	15%	53%
TOTAL				100%

Gráfico del cruce

Ilustración 8 - Uso de software y registro de eventos



Análisis**,** del total de auditores encuestados en un 47% se han encontrado que en las ONG´s mantienen un registro de eventos de los usuarios y de ellos un 44% utilizan software con licencia de ingreso de datos y un 3% no lo hacen; del 53% de los que no mantienen registro de evento de los usuarios, un 38% si utilizan software con licencia mientras que un 15% no hacen uso de software con licencia.

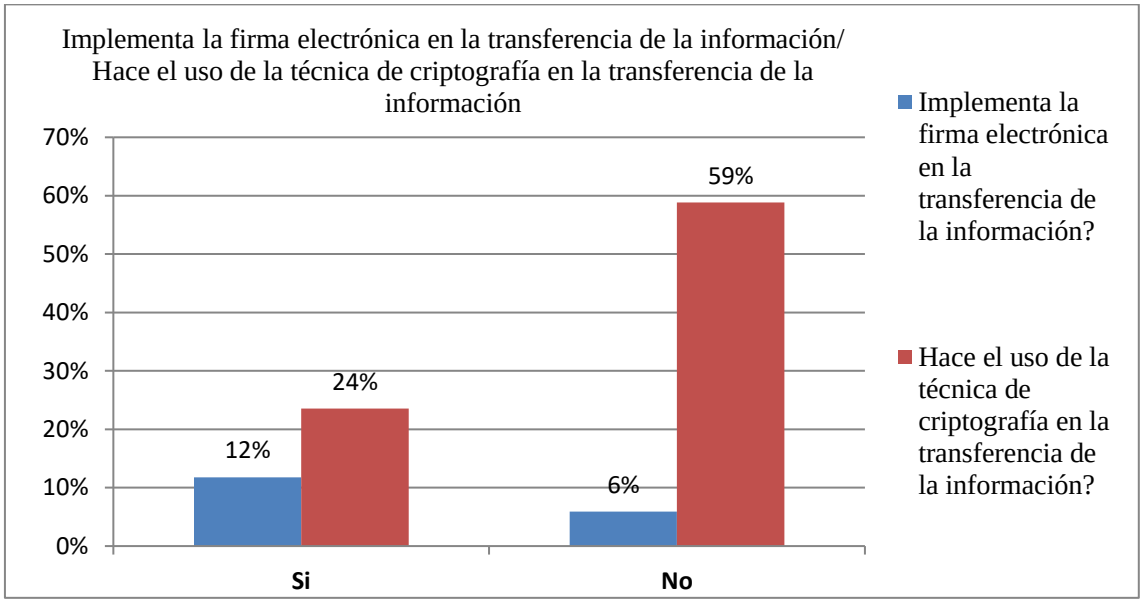
Cruce 6

Tabla 6 - Firma electrónica y Criptografía

		¿Hace el uso de la técnica de criptografía en la transferencia de la información?		TOTAL
		Si	No	
¿Implementa la firma electrónica en la transferencia de la información?	Si	12%	24%	35%
	No	6%	59%	65%
TOTAL				100%

Gráfico del cruce

Ilustración 9- Firma electrónica y Criptografía



Análisis, del total de auditores encuestados en un 35% han encontrado que en las ONG´s implementan la firma electrónica, de ellos un 12% hacen uso de la técnica de criptografía y un 24% no hacen uso de ella; mientras que del 65% que no implementan la firma electrónica, un 6% si hacen uso de la criptografía y un 59% no hacen uso de ella.

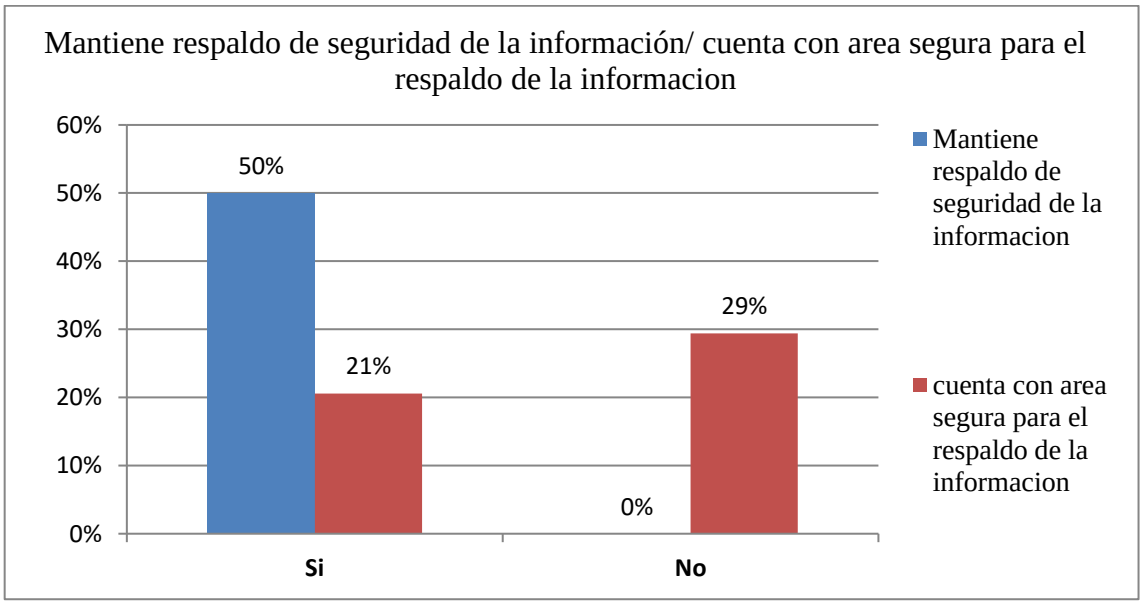
Cruce 7

Tabla 7 - Respaldo de seguridad y existencia de área segura

		Cuenta con área segura para el respaldo de la información		TOTAL
		Si	No	
Mantiene respaldo de seguridad de la información	Si	50%	21%	71%
	No	0%	29%	29%
TOTAL				100%

Gráfico del cruce

Ilustración 10 - Respaldo de seguridad y existencia de área segura



Análisis, del total de auditores encuestados un 71% han encontrado que en las ONG´s mantienen respaldo de seguridad de la información y dentro de ellos un 50% cuenta con área segura para su resguardo mientras que un 21% no cuenta con área segura; en el 29% de los casos no mantienen respaldo de seguridad y de ellos un 29% tampoco cuenta con área segura para el resguardo de respaldos.

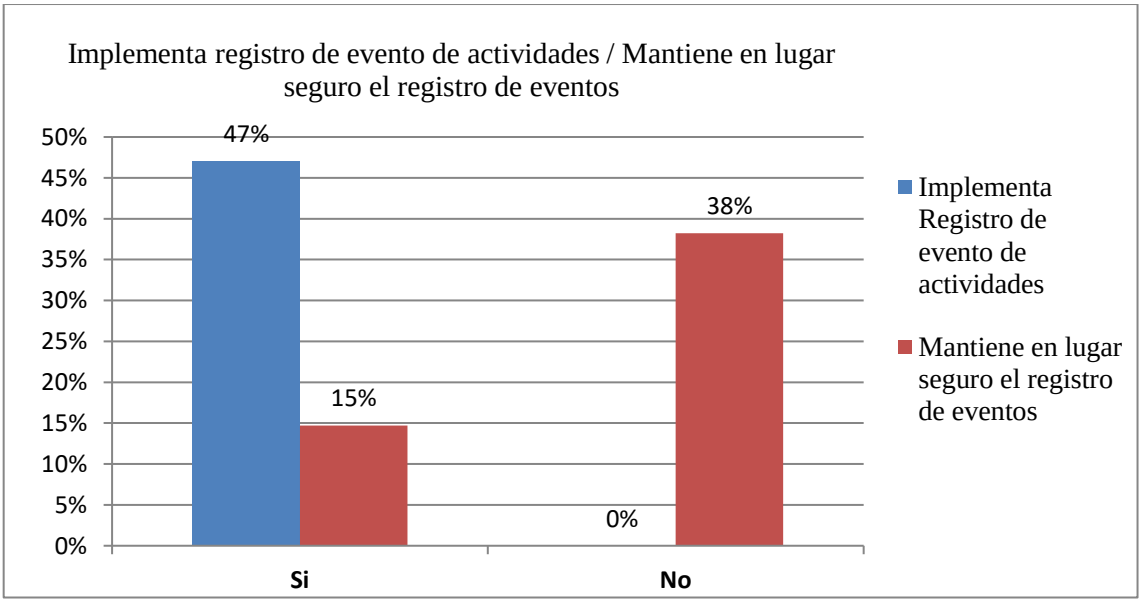
Cruce 8

Tabla 8 - Registro de actividades y registro de eventos

		Mantiene en lugar seguro el registro de eventos		TOTAL
		Si	No	
Implementa registro de evento de actividades	Si	47%	15%	62%
	No	0%	38%	38%
TOTAL				100%

Gráfico del cruce

Ilustración 11- Registro de actividades y registro de eventos



Análisis, del total de auditores encuestados un 62% implementa el registro de evento de actividades y de ellos un 47% mantienen en un lugar seguro ese registro de eventos mientras que un 15% no lo hacen; un 38% no implementa el registro de evento de los usuarios ni tiene lugar seguro para los registros.

3.6.2. DIAGNÓSTICO

De los resultados que se obtuvieron de los encuestados se tomaron los puntos de mayor prioridad que ayudado a cumplir el objetivo planteado para la investigación, esto con el fin de crear una herramienta que facilite a los auditores a realizar una auditoría de sistemas basado en NTS ISO/IEC 27002:2013 Tecnología de la información. Código de prácticas para la gestión de la seguridad de la información.

La técnica de la firma electrónica es implementada en un 35% de las ONG´s mientras que la criptografía en usada en un 17% de ellas, lo que nos deja como resultado que un 65% no usan la firma electrónica y un 82% no hacen uso de la criptografía siendo una medida que debe mejorarse ya que estas prácticas de protección y de legalización de información son necesarias para que Las organizaciones tengan más fortalecido el aspecto de la protección y que cualquier documento que transfieran no puede ser visto por cualquier tercero no autorizado.

- Revisión de los niveles de ingreso a los diferentes programas que utilizan:

Un 47% de las ONG´s mantienen en un lugar seguro el registro de eventos de los usuarios lo que es importante ya que la actividad de procesamiento de la computadora puede registrarse para analizar las funciones del sistema, de ellas un 21% implementan la firma electrónica en la transferencia de información mientras que un 26% no lo hacen; un 53% no mantienen en un lugar seguro el registro de eventos de los usuarios y de ellos un 15% implementan la firma electrónica mientras que un 38% no lo hacen.

En un 88% de las ONG´s se debe poseer autorización previa para el ingreso de datos al sistema de información lo que es importante dado que el permiso de acceso al sistema es vital para hacer algo con un recurso computarizado o informático, en general es decir que es un privilegio técnico por ejemplo la capacidad de leer, crear, modificar o eliminar un archivo o dato. Un 12% no mantiene establecido el control sobre poseer autorización previa para el ingreso de datos al sistema de información lo que no se recomienda ya que podrían ingresar información que no ha sido verificada ni aprobada y podría dañar el resto de datos que previamente han sido almacenados, sin embargo si en la ONG se lleva a cabo la práctica de mantener respaldos de la información procesada entonces no afectaría que un dato no autorizado se ingresara pues bastaría con reemplazar en el sistema la información con el back-up.

Haciendo referencia a los respaldos de información se puede apreciar que un 71% de las ONG´s tiene como práctica llevar respaldos del sistema informático.

- Procedimientos de ingreso a las instalaciones:

Para el ingreso a las instalaciones los auditores han encontrado que en las ONG´s un 76% utiliza personal de seguridad, mientras que un 67% utiliza video vigilancia, un 29% hace uso de tarjetas de acceso y solamente un 11% implementa como medida de seguridad el uso de la huella dactilar.

Es necesario saber que la combinación de varias de las anteriores medidas de seguridad de ingreso a las instalaciones, harán más fuerte la protección de información dentro de la organización, sin embargo en muchos casos se elige una técnica sobre la otra, pero todas tienen ventajas y desventajas sobre otras, por ejemplo: el uso de la video

vigilancia tiene la ventaja que no es necesaria la presencia física de una persona, la desventaja es que sin energía eléctrica no ejecuta su función total, el uso de la huella dactilar tiene la desventaja que al tener un accidente externo (a nivel de palma de la mano), eso afecta su efectividad al momento de tratar de reconocer el patrón de la huella, muchos prefieren un solo control pero la combinación de varios es la mejor decisión si en seguridad de información y datos se trata.

- La existencia de usuarios en estructura de escala según nivel de confianza y responsabilidad:

Cuando un empleado es retirado de la organización en una 79% de los casos consideran retirarles las llaves y tarjetas de identificación, un 70% manifiestan que deben denegar acceso a documentación mientras que un 53% considera que también debe quitárseles el equipo asignado para el desarrollo de su trabajo, es necesario saber que los niveles de estructura de personal es importante tenerlo bien establecido pues de esa manera cada uno en su puesto de trabajo sabe cuáles son sus responsabilidades, conoce quién es su jefe inmediato y sabe ante quien debe rendir cuentas, así mismo conoce las personas que debe guiar para la consecución de cualquier meta que persigan como institución.

La seguridad de la información dentro de una organización es muy importante y cada individuo juega un papel necesario para que este evento se mantenga, para ello se establece en todo lugar de trabajo un organigrama el cual muestra donde está ubicado cada quien.

En concordancia de retirarles una serie de credenciales, llaves o documentos a los ex empleados, también debe implementarse el registro de eventos y resguardarlo en un lugar seguro debido que posteriormente puede necesitarse consultar esa base datos, ya que en

algunas investigaciones se hace necesario conocer que actividades se hicieron de parte de cada trabajador, en qué lugar y hora, así como otros datos más específicos como la dirección física de IP donde fue ejecutada cierta actividad, los resultados obtenidos en la muestra de auditores encuestados muestran que en un 62% de las ONG´s implementa el registro de evento de actividades y de ellos un 47% mantienen en un lugar seguro ese registro de eventos mientras que un 15% no lo hacen; un 38% no implementa el registro de evento de los usuarios ni tiene lugar seguro para los registros, es preocupante saber que casi un 40% de las ONG´s no llevan el registro de eventos y tampoco tienen respaldo seguro.

- Autenticidad del software utilizado en la manipulación de la información

Es útil contar con software legalizado para el uso dentro de una organización debido a la seguridad que representa para el resguardo de información, sin embargo del 82% de las ONG´s en las cuales se hace uso de software legal, solamente un 47% mantiene un registro de eventos de los usuarios y de lo que hacen dentro del sistema, es necesario implementar este control más a detalle por cuestiones de seguridad de la información ya que la combinación de ambos controles es mejor, pues si los programas usados son legales y además el registro de actividades que realizan los usuarios se llevan a cabo, entonces la seguridad de la información se vuelve más fortalecida.

Del 17% de los usuarios que en la ONG´s no tienen software legalizado, solamente un 3% no llevan a cabo el registro de usuarios lo que no es recomendable pero que tampoco es de gran magnitud su daño ante la información pues la mayor proporción de ONG´s llevan registro de usuarios y utilizan software legalizado pues solamente un 15% no hacen uso de software con licencia y tampoco llevan a cabo registro de eventos.

4. CAPÍTULO IV. PROPUESTA DE SOLUCIÓN

MANUAL DE PROCEDIMIENTOS DE AUDITORÍA DE SISTEMAS BASADO EN LA NORMA NTS ISO/IEC 27002:2013, ORIENTADO A ORGANIZACIONES NO GUBERNAMENTALES QUE EJECUTAN PROYECTOS DE EDUCACIÓN.

4.1.Planteamiento del caso

A continuación, en este capítulo se presenta una propuesta de lo que debe contener un manual de procedimientos para la ejecución de una auditoría de sistemas en organizaciones no gubernamentales, basado en la NTS ISO/IEC 27002:2013* Tecnología de la información. Código de prácticas para la gestión de la seguridad de la información.

La seguridad de la información, es fundamental en el ámbito laboral en las Organizaciones no Gubernamentales, las cuales se ven en la necesidad de proteger la información, ante ello los gerentes deben revisar periódicamente el cumplimiento apropiado de las políticas de seguridad, las normas y otros requerimientos de seguridad en cuanto a los procedimientos y procesamiento de la información dentro de su área de responsabilidad. (ISO 27002, 2013)

Los auditores de sistemas se ven en la obligación de prestar un servicio para poder identificar debilidades en las organizaciones e informar a las autoridades correspondientes, por lo tanto, existe la necesidad de diseñar un manual de procedimientos adecuados para la evaluación de las áreas importantes dentro de estas entidades para la seguridad de la información a lo cual se toma como marco de referencia la NTS ISO/IEC 27002:2013 Tecnología de la información. Código de prácticas para la gestión de la seguridad de la información.

Para la realización de los programas que incluirá el manual de procedimientos desarrollar para la buena evaluación de la seguridad de la información en las organizaciones no gubernamentales, de lo cual se lleva a cabo un estudio de cambio para saber de primera mano de los auditores de sistemas cuales son las buenas practicas que ellos implementan y las áreas a evaluar dentro de una entidad como esta.

4.2.Estructura del plan de solución

El manual de procedimientos a implementar surge a partir de la necesidad de aportar una herramienta que constituya una fuente de información para los auditores de sistemas, el cual permita a estos detectar y ayudar a las Organizaciones no Gubernamentales a prevenir actividades sospechosas a las cuales pueden estar expuestas.

Para la implementación de dicha herramienta fue necesaria una investigación de campo, por medio de un instrumento para recolectar la información suficiente para detectar las deficiencias en una auditoría de sistemas.

