UNIVERSIDAD DE EL SALVADOR

FACULTAD DE CIENCIAS ECONÓMICAS

ESCUELA DE CONTADURÍA PÚBLICA

"SISTEMA DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA ISO 27000, APLICADO A LAS ORGANIZACIONES NO GUBERNAMENTALES DE EL SALVADOR"

Trabajo de Investigación Presentado por:

ARIAS VALLADARES, ELSI
PORTILLO ORELLANA, CLAUDIA CAROLINA
VÁSQUEZ PREZA, JENMI BEATRIZ

PARA OPTAR EL GRADO DE:

LICENCIADA EN CONTADURIA PUBLICA

Septiembre 2016

San Salvador, El Salvador, Centro América

UNIVERSIDAD DE EL SALVADOR

AUTORIDADES UNIVERSITARIAS

Rector:	Licenciado José Luis Argueta Antillón
Secretaria:	Doctora Ana Leticia Zavaleta de Amaya
Decano de la Facultad de Ciencias Económicas:	Licenciado Nixon Rogelio Hernández Vásquez
Secretaria de la Facultad de Ciencias Económicas:	Licenciada Vilma Marisol Mejía Trujillo
Directora de la Escuela de Contaduría Pública:	Licenciada María Margarita de Jesús Martínez Mendoza de Hernández
Coordinado General de Procesos de graduación Facultad de Ciencias Económicas	Licenciado Mauricio Ernesto Magaña Menéndez
Coordinador de Seminario:	Licenciado Daniel Nehemías Reyes López
Docente Director	Licenciada María Elena Vidal de Serpas
Jurado Examinador:	Licenciada María Elena Vidal de Serpas Licenciado Mauricio Ernesto Magaña Menéndez Licenciado Henry Amílcar Marroquín

Septiembre 2016

San Salvador, El Salvador, Centroamérica

AGRADECIMIENTOS

Gracias Dios por haberme acompañado en este proceso lo cual no fue fácil desde el inicio, pero Tú me distes la fuerza y ánimos para continuar, a cada persona que me acompaña en este camino hacia Ti. Al Licenciado Mauricio Ernesto Magaña Menéndez por el tiempo que nos dedicó.

Elsi Arias Valladares

Gracias doy primeramente a Dios por su ayuda incondicional, siendo el pilar que me ha sostenido hasta este momento, también agradezco enormemente a mi familia, mi madre y mi hermana que fueron parte de este proceso, y que siempre creyeron en mi capacidad de finalizar este larga carrera.

Claudia Carolina Portillo Orellana

Gracias a Dios por su fidelidad a lo largo de este proceso, a mi mamá por su esfuerzo y apoyo incondicional, a mis abuelos por siempre creer en mí y al Licenciado Mauricio Ernesto Magaña Menéndez por el tiempo que dedico para revisar nuestro trabajo.

Jenmi Beatriz Vásquez Preza

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍDICE DE ANEXOS

Anexo N° 14 Acuerdo de intercambio de información

Anexo N° 15 Reporte y seguimientos de incidentes de seguridad

Anexo N° 16 Detalle de dominios de aplicación para el tratamiento y mitigación de los riesgos

RESUMEN EJECUTIVO

Las Organizaciones No Gubernamentales son instituciones sin fines de lucro, su origen en el país fue a partir de los años 80 con el interés de brindar soluciones de alternativa para el desarrollo de la democracia y combatir la pobreza.

Fue hasta la firma de los acuerdo de paz que tomaron mayor auge y han sido reconocidas en el país como parte del desarrollo económico; por tal razón se estableció la Ley de Asociaciones y Fundaciones sin Fines de Lucro.

Actualmente han sufrido cambios sustanciales para su regulación ya que deben de cumplir con un marco jurídico para su funcionamiento y evitar el lavado de dinero, por lo que asumen un papel fundamental en la economía del país y a su vez el cumplimiento de los objetivos en el desarrollo de cada proyecto ejecutado así mismo también con sus principales donantes, por lo que la información que se procesa a nivel de sistema contable, los equipos informáticos, infraestructura, sus bases de datos, y el personal forman parte de un conjunto de activos para las ONG's; por lo que nace la pregunta que tipos de medidas de seguridad poseen para proteger la información; ya que las tecnologías de información han evolucionado a lo largo del tiempo y cabe mencionar que se debe de proteger todo lo que está en torno al funcionamiento de las ONG, ya que dichos recursos son de vital importancia y debe de ser protegida porque poseen riesgos inherentes internos y externo como el robo o divulgación afectando de forma directa la continuidad de la organización.

Por lo que en la presente investigación brindará una herramienta la cual consiste en la elaboración de un sistema de seguridad de información en base a la ISO

27000, dicho sistema será aplicado a las ONG's que les servirá como instrumento que ayudara a mitigar los riesgos y controlarlos, la propuesta contiene del desarrollo del caso práctico aplicada a la Fundación un Futuro Mejor, se ha desarrollado también el sistema de seguridad de información lo cual está compuesta por la elaboración de la política, formularios de aplicación para la ejecución del sistema cuando ya está el desarrollo de la implementación. .

Y para realizar dicho sistema, se ha trabajado en base a la técnica de investigación hipotética deductiva a través de un estudio de tipo descriptivo, utilizando la herramienta y técnica para la recolección de información de campo se usó el cuestionario, el cual brindó los conocimientos necesarios para realizar el análisis y la evaluación de la necesidad que tienen las ONG's de un sistema de seguridad de información.

Las ONG's, en su mayoría no cuentan con políticas documentadas que les ayuden a proteger la información que se procesa dentro de sus instalaciones y para el personal, no tienen un programa de capacitaciones para la concientización y socialización de sus políticas, y para ello necesitan desarrollar y poner en marcha una cultura organizacional de protección a los activos.

Es importante mencionar que la continuidad de toda una organización depende también del buen manejo de los datos y confidencialidad por parte de los involucrados, ya que la manipulación adecuada por parte del personal interno evitará la exposición ante ataques externos que pueden dañar la integridad de la organización, por tal razón es de vital importancia generar una cultura de prevención y protección de los activos.

INTRODUCCIÒN

En la actualidad, para muchas entidades, la información es uno de los activos más valiosos, ya sea que esté almacenada en medios digitales o físicos, es uno de los pilares fundamentales mediante el cual giran sus operaciones, por esta razón debe estar protegida y garantizar su fiabilidad. Se considera necesaria la implementación de controles adecuados que permitan prevenir daños o riesgos que afecten la confidencialidad, integridad y disponibilidad de la misma.

La seguridad de la información, conlleva a la implementación de una serie de medidas técnicas, organizacionales y legales que abarcan no solo los datos sino también los medios o sistemas que se utilizan para procesarlos y almacenarlos.

Un sistema de seguridad de la información es una herramienta que provee a las entidades un modelo a seguir, que permite establecer, implementar, operar, monitorear, revisar, mantener y mejorar la protección de la información y los sistemas de procesamiento de datos. Ante las amenazas de todo tipo ya sea, pérdida de información, robo, manipulación, entre otros riesgos graves a las que a diario se enfrentan las Organizaciones No Gubernamentales del país, surge la necesidad de la elaboración de un sistema que contenga políticas y procedimientos que faciliten a las organizaciones llevar de manera ordenada y registrada la documentación y registros confidenciales, pero principalmente, garantizar la seguridad a este activo y mitigar riesgos que podrían representar pérdidas graves a las organizaciones.

Para su desarrollo, el trabajo está dividido en cuatro capítulos, en el capítulo I, primeramente se conocen los antecedentes de las ONG´s, también se detallan los aspectos más importantes sobre la seguridad de la información, definiendo a la vez los tipos de riesgos y amenazas que a diario están expuestas estas entidades, seguidamente se establece un marco técnico donde se puede apreciar la normativa aplicada a este tema, y por último se define la base legal, que son las regulaciones establecidas para estas entidades.

En el capítulo II, se plantea la metodología implementada para la obtención de los resultados necesarios que darán la pauta para proponer soluciones, además, en este capítulo, se conocen las unidades de estudio y los métodos utilizados para recabar la información suficiente para establecer los respectivos análisis a la problemática.

En el presente trabajo de investigación ofrece una herramienta novedosa y útil para las Organizaciones No Gubernamental y que puede ser aplicado a cualquier organización sin importar el tamaño o naturaleza, con los resultados obtenidos del capítulo II se logró conocer la necesidad de proteger los activos informáticos y se procede a elaborar el capítulo III donde se desarrolla la propuesta que consiste en la elaboración un sistema de seguridad de información para que ayude a mitigar los riesgos, dar seguimiento a los incidente y controlar las nuevas vulnerabilidades

Y por último está el capítulo IV, después de haber hecho un estudio minucioso con la información obtenida directamente de las unidades de análisis, se establecen las

respectivas conclusiones y recomendaciones, ante los resultados obtenidos en la investigación.

CAPÍTULO I: MARCO TEÓRICO, CONCEPTUAL, TÉCNICO Y LEGAL

1.1 Antecedentes

1.1.1 Antecedentes internacionales de las Organizaciones No Gubernamentales

El término de organizaciones no gubernamentales se le asigna a las instituciones sin fines de lucro, su origen fue a través de iniciativas civiles y no están ligadas al Estado, su impulso es altruista a favor de los sectores más vulnerables. Este tipo de organizaciones ha estado presente desde mediados del siglo XIX, en 1840 se reunieron para realizar la Convención Mundial contra la Esclavitud, que provocó que finalizara el comercio de esclavos a nivel internacional.

En 1909 existían más de 200 ONG´s registradas a nivel internacional, que desempeñaban un papel más oficial en cuerpos internacionales como las Naciones Unidas (ONU), la Organización para la Seguridad y el Desarrollo y la Unión Europea. También son organizaciones efectivas y que disponen un apoyo económico ya que sus actividades permiten influir en las políticas nacionales y multiláteras, por lo que adquieren cada vez más protagonismo. Estas organizaciones también se ocupan de una gran variedad de actividades como intercambios científicos, religión, educación y ayuda humanitaria entre otras acciones; cabe mencionar que las organizaciones que han incrementado este fenómeno de apoyo son: Las Juntas Pugwash sobre Ciencia y Asuntos Mundiales, el movimiento internacional de los Boy Scouts, la Ayuda Cristiana y la Cruz Roja Internacional. (Universia.net).

1.1.2 Antecedentes nacionales de las Organizaciones no Gubernamentales y su entorno en El Salvador

El origen en la región Centroamérica se relaciona con la integración del Mercado Común Centroamericano y la guerra entre El Salvador y Honduras, se inició en los años sesenta a raíz del conflicto armado y la falta de capacidad del Estado para atender las necesidades primordiales de la población como es la salud pública, educación y la producción; en dicha época para el Estado lo primordial era la lucha contra los insurgentes políticos, y durante este proceso que atravesaba el país se violaron los derechos humanos, generando en la sociedad civil la necesidad de organizarse.

La iglesia católica jugó un papel muy importante dentro de su desarrollo, ya que en el año 1960, y según por la práctica de la orientación pastoral del Concilio Vaticano II, los movimientos de acciones católica fueron los primeros impulsadores y luego los campesinos con la fundación de FUNPROCOOP y en 1968 se fundó por iniciativa de la iglesia, FUNDASAL (Fundación de vivienda mínima) y en 1969 La asociación de Fe y Alegría.

En la década de los años 80 surgieron más de estas instituciones, bajo un interés muy evidente, la búsqueda de soluciones para asegurar el rumbo de las transacciones hacia una democracia amplia, un marco de seguridad ciudadana, los derechos humanos, mejores condiciones para batallar contra la pobreza y encontrar nuevas opciones para un progreso humano más digno y sostenible.

Después de la firma de los Acuerdos de Paz en 1992, se desplegaron nuevas condiciones y espacios para la operación de este tipo de organizaciones sin fines de lucro, las cuales crecieron cuantitativa y cualitativamente en estos años, adoptando papeles de asistencia social, desarrollo e integración con las comunidades, pero a la vez exigiendo al Estado el cumplimiento, tanto de los derechos humanos individuales, económicos, sociales y culturales.