Auditoria de sistemas

Alcance	Cobertura
Componentes	Elementos

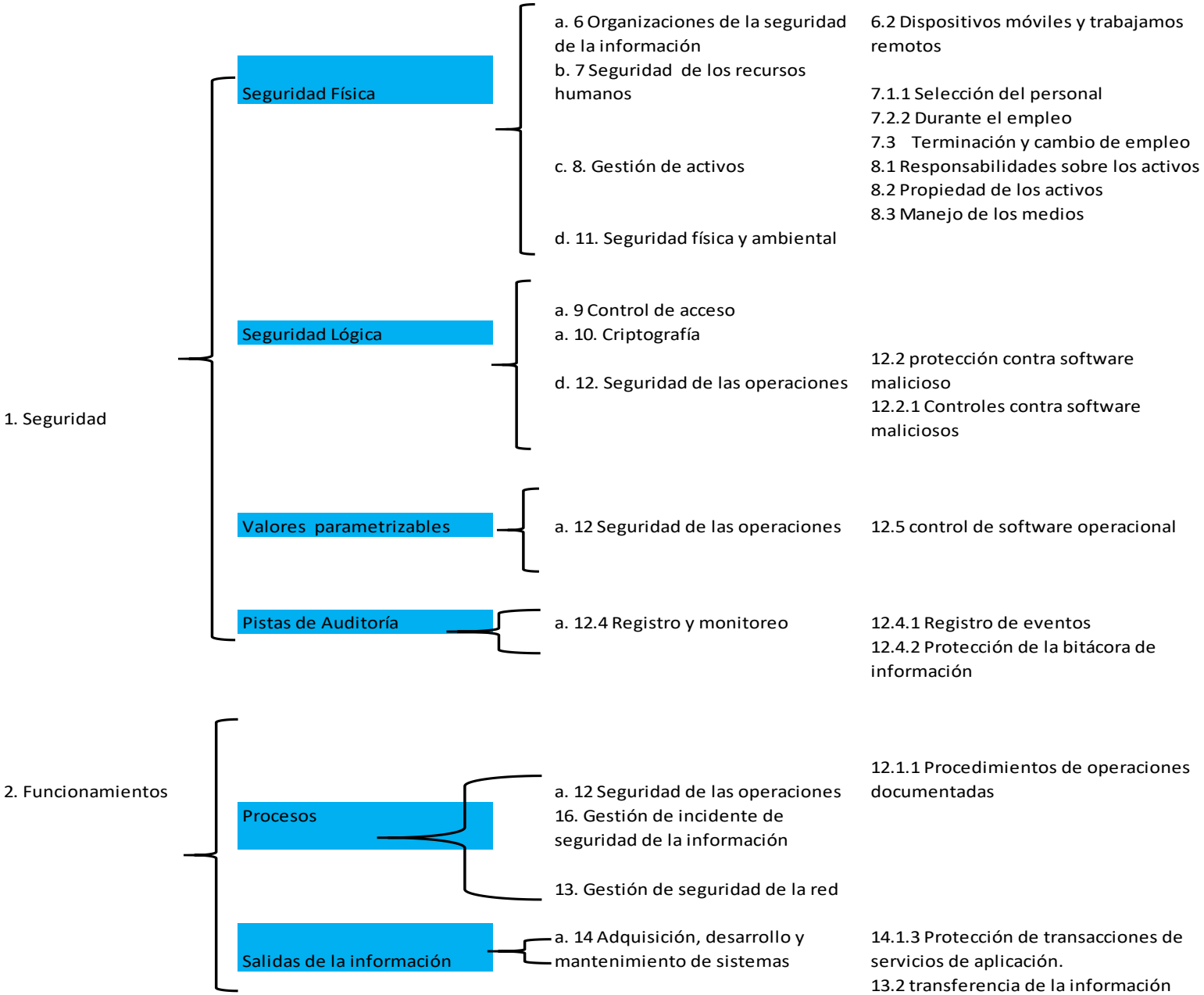


Ilustración 12 Estructura del plan de solución

4.3.Beneficios y limitantes

La implementación de un manual de procedimiento para la auditoría de sistemas dedicado a las entidades no gubernamentales que ejecutan proyectos de educación será una herramienta útil para que los auditores que realizan este tipo de auditorías puedan identificar áreas vulnerables en seguridad de la información.

En este sentido se mencionan a continuación los beneficios y las limitantes que este manual ofrece:

Beneficios a los auditores

- Implementación de buenas prácticas por los auditores.
- Facilidad de operar la auditoría en este tipo de organizaciones.
- Utilización de nuevos procedimientos basados en NTS ISO/IEC 27002:2013
- Ejecución de nuevos programas.

Beneficios a las ONG´s

- Identificación de posibles áreas donde la información sea vulnerable.
- Identificación de registro de eventos.
- Conocimiento y monitoreo a los empleados contratados.
- Monitoreo de los resguardos de información ejecutada por la organización.
- Se observa con mayor precisión las fuentes, ubicación y concentración de actividades ilícitas.

Limitantes

- Aplicación incorrecta del manual procedimientos
- Los auditores no cuenten con un conocimiento previo del contenido de la NTS ISO/IEC 27002:2013*

4.4. Desarrollo de caso práctico

Requisitos de seguridad de la información

De cierta medida es esencial que las organizaciones identifiquen sus requisitos de seguridad. Existen tres fuentes importantes de requisitos de seguridad.

1- La evaluación de los riesgos para la organización, considerando la estrategia y objetivos de negocios de la organización. A través de una evaluación de riesgos, donde se identifiquen las principales amenazas a los activos, la vulnerabilidad y probabilidad de ocurrencia donde se evaluada, asimismo el impacto potencial se estimado.
2- Los requisitos legales, los acordados en los estatutos, los reglamentarios y contractuales que una organización tiene que satisfacer, así como su entorno cultural.
3- El conjunto de principios, objetivos y requisitos de negocio para el manejo, procesamiento, almacenamiento, comunicación y el archivado de información, que una organización ha desarrollado para apoyar sus operaciones.

Estos requisitos importantes para las ONG´s, es también la primera evaluación que hace el profesional en auditoría de sistemas en el conocimiento del cliente.

El auditor de sistemas puede implementar la evaluación de controles que muestren que la organización ejecuta inspecciones balanceadas en contra de probables daños del negocio resultante de los incidentes de seguridad en la ausencia de esos controles.

Los resultados de una auditoría de sistemas enfocada a identificar y resolver en cierta manera la vulnerabilidad en seguridad a la información, ayuda a guiar y determinar las acciones administrativas y prioridades apropiadas para la gestión de riesgos de seguridad de la información y para la implementación de los controles seleccionados para protegerse contra los riegos.

La NTS ISO/IEC 27002:2013 proporciona una orientación para la gestión de riesgos se seguridad de la información, incluido el asesoramiento sobre evaluación, tratamiento, aceptación, comunicación, monitoreo y revisión del riesgo.

SECCIÓN 1: INTRODUCCIÓN Y ALCANCE DEL MANUAL

Introducción

'La seguridad de la información es la preservación de la confidencialidad, integridad y disponibilidad de la información; en adición, otras propiedades, como la autenticidad, responsabilidad, no-repudiación y fiabilidad pueden estar involucradas'. Aunque se puede generar la tendencia que los controles asociados a la seguridad de la información solo están orientados a sistemas de "informática', es importante aclarar que se consideran todos los aspectos relacionados con la información, los medios y los sistemas que la manejan y la soportan.

Los sistemas de información y las redes de las Organizaciones están frente a amenazas de un gran número de fuentes, incluyendo fraudes por computadora, espionaje, sabotaje, vandalismo, incendios o inundaciones. Asimismo, causas de daño como códigos maliciosos, 'hacking", ataques de denegación de servicios se hacen ahora más frecuentes y sofisticadas.

La seguridad de la información no debe limitarse únicamente a los medios tecnológicos, adicionalmente requiere seguridad en los recursos humanos, seguridad física, seguridad en la gestión de los activos, cumplimiento de la ley y gestionar la continuidad del negocio mediante una gestión apropiada soportada por la política y procedimientos respectivos. Identificar los controles que deben estar implementados requiere una cuidadosa planificación y detalle. La gestión de la seguridad de la información requiere el compromiso y la participación de las máximas autoridades, empleados de la Institución, proveedores, terceras partes, contribuyentes y otros.

4.2. Objetivos del manual

1.2.1 Disponer de una herramienta que facilite la práctica de auditoría de sistemas en las Organizaciones no Gubernamentales que ejecutan proyectos de educación.

1.2.2 Unificar criterios en la aplicación de procedimientos basados en la NTS ISO/IEC 27002:2013.

1.2.3 Contribuir al cumplimiento de las normas y legislación en materia de seguridad de la información.

4.3. Normativa técnica

El presente manual se emite de conformidad a lo establecido en:

1.3.1 La NTS ISO/IEC 27002:2013 Tecnología de la información, código de prácticas para la gestión de la seguridad de la información, regulado por el Organismo Salvadoreño de Normalización responsable de elaborar, actualizar, adoptar y divulgar normas técnicas, de acuerdo a la ley del sistema salvadoreño para la calidad, la cual fue publicada en el diario oficial Nº 158 del 26 agosto de 2011.

4.4.1. Dominios del manual de procedimientos de auditoría

La implementación de un manual de procedimientos de auditoría de sistemas basado en NTS ISO/IEC 27002:2013 orientado a organizaciones no gubernamentales que ejecutan proyectos de educación, con el propósito de poder identificar la vulnerabilidad de la información resguardada, a través del desarrollo de procedimientos de controles que cubren los 2 componentes de auditoría de sistemas segregados en 6 elementos como se especifica en la figura Nº 1

SECCIÓN 2. REFERENCIAS

- NTS ISO/IEC 27002:2013* Tecnología de la información. Código de prácticas para la gestión de la seguridad de la información.
- NTS ISO/IEC 27001:2007 Tecnología de la información - técnicas de seguridad – Sistema de Gestión de la Seguridad de la Información – Requerimientos.
- COBIT5 para seguridad de la información.
- Manual de preparación al examen CISA 2014.

SECCIÓN 3: TÉRMINOS Y DEFINICIONES

Esta sección comprende una serie de conceptos utilizados en el presente manual y en la NTS ISO/IEC 27002:2013 Tecnología de la información. Código de prácticas para la gestión de la de la seguridad de la información. Términos y definiciones.

Activo: Recurso del sistema de información o relacionado con éste, necesario para que la Institución funcione correctamente y alcance los objetivos propuestos por su Dirección; en general algo que tiene valor para la organización.

Amenaza: Una causa potencial de un Incidente no deseado, el cual puede producir un daño a un sistema o a la Organización.

Análisis de Riesgos: Uso sistemático de la información para identificar y estimar las fuentes de riesgo.

Confidencialidad: Propiedad de la información de no estar disponible o no ser revelada a individuos no autorizados, entidades o procesos.

Control: Medio para gestionar et riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras organizacionales, las cuales pueden ser de naturaleza administrativas, técnicas, de gestión, o legal. El control también usado como un sinónimo de salvaguarda o contramedida.

Criptografía: La criptografía (del griego kryptos, ocultar, y grafos, escribir, literalmente 'escritura oculta') es el arte o ciencia de cifrar y descifrar información utilizando técnicas matemáticas que hagan posible el intercambio de mensajes de manera que sólo puedan ser leídos por tas personas a quienes van dirigidos.

Gestión de riesgos: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. La gestión de riesgos típicamente incluye la evaluación de riesgos, tratamiento de riesgos, la aceptación de riesgos y la comunicación de riesgos.

Incidente de Seguridad: Uno o una serie de eventos de seguridad de la información no deseada o inesperada que poseen una probabilidad significativa de comprometer las operaciones del negocio amenazando la seguridad de la información.

Integridad: Propiedad de salvaguardarla precisión y lo completo de los activos.

ISO/IEC: Organización Mundial de Estandarización (del griego isas que significa "igual') y la comisión Internacional Electrotécnica (por sus siglas en inglés lntemational Electrotechnical comisión); la cuales una organización que representa una red de institutos de estándares en 156 países. Las siglas preceden a los estándares emitidos por esta organización, ejemplo ISO/IEC 9000; estos estándares se consideran de aplicación internacional.

Norma: Es una especificación técnica u otro documento a disposición del público elaborado con la colaboración y el consenso o aprobación general de todas las partes interesadas, basada en resultados consolidados de la ciencia tecnología y experiencia dirigida a promover beneficios óptimos para la comunidad y aprobada por un organismo reconocido a nivel nacional, regional o internacional.

Política: Orientaciones o directrices que rigen la actuación de una persona o entidad en un asunto o campo determinado.

Registro(s): Documento(s) que presenta(n) resultado(s) obtenido(s) o proporciona(n) evidencia de actividades desempeñadas.

Riesgo: Combinación de la probabilidad de un evento y sus consecuencias.

Unidad de Informática: se refiere a la(s) unidad(es) organizativa(s) que prestan los servicios de tecnologías de la información y comunicaciones para las Direcciones o Dependencias del Ministerio de Hacienda.

Vulnerabilidad: Debilidad de un activo o grupos de activos que mede ser explotada por una amenaza.

SECCIÓN 4. COMPROMISO Y RESPONSABILIDADES DE LA ORGANIZACIÓN

4.5.1 Compromiso de la organización

4.1.1.1 Titulares

Los Titulares adquieren el compromiso de desarrollar, implantar, mantener y mejorar continuamente el Manual de Procedimientos de auditoría a través de establecer y aprobar:

a) La Política de Seguridad dela información
b) Los objetivos del Manual
c) Los roles y responsabilidades para la seguridad de la información
d) Los recursos para el funcionamiento del Manual
e) Los proyectos relacionados a la seguridad de la información

4.4.1. Responsabilidades de la organización

4.1.2.1 Directores, Presidente y Jefes de las Unidades Asesoras al Despacho

Responsables de implantar y operar el SGSI, a través de:

a) Cumplir y hacer cumplir lo establecido en los documentos del SGSI.
b) Incorporar y dar seguimiento a las actividades de seguridad en los planes de trabajo.
c) Efectuar periódicamente el análisis de riesgo de la información.
d) Gestionar los recursos para el tratamiento y aceptación de los riesgos de la información.
e) Aprobar la documentación relacionada con la operación del SGSI en su área.
f) Colaborar en la realización de las auditorías al SGSI.
g) Cumplir los requisitos, ejecutar las mejoras y acciones correctivas señaladas en las auditorías.
h) sugerir cambios en los lineamientos de seguridad según los riesgos detectados.
i) Velar porque existan mecanismos que permitan la continuidad del negocio de los procesos críticos de su Dirección o Dependencia.

4.1.1.2 Propietario de la información

El propietario de la información es el Titular o la(s) persona(s) designada(s), y es en última instancia el responsable de la protección y uso de la información. El propietario de la información tiene la responsabilidad de salvaguardar de forma razonable la confidencialidad, integridad y disponibilidad de la misma, así como asumir la responsabilidad por cualquier acto de negligencia que resulte en la corrupción, destrucción o divulgación de los datos. El propietario decide sobre la clasificación de la información de la cual él es responsable, así como también de actualizar dicha clasificación si el negocio lo considera necesario. Es responsable de asegurar de que estén instalados los controles de seguridad necesarios, que se utilicen los derechos de acceso o puede delegar esta función.

4.1.1.3 Custodio de la Información

El custodio de la información (custodio de los datos en medios físicos y magnéticos) es responsable del almacenamiento y aseguramiento de la información, que le ha sido confiada por el propietario. Cuando se trate de datos en medios magnéticos; este rol es usualmente llevado por la unidad de informática y sus tareas incluyen la realización del respaldo de los datos, la validación periódica de su integridad, restauración, mantener los registros de ésta actividad y de cumplir los requerimientos especificados en la política de seguridad de la Institución, estándares y guías referentes a la seguridad de la información y a la protección de los datos.

4.1.1.4 Dueño de Procesos

Son los jefes de las unidades organizativas que tienen la responsabilidad de la coordinación y administración del flujo de trabajo y las actividades en cada etapa de un proceso. Los dueños de proceso deben asegurarse que los procesos bajo su responsabilidad, incluyan las medidas de seguridad adecuada y consistente con la política de seguridad de la información institucional.

4.1.1.5 Personal de Operaciones

Son responsables de implementar los lineamientos, controles, guías y procedimientos de seguridad de la información autorizados por la organización, en la infraestructura de servidores, clientes y redes de datos, resolver incidentes, aplicar los parches y dar tratamiento a las vulnerabilidades del software. Ante un incidente de ataques a la infraestructura de sistemas y redes, realizan las acciones necesarias para detenerlos y resolverlos utilizando las herramientas y procedimientos adecuados. Son responsables de las actividades de monitoreo de la infraestructura.

4.1.1.6 Usuario

Es cualquier individuo que rutinariamente utiliza los datos para realizar tareas relacionadas al trabajo. Sus accesos deben ser autorizados por los propietarios de la información o quienes éstos hayan delegado, además estos accesos, pueden ser restringidos y monitoreados. El usuario debe de tener los niveles de acceso necesarios para realizar sus funciones y es el responsable de seguir los procedimientos operativos de seguridad para asegurar a los demás la confidencialidad, integridad y disponibilidad de los datos. También son responsables de las aplicaciones de usuario final en donde ellos controlen totalmente la seguridad (por ejemplo, hojas de cálculo, procesadores de palabras, otros).

SECCIÓN 5: LINEAMIENTOS

Esta sección presenta los lineamientos derivados de los controles de la Norma NTS ISO/IEC 27002:2013* Tecnología de la información. Código de prácticas para la gestión de la seguridad de la información, los cuales han sido seleccionados como resultado de la investigación de campo efectuada a los auditores de sistemas enfocado a las ONG`s. dicha investigación proporciona los insumos para la elaboración del manual de procedimientos de auditoría de sistemas.

Es responsabilidad de la gerencia al frente de la ONG`s y empleados, el cumplimiento de estas disposiciones, así como el incluir la seguridad en sus actividades, auxiliándose de los procesos y procedimientos asignados mediante el manual. Asimismo, es recomendable para el auditor el aplicar las disposiciones que establece la NTS ISO/IEC 27002:2013 por el nivel de seguridad de la información.

5.1. Seguridad Física

5.1.1 Dispositivos móviles y trabajo remoto

Objetivo: Asegurar la seguridad del trabajo remoto y el uso de dispositivos móviles.

Control, la adopción de políticas o medidas adecuadas que sirvan de soporte para la seguridad de la información ayudaran a disminuir los riesgos introducidos por el uso de dispositivos móviles.