A continuación se define lo que caracteriza a este tipo de instituciones:

> "Organización de personas desvinculadas a las esferas gubernamentales que busca en general, alcanzar un fin benéfico público, nacional, ya sea con reconocimiento legal como persona jurídica o no. Está descartado por consiguiente el lucro, el proselitismo político o religión, y el interés gremial como preocupación principal de estas asociaciones, lo que no quiere decir que sean totalmente ajenas a estos temas sociales. " Según el (Tobar, 1998)

Es decir que estas organizaciones propias formadas por miembros de la misma sociedad, generalmente no buscan el lucro económico para sus miembros sino un beneficio altruista en diferentes etapas de la vida social, se dedican específicamente al diseño, estudio y desarrollo de programas y proyectos de desarrollo para sectores populares.

Para realizar los proyectos de ayuda humanitaria es necesario contar con apoyo financiero, por lo que algunas son auto sostenibles y a la vez gestionan fondos

con organismos internacionales tales como Unión Europea, Cooperación AECID, y USAID entre otros que ayudan a los países más pobres.

En El Salvador también existen ONG s que son de origen extranjero y que ejecutan proyectos con fondos internacionales entre ellas se encuentra Plan Internacional, CRS, Asociación Cesal, Save the Children; actualmente existen en el país más de 120 Organizaciones no Gubernamentales que ayudan al desarrollo de la economía.

Las ONGs han sido reconocidas por el gobierno como instituciones con propósito benéfico para la población por esa razón se estableció una Ley que rigiera la constitución y su permanencia operativa, lo cual entro en vigencia en diciembre de 1996 según decreto de Ley de Asociaciones y Fundaciones sin fines de lucro (Tobar, 1998)

Actualmente enfrentan cambios y exigencias sustanciales para el funcionamiento, ya que tienen que cumplir con un marco jurídico que rige dichas organizaciones con el objetivo de evitar el lavado de dinero, por lo que están comprometidas a asumir un papel profesional, científico, objetivo y eficaz que exigen la capacidad técnica, habilidades gerenciales y resultados concretos de las actividades realizadas durante el periodo de ejecución, también están obligadas a presentar un juego completo de Estados Financieros al cierre de cada año, lo cual tienen que ser presentados el último día hábil del mes de febrero de cada año , la legalización de libros contables, sistema contables son autorizadas en el Ministerio de

Gobernación y el cumplimiento de obligaciones formales en el Ministerio de Hacienda. Se declara el origen de los fondos por medio del informe de donaciones, estado de origen y aplicación de fondos, declaración de pago a cuenta para reportar las retenciones laborales y profesionales de los impuestos, no están obligadas a pagar el anticipo a cuenta ni el impuesto sobre las ganancias del periodo fiscal.

1.1.3 Antecedentes de la seguridad de la información

La seguridad de la información ha cobrado relevancia desde tiempos antiguos y a la fecha dentro del ámbito informático; al hablar de este tema conlleva a toda una estructura organizativa interna de las instituciones ya que cada día se hace necesario evaluar la importancia de asegurar este activo tan valioso, al analizar los cambios que han sufrido desde que se introdujeron las primeras redes de computadora, las organizaciones guardaban todos los datos en formato físico, contaban con bodegas llenas de grandes archivos en papel; sin embargo, este sistema de resguardo también presentaba amenazas por desastres naturales, inundaciones, incendios y robo siendo esto muy difícil de controlar.

Con el surgimiento de las computadoras y sistemas de red, se agilizó el procesamiento de datos y la digitalización de los documentos, por lo que toda la información procesada se puede resguardar en un disco duro, disminuyendo el espacio físico y facilitando su divulgación.

Fue en los años 80 cuando las computadoras iniciaron con mayor auge, a partir de dicha época surge la preocupación por proteger los activos que procesaban información importante y su integridad de almacenamiento ya que a partir del año 90 empiezan a surgir las nuevas amenazas.

Para poder garantizar protección a la información, se deben involucrar diferentes aspectos técnicos, legales, ambientales, físicos entre otros, ya que dentro de estos se deben analizar términos como hardware, software, códigos, lenguaje de datos, seguridad física y ambiental, esta área ofrece diversidad de especializaciones proporcionando mayores oportunidades en el desarrollo profesional de las personas, por ejemplo: la auditoria de sistemas de información, sistemas de gestión de seguridad, entre otros.

Desde el principio de la humanidad, la información ha estado presente en el diario vivir de los seres humanos, inmersa en diferentes formas y técnicas, la que se consideraba importante y sumamente valiosa se guardaba y protegía en objetos sofisticados, almacenada en lugares de difícil acceso y solamente las personas que estaban autorizadas a ella podían tomarla, desde estos tiempos en pocos lugares y países se construyeron las bibliotecas, este era un lugar de almacenamiento para este tipo de documentación, la cual estaba al alcance de toda aquella persona que deseaba enriquecer sus conocimientos.

Con el pasar de los años, se ha visto la evolución en cuanto a la creación de distintos métodos de procesamiento y almacenamiento, al igual que las redes de

comunicación, estos presentan nuevos escenarios y opciones para proteger este activo que es muy importante para todas las entidades.

Tabla 1

Detalle de las primeras amenazas que surgieron para los sistemas de información

TIPO DE VIRUS	DESCRIPCION
Elk Cloner (1985)	Creado por un estudiante de informática, se caracterizó por dañar todo el sistema operativo de las computadoras.
Brain (1986)	Creado por dos hermanos de apellido Alvi, inicialmente se creó con un propósito positivo, pero este fue utilizado de manera ilegal por otras personas, una vez instalado este virus las maquinas eran infectadas a tal grado que la información contenida en las PC`S difícilmente se podían recuperar.
Virus Jerusalén (1987)	Mejor conocido como viernes 13, este virus se auto instalaba en la memoria RAM de las computadoras, lo cual permitía que se tomara el control total del equipo
El Gusano Morris (1988)	Su creador fue Robert Morris, trataba de descifrar las contraseñas, a través de búsquedas al azar,
Melisa (virus ofimático 1999)	Se caracterizaba por ocultar el código fuente malicioso, dentro de la macro de un documento, almacenado en una computadora
I Love You (2000)	Instalaba un virus troyano para destruir todos los documentos con extensión doc, vbs, vbe, jpg, jpeg.

Fuente: En base a la información de (Portillo, 2016)

1.1.4 Antecedentes generales de la ISO

El surgimiento de las ISO fue luego de la segunda guerra mundial por iniciativa de los delegados de la UNSCC (United Nations Standards Coordinating Commitee), organización que empujaba el desarrollo manufacturero de armamento que fue impulsando la estandarización en conjunto con la **International Federation of the National Standarizing** conocida también como **ISA,** esta unión dio origen a

lo que hoy se conoce como ISO que significa "Organización Internacional para la Estandarización, que regula una serie de normas para fabricación, comercio y comunicación en todas las ramas industriales, las siglas también corresponde a una palabra griega que significa igual" (definicionabc., 2016).

Fue creada en 1946 con la presencia de 64 delegados de 25 países dicha reunión se llevó a cabo en Londres Inglaterra en la sede del Instituto de Ingenieros Civiles estas personas decidieron iniciar con el proyecto que les permitiera la creación de una organización que ayudara a facilitar la unificación de las normas de industrialización y mejora continua de las empresas. (WeblogBlog Calidad ISO,2016)

Pero fue hasta el año siguiente el 27 de febrero 1947 que dio inicio su operaciones ISO desde entonces a la fecha ha desarrollado más 19,500 normas para todos los sectores de producción que incluye el sector salud, la industria el sector alimentario y tecnología, su sede está en Ginebra. (Weblog Blog Calidad ISO)

A lo largo del tiempo la ISO tiene una alta incidencia a nivel mundial, pero la participación y adopción de la normativa es opcional, ya que no posee autoridad de imponer a ningún país u organización su aplicación (definicionabc., 2016).

1.1.5 Antecedentes de la ISO 27000.

En el año 1995 la primera organización que incorporo el primer conjunto de buenas prácticas para la gestión de seguridad de la información fue la organización BSI (British Standards Institution), y se llamaba BS 7799-1, en esta primera fase sufrió varios cambios antes de llegar a convertirse en ISO y que fuera una norma de calidad certificada, en la Figura. 1, se podrá observar lo historia desde su origen.

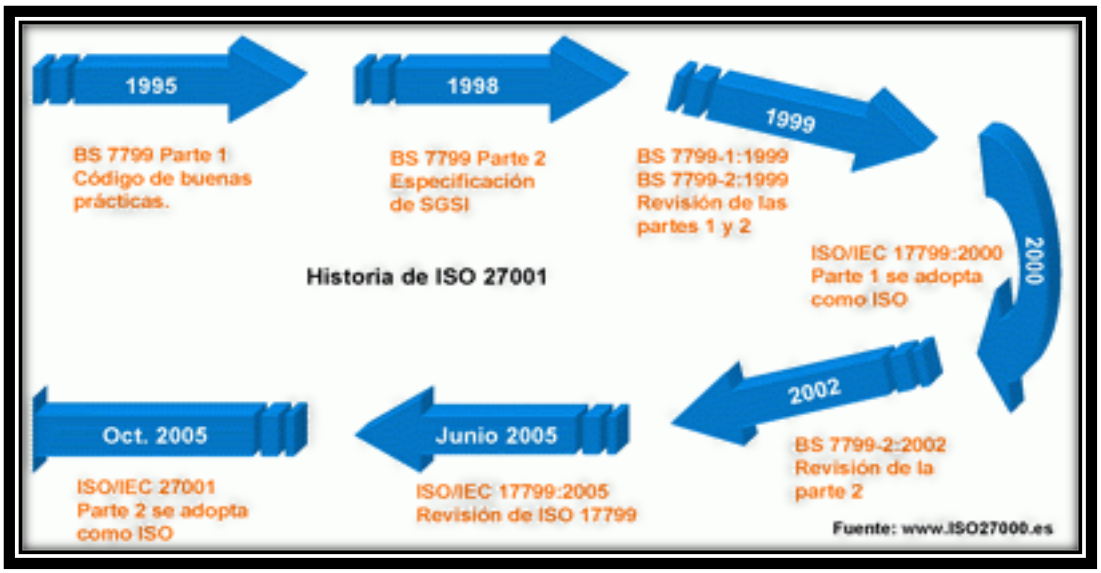


Figura 1 Historia de la ISO 27001

Fuente: www.iso27000.es

La ISO 27000 se resume en un conjunto de normas que indica cómo debe de implementarse un sistema de gestión de seguridad de información basada en la ISO 27001.

Después de su publicación en el 2015 la ISO ha continuado desarrollando otras normas que sirven de apoyo a las organizaciones para la interpretación e implementación de la ISO 27001, en la siguiente Tabla se presenta todas las publicaciones realizadas por ISO y que componen la serie 27000. (ISO 27000. es)

Tabla 2

Detalle del conjunto de normas de las serie 27000

NOMBRE DE LA ISO	FECHA DE PUBLICACION	CONTENIDO
ISO 27000	1 de Mayo del 2009	Esta norma brinda una visión general de cómo está compuesta la serie de ISO 27000, lo cual indica su alcance, el propósito de publicación es proporcionar las definiciones para la serie de normas 27000.
ISO 27001	15 de octubre de1 2005	Esta es la norma principal de la serie 27000 además de ser la única que posee certificación, ya que contiene los requisitos para establecer operar, monitorear y mejorar un sistema de gestión de seguridad de la información, posee el enfoque PDCA (Planear, hacer, chequear, actuar).
ISO 27002	01 de julio del 2007	Es una guía de buenas prácticas donde describe los objetivos de los controles de la seguridad de la información, posee 35 objetivos y 114 controles, agrupados en 14 dominios.
ISO 27003	01 Febrero del 2010	Contiene el diseño e implementación desde el momento de la necesidad del sistema hasta la puesta en marcha de los planes de desarrollo del SGSI.
ISO 27004	15 de diciembre del 2009	Es el desarrollo de métricas y técnicas de medida para la eficacia de un SGSI.
ISO 27005	15 de junio del 2008	Proporciona directrices para la gestión del riesgo de la seguridad de la información.
ISO 27006	01 de diciembre del 2011	Requisitos de acreditación para entidades de auditoría.
ISO 27007	14 de noviembre del 2011	Guía de auditoría de un SGSI.
ISO 27031	01 de marzo del 2011	Posee el apoyo a la continuidad del negocio, referente a las tecnologías de la información y comunicaciones.
ISO 27032	16 de julio del 2012	Proporciona orientación en la mejora de la ciberseguridad.
ISO 27033	15 diciembre del 2009 y revisada el 10 de octubre del 2015	Norma dedicada a la gestión de seguridad, de redes, de arquitectura, redes de referencia, aseguramiento de las telecomunicaciones, acceso remoto, diseño e implementación de la seguridad.
ISO 27034	21 de noviembre del 2011	Desarrolla la norma dedicada a la seguridad en aplicaciones informáticas.