Los dispositivos móviles pueden incluir:

- Teléfonos móviles con funciones completas con la funcionalidad de computadora personal, o "teléfonos inteligentes"
- Laptops y netbooks
- Tabletas
- Asistentes digitales personales (PDA)
- Dispositivos portátiles de bus serial universal (USB) para almacenamiento (como "unidades de almacenamiento portátiles" y dispositivos MP3) y para conectividad (como Wi-Fi, Bluetooth y tarjetas de módem HSDPA/UMTS/EDGEJGPRS)
- Cámaras digitales
- Dispositivos de identificación de frecuencias de radio (RFID) y RFID móviles (M-RFID) para almacenamiento de datos, identificación y gestión de activos
- Dispositivos infrarrojos (lrDA) como impresoras y tarjetas inteligentes

Acceso remoto usando dispositivos móviles

Muchos de los dispositivos móviles más populares se basan en plataformas relativamente incipientes, centradas en el usuario, que no brindan los controles de gestión subyacentes a los que las organizaciones de TI empresariales están acostumbradas. Dado que cada vez más empleados usan su teléfono inteligente o tableta personal para trabajar, el departamento de TI tiene cada vez menos control sobre quién o qué está accediendo a su red. Estos dispositivos a menudo tienen acceso a la web, lo que puede permitir que el usuario acceda de forma remota a datos como, por ejemplo, sistemas de correo electrónico corporativos. Es necesario proteger estos dispositivos con la seguridad adecuada y apropiada, incluso control de acceso y encriptación de datos, antes de permitir su uso.

Ejemplo de controles

- Borrado y bloqueo remoto
- Rastreo por geolocalización
- Autenticación, autorización y responsabilidad en la red
- Respaldo remoto seguro
- Política de uso aceptable

5.1.2 Trabajo remoto

Control, una política y medidas de soporte de seguridad deben ser implementadas para proteger la información accedida, procesada o almacenada en sitios de trabajo remoto.

5.1.3. Seguridad de Acceso Remoto

Los usuarios de acceso remoto pueden conectarse a las redes de la organización con el mismo nivel de funcionalidad que existe dentro de su oficina. En este procedimiento, el diseño de acceso remoto utiliza los mismos estándares y protocolos de red que se aplican a los sistemas a los que se est. TCP/IP)- y sistemas con arquitectura de red de sistemas (SNA).

Una guía de implementación para las organizaciones que permiten las actividades de trabajo remoto debe emitir una política que definan las condiciones y restricciones para el uso del trabajo, cuando se considere aplicable. En este caso se puede concluir lo siguiente:

- La seguridad física existente en el sitio de trabajo remoto.
- El entorno físico de trabajo remoto propuesto.
- Los requisitos de seguridad de las comunicaciones, teniendo en cuenta la necesidad de acceso remoto a los sistemas interno de las organizaciones no gubernamentales.
- La provisión de acceso de escritorio virtual que previenen el `procesamiento y almacenamiento de información.
- La amenaza de acceso no autorizado a información o recursos por parte de otras personas.
- El uso de las redes domésticas y los requerimientos o restricciones a la configuración de la tecnología.
- Las políticas y procesamiento para prevenir las disputas relativas a los derechos de propiedad.
- El acceso a los equipos de propiedad privada.

- Acuerdos tomados por dichas organizaciones de licenciamiento de software tales que permiten a las organizaciones conceder lineamientos para software cliente en estaciones de trabajo.
- protección de software malicioso y requerimientos de corta fuegos.
- Etc.

5.1.4. Seguridad de los recursos humanos.

Objetivo: Asegurar que los empleados y contratistas entiendan sus responsabilidades, y sean idóneos para los roles.

Control, los controles de verificación de los antecedentes de todos los candidatos para el empleo deben llevarse a cabo en concordancia con las leyes, regulaciones y normas de ética pertinentes y, deben ser proporcionales al requerimiento del negocio, la clasificación de la información a ser accedida y los riesgos percibidos.

Deberían estar implementadas prácticas adecuadas de seguridad de la información para asegurar que los empleados, contratistas y terceros usuarios entienden sus responsabilidades, y son aptos para los roles para los que son considerados, y para reducir el riesgo de robo, fraude o abuso de las instalaciones, específicamente:

- Se deben considerar las responsabilidades de seguridad antes de la contratación, en las descripciones adecuadas de los puestos

- Todos los candidatos a empleo, los contratistas y terceros de trabajo y en los términos y condiciones de empleo. usuarios deberían ser adecuadamente filtrados, en especial para los puestos de trabajo sensibles.
- Los empleados, contratistas y terceros usuarios de las instalaciones de procesamiento de información deberían firmar un contrato sobre sus roles y responsabilidades de seguridad, incluyendo la necesidad de mantener la confiabilidad. Los roles y las responsabilidades de seguridad, los contratistas y terceros usuarios deberían ser definidos y documentados en conformidad con la política de seguridad de información de la organización.

5.2. Gestión de activos

Objetivo: identificar los activos organizacionales y definir las apropiadas responsabilidades de protección.

Control, información, otros activos asociados con información e instalaciones de procesamiento de la información deben ser identificables y un inventario de estos activos debe ser levantado y mantenido.

Un control efectivo requiere un inventario detallado de los activos de información. Dicha lista es el primer paso para clasificar los activos y determinar el nivel de protección a proveer para cada uno de ellos.

El registro de inventario de cada activo de información debe incluir:

- Identificación específica del activo
- Valor relativo para la organización

- Implicaciones de pérdida y prioridad de recuperación
- Ubicación
- Seguridad/Clasificación de riesgos

Propiedad de los activos

Un proceso para garantizar la asignación oportuna de propiedad de los activos es usualmente implementado. La propiedad se debe asignar cuando se crean los activos o cuando los activos se transfieren a la organización. El propietario de los activos debe ser responsable de la correcta gestión de un activo durante todo el ciclo de vida de un activo.

Obligaciones del propietario de los activos.

a) Asegurar que los activos son inventariados.
b) Asegurar que los activos están debidamente asegurados y protegidos.
c) Definir y revisar periódicamente las restricciones de acceso y las clasificaciones de los activos importantes teniendo en cuenta las políticas de control de acceso aplicables.
d) Garantizar el manejo adecuado cuando el activo se elimina o destruye.

Manejo de medios

Implementar los procedimientos adecuados para la gestión de los medios es importante porque ayuda a mantener el esquema adoptado por la organización, sin embargo, los criterios que se deben tener en consideración para el buen uso o manejo de los medios son los siguientes:

a) Si ya no es necesario, los contenidos de los medios reutilizables deben ser retirados de la organización; estos no deben ser recuperables.
b) Cuando sea necesario y práctico, deberá exigirse una autorización para remover los medios de la organización y un registro de dichos movimientos debe conservarse a fin de mantener una evidencia de auditoría.
c) Todos los medios deben ser almacenados en un ambiente seguro, de acuerdo con las especificaciones de los fabricantes.
d) Si la confidencialidad o integridad de los datos son consideraciones importantes, deben utilizarse técnicas criptográficas para proteger los datos en medios removibles.
e) Múltiples copias de datos importantes deben almacenarse en medios separados para reducir aun el riesgo de daño o pérdida de los datos por incidente.
f) Las unidades de medios removibles deben habilitarse si hay una razón organizacional para hacerlo.

Para la seguridad de los datos en la organización, no debería permitirse el uso de medios extraíbles personales, para ellos es preferible que existan medios extraíbles propiedad de la organización, evitando que exista fuga de información.

5.3. Seguridad física y ambiental

Objetivo: prevenir el acceso físico no autorizado, daño e interferencia a las instalaciones de procesamiento de la información y a la información de la organización.

Lo que se debe hacer es definir parámetros de seguridad para proteger áreas que contienen información ya sea sensitiva o críticas e instalaciones de procesamiento de la información.

Exposiciones y controles ambientales

Problemas y exposiciones ambientales

Las exposiciones ambientales se deben principalmente a acontecimientos que ocurren de manera natural en tiempo imprevisto, ejemplo: tormentas eléctricas, terremotos, erupciones volcánicas, entre otros.

Un área en particular de preocupación son las áreas de energía a las computadoras y al soporte ambiental como por ejemplo las siguientes:

- Falla total (apagón), que puede abarcar desde un edificio y hasta toda un área geográfica, con frecuencia es causada por condiciones climatológicas.
- Voltaje severamente reducido (caída de voltaje), dicha falla pone un esfuerzo al equipo electrónico y puede limitar su vida operativa o incluso causar daño permanente.
- Depresiones, picosy sobre voltajes - Disminuciones (depresiones) o aumentos (picos y sobre voltajes) temporales y rápidos en los niveles de voltaje. Estas anomalías pueden causar la pérdida de datos, corrupción de datos, errores de transmisión de red o, incluso, daño físico a dispositivos de hardware (por ejemplo, discos duros o chips de memoria).
- Interferencia electromagnética (EMI) - Causada por tormentas eléctricas o equipo eléctrico ruidoso (por ejemplo, motores, iluminación fluorescente, transmisores de radio). Esta interferencia puede ocasionar que los sistemas de computadora se cuelguen o caigan, así como también daños similares a los ocasionados por las depresiones, picos y sobre voltajes.

Las interrupciones por períodos breves, como por ejemplo las depresiones, picos y sobre voltajes, que duran desde unas pocas millonésimas hasta unas pocas milésimas de segundo, se pueden prevenir usando protectores de voltaje debidamente colocados.

Las interrupciones de duración intermedia, que duran desde algunos segundos hasta 30 minutos, se pueden controlar por medio de dispositivos de suministro ininterrumpido de energía (UPS).

Finalmente, las interrupciones de larga duración, que duran desde algunas horas hasta varios días, requieren el uso de generadores alternos de energía. Estos generadores pueden ser dispositivos portátiles o parte de la infraestructura del edificio y usan fuentes alternas de energía, como por ejemplo diésel, gasolina o propano.

Otra área de preocupación trata de daño por agua/inundación, incluso con equipos ubicados en los pisos superiores de edificios altos. Este asunto causa preocupación incluso en instalaciones ubicadas en pisos altos, ya que el daño por agua es un riesgo que por lo general ocurre a raíz de tuberías de agua rotas.

Otras preocupaciones fuera de las amenazas naturales son las provocadas por el hombre. Ellas incluyen amenazas/ataques terroristas, vandalismo, choque eléctrico y falla de equipo.

Algunas preguntas que deben ser atendidas por las organizaciones relacionadas con problemas y exposiciones ambientales incluyen lo siguiente:

- ¿Está el suministro de energía al equipo de computadora debidamente controlado para garantizar que permanezca dentro de las especificaciones del fabricante?

- ¿Son los sistemas de control del aire acondicionado, la humedad y la ventilación para el equipo de computadora los adecuados para mantener las temperaturas dentro de las especificaciones de los fabricantes?
- ¿Está el equipo de computadoras protegido de los efectos de la electricidad estática, usando una alfombra antiestática o un aerosol antiestático?
- ¿Se mantiene el equipo de computadora libre de polvo, humo y otras partículas de materia, como por ejemplo comida?

1. Seguridad asociada al recurso humano

1.1.Responsabilidades y perfiles de puestos.

Cada unidad en los perfiles de puestos de los funcionarios y empleados, las responsabilidades y descripciones específicas sobre seguridad de la información.

1.2. revisión de antecedentes y referencias personales.

Las políticas y procesos de contratación de personal contaran con los controles adecuados en cuanto a la verificación de referencia y antecedentes de los empleados potenciales, cuando estos opten en cargos donde se involucran con el manejo de información confidencial o reservada de la institución.

1.3.términos y condiciones de contrataciones.

Los contratos a empleados contratistas y terceros incluirán condiciones que establezcan su responsabilidad y de la institución en materia de seguridad de la información.

1.4. conocimiento sobre la documentación del SGSI.

El ente realizará tareas de concientización, actualización y divulgación que permitan a los empleados conocer sobre la seguridad de la información de la institución; así como para tener el nivel adecuado de entendimiento de la política, manual, procedimientos u otra documentación.

5.3.5 capacitación en seguridad de la información.

Cada ente será responsable de proveer entrenamiento, capacitación y material de apoyo a sus empleados; con el propósito de lograr un efecto multiplicador de lo dispuesto en el lineamiento

5.3.4 para proteger adecuadamente los activos de información, adicionalmente, podrá incluir la divulgación de los registros y documentos el SGSI correspondiente a la unidad.

5.3.7. Devolución de activos,

Es responsable de asegurar que los empleados, contratistas y terceros devuelvan los activos de información asignados, una vez cambie o concluya su relación laboral o contractual.

5.3.8 revocación de derechos de acceso.

Cada ente regulador deberá dar cumplimiento al procedimiento normativo, gestión de acceso, para revocar los derechos de acceso a la información, aplicaciones del negocio, instalaciones de procesamiento y a cualquier otro software o servicio informático; a los funcionario, empleados, contratistas o terceros al terminar su relación laboral o contractual con la institución.

El departamento de formación y desarrollo del talento humano es responsable de mantener actualizados la información de los empleados respecto a actividades de concientización y capacitación en temas de seguridad en que hubiese participado.

5.4.1 seguridad física

Cada ente debe establecer un perímetro de seguridad (puertas de entrada, paredes, etc) para proteger las áreas que contengan información y sus recursos de tratamiento.

5.4.2 control de acceso físico a la información confidencial o reservada.

El acceso a toda oficina, centro de procesamiento de datos y área de trabajo que contenga información confidencial o reservada debe ser físicamente restringido para limitar el acceso a aquellos que necesitan la información, cada ente definirá los procedimientos y controles adecuados que proporcionen el detalle del personal autorizado al ingreso a estas áreas.

5.4.3 protección contra amenazas externas y del ambiente.

Cada ente solicitara ante la unidad correspondiente, la instalación de protecciones físicas contra incendios, inundaciones, explosiones, disturbios civiles y otras formas de desastres naturales o provocados por el hombre, a los sistemas de información y a la ubicación de los principales activos que lo soportan, tomando como base el análisis de riesgo.

5.4.4 trabajos en áreas seguras.

Cada ente establecerá los controles, procedimientos y protecciones físicas adecuadas, cuando empleados o terceros efectúen trabajos en áreas que contengan conformación confidencial o reservada.

5.4.5 ubicación de sistemas de cómputo y equipos de producción.

Los sistemas de cómputo, equipos servidores en producción de los procesos o servicios críticos y equipos centrales de comunicación, serán ubicados físicamente dentro de los centros de

procesamiento de datos de la institución. Se podrán también alojar equipos servidores de desarrollo y pruebas.

5.4.6 servicios de soporte.

Cada ente solicitara el suministro del mantenimiento de los sistemas de prevención y supresión de incendios, aire acondicionado, sistemas eléctricos, control de humedad y otros sistemas de protección para ambientes computarizados.

Los equipos computarizados que alberguen sistemas críticos, computadores personales y estaciones de trabajo estarán equipados con sistemas de alimentación interrumpida.

5.4.7 protección de equipos informáticos que contengan información.

Se deberá ubicar o proteger el equipo para reducir las amenazas, peligros ambientales y oportunidades para acceso no autorizado.

5.4.8 cables eléctricos y de telecomunicaciones.

Para efectuar trabajos de instalación y el mantenimiento de infraestructura eléctrica y de telecomunicaciones, los responsables cumplirán las normas y estándares de seguridad vigentes, con el objeto de ser protegido contra la interceptación o daños.

5.4.9 Mantenimiento preventivo y correctivo.

Las solicitudes de necesidades para el cumplimiento preventivo y correctivo de los equipos críticos y periféricos, que se encuentren fuera del periodo de garantía que permita la continuidad de las operaciones ejecutadas por los usuarios.

Se revisará y consolidará las solicitudes de necesidades y remitirá al ente interesado lo estimado para la ejecución de los mantenimientos.

5.4.10 seguridades de los equipos fuera de las instalaciones.

Cada unidad que se atienda los lineamientos de seguridad emitidos por la unidad, cuando por razones de trabajo, se utilicen equipo fuera de las instalaciones de la institución, que cuentan con la autorización respectiva.

5.4.11 disposiciones final o reutilización de equipos.

Cada ente establecerá procedimientos y controles para garantizar que los equipos que contengan información en sus medios de almacenamiento sean verificados, garantizándose que la información sea eliminada de forma segura (incineración, trituración, borrado o sobre-escritura con software especial o el uso de hardware) antes de su disposición final o reutilización.

5.4.12 autorizaciones para salida de equipos.

Los jefes de las unidades organizativas deben autorizar la salida de equipos o cualquier de sus partes, fuera de las instalaciones de la institución, cumpliendo los lineamientos establecidos por el ente de los activos fijos de la unidad.

5.5. Gestión de comunicaciones y operaciones

5.5.1 Documentación de sistemas y procedimientos operativos.

Cada ente documentará y mantendrá disponible para el personal autorizado, los procedimientos operativos que soportan los sistemas de información. En adición los servicios

definidos como críticos que incluya, bases de datos, sistemas operativos, equipo de red y seguridad, deberán contar con la documentación respectiva de sus configuraciones.

5.5.2 gestión de cambios.

Cada ente establecerá los procedimientos necesarios para controlar los cambios en los sistemas de información y sus recursos de tratamiento con base a los definidos por la unidad. Los datos de producción serán modificados solo por el personal autorizado de acuerdo con dichos procedimientos.

5.5.3 separación de funciones.

Los responsables de definir los requerimientos de los sistemas y los de ambientes de producción, deben implementar controles que incluyan la separación de funciones incompatibles tales como autorización, ejecución, registro, custodia y control; a fin de reducir la posibilidad de que produzcan modificaciones no autorizadas o el uso indebido de los activos de información de la organización.

5.5.4 separación de ambientes de desarrollo, prueba y producción.

Cada ente deberá separar y utilizar de forma eficiente, los recursos de desarrollo, prueba y producción relacionados a los sistemas de información. Los administradores de sistemas operativos, bases de datos, equipo de comunicaciones servidores de aplicaciones y de estaciones clientes, no deben tener instaladas compiladores o herramientas de desarrollo en sus estaciones de trabajo ni en los servidores que administran, a menos que estén debidamente autorizados, de forma inscrita, por el jefe de la unidad de informática de la dirección o dependencia.

Los usuarios que participen en el proceso de pruebas de aplicaciones del negocio deben utilizar una cuenta de usuario distinta a la que tengan asignada en el ambiente de producción.

No se deberá utilizar datos de producción de ambientes de desarrollo y cuando estos sean confidenciales o reservados no podrán ser utilizados en ambiente de prueba.

5.5.5 gestión de la capacidad.

El uso de los componentes críticos para el tratamiento de la información en las aplicaciones del negocio clasificadas como críticas o vitales será constantemente monitoreado y se tomaran como base los resultados de esta tarea para hacer proyecciones oportunas de futuro crecimiento, para asegurar el desempeño de los sistemas de información automatizados.

5.5.6 aceptación de sistemas y aplicación de producción

Los responsables del desarrollo de las aplicaciones del negocio deben obtener por pate los solicitantes, evidencia de la aceptación de los nuevos sistemas y aplicaciones o modificaciones mayores, antes de que estas se desplieguen en productos.

5.5.7. Código Malicioso

Los jefes de las unidades de informática de casa dirección o dependencia deben establecer controles, procedimientos y mecanismos de divulgación o concientización para prevenir, detectar y recuperarse del código malicioso.

5.5.8 configuración de software y controles de seguridad de equipos cliente.

La unidad de informática de cada dirección o dependencia debe asegurarse que las estaciones clientes y computadoras portátiles, antes de que sean entregados al usuario final, cuentan con las medidas de seguridad establecidas en los documentos normativos del SGSI.

5.5.9 Respaldo de la información en medios magnéticos

Los responsables de efectuar los respaldos del software y de la información de cada dirección o dependencia. Deben llevarlos a cabo de acuerdo a los lineamientos específicos establecidos para tal efecto y realizar pruebas a los mismos de forma regular.

5.5.11 Seguridad en los servicios de red de datos.

La organización definirá y establecerá controles, estándares de seguridad y niveles de servicios incluir en los contratos relacionados con la utilización o entrega de los servicios de red, a través de redes de terceros y donde sea aplicables a las redes propias de la institución.

5.5.12 Eliminación de soportes

Cada dirección o dependencia eliminara de forma segura la información contenida en soportes de almacenamiento de datos (cintas, discos, memorias USB, discos duros removibles, discos duros USB, discos blu ray DVD, CD, diskettes, memorias SD, etc.) cuando sean dados de baja, pudiendo aplicar los criterios de referencias publicados en el SGSI, con el objeto de evitar la divulgación o el uso no autorizado de la información contenida en los mismo.

5.5.13 Utilización de la información

Cada dirección o dependencia establecerá los controles y procedimientos para la utilización y almacenamiento de la información en medios físico o magnético, con el objeto de protegerla del mal uso divulgación y acceso no autorizados.

5.5.15 soportes físicos en tránsito.

Para el caso del transporte de medidas de respaldo de los equipos y servidores del centro de procesamiento de datos se regirán por los lineamientos específicos de seguridad de la información para la gestión, de respaldos de información.

5.5.16 mensajería electrónica.

La organización establecerá los lineamientos específicos de la seguridad para el servicio de correo electrónico, acceso y uso del servicio de internet que contenga los controles para la protección de la información contenida, relacionada o transmitida por medios electrónicos.

5.5.18 comercio electrónico.

Las aplicaciones de negocio que permitan el intercambio de información o registros de transacciones en línea con terceros a través del internet, debe implementar controles orientados a proteger la confidencialidad de información sensible en tránsito y la autenticidad del sitio web de la organización.

5.5.19 pagos a empleados y terceros

La institución en su relación con proveedores y empleados que involucren el pago de bienes, servicios, remuneraciones u otros sea necesario efectuarlos a través de medios electrónicos o manuales, garantizara que el medio y los mecanismos para el manejo de la información cuenten con las características de seguridad razonables para evitar comprometer dicha información.

5.5.20 información disponible al público.

Los responsables de administrar los equipos o medios que contengan información disponible al público (oficiosa y pública), implantaran los controles para proteger la información ante modificaciones no autorizadas.

5.5.21 Registros o huellas de auditoría.

Las aplicaciones del negocio que manejen información reservada o confidencial, aplicaciones del negocio clasificadas como críticas o vitales, directorios de usuarios y los componentes críticos de infraestructura contaran con registros que capten las actividades de los usuarios, administradores y operadores de toda consulta, adición, cambio o eliminación de información relacionada a las transacciones del negocio.

5.5.22 protecciones de los registros o huellas de auditoría.

Los registros o huellas de auditoría deben protegerse para evitar su modificación y solo podrá ser accedido por personal autorizado.

5.5.23 registros de fallas

Se identificará y registraran las fallas de los componentes críticos de infraestructura asociadas a las aplicaciones del negocio clasificados como críticas, vitales y aquellas que manejan información reservada o confidencial con el objeto de tomar las acciones apropiadas.

5.5.25 políticas de retención de información electrónica.

Se determinará el periodo de conservación de la información electrónica en las bases de datos de las aplicaciones del negocio bajo su responsabilidad en ambiente de producción, de acuerdo a la normativa legal y técnica vigente que aplique a esa información y conforme a lo establecido en los lineamientos específicos para la gestión de respaldo de información en medio magnéticos y definición de periodos de retención de información electrónica.

5.5.26 políticas de disponibilidad en línea de la información electrónica.

Se determinarán el periodo de disponibilidad en línea de la información electrónica en las bases de datos de las aplicaciones del negocio bajo su responsabilidad de acuerdo a sus necesidades y considerando los costos económicos para este tipo de servicios y conforme a lo establecido en los lineamientos específicos para la gestión de respaldos de información en medios magnéticos y definición de periodos de retención de información.

5.5.27 Eliminación de información electrónica con periodo de conservación vencido.

Que tengan información en las bases de datos de las aplicaciones del negocio en ambiente de producción y cuyo periodo de conservación de la información electrónica haya vencido, autorizara la eliminación de esta.

5.6. Control de accesos

5.6.1 Políticas de control de acceso.

Se controlará el acceso a su información y recursos de tratamiento, basados en los lineamientos de control de acceso emitidos.

5.6.2 Registros de usuarios.

Se debe establecer un procedimiento formal de registro y desactivación de usuarios para conceder y revocar el acceso a todos los sistemas y servicios de información de acuerdo a los lineamientos de control de acceso emitidos.

5.6.3 Gestión de privilegios.

La asignación de contraseñas debe ser controlada a través de un proceso de gestión formal de acuerdo a los lineamientos de control de acceso emitidos.

5.6.4 Gestión de contraseñas de usuarios.

La asignación de contraseñas debe ser controlada a través de proceso de gestión formal de acuerdo a los lineamientos de control de acceso emitidos.

5.6.5 Directorios de usuarios.

Se definirá por la unidad responsable el estándar para el servicio de directorio que contengan a los usuarios y recursos asociaos de la institución.

5.6.6 Revisión de los derechos de acceso de usuario.

Semestralmente se efectuará la revisión de los derechos de acceso de los usuarios a la red, a las aplicaciones del negocio clasificadas como críticas o vitales y aquellas aplicaciones del negocio que manejan información confidencial o reservada, a efecto de revocar estos derechos después de 60 días o más de inactividad sin justificación.

5.6.7 Uso y estructura de las contraseñas.

Las contraseñas son estrictamente personales e intransferibles y es responsabilidad directa del usuario, los incidentes de seguridad que puedan ser causados por descuido o mala utilización de esta. Adicionalmente, los usuarios seguirán los lineamientos de control de acceso emitidos por el ente regular para su creación y buenas prácticas de seguridad.

5.6.8 Computadores desatendidos, los usuarios deben activar el protector de pantalla protegido por contraseña, cuando vayan a dejar sus estaciones de trabajo desatendidos.

5.6.9 Uso de los servicios de red.

Se atenderá los lineamientos de red establecidos por ente regular para el uso de los servicios de red de la institución los cuales serán asignados conforme a las funciones de los puestos de trabajo de los empleados, contratos o convenios suscritos con terceros.

5.6.10 Autenticación de conexiones externas.

Los administradores de la red de datos deben aplicar mecanismos que aseguren la autenticación de los usuarios remotos que acceden a la red interna de la institución, excepto el acceso externa información pública u oficiosa dispuesta a en los sitios web de la institución destinara para el público en general, ubicando los equipos de esta última en zona de seguridad separada de la red interna.

5.6.11 Diagnostico remoto y protección de los puertos de configuración.

El acceso a los puertos de diagnóstico y de configuración se controlará de conformidad a los lineamentos de red definidos por la unidad reguladora.

5.6.12 Segregación de redes de datos.

Los administradores de redes de la institución deben segregar en subredes, los grupos de servicios de información, usuarios y sistemas de información.

5.6.13 Control de conexiones de la red.

Los administradores de redes deben limitar el acceso de los usuarios para conectarse a la red de acuerdo a los lineamientos de seguridad de la información para el control de acceso a la información de la organización, los lineamientos de seguridad de la información para los servicios y gestión de acceso a la red de datos.

5.6.14 procedimientos para inicio de sesión.

El acceso a los sistemas operativos se debe controlar por medio de un procedimiento seguro de inicio de sesión, en cumplimiento a lo definido en los lineamientos de control de acceso.

5.6.15 identificación y autenticación de usuario.

Todos los identificadores de usuario se construirán de conformidad con los lineamientos de control de acceso emitidos por la unidad reguladora, eligiendo una técnica adecuada de autenticación para confirmar la identidad solicitada al usuario

5.6.16 uso de los recursos del sistema.

Se debe restringir y controlar rigurosamente el uso de programas y utilidades que puedan ser capaces de invalidar los controles del sistema de las aplicaciones del negocio de acuerdo a los lineamientos de control de acceso emitidos por la unidad reguladora.

5.6.17 software estándar e estaciones de trabajo.

Las estaciones de trabajo de cada unidad, departamento, etc. Contaran con un software definidos como estándar para efectos de trabajo, de conformidad a los lineamientos establecidos por estas.

5.6.18 desinstalaciones de herramientas.

Los usuarios no desinstalaran las herramientas de seguridad, administración y control de inventario de ce las estaciones de trabajo asignadas.

5.6.19. Instalaciones o desinstalaciones de software.

La instalación o desinstalación de software en los equipos de computación debe ser realizado únicamente por el personal informático autorizado, atendiendo los procedimientos establecidos para tal fin.

5.6.20. Computadores portátiles con la información reservada o confidencial.

Los usuarios responsables de computadores portátiles que tengan información reservada o confidencial, se apoyaran en las unidades de informativa de la dirección o dependencia para garantizar que dichos equipos cuenten con medidas de seguridad, por ejemplo: contraseña de arranque, usuario y contraseña de sistema operativo.

5.7. Adquisición, desarrollo y mantenimiento de sistemas de información

5.71 análisis y especificación de los requisitos de seguridad.

Los propietarios de la información o las personas que designen para definir los requerimientos de las aplicaciones del negocio, deben incluir los controles de seguridad a ser implementados, tanto para los sistemas de información nuevos o para mejoras a los mismo atendiendo los lineamientos para el desarrollo, mantenimiento o adquisición de aplicaciones del negocio emitidos por la unidad reguladora.

5.7.2 validación de los datos de entrada.

La introducción de datos en las aplicaciones de negocio debe validarse para garantizar que dichos datos son correctos y adecuados conforme al proceso de negocio que soportan. Los propietarios de la información o las personas que designen son responsables de definir estas validaciones.

5.7.3 control del procesamiento interno.

Los propietarios de la información de las personas que designen para definir requerimientos de las aplicaciones del negocio, deben definir los procesos críticos para incorporar comprobaciones de validación que detecten cualquier corrupción de la información, debido a errores de procesamiento o actos intencionados.

5.7.4 integridad de los mensajes.

Se deben identificar los requisitos para garantizar la autenticidad y proteger la integridad de los mensajes en los servicios web y se deben identificar e implementar los controles adecuados.

5.7.5 validación de los datos de salida.

Los propietarios de la información o las personas que designen para definir requerimientos de las aplicaciones del negocio, deben especificar los controles para vigilar que la información almacenada es correcta y adecuada a las circunstancias.

5.7.7. Falla de las aplicaciones del negocio.

Los responsables del desarrollo de las aplicaciones del negocio deben asegurar que cuando estas fallen y no produzcan los resultados esperados, proporcione un mensaje de error comprensible o alguna otra indicación de falla como respuesta al usuario.

5.7.8 retroalimentación de las aplicaciones del negocio al usuario.

Los responsables del desarrollo de las aplicaciones del negocio deben asegurara que cuando ejecuten en una transacción, esta dará respuesta cuando amerite según los requerimientos del solicitante, indicando si se llevó a cabo la solicitud.

5.7.9 prueba de las aplicaciones del negocio.

Todas las aplicaciones del negocio adquiridas o desarrolladas internamente, pasaran por un proceso de pruebas documentado que garantice la calidad y seguridad de las mismas.

5.7.10 Instalación de las aplicaciones del negocio en producción.

Las aplicaciones del negocio serán trasladadas al ambiente de producción por personal de tecnología autorizado e independiente a las áreas de desarrollo.

5.7.11 Protección de los datos de prueba del sistema.

Los datos de prueba deben seleccionar cuidosamente, estar protegidos y controlados, adicionalmente, no deben efectuarse pruebas de software directamente en producción.

5.7.12 Control de acceso a código fuente de los programas.

Los responsables del desarrollo de aplicaciones del negocio de cada dirección o dependencia restringirán el acceso a los códigos fuentes de los programas y aplicaciones utilizados en sistemas de información automatizados, de acuerdo a los lineamientos de control de acceso emitidos por el ente regulador.

5.7.13 procedimientos de control de cambios.

Cada dirección o dependencia empleara procedimientos de control de cambios, para autorizar y desplegar las modificaciones al software y aplicaciones del negocio en el ambiente de producción.

5.7.14 Control de cambios del código fuente.

Para controlar el cambio de las aplicaciones del negocio en producción, se debe emplear un sistema de control de versiones del código fuente.

5.7.15 revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.

Se deben revisar y aprobar las aplicaciones del negocio críticas, cuando se apliquen cambios mayores a los sistemas operativos del ambiente de producción, para garantizar que no existen efectos adversos en las operaciones o en la seguridad.

5.7.16 desarrollo de software por terceros.

El ente regulador solicitante de proyectos de desarrollo de software por terceros, debe incluir en los requerimientos de contratación adicionalmente a las especificaciones técnicas, los siguientes aspectos.

a) Definiciones de arreglos de licencia
b) Propiedad intelectual
c) Cumplimiento de las políticas de seguridad de la información de a organización
d) Seguridad y calidad del software desarrollado
e) Acuerdos de garantías
f) Entrega del código fuente
g) Requerimientos de pruebas en producción.

5.7.17 controles de vulnerabilidades de software

El personal responsable de administrar equipos de computación, de comunicación de datos y el software desplegado en estos, deben revisar de forma periódica y oportuna, la información sobre vulnerabilidades de sistemas operativos y aplicaciones de software en operación utilizadas en su dirección o dependencia y aplicar las medidas adecuadas para mitigar el riesgo asociado.

5.8. Gestión de incidentes de seguridad de la información

5.8.1 notificaciones de los eventos de seguridad de la información.

Los empleados contratistas y usuarios de las aplicaciones del negocio, software en general y servicios de información de la institución, deben reportar oportunamente los eventos de seguridad de la información a través del sistema de mesa de servicios, proporcionado por el ente.

5.8.2 responsabilidades y procedimientos de gestión de incidentes de seguridad.

Cada ente regulador definirá procedimientos de gestión, dicten los pasos a seguir para corregir y prevenir incidentes de seguridad de la información, mediante una respuesta rápida, efectiva y ordenada, de acuerdo a los lineamientos para la gestión de incidentes de seguridad de la información emitidos por el ente.

5.9. Gestión de continuidad del negocio

5.9.1 seguridad de la información en el proceso de continuidad del negocio.

Cada ente debe desarrollar y mantener un proceso para la continuidad del negocio, que gestione los requisitos de seguridad de la información necesarios para la continuidad del negocio basado en el modelo proporcionado por tal.

5.9.2 continuidad del negocio y evaluación de riesgos.

Cada ente debe de identificar los eventos que puedan causar interrupciones en sus procesos de negocio, así como la probabilidad de que se produzcan tales interrupciones basado en el modelo proporcionado.

5.9.3 desarrollo e implantación de planes de continuidad del negocio que incluyan la seguridad de la información.

El ente debe desarrollar e implantar planes para mantener o restaurar las operaciones y garantizar su disponibilidad de la información en el tiempo requerido, después de una interrupción o fallo en los procesos de negocio críticos.

5.9.4 Pruebas mantenimiento y reevaluación de los planes de continuidad del negocio.

El ente debe probar y actualizar al menos una vez al año, los planes de continuidad del negocio para asegurar que está al día y son efectivos, las pruebas deben ser planificadas y documentas conforme al modelo proporcionado, y se deberá informar a los titulares sobre los resultados de estas.

5.10. Conformidad

Identificaciones de la legislación aplicable.

El ente debe identificar las disposiciones legales que les aplican y gestionar su cumplimiento considerando implementar procedimientos registrados en el sistema de gestión de la calidad o cambios en los documentos del SGSI para tal efecto.

5.10.2 registro de software de desarrollo interno y derechos de autor.

Cada ente será responsable de gestionar el registro en la entidad competente del software desarrollado para aplicaciones del negocio clasificadas como críticas o vitales, a efectos de garantizar los derechos de propiedad intelectual y auditoría nombre de la institución.

5.10.3 Cumplimiento de las políticas y normas de seguridad.

Al despacho deben apoyar para el cumplimiento de lo establecido en el sistema de seguridad de la información dentro de su área de responsabilidad.

5.10.4 Protección de herramientas de auditoría.

El acceso a las herramientas de auditoría de los sistemas de información debe estar protegidos por los responsables de estos, para evitar cualquier posible peligro o uso indebido.

SECCIÓN 6: PROCEDIMIENTOS DE AUDITORÍA DE SISTEMAS

SEGURIDAD FÍSICA

Procedimiento 1. Obtenga acceso a las instalaciones de la Organización no Gubernamental y elabore un listado de chequeo con los atributos de la misma y verificar lo siguiente: (NTS ISO/IEC 27002:2013 A.11.1.1; CISA 5.2.4)

- El equipo informático se encuentra en lugares seguros tales como habitaciones, oficinas, bodegas entre otros lejos del personal no autorizado y personas ajenas a la institución.

- Se encuentra resguardado en lugares con puertas que eviten el robo o daño de dichos recursos.

- Se deja el equipo informático bajo llave para evitar posibles robos del equipo.

- Existe alguna área de recepción que impida la incorporación de personas no autorizadas a la instalación.