Fuente: Elaborado en base al sitio web (ISO 27000. es)

1.2 Conceptos

A continuación se presentan algunas definiciones que se emplearan en el proceso del SGSI:

- **Activo:** según la ISO se refiere a cualquier información o elemento relacionado con el tratamiento de la misma está compuesto por sistemas, soporte, edificios y personas.
- **Control:** medios para manejar el riesgo, incluyendo políticas, lineamientos, procedimientos, prácticas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas, de gestión o de naturaleza legal.
- **Medios de procesamientos de la información:** cualquier sistema, servicio o estructura de procesamiento de la información.
- **Política:** intención y dirección general expresada formalmente por la gerencia.
- **Riesgo:** combinación de la probabilidad de un evento y su ocurrencia. (ISO/IEC GUIA 73:2002)
- **Vulnerabilidad:** la debilidad de un activo o grupo de activos. (ISO/IEC 13335-1:2004)

- **Seguridad informática**

Se refiere a las características y condiciones de un sistema de procesamiento de datos y su forma de almacenamiento que garantizara su seguridad en base a los atributos de confidencialidad, integridad, y disponibilidad, que busca considerar los peligros que causa la vulnerabilidad a este activo, clasificar la información en pública y privada y protegerse de los daños por las amenazas.

1.3 Organizaciones No Gubernamentales, ámbito, propósito y objetivos

1.3.1 Tipos de Organizaciones No Gubernamentales

Las Organizaciones No Gubernamentales que trabajan en el país en la búsqueda del bienestar de la población salvadoreña, se registran en el Ministerio de Gobernación y Desarrollo Territorial, y se identifican o denominan según su constitución como fundaciones y asociaciones sin fines de lucro.

1.3.2 Ámbito de acción de las Organizaciones No Gubernamentales

En la actualidad el ámbito de acción de las ONGs en El Salvador abarca varios aspectos para el desarrollo y crecimiento de la población salvadoreña, a continuación presenta algunas de ellas:

Tabla 3

Detalle de ONGs que trabajan en diferentes ámbitos en El Salvador

Asistencia a Microcréditos	
Asociación El Bálsamo	Fue creada en 1990 por la necesidad de los desplazados del conflicto armado de los departamentos de San Salvador, Cabañas, Usulután y Cuscatlán; promueve el desarrollo integral comunitario, las redes micro empresariales, son autogestoras en la protección ambiental y producción agroecológica.
Asociación Salvadoreña de Extensionistas Empresariales del INCAE - ASEI	Fue fundada por el Ing. Ricardo Arturo Segovia, con el deseo de contribuir al desarrollo de la microempresa, en 1993 implementa el programa de Bancos Comunales.

PROCOMES	Se registra en 1998, nace con la misión de contribuir al desarrollo comunitario sostenible a nivel local, micro regional y nacional, a través de iniciativas económicas empresariales, con capacitación, créditos y asistencia técnica.
Asistencia Educativa	
Asociación Fe y Alegría	Es una de las primeras organizaciones no gubernamentales se constituyó en El Salvador, se crea entre mayo y junio de 1969, con la iniciativa del Padre Joaquín López que inicio dando catequesis a los niños y jóvenes de la zona rural, después se dio cuenta que no bastaba con la educación religiosa y que era necesario una educación integral para combatir la miseria y dignificar al ser humano, con el apoyo de 13 personas entre ellos religiosos y laicos crearon los estatutos.
Fundación Salvador del Mundo (FUSALMO)	Es creada el 17 de agosto de 2001, surge como alternativa para la población nacional de la niñez y la juventud en condiciones de riesgo, apostando por una educación complementaria con calidad generando destrezas y habilidades para la vida, esta nace a través de Alianza Pública- Privada para ofrecer a los jóvenes alternativas de desarrollo integral.
Fundación Salvadoreña Educación y Trabajo	Nace en 1985 con iniciativa del Padre José María Moratalla desde entonces se creó el Instituto Tecnológico que alberga a cinco taller de formación profesional , empresas pequeñas industriales, fomenta el arte por medio de la música, actualmente cuenta con la Orquesta Juvenil Don Bosco.

Asistencia para la protección del medio ambiente	
Unidad Ecológica Salvadoreña	Es una organización que lucha por la conservación y protección del medio ambiente en El Salvador y a nivel regional.
Fundación Zoológica de El Salvador	Nace en 1989 con el propósito de proteger y conservar la fauna silvestre, desde esa fecha desarrolla programas de investigación, rehabilitación de especies y atención medico veterinaria
Salvanatura	En 1989 nace por iniciativa de profesionales del Club Activo 20-30, su objetivo es canalizar alianzas entre la empresa privada y el gobierno para detener el deterioro de los recursos naturales.
Asistencia para la defensa de los derechos humanos	
IDHUCA	Desde su fundación su objetivo ha sido de garantizar el respeto al derecho humano, nació en medio del conflicto armado debido a la represión y atropello de los derechos humanos, por iniciativa del Padre Segundo Montes Jesuita de nacionalidad Española, él se preocupaba por registrar cuidadosamente las violaciones a los derechos humanos y en 1989, la UCA e IDHUCA sufre un atentado ya que matan a 6 sacerdotes Jesuitas entre ellos el padre Segundo Montes.
Asociación Tutela legal Dra. María Julia Hernández	Anteriormente conocida como Tutela Legal del Arzobispado de San Salvador, creada por iniciativa de Monseñor Oscar Arnulfo Romero hoy beato de El Salvador, en 1977, conocido como Socorro Jurídico, fue hasta 1982 cuando se cambia el nombre por iniciativa de Monseñor Arturo Rivera Damas el cual contaba con un equipo de trabajo de

	abogados que registraban la violaciones graves de los derechos humanos, su propósito era defender los derechos humanos durante y después del conflicto armado. Fue cerrada por el arzobispo Monseñor Luis Escobar Alas. Y por iniciativa de exempleados de Tutela legal, se crea la Asociación Tutela Legal Dra. María Julia Hernández con el objetivo de seguir trabajando por defender los derechos y la investigación de las víctimas que sufrieron múltiples violaciones durante el conflicto armando y que actualmente se siguen violando

Fuente: Información tomada de los sitios Web de cada organización

1.3.3 Propósito de las ONG´s

Las ONGs tienen diversos propósitos pero es necesario destacar los siguientes:

- **Promoción del desarrollo**: Buscan autonomía en las comunidades y beneficiarios de los proyectos por medio de una promoción integral de las personas y su entorno.
- **Ejecución de proyectos de emergencia y asistencia humanitaria**: ayudan a las personas para que sean capaces de responder a las emergencias y aumentar la calidad de vida.
- **Gestión de recursos materiales y financieros:** para el desarrollo de los proyectos dichos fondos pueden ser nacionales o internacionales.
- **Consultoría y asistencia técnica:** facilitar la ejecución y administración de proyectos, por medio de evaluaciones

- **Capacitación de recurso humano**: brindar los conocimientos necesarios a las personas que están involucradas con los proyectos.
- **Coordinación:** establecer acuerdos con las instituciones públicas y privadas. (Blandón Morales, Córdova Santamaria, & Juárez Rivera, 2000)

1.3.4 Objetivos de las ONG´s

Los objetivos principales de las ONGs son los siguientes:

- La sostenibilidad: cada organización necesita personal humano capacitado, una apropiada estructura organizativa para su administración y debidamente registrada como una entidad jurídica y medios económicos que le permitan desarrollar las actividades.
- Elevar la capacidad de debate en todos los ámbitos
- Incrementar el apoyo a quienes más lo necesitan a la población más pobre ya que su búsqueda es luchar contra la pobreza.

Tabla 4

Clasificación de las ONGs

Finalidad	Actividades	Origen
Productivas: Capacitar y proporcionar una herramienta para el desarrollo del trabajo. Asistencialista: Se dedica a brindar ayuda gratuita a los beneficiarios que más lo	Existen organizaciones que se dedican a movilizar personas con el fin de ejercer presión al gobierno. Ayudan a la promoción humana y los sectores más vulnerables.	Solidaria: La necesidad surgió de grupos de personas que han trabajado con la cooperación internacional. Político –Sindicales: Surge a través de iniciativas populares, que tienen una

necesitan. Educativas: Capacitar al capital humano para tener mejores condiciones y así obtener oportunidades. Humanitarias: se dedica para proporcionar servicios de atención de medicamentos, primeros auxilios. Integral: Se enfoca en actividades de salud y nutrición. Crediticia: se encamina a proporcionar recurso financiero, por medio de créditos comerciales.	Desarrollo de actividades de prevención comunitaria	base social muy fundamentada. Confesionales: Surge a través de experiencias misioneras con estatuto jurídico civil y que están apoyados con estructuras religiosas. Asistenciales: Formación de grupos de formación profesional que brindan asistencia técnica

Fuente: (Blandón Morales, Córdova Santamaria, & Juárez Rivera, 2000)

Las organizaciones no gubernamentales apoyan al país con programas de arte, prevención de violencia, generando microempresas, y emprendedurismo juvenil, estas organizaciones apuestan por la juventud salvadoreña ya que la educación es el arma para combatir la miseria y pobreza.

Es importante mencionar que los datos procesados dentro de las organizaciones son vitales para su funcionamiento, ya que cualquier pérdida de credibilidad de la misma, robo o divulgación de información clasificada como confidencial, ocasionaría el cierre de dichas instituciones y los principales donantes o benefactores dejarían de apoyar. Actualmente los organismos internacionales como la Unión Europea, AECID, USAID entre otros exigen que cuenten con estructuras administrativas y financieras,

la credibilidad en el buen manejo de los fondos y la ejecución de los proyectos garantiza el éxito y el funcionamiento de las mismas.

1.4 Seguridad de la información

Según la ISO/IEC 27002 Código para la práctica de la gestión de la seguridad de la información se define de la siguiente manera:

"Es la protección de la información de todas aquellas que se consideran como amenazas y riesgos, para garantizar la continuidad del negocio, manteniendo la confidencialidad, integridad y disponibilidad de la misma".

Para su protección, es necesario diseñar normas, procedimientos, métodos y técnicas que garanticen una correcta administración de los datos, para lograrlo es necesario mantener los tres atributos que el estándar ISO recomienda según se describe a continuación:

Figura 2 Atributos para la seguridad de la información, según ISO/IEC 27001

- Confidencialidad**:** Significa que la información se revela únicamente al personal que está autorizado.
- Integridad: Se refiere que la documentación que se procesa es precisa y coherente desde su creación hasta su distribución, no puede ser modificada por personal no autorizado.
- Disponibilidad: Este atributo busca asegurar el acceso de la información y que sea oportuna en cualquier medio que se requiera.

Los elementos de la información están compuestos por varios aspectos que también se les llaman activos o recursos. A continuación se presentan dichos elementos:

Tabla 5

Elementos que componen la seguridad de la información

Datos e información	• La información que procesa finanzas • Recursos humanos • Llamadas telefónica • Correo electrónico • Base de datos
Sistema e infraestructura	• Equipos de red • Edificio • Computadoras portátiles y dispositivos USB • Computadoras de escritorio • Memorias portátiles • UPS • Celulares • Servidores
Personal	• La junta directiva • Administrador • Personal en general • Personal técnico

Fuente: En base a (protejete.wordpress.com)

Estos son los activos que se tienen que proteger para evitar la pérdida, modificación, y uso inadecuado de la información; es importante destacar que el compromiso principal debe ser adoptado por todos los niveles jerárquicos.