Procedimiento 2: Visitar las instalaciones de la entidad y observar e inspeccionar si llevan un registro de los visitantes que contenga la fecha y hora de entrada y salida, solicitar identidad mediante documento adecuado, así como también restringir el acceso en áreas donde la información es confidencial. (ISO 27002 A.11.1.2)

Procedimiento 3: Verificar el control que aplican en el área de informática para permitir el ingreso a un usuario, cumpliendo: (NTS ISO/IEC 27002:2013 A.11.2.1; CISA 5.2.4)

- Solicite el sistema de control interno implementado al área de informática de la entidad.
- Revise las políticas de control interno y compruebe la existencia como medida mitigadora, el uso de carnet o cualquier distintivo que permita la identificación del personal que está autorizado para entrar y manipular el centro informático.
- Además, Mediante el procedimiento de la inspección y observación corroborar que esta medida es llevada a cabo por todos los empleados de la entidad.

Procedimiento 4: Realizar visitas repentinas durante el periodo de la auditoría. Elabore un listado de chequeo con los atributos de la misma e indague los siguientes aspectos: (ISO 27002 A.11.1.3)

- Las instalaciones claves están ubicadas de forma tal que se evita el acceso al público.
- Si es aplicable, los edificios deben ser discretos y dar una indicación mínima de su propósito, sin signos evidentes, fuera o dentro del edificio, identificando la presencia de actividades de procesamiento de información.
- Las instalaciones deben estar adecuadas para prevenir que la información confidencial o actividades sean visibles y audibles desde el exterior.
- Los directorios y guías telefónicas internas que identifican la ubicación de instalaciones de procesamiento de la información no deben ser fácilmente accesibles.

Procedimiento 5: Mediante el procedimiento de la observación e inspección verificar que la entidad cuente con las medidas e instrumentos preventivos necesarios para la mitigación de riesgos de incendios y catástrofes naturales cumpliendo con: (ISO 27002 A.11.1.4)

- Observar si se encuentran dentro de la entidad de manera escrita y a la vista de todo público las medidas preventivas a tomar en caso de terremotos incendios o inundaciones.
- Inspeccionar la colocación de extintores en puntos estratégicos y verificar su fecha de caducidad.
- La existencia de detectores de humo en buenas condiciones y debidamente ubicados

Procedimiento 6: Verificar mediante la observación las áreas de trabajo seguras que cumplan con: (ISO 27002 A.11.1.5)

- El personal debe estar consciente de la existencia de áreas seguras o de actividades dentro de ellas, en lo que le corresponde.
- Se debe evitar el trabajo sin supervisión en áreas seguras, tanto por razones de seguridad como para prevenir que se den actividades maliciosas.
- Las áreas seguras vacantes permanecen bloqueadas físicamente y se revisan periódicamente.
- Los equipos fotográficos, de video, audio u otro equipo de grabación, como cámaras en los dispositivos móviles, no deben estar permitidos.

Procedimiento 7: Verificar la existencia de controles para puntos de acceso en áreas de carga y descarga de productos o materiales necesarios a fin de que estén aislados de los medios de procesamiento de la información. Llenar lista de cumplimiento: (ISO 27002 A.11.1.6)

- El acceso al área de carga y descarga desde el exterior debe limitarse al personal identificado y autorizado.
- Debe estar diseñada de manera que los suministros pueden ser cargados y descargados sin que el personal de entrega pueda obtener acceso a otras áreas.
- Las puertas externas deben estar aseguradas cuando las puertas internas de esta área se abren.
- El material entrante debe ser inspeccionado y examinado en busca de explosivos, productos químicos u otros materiales peligrosos, antes de que se trasladen desde un área de carga y descarga.
- Los envíos entrantes y salientes deben estar separados físicamente, siempre que sea posible.

Procedimiento 8: Realizar Inspecciones del cumplimiento de las medidas de control interno en cuanto a la ubicación y protección del equipo para reducir riesgos de amenazas y peligros ambientales; elabore un listado de chequeo con los atributos de la misma evaluando y revisando los siguientes aspectos: (ISO 27002 A.11.2.1)

- Los equipos están ubicados de manera que se minimiza el acceso innecesario a las áreas de trabajo.
- Las instalaciones de procesamiento de información sensible están ubicadas cuidadosamente para reducir que sea vista la información.
- las instalaciones de almacenamiento de información están aseguradas para evitar el acceso no autorizado.
- Se han establecido directrices para: comer, beber y fumar en proximidad a las instalaciones de procesamiento de información.

- El cableado de red como el de energía eléctrica posee la seguridad necesaria para no ser dañado.

Procedimiento 9: Revisar mediante la observación que los equipos informáticos estén protegidos contra fallas de energía, cumpliendo: (ISO 27002 A.11.2.2)

- Las especificaciones del fabricante del equipo y los requisitos legales locales.
- Ser evaluados regularmente por su capacidad para satisfacer el crecimiento de los negocios y la interacción con otros servicios de apoyo.
- Ser inspeccionados y probados con regularidad para asegurar su buen funcionamiento
- Si es necesario tener múltiples alimentaciones con diversos enrutamientos físicos.

Procedimiento 10: Inspeccionar el nivel de protección que presenta el cableado de los equipos que transportan datos o soportan servicios de información, para ello considerar: (ISO 27002 A.11.2.3)

- Las líneas de energía y telecomunicaciones en las instalaciones deben estar bajo tierra, cuando sea posible.
- Los cables de energía y telecomunicación deben estar separados para evitar interferencias.
- Acceso controlado a los paneles de conexión y salas de cableado.
- Para sistemas sensibles o críticos, los controles pueden incluir: instalación del conducto blindado, cajas de inspección, uso de protección electromagnética para proteger los cables.

Procedimiento 11: Verificar que la entidad se cerciora de tomar todas las medidas necesarias para el desecho del equipo obsoleto de la entidad. Para ello elaborar un check list con sus respectivos atributos e inspeccionar los siguientes aspectos: (ISO 27002 A.11.2.7)

- el personal de mantenimiento se asegura que realmente el equipo se encuentra realmente obsolescente.
- Previamente se adquiere la autorización gerente general de la entidad para llevar acabo el desecho del equipo informático.
- se aseguran que se haya resguardado y sobrescrito de manera segura la información.
- Para sus ventas o desecho además de necesitar la autorización de los gerentes generales se necesita de la documentación de requisición del equipo informático.

Procedimiento 12: Cerciorarse mediante la inspección que el equipo informático recibe un correcto mantenimiento para asegurar su disponibilidad, continuidad e integridad, considerando: (ISO 27002 A.11.2.4)

- El equipo deberá mantenerse de acuerdo con los intervalos de mantenimiento recomendados por el proveedor y las especificaciones.
- Deben mantenerse registros de todos los fallos sospechosos o reales, y de todo el mantenimiento preventivo y correctivo.
- Solo el personal de mantenimiento autorizado debe llevar a cabo las reparaciones a los equipos de servicio.
- Deben cumplirse todos los requisitos de mantenimiento impuestos por las pólizas de seguro.

Procedimiento 13: Mediante el procedimiento de la observación verificar que la entidad cuente con las medidas adecuadas para el retiro de activos, llenando una lista de chequeo que incluya: (ISO 27002 A.11.2.5)

- Identificar los empleados y usuarios de terceras partes que tengan autoridad para permitir el retiro de activos fuera de las instalaciones de la organización
- Fijar límites de tiempo para el activo retirado y verificar el cumplimiento de su retorno.
- Cuando sea necesario debe registrarse tanto la salida del equipo como el retorno a la institución.
- Debe documentarse la identidad, el rol y la afiliación de cualquier persona que gestiona o utiliza activos.

Procedimiento 14: Indagar sobre la seguridad de los equipos y activos fuera de las instalaciones, llenar una lista de chequeo que cumpla: (ISO 27002 A.11.2.6)

- Los equipos y medios extraídos de las instalaciones no deben dejarse desatendidos en lugares públicos.
- Deben observarse siempre las instrucciones del fabricante para proteger los equipos, por ejemplo, contra exposiciones a campos electromagnéticos intensos.
- Cuando el equipamiento que esta fuera de las instalaciones sea transferido entre diferentes personas o partes externas, debe mantenerse un registro que defina la cadena de custodia.

Procedimiento 15: Verificar mediante la observación que al equipo informático desatendido se le implementan las medidas siguientes. (ISO 27002 A.11.2.8)

- Cerrar sesiones activas cuando hayan terminado, salvo que se pueda asegurar por un mecanismo de bloqueo apropiado.
- Desconectarse de aplicaciones o de servicios de red cuando ya no se necesiten.
- Asegurar a las computadoras o dispositivos móviles de uso no autorizado mediante una cerradura o un control equivalente.

Procedimiento 16: Investigue si en la organización aplican medidas de protección de la información relacionadas con la política de escritorio limpio, llene una lista de chequeo considerando: (ISO 27002 A.11.2.9)

- La información sensible o crítica como USB, discos o documentación deben asegurarse bajo llave cuando no sea requerida, especialmente cuando la oficina está vacía.
- Las computadoras y terminales deben desconectarse o protegerse con un mecanismo de bloqueo, y debe protegerse con cerradura.
- Se previene el uso no autorizado de fotocopiadoras u otras tecnologías de reproducción como escáneres.

SEGURIDAD LÓGICA

Procedimiento 1: Obtener por medio de un documento formal de la alta gerencia las políticas establecidas para el control de la información y verifique que los manuales de control de información realmente existan. (ISO 27002 A.9.1.1)

Procedimiento 2: Inspeccionar que exista una política apropiada para la protección de acceso a la red, que cubra: (ISO 27002 A.9.1.1)

- Las redes y los servicios de red que están autorizados a acceder
- Los procedimientos de autorización para determinar quién puede acceder a qué redes y servicios en red.
- Los controles y procedimientos para proteger el acceso a las conexiones de red y servicios de red de gestión.
- Los requisitos de autenticación de usuario para acceder a varios servicios de red.

Procedimiento 3: Verificar que exista control sobre el registro y anulación de usuarios para controlar los derechos de acceso formal al sistema de información, llenando una lista de chequeo que incluya: (ISO 27002 A.9.2.1)

- Uso de ID único para cada usuario y generar así responsabilidad directa en sus acciones.
- Desactivar o quitar los IDs de usuarios que han abandonado la organización.
- Eliminación o desactivación periódica de los usuarios redundantes.
- Asegurarse que los IDs de los usuarios redundantes no se emiten a otros usuarios.

Procedimiento 4: Verificar que el proceso de provisión de acceso de usuario sea el apropiado y cumpla con los criterios siguientes: (ISO 27002 A.9.2.2)

- Obtener autorización del propietario del sistema de información o servicio para el uso del servicio.
- Verificar que el nivel de acceso otorgado es adecuado a las políticas de acceso.
- Garantizar que los derechos de acceso no están activados antes de que se completen los procedimientos de autorización.
- Exista mantenimiento del registro central de los derechos de acceso concedidos a un ID de usuario.

Procedimiento 5: Verifique que exista control sobre la gestión de la información de autenticación secreta de los usuarios donde compruebe que: (ISO 27002 A.9.2.4)

- Los usuarios firman una declaración de confidencialidad de información
- Se han establecido procedimientos para verificar la identidad de un usuario antes de proporcionar información de autenticación secreta
- La información de autenticación secreta temporal debe ser única para un individuo
- Los usuarios hacen acuse de recibo de la información secreta.

Procedimiento 6: Verificar que la estructura de las contraseñas cumpla con criterios mínimos, llenar una lista de chequeo de ello, que cumpla con: (ISO 27002 A.9.3.1)

- No sean fáciles de recordar
- No son basadas en nada que alguien podría adivinar u obtener con facilidad utilizando la información relacionada a la persona
- No son vulnerables a los ataques de diccionario

- Son libres de caracteres consecutivos idénticos
- Si es temporal cambiarla de inmediato
- Garantizar una adecuada protección de las contraseñas cuando estas se utilizan como información secreta de autenticación
- No usar la misma información secreta de autenticación para fines del negocio y para otros fines.

Procedimiento 7: Verificar que el acceso a los sistemas y aplicaciones están restringidos y se aplica un control que cumpla con: (ISO 27002 A.9.4.1)

- Proporcionar menús para controlar el acceso a las funciones del sistema de aplicación
- Controlar que datos pueden ser accedidos por un usuario en particular
- Controlar los derechos de acceso de los usuarios
- Limitar la información contenida en las salidas
- Proporcionar controles de acceso físicos o lógicos para el aislamiento de aplicaciones sensibles.

Procedimiento 8: Comprobar la efectividad del inicio de sesión que cumpla con: (ISO 27002 A.9.4.3)

- No mostrar identificador de sistemas o aplicaciones hasta que el proceso de inicio de sesión se ha completado con éxito.
- Mostrar un aviso general advirtiendo que al equipo solo debe tener acceso los usuarios autorizados.
- No dar mensajes de ayuda durante el proceso de inicio de sesión que podría ayudar a un usuario no autorizado

- Se valida la información de inicio de sesión solo cuando se han completado todos los datos de entrada
- Proteger contra los intentos de inicio de sesión de fuerza bruta
- Registrar los intentos fallidos y exitosos, mostrar un detalle del inicio de sesión exitoso anterior.

Procedimiento 9: Solicitar a la gerencia por medio de un documento formal el control que implementan para el uso de software, llenar una lista de chequeo que incluya: (ISO 27002 A.12.5.1)

- La actualización de software, aplicaciones y librerías de programas solo deben realizarse por administradores entrenados con la autorización apropiada
- Debe mantenerse una bitácora de actualizaciones realizadas
- Debe conservarse la versión anterior de cada software como medida de contingencia.

Procedimiento 10: Solicitar a la gerencia por medio de un documento formal los back-up de la empresa completos para un mejor control sobre la seguridad de la información. (ISO 27002 A.12.3)

Procedimiento 11: Verificar si la empresa posee un Software de antivirus y si este se encuentra debidamente actualizado. (ISO 27002 A.12.2)

Procedimiento 12: Observar si se encuentran restricciones en el acceso de todo tipo de páginas en los navegadores web. (ISO 27002 A.12.2.1).

Procedimiento 13: Compruebe los niveles de seguridad que posee las conexiones inalámbricas del router en cuanto a su nivel de protección de contraseñas para acceso. (ISO 27002 A.13.1.1).

PISTAS DE AUDITORÍA

Procedimiento 1: Verificar con la alta dirección la existencia de un control adecuado ante las revisiones de auditoría de sistemas de manera que no afecten la funcionalidad del mismo, el cual cumpla: (ISO 27002 A.12.7.1)

- Acordar con la dirección correspondiente los requisitos de auditoría para acceder a los sistemas y datos.
- Acordar y controlar el alcance de las pruebas técnicas de la auditoría.
- Las pruebas de auditoría deben limitarse a accesos de solo lectura al software y a los datos.
- Otro acceso distinto al de solo lectura solamente debe permitirse para copias aisladas de archivos de sistema que deban borrarse luego de la auditoría.
- Los requisitos para procesos especiales deben identificarse y acordarse.
- Las pruebas de auditoría que puedan afectar la disponibilidad del sistema deben ejecutarse fuera de horario laboral.
- Todo acceso debe monitorearse y registrarse para generar una huella historia de referencia.

Procedimiento 2: Inspeccionar que exista una bitácora de monitoreo apropiado que permita el registro y la detección de las acciones que puedan afectar o sean relevantes a la seguridad de la información. (ISO 27002 A. 13.1.1)

Procedimiento 3: Verificar que exista un control adecuado que registre los eventos ocurridos en el sistema, llene una lista de chequeo que incluya: (ISO 27002 A.12.4.1)

- ID de usuario.
- Actividades del sistema.
- Fecha, hora y detalle de los eventos.
- Identidad o ubicación del dispositivo.
- Registro de intentos exitosos y rechazados.
- Cambios en la configuración del sistema.
- Uso de utilitarios y aplicaciones del sistema.
- Archivos accedidos y tipo de acceso.
- Alarmas activadas por el sistema de control de acceso.

Procedimiento 4: Verificar que la bitácora de información se mantenga protegida en instalaciones que eviten manipulaciones indebidas y accesos no autorizados, dicha instalación debe cumplir:

PROCESOS

Procedimiento 1: Verificar que exista protección en redes públicas sobre servicios de aplicación para ser protegidos de actividades fraudulentas o modificación no autorizada, llenar lista de chequeo donde cumpla con: (ISO 27002 A. 14.1.2)

- El nivel de confianza que cada parte requiere en la identidad alegada de cada uno.
- Los procesos de autorización asociados con quien puede aprobar el contenido de, emitir o firmar los documentos transaccionales clave.
- Asegurar que los socios estén plenamente informados de sus autorizaciones para la prestación o uso de los servicios.
- Determinar y cumplir con los requisitos de confidencialidad, integridad, prueba de envío y recepción de documentos clave y el no repudio.

Procedimiento 2: Verificar la existencia de un control en el proceso de pagos electrónicos, llenar lista de cumplimiento: (ISO 27002 A.14.1.2)

- Existencia de confidencialidad y la integridad de las transacciones de pedidos, la información de pago, detalles de la dirección de entrega y la confirmación de recibos.
- La selección del formulario de liquidación de pago más adecuado para evitar el fraude.
- El nivel de protección requerido para mantener la confidencialidad y la integridad de la información del pedido.
- La prevención de la pérdida o duplicación de la información de transacción.
- La responsabilidad asociada con cualquier transacción fraudulenta.
- Los requisitos del seguro.

Procedimiento 3: Verificar que existan controles adecuados en la transacción de servicios de aplicación a fin de proteger la información y prevenir transacciones incompletas, mal enrutamiento, alteración no autorizada de mensajes, divulgación no autorizada, duplicación o replicación no autorizada. Llenar lista de cheque que considere: (ISO 27002 A. 14.1.3).

- El empleo de firmas electrónicas por cada una de las partes implicadas en la transacción.
- Asegurar que la información secreta de autenticación del usuario de todas las partes son validadas y verificadas.
- La transacción permanece confidencial.
- La privacidad asociada con todas las partes involucradas es conservada.
- El canal de comunicación entre todas las partes involucradas es cifrado.
- Los protocolos utilizados entre las partes involucradas son seguros.