Si se desea implementar un correcto y adecuado sistema de gestión, se deben tomar en cuenta los siguientes componentes:

1.4.1 Evaluación del riesgo

Es importante conocer los riesgos a los que se enfrentan las organizaciones en materia de seguridad de la información, para implementar los mejores procedimientos que los proteja, la gestión de riesgos es un método que permite determinar, analizar, valorar y clasificar los riesgos, para posteriormente implementar las medidas necesarias que los permita controlar.

La evaluación del riesgo, incluye cuatro valiosos aspectos a considerar:

- **Análisis:** En esta etapa se deben determinar los activos que son vulnerables ante posibles riesgos que puedan afectar el proceso normal de la organización, permite identificar hasta qué grado es posible controlar los riesgos encontrados.
- **Clasificación:** Una vez identificados los riesgos, estos se deben clasificar estableciendo cuales podrían controlar la organización, aquellos que sean aceptables.
- **Reducción:** Se implementan las medidas, políticas y procedimientos necesarios para reducir en la medida posible los riesgos identificados.

- **Control:** Se debe vigilar la efectividad y funcionamiento de los procedimientos aplicados, para determinar si estos están dando los resultados esperados.

1.4.2 Clasificación del acceso de la información

Esta debe ser clasificada como restringida, confidencial, uso interno o general, según sea el caso, se debe documentar por el propietario, aprobada por la gerencia responsable y distribuida a quien corresponda durante el proceso de desarrollo de sistemas o antes de la distribución de los documentos o datos. Para determinar el grado de acceso a la información, se debe establecer los tipos de activo de procesamiento de datos que la organización posee.

En esta parte se debe establecer el tipo y el grado de disponibilidad de la misma, que tendrá cada área dentro de la organización.

La información puede clasificarse de la siguiente manera:

- Confidencial: Estará disponible para personal autorizado, definiendo quienes tendrán acceso y a que información.
- Privado: Disponible para personal autorizado interno
- Sensitivo: Acceso controlado, ya sea para el personal interno o externo
- Público: Disponible a nivel general, para todo persona que desea hacer uso de ella en cualquier momento.

Una vez identificados los riesgos, se puede aplicar los métodos de protección que permitan disminuirlos o controlarlos, se pueden implementar medidas físicas y técnicas, como por ejemplo: definir controles de acceso, contraseñas, barreras físicas, también se pueden crear controles personales: aquí se implementan procesos de contratación de personal y capacitaciones, y por ultimo pero no las menos importantes, creación de técnicas organizativas: normas, reglas, procedimientos, seguimiento de controles, auditorias, entre otros.

1.4.3 Amenaza que afectan la seguridad de la información

Es una condición en el entorno de la seguridad que puede generar un abuso a la confidencialidad, integridad y disponibilidad de la información.

El riesgo la seguridad de la información son las personas, que también puede llamarse como criminalidad común o política, además del factor humano también se consideran como riesgos: todos aquellos sucesos físicos o ambientales, como incendios, inundaciones, terremotos, sismos, huracanes, entre otros, y por último las relacionadas a las negligencias y malas decisiones organizacionales como por ejemplo: falta de reglas, capacitación y procedimientos, las cuales también son cometidas por el factor humano pero desde el punto de vista organizacional.

A continuación se presenta el siguiente listado donde se podrá observar los tipos de amenazas a los que están expuestos los sistemas de información:

Tabla 6

Listado de amenazas

Amenazas	**Concepto**
Malware(Virus maliciosos)	Infecta las computadoras para dañar la información
Spam	Son correos no deseas que llegan de forma masiva, tienen el fin de propagar virus maliciosos
Virus	Es un programa informático para producir daño la computadora, actúa de forma transparente con los usuarios
Spyware	Son programas espías que significa: son aplicaciones que recopilan información sin el consentimiento del usuario.
Phishing.	Consiste en el robo de información personal y financiera del usuario, a través de la falsificación de un ente de confianza.
Ingeniería social	Es la manera de manipular, engañar a las personas de confianza que busca conseguir información personal.
Adware	Es un programa malicioso que se instala en el computador sin que el usuario lo note, cuya función principal es descargar y mostrar anuncios publicitarios en la pantalla.
Botnest	Es una red de equipos infecciosos controlados por un delincuente informático, el cual manipula de manera remota el equipo y hace uso de sus recursos.
Gusanos	El propósito principal de este virus es expandirse e infectar a otros ordenadores, agotando los recursos del sistema como la memoria y ancho de banda.
Scam	Se denomina estafas a través de medios tecnológicos, su objetivo es lucrarse de forma directa a través del engaño.
Rootkit	Son herramientas o programas diseñados para mantener en forma encubierta el control del computador.
Crimen informático	Consiste en el acto que realiza una persona para clasificar o desclasificar datos, filtrar información, alterarla o borrarla, usurpar entre otras actividades malintencionadas.

Fuente: Cuadro elaborado hecho en base la información (enter.co)

1.4.4 Políticas de seguridad

Se entiende como política todo lineamiento de carácter obligatorio dentro de una empresa, dirige y da soporte a la gestión de seguridad de la información, con la intención de resolver o minimizar riesgos ante una posible amenaza, refleja las expectativas de la organización en materia de seguridad, a fin de suministrar datos importantes con dirección y soporte.

La política también puede utilizarse como base para el estudio y evaluación de la información.

Existen tres recursos esenciales para la identificación de los requerimientos de seguridad.

- El primero consiste en evaluar los riesgos que enfrenta las organizaciones, mediante la evaluación de estos riesgos se identifican las amenazas a los activos, se evalúa la vulnerabilidad y probabilidad de ocurrencia.
- El segundo está constituido por los requisitos legales, normativos, reglamentarios y contractuales que debe cumplir la fundación, sus socios comerciales, contratistas y los prestadores de servicios
- Y el último recurso es el conjunto específico de principios, objetivos y requisitos para el procesamiento de la información, que ha desarrollado la fundación para respaldar sus operaciones. (17799, ISO/IEC)

Se debe tomar en cuenta el impacto potencial de una falla de seguridad en la ONG, teniendo en cuenta las posibles consecuencias por una pérdida de la confidencialidad, integridad o disponibilidad de la información y otros recursos, así como también la probabilidad de ocurrencia de dicha falla tomando en cuenta las

amenazas y vulnerabilidades predominantes y los controles que actualmente implementan las organizaciones.

1.4.5 Procedimientos de seguridad

Son la descripción detallada de la manera como se implanta una política, el procedimiento incluye todas las actividades requeridas, los roles y responsabilidades de las personas encargadas de llevarlos a cabo.

Determinan las acciones o tareas a realizar en el desempeño de un proceso relacionado con la seguridad y las personas o grupos responsables de su ejecución, son por tanto la especificación de una serie de pasos en relación a la ejecución de un proceso o actividad que trata de cumplir con una norma o garantizar que en la ejecución de actividades se considerarán determinados aspectos de seguridad, un procedimiento debe ser claro, sencillo de interpretar y no ambiguo en su ejecución.

Entre estos procedimientos se mencionan los siguientes:

- Administrador de cuentas de usuarios
- Manejo de incidentes
- Procedimientos de acceso a las instalaciones
- Procedimientos de respaldo de información.
- Longitudes de contraseña
- Seguridad del personal
- Capacitación de usuarios
- Seguridad física y ambiental

- Seguridad del equipamiento y mantenimiento de activos
- Resguardo de la información
- Registro de fallas
- Control de accesos a redes

1.5 Sistema de Gestión de la Seguridad de la Información (SGSI)

Es un conjunto de responsabilidades, políticas y procesos para gestionar de manera eficiente la accesibilidad de la información**,** asegurando su completa confidencialidad, integridad y disponibilidad de los activos, minimizando los riesgos ya que es un proceso sistemático documentado y conocido por toda la organización para su fiel cumplimiento.

Para su implantación en cualquier organización como las ONGs se necesita de los siguientes aspectos.

- Definición del alcance y los límites del SGSI , lo cual tiene que ser adaptado al tipo de la ONG s sea grande o pequeña, la ubicación, de activos que posee y la tecnología
- Definir la política de acuerdo a las características reales que posee cada organización, lo cual se definirán de acuerdo a los siguientes aspectos

a) Determinar el marco de referencia para establecer los objetivos de los procesos.
b) Requerimientos legales, comerciales, regulaciones y obligaciones
c) Estrategia en el manejo de riesgos

d) Establecimiento de criterios para la evaluación del riesgo

e) Alineamientos estratégicos para el contexto de la gestión del riesgo, sobre el cual se establecerá el SGSI.

f) La aprobación de las políticas de parte de la gerencia o junta directiva.

- Se definiera el enfoque de la valuación del riesgo de la organización

a) Se identificara la metodología de cálculo del riesgo y que esté de acuerdo con el SGSI.

b) Desarrollo de criterios para aceptar los riesgos e identificar los niveles aceptable.

- Identificación del riesgo:

a) Se identifican los activos que se incluirán en el alcance del SGSI

b) Evaluar las amenazas de que afectan los activos

c) Identifiquen las vulnerabilidades que podrían convertirse en amenazas.

d) Conocer el impacto por perdida de confidencialidad integridad y disponibilidad que poseen los activos.

- Análisis y Evaluación del riesgo:

a) Calculo del impacto que ocasionaría la pedida de la información

b) La probabilidad de que ocurra una falla a consecuencia de las amenazas, vulnerabilidades, y el impacto que ocasionaría a los activos.

c) Determinar la aceptación de los riesgos

d)

- Identifiquen y evalúen las opciones para el tratamiento de los riesgos

a) Aplicación de controles apropiados a cada organización

b) Acepten los riesgos y que sean consciente, objetivas las políticas basados en el criterio de aceptación.

- Selección de objetivos y control para el tratamiento del riesgo
- Obtener la aprobación y autorización para la implementación del SGSI.

Un sistema de seguridad bien elaborado y correctamente ejecutado, puede minimizar el riesgo de que la información se exponga a ser mal usada. Con la implementación de un SGSI, que contenga buenas políticas y adecuados procedimientos, según las ISO 27,000 las ONG podrán garantizar los siguientes beneficios:

Tabla 7

Beneficios de implementar un sistema de gestión para la seguridad de la información

NORMATIVA	**BENEFICIOS**
ISO 27,000	• Establecimiento de una metodología de gestión de la seguridad clara y estructurada. • Reducción del riesgo de pérdida, robo o corrupción de información. • Los clientes tendrán acceso a la información requerida según sus necesidades, a través de medidas de seguridad. • Los riesgos y sus controles son continuamente revisados. • Confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial. • Las auditorías externas ayudan cíclicamente a identificar las debilidades del sistema y las áreas a mejorar. • Continuidad de las operaciones necesarias de negocio tras

	incidentes de gravedad. • Confianza y reglas claras para las personas de la organización. • Reducción de costos y mejora de los procesos y servicios. • Aumento de la motivación y satisfacción del personal. • Aumento de la seguridad en base a la gestión de procesos en vez de la compra sistemática de productos y tecnologías.

Fuente: Elaboración hecha con base a la ISO 27000

1.6 Etapas para el desarrollo del Sistema de Gestión de Seguridad de Información.

Para el desarrollo de la implementación del SGSI se identifican según la ISO 27001, 5 etapas que se muestran en la siguiente figura:

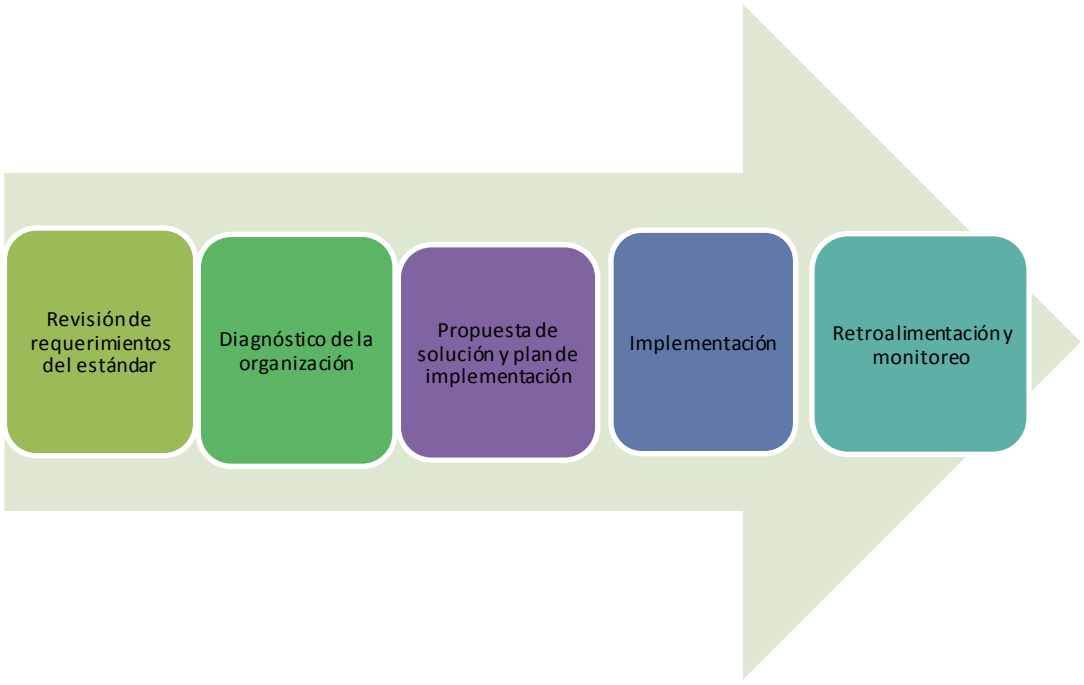


Figura 3 Etapas del desarrollo del SGSI

Etapa 1. Revisión de requerimientos de estándares

En esta etapa de identifica la necesidad de establecer políticas debidamente documentadas, por lo que se evaluara los requerimientos que la organización necesita partiendo del diagnóstico lo cual se identificara las áreas de estudio

Etapa 2. Diagnóstico de la organización

Para realizar el diagnóstico se aplicará la técnica de análisis, entrevistas al personal y la observación a los procesos, lo cual brindara las pautas de los requerimientos que la organización necesita.

Etapa 3 Propuesta de solución

Una vez identificado los requerimientos se elabora un plan de solución e implementación lo cual se desarrollara de forma cronología en todas las áreas para su ejecución.

Etapa 4 Implementación

En esta fase de implementación se trabajara con un plan de trabajo donde se indicara los resultados obtenidos y la estrategia a utilizar para su desarrollo.

Etapa 5 Retroalimentación y Monitoreo

En este proceso es muy importante la mejora continua ya que asi lo requiere el enfoque PDCA, debido a que permite la integración del SGSI y permite la identificación de los aspectos a mejorar o ajustar los procesos.

El SGSI está basado en el enfoque del modelo de la mejora continua que constituye un ciclo de vida, lo cual consiste en implementar, operar, establecer, mantiene y monitorea y revisar, según se muestra en la siguiente figura

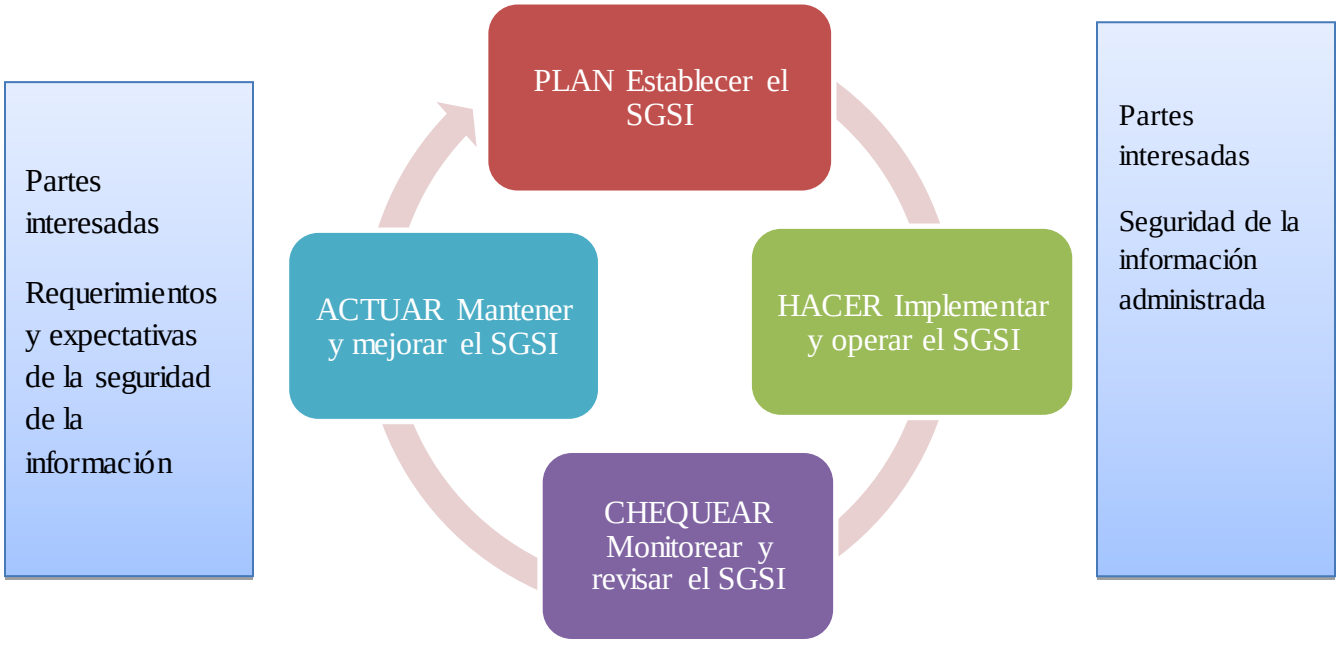


Figura 4 Enfoque del modelo PDCA (ISO/IEC 27001, 2005)

El estándar ISO 27001 es compatible con otros estándares como es el caso de la ISO 9001 que consiste en un Sistema de Gestión de Calidad y la ISO 14001 lo cual es un Sistema de Gestión Ambiental, lo cual puede ser integrado en cualquier organización. (ISO/IEC 27001, 2005)

Los objetivos que se espera obtener para la implementación del SGSI son los siguientes:

- Identificar el riesgo de seguridad de la información dentro de la organización.

- Establecer los controles necesarios ante los riesgos y que estén de acuerdo a las vulnerabilidades identificadas
- Definir políticas del SGSI de acuerdo a la organización
- Evaluar y medir el desempeño y la eficacia del procesos
- Tomar decisiones ante los posibles incidentes o amenazas
- Realizar acciones correctivas y preventivas basada en la revisiones

1.7 Marco Técnico

Las organizaciones tienen que identificar y manejar las actividades para poder funcionar adecuadamente, visualizar los riesgos inherentes a la información que se procesa a través de las entradas y salidas de ella, razón por la cual es necesario establecer procedimientos que permitan tener control y seguridad, para ello el enfoque de la ISO/IEC 27001 permite poder implementar, operar, monitorear, revisar, mantener y mejorar el SGSI.

Entiéndase que es conjunto de datos organizados en poder de una entidad, esta puede estar impresa en papel, almacenada por medios electrónicos, o transferirse por correo, toda debe estar debidamente protegida por la organización que la posee, razón por la cual se recomienda la implementación de sistema de seguridad que ofrece los estándares internacionales como son las ISO/IEC 27000, que servirá para minimizar los riesgos inherentes a la información ya que actualmente todas las organizaciones están expuestas a cualquier tipo de amenaza debido a la vulnerabilidad que inicia por

parte de los usuarios que procesan y transfieren datos por los diversos medios de almacenamiento, también los ataques de virus, el sabotaje, fraude cibernético, el hacking, cabe mencionar que también existen riesgos por desastres naturales, fallas técnicas, en fin todo aquello que puede significar un riesgo y que afecta directamente a los intereses de las instituciones. Según las ISO/IEC 27001, la forma de garantizar la seguridad de la información radica en tres fundamentos importante que es la confidencialidad, integridad y disponibilidad.

Es importante mencionar que el propósito de tener un Sistema de seguridad de información es garantizar que los riesgos sean conocidos gestionados y minimizados por los miembros de la institución y cada procedimiento deber de quedar documentado, sistematizada y estructurada, esto permitirá establecer políticas y procedimientos que esté relacionado con los objetivos de la organización y para obtener mejor el máximo beneficio de se recomiendan los estándares internacionales que a continuación se detallan según (ISO/IEC 27001, Sistema de Gestion de Seguridad, 2005)

Tabla 8

Normativa para la seguridad de la información

Normativa	**Contenido**
ISO/ IEC 27000	Para la elaboración del SGSI es necesario tener conocimiento general de la terminología y definiciones que se van a utilizar dentro del proceso, para evitar tener distintas interpretaciones.
ISO/ IEC 27001	El sistema de seguridad de información se elabora en base a las Especificaciones y requisitos para la implementación de SGSI, en esta se promueve la mejora continua y adopta una gestión de riesgo para la prevención (ver tabla 9) dentro del grupo de la seria 27K es la única normativa que se certifica.
ISO/ IEC 27002	Esta normativa desarrolla por medio de controles más amplios la aplicabilidad de la gestión de buenas prácticas para seguridad de la información. A través de diferentes dominios que se detallan en la Tabla 10
ISO/ IEC 27003	Permitiera elaborar una guía para el sistema de seguridad la implementación de un sistema de SGSI, enfocada en los aspectos requeridos para su diseño, el objetivo de dicha norma es dar instrucciones de cómo se tiene que abordar la planificaron y gestión para implementar. Se detalla a continuación el proceso • Listado de recomendación para la implementación de SGSI según el anexo A • Responsabilidades y roles de la seguridad de la información según el anexo B • Información sobre las auditorías externas según anexo C • Estructura con las políticas relacionadas con la seguridad de la información lo recomienda el anexo D • Seguimiento y Monitoreo del SGSI
ISO/ IEC 27005	Se aplicara para el manejo y control del riesgos es una herramienta que ayudara de forma satisfactoria el manejo de las amenazas y vulnerabilidades, bajo el enfoque de la gestión del riesgo
ISO 31000	Proporcionará un marco de referencia para establecer todo lo relativo a la gestión del riesgo ya que provee servicios y directrices para su tratamiento.
COBIT 5	Tener conocimientos generales de la normativa y los objetivos de COBIT: significa entender un buen gobierno mediante las "mejores prácticas para la seguridad de la información en las organizaciones. Este proporciona una guía de alto nivel para el cumplimento de las medidas de seguridad tales como las siguientes.

	• Asegurar el buen gobierno, protegiendo los intereses de los clientes, accionistas, empleados. • Garantizar el cumplimiento normativo del sector al que pertenezca la organización • Mejorar la eficacia y eficiencia de los procesos y actividades de la organización • Garantizar la confidencialidad, integridad y disponibilidad de la información. Para la tecnología de información COBIT 5 ofrece también 4 dominios que ayudaran a la mejora continua de los sistemas de información. • Planificación y organización • Adquisición e implementación • Entrega y soporte • Supervisión y evaluación
COSO	Es una herramienta de control interno que proporciona 5 componentes lo cual se detallan a continuación. • Ambiente de control: Provee un conjunto de normas de control y procesos y se desarrolla a través de la alta gerencia, desde esta base se crea disciplina y estructura organizacional. • Evaluación del riesgo : En esta fase se evalúa el riesgo que contiene un proceso, al identificar los riesgos permitirá poder administrarlos y controlarlos • Actividades de control: En este proceso de establecen los procedimientos y políticas a seguir para mitigar el riegos. • Información y comunicación: En este componente se determina la importancia de la información ya que la entidad ejerce responsabilidades de control y la comunicación le permite a la administración que el personal comprenda la responsabilidad de la información y la importancia de alcanzar los objetivos. • Monitoreo: Evaluaciones recurrentes y por separado de todos los componentes, para obtener un mejor resultado en los procesos de control.