SALIDAS DE INFORMACIÓN

Procedimiento 1: Verificar que exista un control sobre la salida de información el cual evite la intercepción, copiado, modificación, desviación y destrucción. (ISO 27002 A. 13.2.1)

Procedimiento 2: Verificar que en la transferencia de información esté siempre activo el antivirus o firewall de manera que detecte y proteja ante software malicioso que pueda ser incluido en comunicaciones electrónicas o mediante archivo adjunto en mensajes. (ISO 27002 A.13.2.1)

Procedimiento 3: Indagar con la gerencia la existencia de una especie de carta de confidencialidad o de no divulgación de información la cual se aplique a los empleados y terceras personas con acceso a información en la organización. (ISO 27002 A.13.2.1)

Procedimiento 4: Comprobar que las maquinas contestadoras no tengan mensajes pendientes de escuchar los cuales puedan comprometer la confidencialidad, lo mismo debe verificarse en las impresoras a fin de que no tengan impresiones pendientes. (ISO 27002 A.13.2.1)

Procedimiento 5: Verificar que exista actualización de la agenda telefónica y el proceso de envío de mensajes a fin de no enviar información a número equivocados. (ISO 27002 A.13.2.1)

Procedimiento 6: Verificar con gerencia que exista un modelo de acuerdo de transferencia de información entre la organización y partes externas, marcar una lista de cheque que cumpla con: (ISO 27002 A.13.2.2.)

- La existencia de responsabilidad de gestión para controlar y notificar la transmisión, el envío y recepción.
- Existencia de no repudio al recibir la información.
- Normas técnicas mínimas para el empaquetado y transmisión.
- Responsabilidades y compromisos en el caso de incidentes de seguridad.
- Acuerdos de custodia.
- Responsabilidades y compromisos en el caso de pérdida de datos.
- Cualquier otro control adicional a información crítica o sensible como el encriptado.

Procedimiento 7: Verificar que existan controles que deban cumplirse para la manipulación de mensajes electrónicos, marcar los que se cumplan. (ISO 27002 A. 13.2.3.)

- Proteger mensajes de acceso no autorizado, modificación o negación del servicio.
- Asegurar el correcto direccionamiento y transporte de los mensajes.
- Confiabilidad y disponibilidad del servicio.
- Considerar requisitos para firmas digitales.
- Obtener aprobación antes de utilizar servicio público externos, tales como mensajería instantánea, redes sociales o compartir archivos.
- Fuertes niveles de autenticación controlando el acceso desde redes de acceso público.

Procedimiento 8: Verificar la existencia de un acuerdo de confidencialidad que aplique terceras partes y empleados, llenar lista de cheque donde cumpla con: (ISO 27002 A. 13.2.4)

- Una definición de la información a ser protegida.
- Duración prevista del acuerdo, incluyendo los casos en que sea necesario mantener la confidencialidad indefinidamente.
- Acciones requeridas cuanto termina un acuerdo.
- Responsabilidades y acciones de los firmantes para evitar la divulgación no autorizada.
- Propiedad de la información, secretos comerciales y propiedad intelectual.
- El uso permitido de la información confidencial y los derechos del firmante.
- El derecho de auditar y de supervisar actividades que involucran información confidencial.
- Términos vinculados a la destrucción o devolución de información cuando cesa un acuerdo.

CONCLUSIONES

1- Los profesionales que ejecutan auditorías de sistemas en ONG conocen la normativa NTS ISO/IEC 27002 y los elementos que la conforman, su aplicación en auditorías para ese sector es lo que necesitan implementar pues no toda la norma es aplicable, se deben seleccionar los elementos que le aplican según el tipo de área que se analice en la auditoría, pues aspectos propios de seguridad de datos como en bancos, no se consideraran en una auditoría de sistemas que pretenda validar la seguridad de información en una ONG, ya que esta buscaría comprobar que la información es procesada, guardada y respaldada en lugares seguros tanto de usuarios como de terceros ajenos a la entidad.

2- Dentro del sector de Organizaciones no Gubernamentales no se aplica la Normativa ISO 27002 de forma completa, algunos aspectos son implementados como las medidas de resguardo de información, con los respaldos de seguridad o backup del sistema, un 70% aplican esta práctica de protección de información.

3- Los auditores de sistemas en Organizaciones no Gubernamentales que ejecutan su función y la implementan tomando de referencia la normativa NTS ISO/IEC 27002 tendrían mejores resultados con la ayuda de un manual de aplicación de procedimientos ideal para el sector de ONG.

4- El manual de procedimientos elaborado en este informe de investigación se acopla para ser aplicado en una auditoría de sistemas para ONG que busque validar la seguridad de la información que es manipulada dentro de una entidad, desde su origen, pasando por el procesamiento de datos para convertirse en información que sustente reportes.

5- Las ONG del sector educativo tendrán que tomar en cuenta el manual de procedimiento de auditoría de sistemas basado en la norma ISO 27002 de manera tal que su información permanezca protegida cumpliendo los requisitos (no obligatorios) de suma relevancia para resguardo de los datos de la entidad.

RECOMENDACIONES

1- A expandir los controles de seguridad que ya poseen utilizando controles adicionales como los propuestos en el presente manual de procedimientos tomando los que le sean aplicables a cada ONG en particular, ya que algunas son de mayor volumen en instalación y personal que requieren controles más robustos y fortalecidos, otras de menor exigencia con departamentos e instalaciones pequeñas, pero de igual cumplimiento necesitan controles para protección de la información.

2- Velar que su departamento de informática cumpla y haga cumplir el manual de seguridad (si es que existe) en todo lugar y momento dentro de la Organización, a falta de él, elaborar uno y mantenerlo en práctica.

3- Utilizar el presente manual de procedimientos de auditoría de sistemas ya que es una extracción de los procedimientos que particularmente se acoplan a una auditoría de sistemas que estaría respondiendo a los requisitos que debe implementarse en el ambiente de seguridad para una ONG.

4- A realizar las auditorías de sistemas en ONG de manera integral utilizando herramientas adicionales, asegurando que la información procesada sea protegida tomando como referencia otras normativas, aunque no sean de cumplimiento obligatorio para el sector, como es la ISO/ IEC 27002.

5- Cuando una ONG no aplique controles tales como los que establece la ISO 27002, a manera de mejorar su nivel de protección de datos, el auditor podría proponer el uso de esta normativa explicándoles su beneficio.

BIBLIOGRAFÍA

Aguilar, Q. (17 de noviembre de 2016). *It Now*. Recuperado el 7 de abril de 2017, de https://revistaitnow.com/el-salvador-y-guatemala-las-mayores-presas-del-cybergate/

Cornejo, M. (2017). Seguridad Lógica. El Salvador.

Críado, M. Á. (21 de octubre de 2008). *Informática libre para las ONG*. Recuperado el 22 de junio de 2017, de http://www.publico.es/ciencias/tecnologia/informatica-libre-ong.html

Cupul, A. (6 de junio de 2012). *blogspot*. Recuperado el 15 de junio de 2017, de http://aly-acceso-remoto.blogspot.com/2012/06/ventajas-y-desventajas-que-tiene-una.html

IFAC, F. I. (agosto de 2008). Manual de Pronunciamientos Internacionale de Formación. Nueva York, Estados Unidos.

ISACA. (2012). COBIT 5 Para seguridad de la información. Madrid, España.

ISACA. (2012). COBIT 5, Para Seguridad de la Información. *COBIT 5, Para Seguridad de la Información*. EStados Unidos, Estados Unidos.

ISACA. (2014). Manual de preparacion al examen CISA . *Manual de preparacion al examen CISA* . Estados Unidos : inkorporation enigmah.

ISMS, S. (2011). *Protege tu información*. Recuperado el 20 de junio de 2017, de http://www.protegetuinformacion.com/perfil_tema.php?id_perfil=9&id_tema=78

ISO. (11 de julio de 2005). Recuperado el 13 de marzo de 2017, de https://www.iso.org/standard/54533.html

ISO 27002. (2013). En *Tecnología de la información. Código de prácticas para la gestión de la seguridad de la información.* (pág. 114). San Salvador: Organismo Salvadoreño de Normalización.

Legislativa, A. (17 de diciembre de 1996). San Salvador. Obtenido de http://www.asamblea.gob.sv/eparlamento/indice-legislativo/buscador-de-documentos-legislativos/ley-de-asociaciones-y-fundaciones-sin-fines-de-lucro

Legislativa, A. (29 de Febrero de 2000). Obtenido de http://www.asamblea.gob.sv/eparlamento/indice-legislativo/buscador-de-documentos-legislativos/ley-reguladora-del-ejercicio-de-la-contaduria

Legislativa, A. (29 de Febrero de 2000). 4. San Salvador, El Salvador.

Legislativa, A. (26 de Octubre de 2015). LEY DE FIRMA ELECTRÓNICA. San Salvador.

Legislativa, A. (26 de Febrero de 2015). Ley especial contra delitos informáticos y conexos. San Salvador.

Legislativa, A. (25 de mayo de 2017). Ley de propiedad intelectual. San Salvador.

Naranjo, A. (06 de 07 de 2005). *galeon.com.* Obtenido de anaranjo.galeon.com/: http://anaranjo.galeon.com/

NTS ISO/IEC 27002; 2013; Organismo Salvadoreño de Normalización. (2013). Tecnologia de Información. *Tecnologia de Información*. El Salvador, San Salvador: Organismo Salvadoreño de Normalización.

Solís, P. (15 de julio de 2013). *elsalvador.com*. Recuperado el abril de 23 de 2017, de http://www.elsalvador.com/noticias/negocios/109627/

ANEXOS

ÍNDICE DE ANEXOS

ANEXO 1 - Encuesta de uso didáctico

ANEXO 2 - Tabulación de resultados

ANEXO N° 1

UNIVERSIDAD DE EL SALVADOR

FACULTAD DE CIENCIAS ECONÓMICAS

ESCUELA DE CONTADURÍA PÚBLICA

Encuesta de uso didáctico

Proyecto de investigación: Manual de procedimientos de auditoría de sistemas basado en la norma ISO 27002:2013, orientado a Organizaciones no Gubernamentales que ejecutan proyectos de educación**."**

Dirigida a: los contadores debidamente inscritos en el Consejo de Vigilancia de la Profesión de Contaduría Pública y Auditoría.

Objetivo de la encuesta: Conocer si los contadores que ejercen la función de auditoría de sistemas cuentan con un manual de procedimientos basados en la norma ISO 27002:2013, aplicables en Organizaciones no Gubernamentales que ejecutan proyectos de educación.

Indicaciones: marque con una "X" la respuesta o respuestas que considere conveniente ya que en algunas preguntas puede elegir más de una.

A.6 Dispositivos móviles y trabajo remoto

(Si responde que "No" pasar a la pregunta 3)

1. ¿Las ONG`s cuentan con políticas de seguridad para el uso de dispositivos móviles en conexiones de acceso remoto?

Objetivo: Conocer el grado de seguridad que poseen las organizaciones sobre las conexiones de dispositivos móviles, y los sistemas de información.

Sí ☐

No ☐

2. ¿Cuáles de los siguientes controles aplica la organización para el uso de dispositivos móviles de acceso remoto? *(Ref. A 6.2. Dispositivos móviles y trabajo remoto,Pág. 372 CISA, DSS05.03)*

Objetivo: Conocer si en la ONG se han implementado controles que mitiguen riesgos de seguridad de la información, por el uso de dispositivos móviles.

- Borrado y bloqueo remoto ☐
- Cumplimiento de requerimientos de seguridad ☐
- Registro de dispositivos móviles ☐
- Autenticación, autorización y responsabilidad en la red ☐
- Rastreo por geolocalización ☐
- Respaldo remoto seguro ☐
- Borrado y bloqueo remoto de acceso a dispositivos móviles ☐

3. ¿Qué medidas de seguridad son aplicadas para el control de acceso a las instalaciones? *(Ref. A. 9 Control de Acceso ISO 27002:2013)*

Objetivo: Conocer el grado de fortalecimiento en seguridad que poseen las organizaciones mediante el uso de técnicas de control para el acceso a las instalaciones por parte de personal externo.

- Personal de seguridad (vigilancia) ☐
- Video vigilancia ☐
- Tarjetas de acceso ☐
- Reconocimiento de voz ☐
- Huella dactilar ☐

4. ¿Cuáles de los siguientes controles de comunicación implementan? (*A. 13.1 Gestión de seguridad de red ISO 27002:2013 CISA 5.4 pág. 377 DSS05.02)*

Objetivo: Investigar sobre el nivel de seguridad que se lleva a cabo dentro de la organización, al manipular información mediante la red de comunicación interna.

Las funciones deben ser realizadas por operadores con capacitación	☐
Las funciones deben ser rotadas periódicamente si es posible	☐
El software de control debe restringir funciones de eliminar registros	☐
Las pistas de auditoría del software deber revisarse periódicamente	☐
Los protocolos de operación deben ser documentados	☐
Llevar a cabo análisis de equilibrio de sistema	☐
El software debe mantener un archivo de identificación de terminales	☐

A.7 Seguridad de los recursos humanos

5. Cuando se termina el contrato de un empleado, ¿Cuáles de los siguientes derechos de acceso se deniegan? *(Ref. A 7.3 Terminación y cambio de empleo ISO 27002:2013, Pág. 353 CISA, DSS05.04)*

Objetivo: Identificar las medidas de seguridad y procedimientos de gestión que se implementan para proteger la información, respecto a los empleados que terminan su contrato laboral.

Llaves y tarjetas de identificación	☐
Acceso a documentación	☐
Equipo asignado para el desarrollo de su trabajo	☐

A.12 Seguridad de las operaciones

6. ¿Mantienen respaldos de seguridad de la información de toda la organización? *(Ref. A. 12 Copia de la seguridad de la información, ISO 27002:2013)*

Objetivo: Indagar si la organización implementa la práctica de resguardo de información mediante copias de seguridad para prevenir la perdida de datos.

Sí ☐

No ☐

7. ¿La organización cuenta con un área segura para el resguardo de los respaldos de información? *(Ref. A. 12 Copia de la seguridad de la información, ISO 27002:2013)*

Objetivo: Conocer si la organización comprende lo importante que es tener un área de resguardo de la información para que los respaldos realizados no se dañen si la fuente de información principal sufre algún incidente.

Sí ☐

No ☐

A.12 Registro y Monitoreo

8. ¿Implementan un registro de eventos de las actividades de los usuarios dentro de la organización? *(Ref. A. 12.4.1 Registro de eventos, ISO 27002:2013)*

Objetivo: Conocer si las organizaciones monitorean las actividades de los usuarios de tal manera que puedan generar evidencia de auditoría.

Sí ☐

No ☐

9. ¿Mantienen en un lugar seguro el registro de eventos de actividades de los usuarios? *(Ref. A. 12.4.2 Protección de la bitácora de información, ISO 27002:2013)*

Objetivo: Conocer si la organización cuenta con la debida protección ante la manipulación indebida y acceso no autorizado a la bitácora de información.

Sí ☐

No ☐

10. ¿Utilizan software con licencia para el ingreso de los datos que se procesan dentro del sistema de información de la organización? *(Ref. A. 12.2.1 Controles contra software malicioso)*

Objetivo: Indagar sobre el uso de software autorizado dentro de la organización de manera que se evite el ingreso de usuarios no permitidos por medio de software malicioso.

Sí ☐

No ☐

11. ¿Cuenta con autorización previa para el ingreso de los datos los sistemas de información? *(Ref. A. 12. Seguridad de las operaciones)*

Objetivo: Verificar que la información existente dentro de los sistemas informáticos de la organización, ha sido previamente revisada para su autorización de manera que el ingreso sea definitivo.

Sí ☐

No ☐

A.13 Seguridad de las comunicaciones

12. ¿Implementan en su organización controles de seguridad para el manejo de información?*(Ref. A. 13.1 Gestión de seguridad de red, ISO 27002:2013, CISA 5.4.4 pág. 383 DSS05.02)*

Objetivo: Conocer sobre la existencia de controles para asegurar la protección de la información en redes y su soporte a las instalaciones de procesamiento.

Sí ☐

No ☐

13. ¿Cuáles de los siguientes controles de seguridad implementan para el manejo de información?*(Ref. A. 13.1 Gestión de seguridad de red, ISO 27002:2013, CISA 5.4.4 pág. 383 DSS05.02)*

Objetivo: Evaluar los aspectos mediante los cuales una organización pueda desarrollar directrices específicas para sus circunstancias mediante la definición del nivel de controles de seguridad.

Evaluacion de riesgos periodicos ☐

Capacitacion sobre seguridad a los empleados ☐

Estandares de corta fuegos ☐

Estandares de deteccion de intrusos ☐

Gestion de insidentes ☐

Monitore de actividades ☐

Ambiente comun de computadoras ☐

14. ¿Implementan la firma electrónica en la transferencia de información de parte de la organización y el receptor de la transacción?*(Ref. A. 14.1.3 Protección de transacciones de servicios de aplicación)*

Objetivo: Conocer el grado de seguridad aplicado a la información transferida de parte de la organización a un tercero involucrado para prevenir alteración, divulgación o duplicación no autorizada.

Sí ☐

No ☐

15. ¿Hacen uso de la técnica de criptografía en la transferencia de información al utilizar dispositivos móviles?*(Ref. A. 6.2.1 Política de dispositivos móviles)*

Objetivo: Conocer acerca del uso de medidas de seguridad por parte de la organización ante la transferencia de información para asegurar que no es comprometida ante terceros no involucrados.

Sí ☐

No ☐

Cierre cuestionario

16. ¿Considera que la aplicación de procedimientos de auditoría de sistemas le ayudaría a la ONG, a evaluar y saber el estado de la seguridad y el funcionamiento de sus sistemas, para implementar y/o reforzar controles de seguridad?

Objetivo: indagar sobre la utilidad que representa aplicar un manual de procedimientos de auditoría de sistemas basada en la norma ISO 27002:2013 Tecnología de la información. Código de prácticas para la gestión de la seguridad de la información.

Si ☐

No ☐

17. ¿Estaría interesado que en la ONG se auditaran los sistemas de información aplicando procedimientos técnicos, fundamentados en la norma ISO 27002:2013 Tecnología de la información Código de prácticas para la gestión de la seguridad de la información?

Objetivo: Verificar la importancia que representa para las ONG`s cumplir los requerimientos contenidos en la ISO 27002:2013 Tecnología de la información. Código de prácticas para la gestión de la seguridad de la información.