Tabla 9 *Detalle de la aplicación y enfoque de la ISO/ IEC 27001 y la relación con las buenas prácticas de ITIL s*

Enfoque de la ISO/IEC 27001	aplicación de los modelos para la implementación	Relación con otras normas internacionales para la seguridad de la información	Similitudes de las ISO con respecto a otras Normas	Diferencia de las ISO con respecto a otras Normas
Promueve la adopción de establecer, implementar, operar, monitorear , revisar, mantener y mejorar los SGSI	**Identifiación de requerimienos y objetivos para la información de las entidades interesadas**	Las buenas prácticas de ITIL, para la gestión de servicios tecnológicos de información.	ITIL : Es un conjunto de buenas practicas donde se puede destacar dos procesos importantes como lo es la **Gestión de la Seguridad** quienes son los responsables de diseñar las políticas de seguridad de la información de los servicios de TI, y **la Gestión de accesos** quienes se encargan del cumplimiento de las políticas diseñadas para la seguridad de la información y el modelo PDCA.	ITIL: Es un conjunto de buenas practicas en la seguridad de la información, aunque no se pueden certificar por no ser un estándar, existen certificaciones de forma individual que de mayor a menor valor permite la aplicación.
Ayuda a identificar la necesidad de los requerimientos, establecer políticas y objetivos para la seguridad de la información.	**Plan para establecer SGSI**: Se establece las políticas, objetivos, procesos relacionados a la gestión de los riesgos y mejorar la seguridad de información, y para ello es necesario: **Identificar lo que se requiere mejorar, recolectar datos de los riesgos, analizar los datos recolectados, establecer objetivos de mejora, detallar los resultados esperados, definir los procesos para lograr los objetivos trazados.**	ITIL: Se basa en la idea del ciclo de vida del servicio de las TI, a través de la planificación de una estrategica que permita que el diseño, implementación, operatividad y mantenimiento, esta sujeto a la mejora continua y al modelo de PDCA.		ITIL: Está relacionado con una norma de Gestión de servicio de TI a lo cual pertenece la ISO/IEC 20000, donde las organizaciones se certifican bajo el conjunto de bunas prácticas.
Implementar y operar controles para manejar los riesgos relacionados al resguardo de la información en la institución.	**Hacer o ejectutar**: En este proceso de implementa y se gestiona el SGSI, de acuerdo a los controles trazados en la planificación			
Para todo proceso es necesario el monitoreo que conlleve a revisar el desempeño y la efectividad de los SGSI	**Chequear o seguimiento** : En este paso se verifica y se mide los procesos establecidos en la SGSI, este paso permite comprobar que las medidas establecidas han dado resultado			
Mejoramiento continuo a los objetivos diseñados en el proceso.	**Monitorear y Mejorar :** En este proceso se permite tomar acciones correctivas y preventivas que se basan en las revisiones hechas por auditoría y por la administración.			

Fuente : Elaboracion en base la ISO 27000 y las buenas practicas de ITIL

Tabla 10 *Controles de seguridad según la ISO/IEC 27002*

5.Politicas de seguridad	Estructura de las políticas	Directris principal	Actividades de control de riesgo
Documentos que expresan los lineamientos, objetivos y procedimientos generales que establece la Dirección de las organizaciones; dichas politicas deben cumplirse en cada una de las áreas.	Resumen de politica : Debe contener una breve vision general de lo que se espera obtener con la ejecucion de la politica.	5.1 Directrices de la Dirección en seguridad de la información.	5.1.1 Conjunto de políticas para la seguridad de la información.
	Introducción : Se deberá expresar una breve explicación del porque se genera dicha política.		Corresponde al conjunto de politicas aprobadas por la dirección que será publicada, comunicando a los empleados, y partes involucradas para el cumplimiento de ellas.
	Ambito de la aplicación : Se describe el area o departamento donde se aplicará dicha medida.	Los directores de las organizaciones deberán de expresar líneas claras de las políticas para el dasarrollo de ellas, comprometiendose y manisfestando apoyo en la seguridad de la información a través de publicaciones oportunas.	5.1.2 Revisión de las políticas para la seguridad de la información.
	Objetivo de la política: La intención fundamenta el porque se crea una politica.		Deben ser revisadas y planificadas con regularidad, por si existiera un cambio relevante que impacte la seguridad de la información.
	Principios : Detalle de las reglas que conciernen a las acciones y direcciones para alcanzar los objetivos.		
	Responsabilidades: Corresponde a la asignación de quién sera el responsable del cumplimiento y aplicación de las politicas, en este proceso se puede incluir los mecanismos para obtener los resultados esperados.		
	Resultado clave: La descripción de los resultados que se espera obtener en la aplicación de la politica.		
	Politicas relacionadas : Detalla la relación de otras politicas para el cumplimiento de los objetivos.		

6 . Organización de la seguridad de la información	Actividades de control de riesgo	Lineamientos a implementar
	6.1.4 Autorización de proceso para facilidades procesadoras de información	1. Las áreas deben tener autorizaciones gerenciales, para el apropiado uso en el ambiente de seguridad de información
	La gerencia deberá autorizar la facilitación de nuevos procedimientos	2. Revisión y chequeo de hardware y el software para asegurar la compatibilidad
		3. La incorporación de sistemas de procesamiento de datos en la institución para implementarde los controles
	6.1.5 Acuerdos de confidencialidad	1. Proteger la información confidencial
		2. Determinar la duración de los acuerdos de confidencialidad
		3. Acciones requeridas para la terminación de los contratos
		4. Responsabilidad y acciones de los firmantes para evitar divulgación de información
		5. Propiedad del secreto comercial para el manejo de la seguridad de la información
		6. Uso permitido de la información confidencial y los derechos del firmante para utilizarla
		7.Establecer procesos de notificación y soporte de la divulgación no autorizada
		8. Condiciones para el retorno y destrucción de la información unas vez terminado los acuerdos
		9. Realizar acciones por el incumplimiento de los acuerdos
	6.2. Grupo o personas externas	Identificación de los riesgos de los usuarios externos
	Este control corresponde a la información procesada y utilizada por grupos externos	1. Los medios de procesamiento a los cuales necesita tener acceso a la información
	6.2.1 Identificación de los riesgos relacionados con los grupos externos	2. Que tipo de acceso tendrán los usuarios externos de los cuales se tiene que definir en físico, lógico o conectividad a la red
		3. La sensibilidad de la información involucrada y el grado crítico para su uso
		4. Controles para proteger la información que no esta al acceso de los usuarios externos
	6.2.2 Tratamiento de la seguridad cuando se lidia con clientes	Proteger los activos
		1.Establcer procedimientos para proteger los activos
		2.Determinar si algún activo esta comprometido cuando se haya realizado modificación de data
		3. Integridad de la información
		4. Establecer restricciones para copiar y divulgación de información

7. Gestión de Activos	Actividades de control de riesgo	Lineamientos a implementar
En este dominio lo importante es que las organizaciones tenga conocimiento de los activos que poseen.	7.1.1 Inventario de los activos	1. El inventario de los activos deben de incluir la ubicación, información de respaldo, licencias, y el valor comercial.
	Las instituciones deberán identificar todos los activos y designar responsabilidades para el uso y mantenimiento.	2. Identificación de los activos : La información de la base de datos, archivos de data, acuerdo y documentación del sistema, manuales de usuarios, material de capacitación , procedimientos operaciones o de soporte , planes de continuidad del negocio, rastros de auditoria, acuerdos de contingencias
		3. Activos de software: software de aplicación y del sistema, herramientas de desarrollo y utilidad.
		4. Activos físicos: equipo de cómputo y de comunicación, medios removibles y otro dispositivo.
		5. Servicios de comunicación y computación
		6. Capacidades y habilidades de las personas a contratar
		7.Intangibles el valor de la imagen de las instituciones
	7.1.2 Propiedad de los activos	
	Todos los activos deberán de pertenecer la organización	1. Asegurar que la información de los activos que estén asociados con los medios de procesamiento de la misma estén clasificados debidamente
		2. Revisar y definir procedimientos de las restricciones de los accesos
	7.1.3 Uso aceptable de los activos	
	Establecer reglas para el uso de los activos	1. Definir reglas para uso del correo electrónico
		2. Formar lineamientos para el uso adecuado de dispositivos móviles
	7.2 Clasificación de la información	
	La información debe estar clasificada según la necesidad y grado de protección	1. Utilizar un esquema apropiado para la clasificación de la información
	7.2.1 Lineamientos de clasificación	
	Se clasificará según el valor, requerimientos legales y sensibilidad y grado critico	1. Identificar las necesidades comerciales de intercambiar o restringir la información
		2. Establecer protocolos para la clasificación inicial y a largo plazo

8 Seguridad de recursos humanos	Actividades de control de riesgo	Lineamientos a implementar
Este dominio representa la seguridad enfocada al recurso humano , ya que requiere la necesidad de educar e informar a los empleados desde el inicio de su contratación según las políticas de la institución.	8.1 Antes del empleo En este proceso se debe asegurar que los empleados entiendan las responsabilidades dentro de la institución.	1. La responsabilidad de seguridad de la información debe ser tratada con los empleados desde el inicio de su contratación.
		2. Solicitar antecedentes de los candidatos que formaran parte de la institución, sobre todo para el trabajo que requiere confidencialidad.
		3. El empleado de deberá de firmar un acuerdo sobre su rol y la responsabilidad de la información que maneja.
	8.1.1 Roles y responsabilidades	
	Se deberá documentar el rol y la responsabilidad de la seguridad de información	1. El empleado deberá de implementar y actuar en concordancia con las políticas de seguridad de la información.
		2. Proteger los activos que están a su cargo para evitar la divulgación o acceso no autorizado.
		3. Ejecutar los proceso y políticas de la seguridad de la información.
	8.1.2 Investigación de antecedentes	1. Disponibilidad de referencia de los candidatos a contratar.
		2. Chequeo de currilum vitae del postulante al puesto.
		3. Certificaciones de calificaciones académicas.
	8.1.3 Términos y condiciones del empleo	El postulante deberá firmar contrato donde se detalle los aspecto de la seguridad de información y su responsabilidad dentro de la institución.

Fuente: Elaboración hecha por el grupo en base a la ISO 27002

1.8 Base Legal

La seguridad de la información posee un marco legal que la regula, permitiendo desarrollar y aplicar lineamientos para el resguardo de la información que se genera dentro de las organizaciones. A continuación se muestra en la siguiente tabla la normativa legal aplicable a la seguridad de la información:

Tabla 11

Marco Legal aplicable a la seguridad de la información

LEY	ARTÍCULOS	DESCRIPCIÓN
Ley De Firma Electrónica	Art. 1 Objeto de la ley	Toda organización que aplique la Ley de Firma Electrónica debe tener conocimiento que el objeto principal, es crear una igualdad entre la firma electrónica simple, la certificada y el autógrafo de cada persona. Además de reconocer el valor jurídico de la misma y de la información de forma electrónica.
	Art. 5 Reglas para el Tratamiento de los Datos personales	Las personas e instituciones que presten servicios a las Organizaciones deben cumplir con los lineamientos para llevar a cabo las actividades de procesamiento y almacenamiento de los datos personales.

	Art. 7 Equivalencia funcional	Toda información que la organización lleve y que haya hecho uso de la firma electrónica tendrá igual valor que aquella que se obtenga de forma física.
	Art. 8 Equivalencia de los documentos en soporte electrónico	Todo documento que la organización genere de forma electrónica y que lleve consigo la firma electrónica, tendrá el mismo valor que los establecidos de forma habitual.
	Art. 12 Forma de conservación de documentos	Las organizaciones que lleven información de forma electrónica, será obligatorio conservar los documentos, registros e información; y puede hacerlo por cuenta propia o por medio de terceros.
	Art. 13 Requisitos para la conservación de documentos	Una de las características fundamentales de la ISO 27000 es la disponibilidad de la información, la Ley de Firma electrónica establece que la información debe estar disponible para cualquier consulta, conservada en el formato que fue creada o recibida de forma completa, sin alteraciones para salvaguardar su integridad.