Si ☐

No ☐

ANEXO N° 2

UNIVERSIDAD DE EL SALVADOR

FACULTAD DE CIENCIAS ECONÓMICAS

ESCUELA DE CONTADURÍA PÚBLICA

Encuesta de uso didáctico

Proyecto de investigación:

Manual de procedimientos de auditoría de sistemas basado en la norma ISO 27002:2013, orientado a Organizaciones no Gubernamentales que ejecutan proyectos de educación**."**

Dirigida a:

Los contadores debidamente inscritos en el Consejo de Vigilancia de la Profesión de Contaduría Pública y Auditoría.

Objetivo de la encuesta:

Conocer si los contadores que ejercen la función de auditoría de sistemas cuentan con un manual de procedimientos basados en la norma ISO 27002:2013, aplicables en Organizaciones no Gubernamentales que ejecutan proyectos de educación.

Indicaciones:

Marque con una "X" la respuesta o respuestas que considere conveniente ya que en algunas preguntas puede elegir más de una.

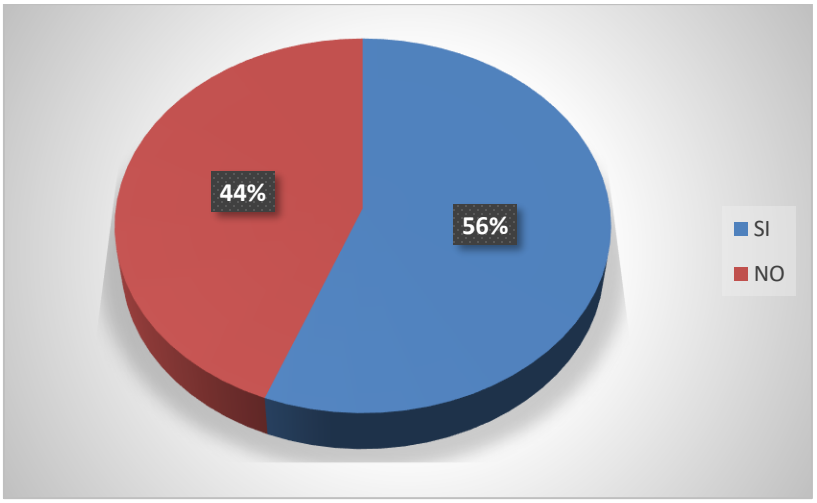
1. ¿Las ONG`s cuentan con políticas de seguridad para el uso de dispositivos móviles en conexiones de acceso remoto?

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Si	19	55,9	55,9	55,9
No	15	44,1	44,1	100,0
Total	34	100,0	100,0	

Políticas de seguridad en dispositivos móviles

Grafico N° 1.

Políticas de seguridad en dispositivos móviles



Análisis e interpretación:

Debido al uso de políticas que contribuyen para la implementación de controles en las organizaciones no gubernamentales, un buen porcentaje de nuestra unidad de estudio hizo notar las buenas prácticas manejadas en estas.

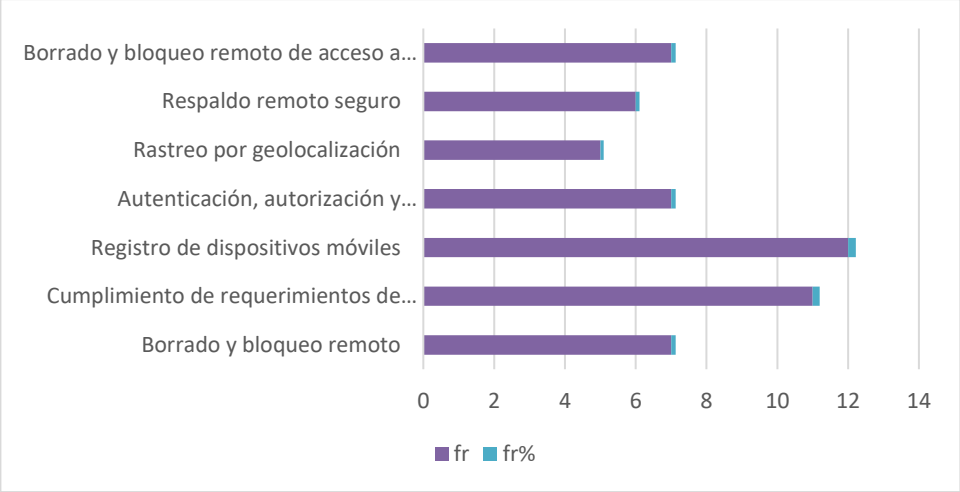
2. ¿Cuáles de los siguientes controles aplica la organización para el uso de dispositivos móviles de acceso remoto?

Tabla N° 2
Controles para el uso de dispositivos móviles de acceso remoto

	Respuestas		Porcentaje de casos
	N	Porcentaje	
Borrado y bloqueo remoto	7	12,7%	38,9%
Cumplimiento de requerimientos de seguridad	11	20,0%	61,1%
Registro de dispositivos móviles	12	21,8%	66,7%
Autenticación, autorización y responsabilidad en la red	7	12,7%	38,9%
Rastreo por geolocalización	5	9,1%	27,8%
Respaldo remoto seguro	6	10,9%	33,3%
Borrado y bloqueo remoto de acceso a dispositivos móviles	7	12,7%	38,9%
Total	55	100,0%	305,6%

Grafico N° 2.

Controles para el uso de dispositivos móviles de acceso remoto



3. ¿Qué medidas de seguridad son aplicadas para el control de acceso a las instalaciones?

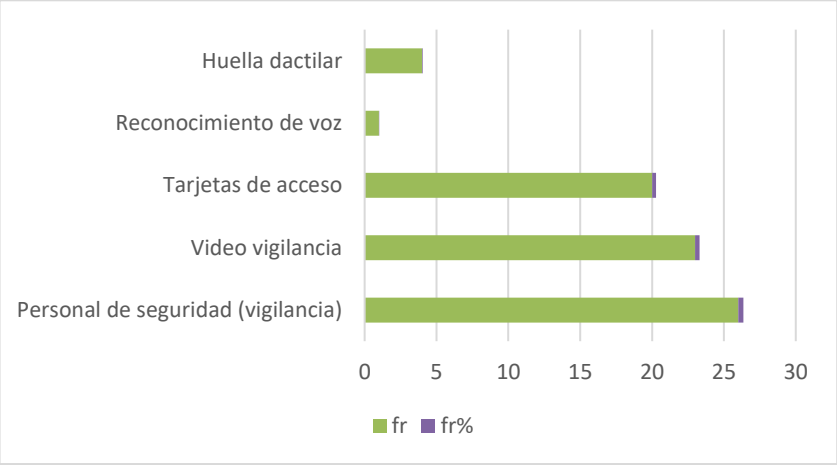
Tabla N° 3

Medidas de seguridad para el control de acceso a las instalaciones.

	Respuestas		Porcentaje de casos
	N	Porcentaje	
Personal de seguridad (vigilancia)	26	40,6%	76,5%
Video Vigilancia	23	35,9%	67,6%
Tarjetas de acceso	10	15,6%	29,4%
Reconocimiento de voz	1	1,6%	2,9%
Huella dactilar	4	6,3%	11,8%
Total	64	100,0%	188,2%

Grafico N° 3.

Medidas de seguridad para el control de acceso a las instalaciones



Análisis e interpretación:

De las medidas de seguridad aplicadas para el control de acceso a las instalaciones en las ONG´s según los auditores encuestados hicieron constar de manera significativa que el personal de seguridad (vigilancia) es el más utilizado; además un dato notorio en el uso de tarjet ` acceso que también es implementado como medida de seguridad para el acceso a la informa

4. ¿Cuáles de los siguientes controles de comunicación implementan?

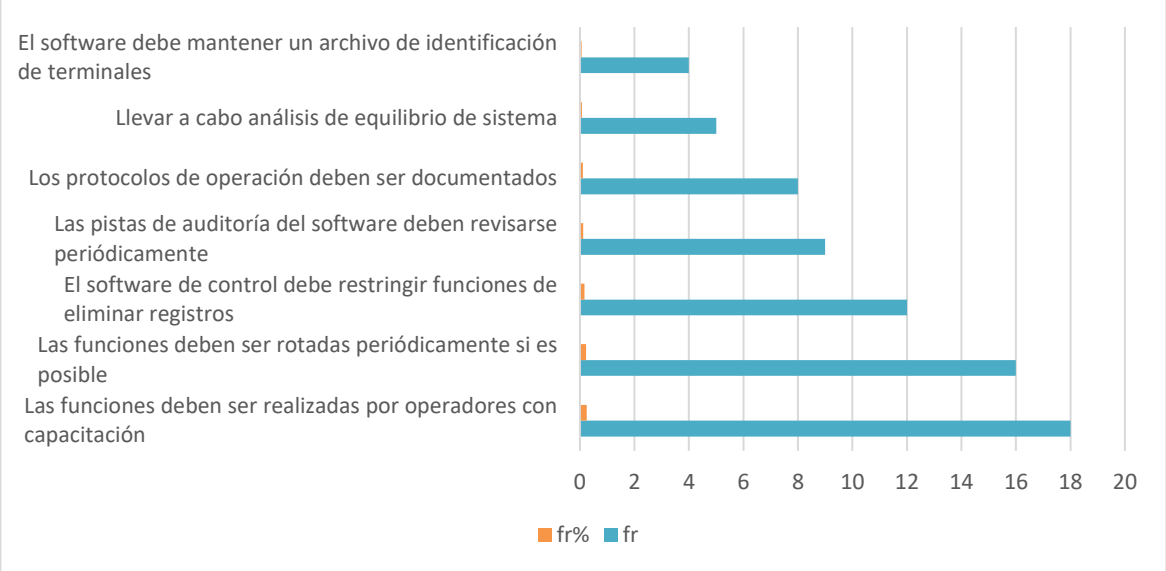
Tabla N° 4.

Controles de comunicación

Pregunta 4	Respuestas		Porcentaje de casos
	N	Porcentaje	
Las funciones deben ser realizadas por operadores con capacitación	18	25,0%	52,9%
Las funciones deben ser rotadas periódicamente si es posible	16	22,2%	47,1%
El software de control debe restringir funciones de eliminar registros	12	16,7%	35,3%
Las pistas de auditoría del software deben revisarse periódicamente	9	12,5%	26,5%
Los protocolos de operación deben ser documentados	8	11,1%	23,5%
Llevar a cabo análisis de equilibrio de sistema	5	6,9%	14,7%
El software debe mantener un archivo de identificación de terminales	4	5,6%	11,8%
Total	72	100,0%	211,8%

Grafico N° 4.

Controles de comunicación



5. Cuando se termina el contrato de un empleado, ¿Cuáles de los siguientes derechos de acceso se deniegan?

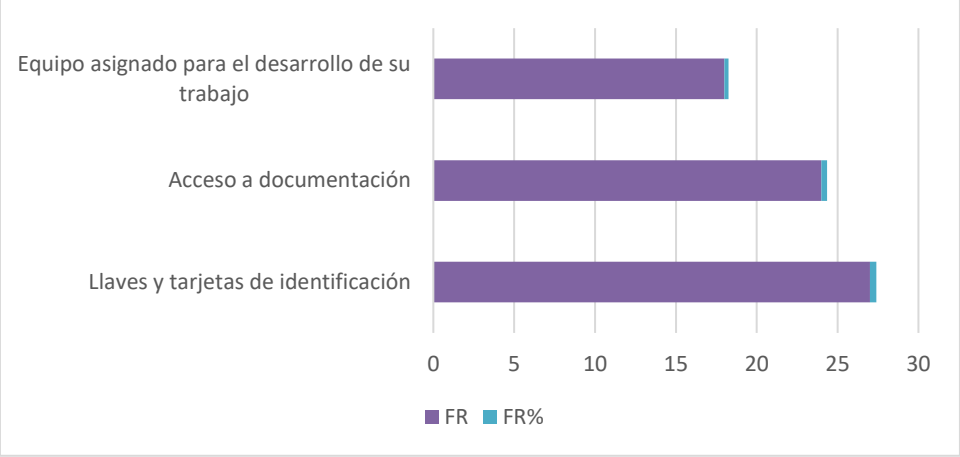
Tabla N° 5.

Derechos al acceso de la información

	Respuestas		Porcentaje de casos
	N	Porcentaje	
Llaves y tarjetas de identificación	27	39,1%	79,4%
Acceso a documentación	24	34,8%	70,6%
Equipo asignado para el desarrollo de su trabajo	18	26,1%	52,9%
Total	69	100,0%	202,9%

Grafico N° 5.

Derechos al acceso de la información



Análisis e interpretación:

Para habilitar la asignación de derechos de acceso se debe implementar un procedimiento formal para la creación y anulación de usuarios, en este caso la denegación de llaves y tarjetas de identificación es una de las más utilizadas, asimismo la prohibición al acceso a la documentación y al equipo asignado.

6. ¿Mantienen respaldos de seguridad de la información de toda la organización?

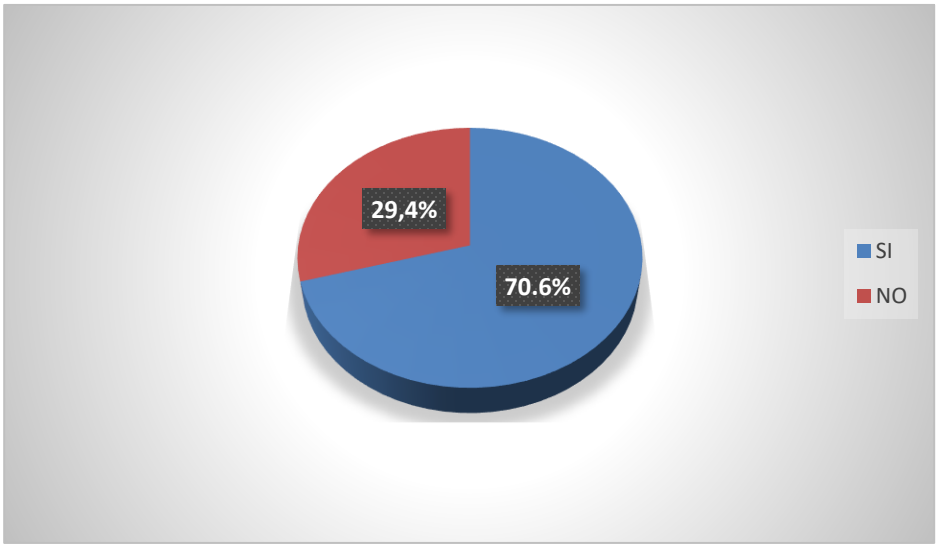
Tabla N° 6.

Respaldo de seguridad de la información

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Sí	24	70,6	70,6	70,6
No	10	29,4	29,4	100,0
Total	34	100,0	100,0	

Grafico N° 6.

Respaldo de seguridad de la información



Análisis e interpretación: Los respaldos en la vida cotidiana de la empresas se ha vuelta la alternativa más común para almacenar y proteger la información más importante contra la perdida de datos, se deben hacer copias de seguridad de software e imágenes del sistemas y probarlas periódicamente, establecer una política para definir los requisitos de la organización para las copias y proporcionar las instalación adecuada para garantizar que la información esencial se puede recuperar después de un desastres.

7. ¿La organización cuenta con un área segura para el resguardo de los respaldos de información?

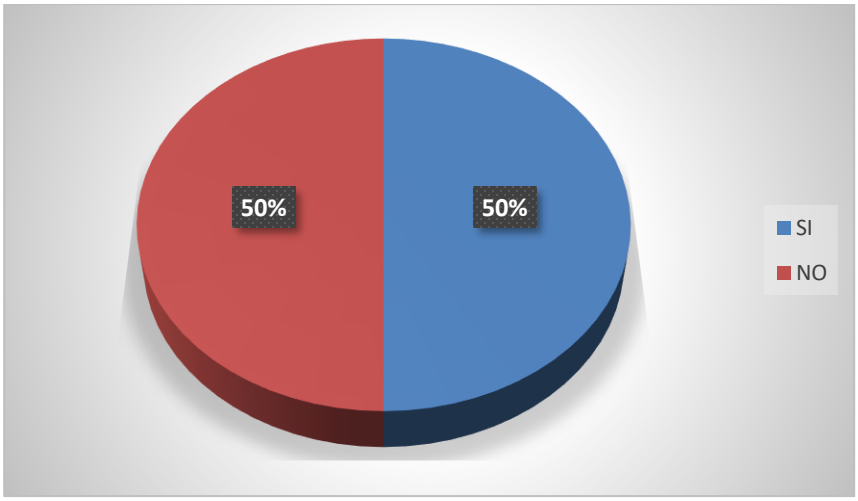
Tabla N° 7.

Áreas de resguardo para los respaldos de la información

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Si	17	50,0	50,0	50,0
No	17	50,0	50,0	100,0
Total	34	100,0	100,0	

Grafico N° 7.

Áreas de resguardo para los respaldos de la información



Análisis e interpretación:

Nuestras unidades en estudio coincidieron en que las Organizaciones no gubernamentales puedo o no contar con buenos lugares para resguardar de manera segura los respaldos efectuados en fechas anteriores.

8. ¿Implementan un registro de eventos de las actividades de los usuarios dentro de la organización?

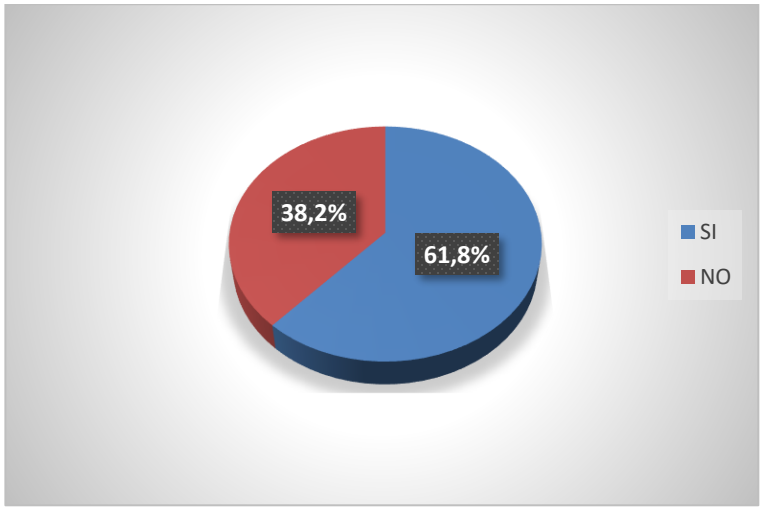
Tabla N° 8.