	Art. 14 Garantías mínimas que debe cumplir el Sistema de Almacenamiento de Documentos Electrónicos	La integridad es una característica importante de la seguridad de la información, en este contexto, los documentos almacenados en forma electrónica se deben conservar en medios adecuados que garanticen la integridad y seguridad absoluta de la información, además deben cumplir con la normativa y reglamentos técnicos establecidos por las autoridades.
	Art. 15 Declaración de prácticas de Almacenamiento de Documentos	Las Organizaciones como persona jurídica que realice el almacenamiento de documentos electrónicos deben redactar una declaración de prácticas de almacenamiento en la que se describan las obligaciones a que se comprometen, las medidas de seguridad técnica, física y organizativa.
	Art. 18 Supervisión y Control	Los prestadores de servicios de almacenamiento de documentos electrónicos, quedaran obligados a la supervisión y el control por parte de la Unidad de Firma Electrónica, para garantizar que el servicio que se proporciona sea confiable y de calidad.

	Art. 35 La Autoridad de Control y Vigilancia	El Ministerio de Economía es el responsable de nombrar un funcionario que estará a cargo de la Unidad de Firma Electrónica para asegurar que los prestadores de servicio electrónico cumplan con las obligaciones que establece la Ley.
	Art. 44 Acreditación de los proveedores de Servicios de Certificación.	Todo proveedor que requiera prestar el servicio electrónico, deberá presentar ante la Unidad de Firma electrónica la solicitud y documentos que acrediten el cumplimiento de requisitos como; capacidad técnica y personal con conocimientos especializado, contar con la facilidad económica suficiente para prestar los servicios, entre otros. La verificación de los requisitos la realizará la unidad de Firma electrónica por medio de una auditoria preliminar.
	Art. 54 Obligaciones de los prestadores de Servicios de Almacenamiento de Documentos Electrónicos	Como parte de las obligaciones que tienen los prestadores de servicios electrónicos ante las organizaciones; es colocar el personal con los conocimientos y experiencia comprobable para prestar el servicio de resguardo de la información, utilizando

		sistemas que proporcionen seguridad técnica para toda la información generada de forma electrónica, protegiendo la información proporcionada por el usuario del servicio. Es importante que el prestador de servicios tenga un plan de contingencia por cualquier eventualidad y que utilice sistemas que sean confiables para guardar los documentos electrónicos que permitan demostrar que son auténticos evitando así alteración de la información. (Asamblea Legislativa de la Republica de El Salvador, Decreto No133, Tomo 409, 2015)
Ley De Marcas y Otros Signos Distintivos	Art. 3 Persona que pueden acogerse a la ley	Toda persona ya se natural o jurídica puede adquirir y beneficiarse de los derechos que otorga el uso de una marca. Las organizaciones que cumplan con los requisitos establecidos en esta Ley, pueden ampararse en ella para el registro de su marca.
	Art. 5 Adquisición del Derecho sobre la Marca	Para que las organizaciones hagan uso de la marca que los identifica, deben adquirir el derecho sobre la misma, según lo establece la ley.

	Art. 10 Solicitud de Registro	Dentro de los requisitos que las personas naturales o jurídicas deben presentar ante el Registro, es una solicitud que debe contener: A quien va dirigida, nombre, razón social o denominación, domicilio y demás generalidades, una lista con los nombres de los productos o servicios que diferenciará la marca, reservas relacionadas al tipo de letra, combinación de colores, diseños, entre otros. Dirección exacta para recibir notificaciones, lugar y fecha de la solicitud y firma del solicitante, apoderado o representante legal.
	Art. 20 Certificado de Registro	Después de haber presentado la solicitud ante el Registro y quedar inscrita la marca, se extenderá un certificado al titular en un plazo no mayor a 30 días, que deberá contener toda la información relacionada con la marca incluyendo un modelo de la misma, firmada y sellada por el Registrador.
	Art. 41-B Uso de la Marca	Se presume que una marca ya está en uso cuando las organizaciones e instituciones colocan a disposición los productos o servicios que representa y tiene las características según su registro. (Asamblea Legislativa de la Republica de El Salvador , Decreto No 868, Tomo No 356, 2002)

Ley De Propiedad Intelectual	Art. 1	El objeto principal de la ley, es proteger los derechos sobre las creaciones hechas por el hombre. De acuerdo al artículo 2 del convenio de parís y lo que establece la ley dentro de las creaciones protegidas, se encuentran las marcas de fábrica, comercio y servicio, los nombres y denominaciones comerciales. A través de la ley, el Estado protege el esfuerzo creador de las personas naturales como de las organizaciones. (Asamblea Legislativa de la Republica de El Salvador , Decreto 150, Tomo 320, 1993)

Nota: La Ley de Firma Electrónica es una herramienta para dar seguridad a las redes de comunicación, da cumplimiento a la integridad de la firma y atribuye el documento al firmante.

La Ley de Marcas y Otros Signos Distintivos protege los signos que identifican y diferencian los productos o servicios de una persona (empresa) de los demás que están registrados.

Tabla 12

Régimen tributario aplicado a las Organizaciones no Gubernamentales

LEY	ARTÍCULO	CONTENIDO
Ley de Asociaciones y Fundaciones Sin Fines de Lucro	Art. 11	Son asociaciones todas las personas jurídicas de derecho privado, que se constituyen por la agrupación de personas para desarrollar de manera permanente cualquier actividad legal.
	Art. 12	Las asociaciones se constituyen por los miembros fundadores por medio de escritura pública.
	Art. 18	Se entenderán por fundaciones, las entidades creadas por una o más personas

		para la administración de un patrimonio destinado a fines de utilidad pública, que los fundadores establezcan para la consecución de tales fines.
	Art. 19	La Fundación se constituye por escritura pública o por testamento del fundador.
	Art. 28	Para las fundaciones y asociaciones se constituye un ordenamiento por medio de estatutos básicos que regirán las actividades que deberán cumplir los administradores y los miembros. (Asamblea Legislativa de la República de El Salvador, Decreto No 894, 1992)
Código Tributario	Art. 86	Las organizaciones están sujetas al cumplimiento de las obligaciones formales como son: a) Informar a la Administración Pública todo cambio que ocurra en los datos básicos proporcionados en el registro; b) Declarar los tributos dentro del plazo estipulado y c) Presentar declaración e informe fiscal.
	Art. 131	Las organizaciones estarán obligadas a contratar auditor fiscal cuando cumplan cualquiera de los siguientes requisitos: a) Tener un activo total al treinta y uno de diciembre del año inmediato anterior al que se dictamine superior a diez mil colones, b) Haber tenido ingresos durante el año

		anterior superiores a cinco millones de colones, c) Las personas naturales o jurídicas que resulten de fusiones o transformaciones de sociedades y por último d) Las sociedades en liquidación. (Asamblea Legislativa de la Republica de El Salvador , Decreto No 230,Tomo No 349,2000)
Ley de Impuesto a la Transferencia de Bienes Muebles y Prestación de Servicios	Art. 1 y 2	Las Organizaciones no Gubernamentales están sujetas a las disposiciones de estos artículos por las operaciones que realizan, entre las que se mencionan: comisiones, otorgamientos de préstamos y la exoneración de intereses normales y penales.
	Art. 4	Establece la existencia una transferencia de dominio a título oneroso de bienes muebles corporales. (Asamblea Legislativa de la Republica de El Salvador , Decreto No296,Tomo No 316, 1992)
Ley General Tributaria Municipal	Art. 18	Las personas naturales y jurídicas e incluso las sociedades son sujetos pasivos de la obligación tributaria municipal, por lo tanto esto incluye a las asociaciones, corporaciones y fundaciones que se encuentren en un municipio del país (No existe exclusión del pago de los impuestos). (Asamblea Legislativa de la Republica de El Salvador , Decreto No 86, Tomo No 313, 1991)

Ley de Impuesto Sobre la Renta	Art. 1	Establece como hecho generador la obtención de rentas por los sujetos pasivos en el ejercicio o periodo de imposición de que se trate.
	Art.6 literal c)	En este artículo establece que las organizaciones quedan exentas del pago del impuesto siempre y cuando sean calificadas previamente por la Dirección General de Impuestos Internos. (Asamblea Legislativa de la Republica de El Salvador , Decreto No 134, Tomo No 313, 1991)
Reglamento de la Ley de Impuesto Sobre la Renta	Art. 7	Los sujetos excluidos del pago del impuesto según lo establece el artículo 6 de la Ley deben obtener calificación previa de la Dirección General de Impuestos Internos, presentando una solicitud por escrito a la Dirección General e incluir el diario oficial donde aparezcan publicados el acto constitutivo, los estatutos de la entidad y el acuerdo de otorgamiento de personería jurídica, certificación de punto de acta, entre otros. (Asamblea Legislativa, Deccreto No101, 1991)

Es importante mencionar que la exclusión del pago del impuesto no la exonera de las obligaciones formales para la liquidación del mismo, como lo establece el artículo 100 del Código Tributario y tiene la obligación de informar a la Dirección General de Impuestos Internos toda donación recibida dentro de los primeros diez días hábiles del mes siguiente. (Artículo 146 CT)

CAPÍTULO II: METODOLOGÍA DE INVESTIGACIÓN Y DIAGNÓSTICO

2.1 Tipo de estudio

La investigación se basó en un estudio de tipo hipotético-deductivo partiendo del conocimiento general del problema al conocimiento específico, debido a que se observó el problema en estudio, se han creado las hipótesis para identificar dicho fenómeno, así como su verificación y comprobación a través de la implementación de instrumentos de investigación que permiten validar dichos resultados

2.2 Unidad de análisis

El personal técnico o jefe de sistemas y el personal claves de las Organizaciones no Gubernamentales de El Salvador son las unidades de estudio que servirán para llevar a cabo el desarrollo del trabajo de investigación.

2.3 Universo y muestra

Universo

Con las unidades de análisis detalladas anteriormente se identificó el siguiente universo: Listado de Organizaciones No Gubernamentales autorizadas e inscritas en el Ministerio de Gobernación y Desarrollo Territorial, según registró publicado en la página web de dicho Ministerio.

Muestra

El número de Organizaciones No Gubernamentales a tomar en cuenta para encuestar, ha sido determinado utilizando la siguiente fórmula estadística para poblaciones finitas: $$n=\frac{N.P.Q.Z^2}{(N-1)e^2+P.Q.Z^2}$$

Terminología

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= 0.05

N=3,337 P=0.96

Z=1.96 Q=0.04

Sustituyendo se obtienen los siguientes resultados:

$$n = \frac{3{,}337\ (0.96)\ (0.04)^2(1.96)}{(3{,}337-1)\ (0.05)^2 + (0.96)\ (0.04)\ (1.96)^2}$$

$$n = \frac{492.27}{8.49}$$

n= 58.02

n= 58 Organizaciones No Gubernamentales

Se tomó como probabilidad de éxito y fracaso el 0.96 y 0.04 respectivamente, debido a las estimaciones probabilísticas donde se detalla que la posibilidad de éxito sea alta no obviando la perspectiva inherente del error que como grupo de investigación se puede tolerar y que no impacte en el estudio a realizar.

2.4 Instrumentos y técnicas a utilizar en la investigación

2.4.1 Instrumentos

La herramienta que se aplicó para la recolección de la información fue el cuestionario, dirigido a las ONG´S de El Salvador, específicamente al personal clave y al técnico o jefe de sistemas de las Organizaciones no Gubernamentales de El Salvador.

2.4.2 Técnicas

La herramienta que se aplicó para la recolección de la información fue el cuestionario, con preguntas cerradas y de selección múltiple, se elaboraron dos cuestionarios, uno dirigido al personal clave que hace uso de algún sistema de información y el otro al técnico o jefe del área informática quienes son los

responsables de manejar y administrar los recursos tecnológicos de las Organizaciones no Gubernamentales de El Salvador.

2.5 Recolección de la información

Se utilizó información contenida en libros, documentales, tesis, páginas web, entre otros, esto permitió enriquecer y profundizar en los aspectos más importantes sobre la problemática en estudio, siendo principalmente las ISO 27,000 a la 27,002 la principal fuente bibliográfica consultada.

2.6 Bibliografía

En la etapa de la elaboración de la propuesta, se tomó como base principal las normas ISO 27,000, 27,001, 27,002 y 31,000, las cuales servirán como modelo para poder establecer los controles que deben ser aplicados e implementados en la elaboración del sistema de seguridad de la información.