Registro de eventos de actividades

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Sí	21	61,8	61,8	61,8
No	13	38,2	38,2	100,0
Total	34	100,0	100,0	

Grafico N° 8.

Registro de eventos de actividades



Análisis e interpretación: El registro de eventos, se deben producir, mantener y revisar periódicamente. Los registros de eventos pueden contener datos confidenciales e información de identificación personal, siempre que sea posible, los administradores de los sistemas no deben tener permisos para borrar o desactivar los registros de sus propias actividades, según valoraciones hechas por las unidades de estudio.

9. ¿Mantienen en un lugar seguro el registro de eventos de actividades de los usuarios?

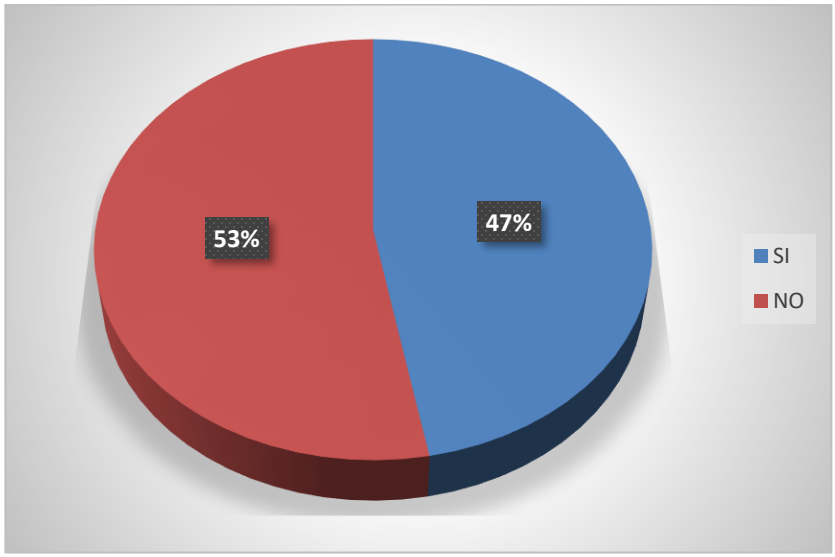
Tabla N° 9.

Protección de la bitácora de información

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Si	16	47,1	47,1	47,1
No	18	52,9	52,9	100,0
Total	34	100,0	100,0	

Grafico N° 9.

Protección de la bitácora de información



Análisis e interpretación:

Un poco más de la mitad de los auditores encuestados hacen notar que las organizaciones no gubernamentales no mantienen sus registros de eventos de las actividades efectuadas por los usuarios en lugares seguros.

10. ¿Utilizan software con licencia para el ingreso de los datos que se procesan dentro del sistema de información de la organización?

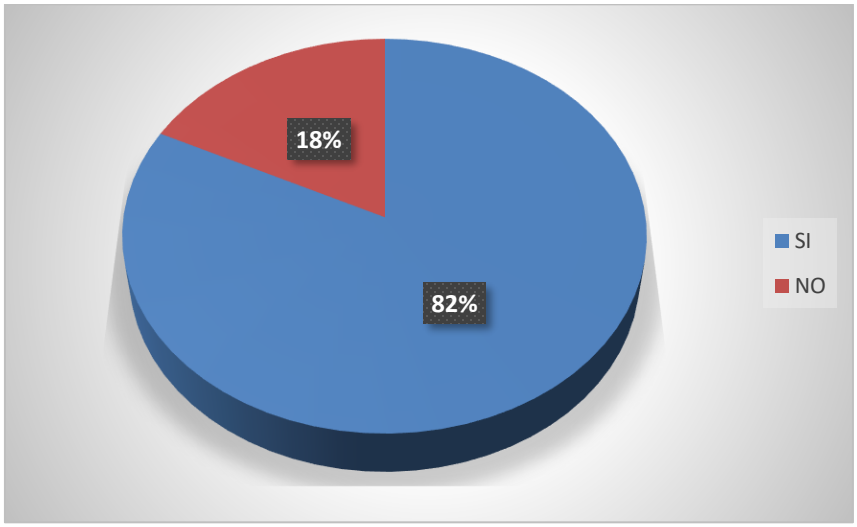
Tabla N° 10.

Legalidad de los Software

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Sí	28	82,4	82,4	82,4
No	6	17,6	17,6	100,0
Total	34	100,0	100,0	

Grafico N° 10.

Legalidad de los Software



Análisis e interpretación: La mayoría de los auditores encuestados coinciden que las ONG´s son entidades que no cuentan con software legales, esto hace que la información sea más vulnerable para estas. Se realizan buenas prácticas dentro de las instalaciones como por ejemplo la ejecución de respaldos periódicos, pero esto no bloquea que el software de “x” compañía pueda ser víctima de un ataque cibernético por un tercero.

11. ¿Cuenta con autorización previa para el ingreso de los datos los sistemas de información?

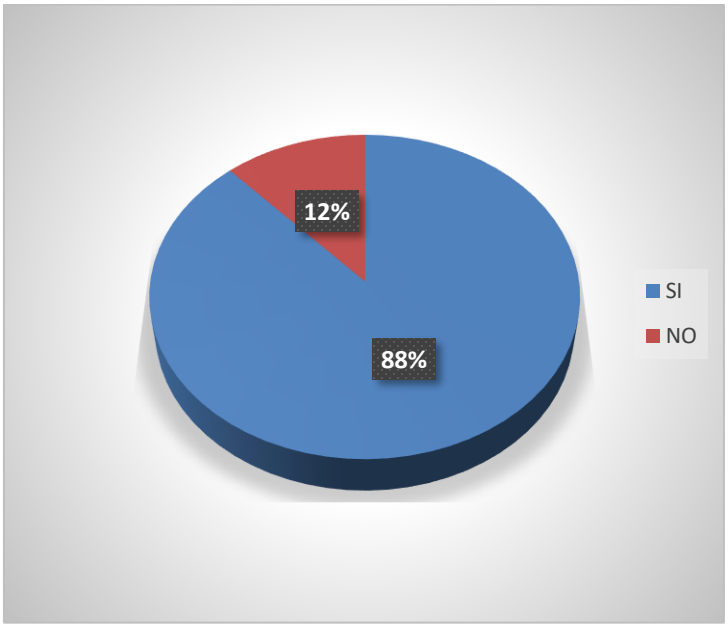
Tabla N° 11.

Seguridad de las operaciones

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Sí	30	88,2	88,2	88,2
No	4	11,8	11,8	100,0
Total	34	100,0	100,0	

Grafico N° 11.

Seguridad de las operaciones



Análisis e interpretación:

Los encuestados acertaron casi en su totalidad de que las empresas en su mayoría cuentan con filtros de entradas, tanto como primer acceso al sistema de información, así como la solicitud de identificación de usuarios para cada software, siendo esto lo más adecuado para mantener protegido la información.

12. ¿Implementan en su organización controles de seguridad para el manejo de información?

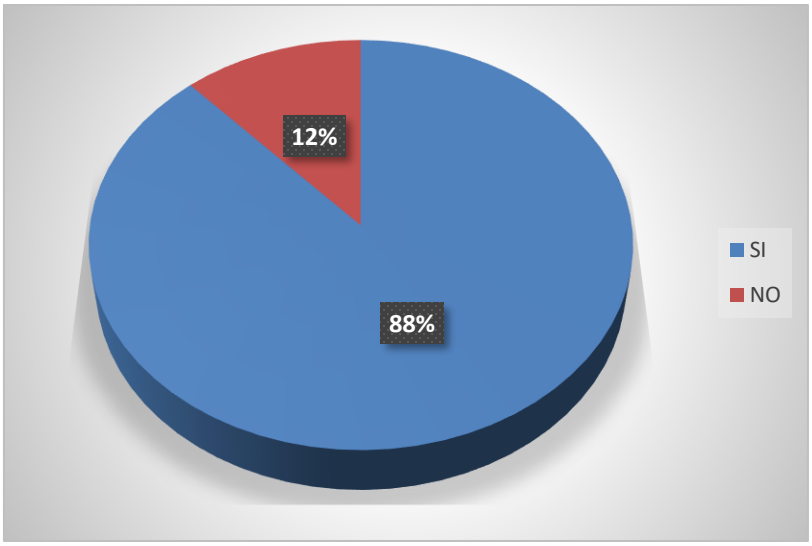
Tabla N° 12.

Controles de seguridad para el manejo de la información

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Sí	30	88,2	88,2	88,2
No	4	11,8	11,8	100,0
Total	34	100,0	100,0	

Grafico N° 12.

Controles de seguridad para el manejo de la información



Análisis e interpretación:

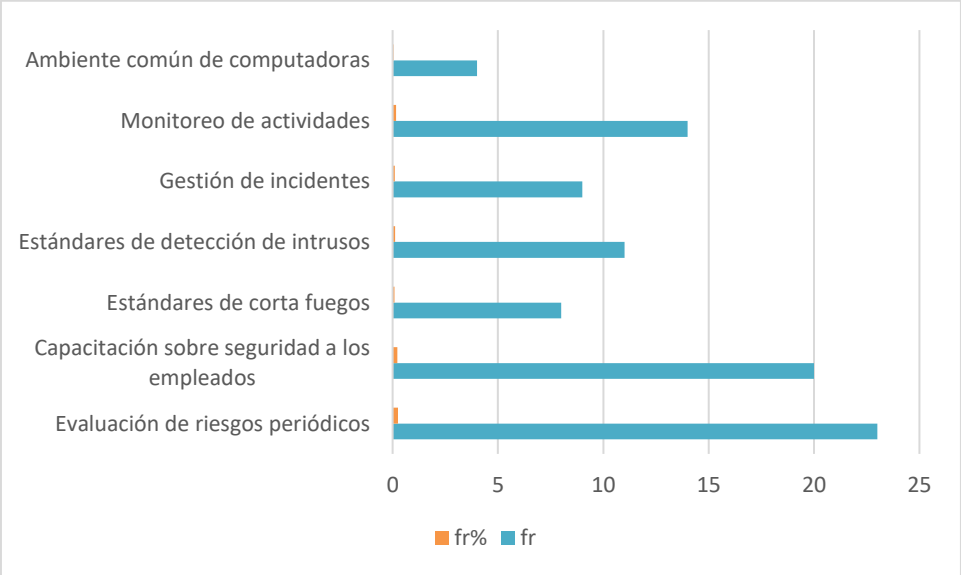
El manejo de controles es fundamental para mantener resguardada la información en este tipo de entidades, cabe mencionar que el uso de políticas contribuye para la implementación de controles, a lo cual según el estudio de campo efectuado se refleja en 88% de auditores encuestados que si se implementan controles de seguridad.

13. ¿Cuáles de los siguientes controles de seguridad implementan para el manejo de información?

Gestión de seguridad de red

	Respuestas		Porcentaje de casos
	N	Porcentaje	
Evaluación de riesgos periódicos	23	25,8%	67,6%
Capacitación sobre seguridad a los empleados	20	22,5%	58,8%
Estándares de corta fuegos	8	9,0%	23,5%
Estándares de detección de intrusos	11	12,4%	32,4%
Gestión de incidentes	9	10,1%	26,5%
Monitoreo de actividades	14	15,7%	41,2%
Ambiente común de computadoras	4	4,5%	11,8%
Total	89	100,0%	261,8%

Gestión de seguridad de red



Análisis e interpretación:

De los 34 auditores encuestados 23 coincidieron que la evaluación de riesgos periódicos dentro de las entidades en el más utilizado para evaluar los niveles de seguridad y la eficacia de los controles implementados.

14. ¿Implementan la firma electrónica en la transferencia de información de parte de la organización y el receptor de la transacción?

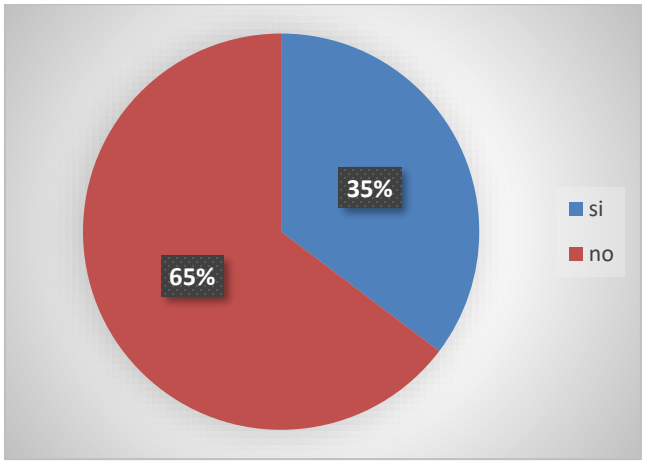
Tabla N° 14.

Firma electrónica

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Sí	12	35,3	35,3	35,3
No	22	64,7	64,7	100,0
Total	34	100,0	100,0	

Grafico N° 14.

Firma electrónica



Análisis e interpretación

Del total de los auditores encuestados un 65% afirmaron que las instituciones no hacen uso de la firma electrónica para dejar un registro de eventos o actividades entre los usuarios e identificar quien realiza tal acción.

15. ¿Hacen uso de la técnica de criptografía en la transferencia de información al utilizar dispositivos móviles?

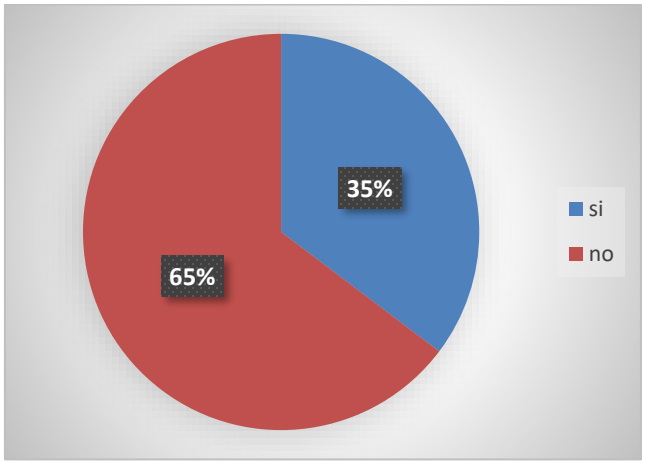
Tabla N° 15.

Criptografía

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Sí	6	17,6	17,6	17,6
No	28	82,4	82,4	100,0
Total	34	100,0	100,0	

Grafico N° 15.

Criptografía



Análisis e interpretación

La mayoría de los auditores encuestados hicieron constar que el uso de la criptografía en este tipo de organizaciones no es empleado muy frecuentemente para el resguardo y protección de la información.

16. ¿Considera que la aplicación de procedimientos de auditoría de sistemas le ayudaría a la ONG, a evaluar y saber el estado de la seguridad y el funcionamiento de sus sistemas, para implementar y/o reforzar controles de seguridad?

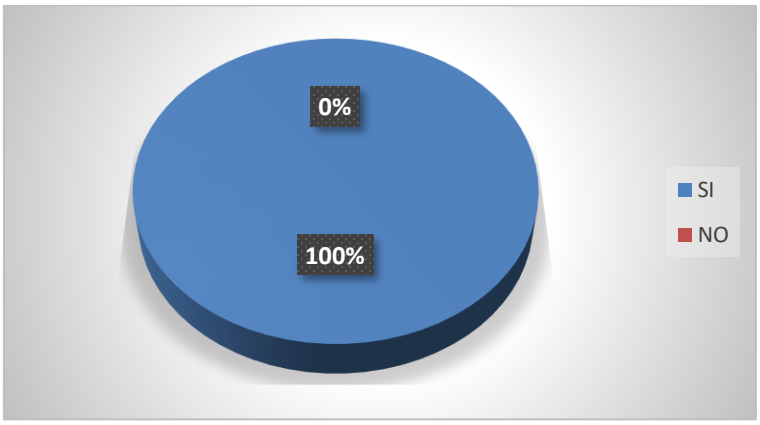
Tabla N° 16.

Considera de beneficio implementar procesamiento de auditoría

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Si	34	100,0	100,0	100,0

Grafico N° 16.

Considera de beneficio implementar procesamiento de auditoría



Análisis e interpretación:

En un 100% de los auditores encuestados afirmaron que la aplicación de procedimientos de auditoría le ayudaría en gran manera para la evaluación y conocer del funcionamiento de sus sistemas, para implementar y/o reforzar controles de seguridad dentro de las ONG´s.

17. ¿Estaría interesado que en la ONG se auditaran los sistemas de información aplicando procedimientos técnicos, fundamentados en la norma ISO 27002:2013 Tecnología de la información código de prácticas para la gestión de la seguridad de la información?

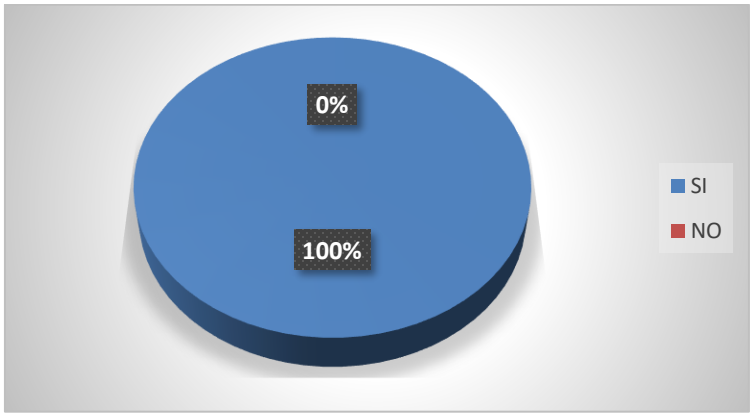
Tabla N° 17.

Muestra interés en nuevos procedimientos implementando la norma ISO 27002:2013 Tecnología de la información

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Sí	34	100,0	100,0	100,0

Grafico N° 17.

Muestra interés en nuevos procedimientos implementando la norma ISO 27002:2013 Tecnología de la información



Análisis e interpretación: El 100% lo auditores encuestados mostraron interés en la creación de un manual de procedimientos de auditoría de sistemas basado en la NTS ISO/IEC 270012:2013 aplicado a organizaciones no gubernamentales ya que les facilitara en gran medida la evaluación en este tipo de entidades.