2.7 Procesamiento de la información

El procesamiento de la información se llevó a cabo de la siguiente manera:
Las respuestas obtenidas de los cuestionarios se procesaron con la herramienta de Formularios de Google, donde se elaboró una base de datos para obtener los resultados, y de esta manera presentar las respuestas a través de gráficos, donde se puede observar en términos porcentuales cada respuesta obtenida para efectos de facilitar su respectivo análisis a cada interrogante de ambos cuestionarios

2.8 Análisis e interpretación de los datos

Tomando en cuenta la utilización de la herramienta de Excel, se realizó una consolidación de las respuestas de cada una de las interrogantes presentadas de ambos cuestionarios y se muestra la información tabulada con los resultados obtenidos.

2.9 Diagnóstico de la investigación

De los resultados obtenidos de los dos cuestionarios aplicados a la muestra determinada, se realizan las interpretaciones y análisis respectivos, el cual será la principal guía para establecer los lineamientos correctos para la elaboración del sistema de seguridad de la información.

Resultados obtenidos del personal clave de las ONG´S

A continuación se detalla el resultado obtenido de las encuestas realizadas al personal clave de las ONG s para determinar el diagnóstico de dicha investigación.

Relación entre la pregunta 1,2 y 3:

PREGUNTA	CRITERIOS	ALTERNATIVAS	FRECUENCIA	
			ABSOLUTA	RELATIVA
1	Identificar si el personal tiene conocimientos sobre la seguridad de la información	Si	46	79%
		No	12	21%
2	Determinar las causas por la que no se tiene conocimiento de seguridad informática	La organización no proporciona capacitaciones sobre el tema.	33	57%
3	Forma de capacitación del personal	Autodidacta	24	41%

Como primer punto, interesa saber si el personal clave posee conocimientos sobre seguridad relacionada a la información, se determinó que en su mayoría el personal conoce sobre este tema, según lo afirmaron el 79% de los encuestados, lo que indica que no desconocen la importancia de contar con dicha seguridad dentro de las organizaciones, pero este conocimiento es de manera general ya que no existe una cultura de protección en las áreas sensibles en las instituciones, siendo el 21% los que no tiene conocimiento al respecto, se pudo deducir en la pregunta dos, que este 21% que estima no saber nada sobre la seguridad de la información es debido a que la organización en la que laboran no proporciona capacitaciones sobre este tema, así lo expresó el 57%, lo cual se evalúa que es necesario que sean capacitados para generar conciencia de la importancia de proteger los activos las ONG, el 79% afirmó tener noción sobre el tema y el 41% manifestó que han adquirido estos conocimientos de manera autodidactica, según se demuestra en la pregunta tres.

Relación entre pregunta 4 y 5:

PREGUNTA	CRITERIOS	ALTERNATIVAS	FRECUENCIA	
			ABSOLUTA	RELATIVA
4	Identificar las medidas de seguridad que aplica el personal de las ONG	Análisis de antivirus a las de USB	42	72%
		Cambia periódicamente la contraseña de su computadora	7	12%
5	Conocer los tipos de restricciones que posee el personal	Facebook	19	33%
		You Tube	16	28%

Con la pregunta 4 se procuró conocer cuáles son las medidas de seguridad más comunes que aplican las ONG`S, dentro de los resultados obtenidos se determinó que las más practicada por el personal clave es la de realizar análisis de antivirus a los

dispositivos USB, según lo manifestó el 72% del total de los encuestados, pero también interesó si las instituciones aplicaban medidas de seguridad a través de la restricciones de páginas web o instalaciones de programas, entre otras, a lo cual se confirmó que estas entidades también aplican este tipo de medidas, siendo principalmente la restricción de acceso a las páginas de redes sociales como Facebook y You Tube, según comentó el 33% y el 28% respectivamente.

Relación entre pregunta 6 y 7:

PREGUNTA	CRITERIOS	ALTERNATIVAS	FRECUENCIA	
			ABSOLUTA	RELATIVA
6	Descubrir si las instituciones permiten que los empleados saquen información fuera de la institución.	Si	35	60%
		No	23	40%
7	Conocer los medios que son utilizados para sacar información fuera de la institución.	Información Procesada y almacenada en USB	20	34%

Un factor que afecta a las instituciones es el robo y mal uso de la información ya que en muchas entidades permiten a los empleados extraer información importante para trabajarla fuera de horarios laborales ocasionando riesgo de ser divulgada y manipulada incorrectamente, esto se pudo comprobar con la pregunta 6, donde el 60% manifestó que les permiten poder llevar información fuera de la institución, con la pregunta 7, se determinó que el principal medio que utilizan los empleados para esta práctica es a través del uso de USB, según lo indicaron 20 empleados equivalente al 34%.

Relación entre la pregunta 8 y 9:

PREGUNTA	CRITERIOS	ALTERNATIVAS	FRECUENCIA	
			ABSOLUTA	RELATIVA
8	Conocer si las ONG`S aplican políticas y procedimientos de seguridad para la información.	Si	25	43%
		No	33	57%
9	Conocer las razones porque no poseen un sistema de seguridad de información	Por falta de recursos	23	40%
		Falta de conocimiento de los riesgos y amenazas	19	33%

Respecto a si las ONG´S aplican políticas y procedimientos que garanticen la seguridad de la información, se obtuvo como resultado que en su mayoría no utilizan, representado con un 57%, que permite determinar la evidente necesidad de la existencia de un sistema que brinde seguridad a la información que se maneja en cada organización, y siendo solamente el 43% de ONG`S las que si las implementan.

Una vez que se determinó si las ONG´S implementan políticas y procedimientos de seguridad a la información, el cual no dio resultados favorables siendo más del 50% de organizaciones que no las aplica, también se consideró necesario investigar algunos de los motivos por los cuales no son utilizadas, teniendo como principal razón la falta de recursos económicos y de conocimiento de los riesgos y amenazas que esto conlleva con el 40% y 33% respectivamente.

Relación entre la pregunta 10 y 11:

PREGUNTA	CRITERIOS	ALTERNATIVAS	FRECUENCIA	
			ABSOLUTA	RELATIVA
10	Descubrir si los organismos donantes exigen a las instituciones algún tipo de estructura organizativa	Si	49	84%
		No	9	16%
11	Conocer qué tipo de requerimientos exigen los donantes externos	Estructura organizativa	29	50%
		Sistema Contable	27	47%

Como ya se estudió en el capítulo uno, se determinó que en su mayoría las ONG´S obtienen fondos de entidades externas, para lo cual se consideró importante saber si estos donantes exigen alguna estructura organizativa, dando como resultado que en su mayoría si exigen este requerimiento, según lo expresó 84% de los encuestados en la pregunta 10, y con respecto a la pregunta 11 se pretendió conocer cuáles son estas exigencias que establecen dentro de los convenios entre los organismos que realizan las donaciones y las ONG´S, donde el personal clave encuestado manifestó que es el de poseer una adecuada estructura organizativa y un buen sistema contable con el 50% y 47% respectivamente.

Resultados obtenidos del personal técnico o jefe de sistemas de las ONG´S

Relación entre la pregunta 1, 2 y 3:

PREGUNTA	CRITERIO	ALTERNATIVA	FRECUENCIA	
			ABSOLUTA	RELATIVA
1	Identificar cual es el departamento que suministra el mantenimiento al los activos informáticos	Departamento de informática	35	60%
		Mantenimiento y monitorio externo del equipo	18	31%
		Contabilidad	5	9%
		No posee	3	5%
2	Descubrir si los mantenimientos a los sistemas informativos están debidamente programados y organizados periódicamente	Si	39	67%
3	identificar el tiempo de periodicidad con la que se implementa el mantenimiento de soporte a los activos informático	Mensualmente	14	24%
		Trimestralmente	14	24%
		Anualmente	10	17%

Es importante conocer de qué manera es suministrado el soporte técnico a las ONG´S, para lo cual se investigó cuál es el ente que proporciona este servicio, siendo el departamento de informática el principal responsable de brindar soporte técnico dentro de las ONG´S, representado en un 60%, y solamente el 5% del total de las organizaciones encuestadas manifiestan no tener un departamento definido que les de este servicio.

Para poder estar preparado ante todas las amenazas que a diario enfrentan las ONG´S en cuanto a la seguridad de su información, se considera importante que estas cuenten con un programa de soporte y mantenimiento a los sistemas informáticos según como se expresó en la pregunta 1, por lo que se detectó que únicamente el 67%

de las ONG´S poseen este programa, el cual es ejecutado en su mayoría entre uno y tres meses, según lo manifestó el 24%, seguido de otro 17% que menciono que también poseen este tipo de programas, pero que estos son ejecutados de manera anual

Relación entre la pregunta 5 y 6:

PREGUNTA	CRITERIO	ALTERNATIVA	FRECUENCIA	
			ABSOLUTA	RELATIVA
5	Analizar las diferentes vulnerabilidades sufridos en las ONG´S	Falta de Hardware	17	29%
		Falta se seguridad para archivos digitales	20	34%
		Cuenta de usuarios mal configurados	1	2%
6	Analizar los tipos de medidas que son implementados en las ONG´S para minimizar riesgos de pérdida de información.	Autenticación de usuarios (contraseñas)	33	57%
		UPS	35	60%
		Implementación de sistema de acceso CPD	2	3%

Para tener un diagnostico real en cuanto a situaciones de vulnerabilidad sufridas por las unidades sujetas de estudio , se procedió a investigar si estás han experimentado a lo largo de su actividad algún tipo de situación que ha puesto en peligro la seguridad de la información, teniendo como resultados que todas en alguna medida han presentado este tipo de situaciones, siendo las principales razones falta de seguridad para los archivos digitales y la no disponibilidad de hardware lo que ha provocado este tipo de incidentes con un 34%, y 29% y solamente un 2% debido a cuentas de usuarios mal configurados.

Anteriormente se comprobó que las ONG´S en alguna medida aplican políticas y procedimientos que les garantice la seguridad de la información, algunas de estas medidas son la instalación de UPS en cada computadora con el 60% y la autenticación

de usuarios por medio de contraseñas con un 57% y las menos practicadas son la implementación de sistemas de acceso CPD y la socialización a los usuarios de normas o políticas de seguridad ambas con el 3%.

Relación entre pregunta 8, 9 y 10:

PREGUNTA	CRITERIO	RESPUESTA	FRECUENCIA	
			ABSOLUTA	RELATIVA
8	Descubrir si las ONG´S sufren o han sufrido ataques a la seguridad de la información	Si	32	55%
		No	26	45%
10	Conocer que ataques a la seguridad de la información han sufrido las ONG`S	Acceso no autorizado	20	34%
		Correo spoofing	15	26%
		Ataque de fuerza-Bruta	1	2%
		Puertos abiertos	14	24%
9	Analizar las medidas de seguridad que implementan las ONG´S ante los ataques a la seguridad de la información	Sistema de detección de intrusos	16	28%
		Antivirus	27	47%

Toda ONG´S ha sufrido algún tipo de ataque o incidente por muy pequeño que sea, por lo que se consideró importante conocer cuáles son los más comunes a los que las ONG´S se exponen en el día a día, siendo el acceso no autorizado a la información el principal con un 34%, correo spoofing con el 26% y el uso de puertos abierto según el 24%, y el que representa menos riesgo con un 2% es el ataque de fuerza bruta, a la vez es importante identificar cuáles son las medidas de seguridad que las ONG`S implementan para contrarrestar estos ataques para minimizar el riesgo, en esta parte se obtuvo como resultado que la principal medida es la instalación de antivirus a cada computadora así como la implementación de programas de detección de intrusos, con el 47% y 28% respectivamente.

Relación entre pregunta 14 y 21

PREGUNTA	CRITERIO	ALTERNATIVA	FRECUENCIA	
			ABSOLUTA	RELATIVA
14	Análisis de normativa técnica en la implementación de políticas y procedimientos	COBIT	6	10%
		ISO 27000	8	14%
		Ninguna	37	64%
21	Aplicación de normativa ISO	Si	49	84%
		No	9	16%

De las ONG´S que cuentan con políticas y procedimientos para la seguridad de la información, el 64% no lo hace con base a una normativa técnica, solamente el 14 % y 10% lo hace en base a los estándares de las ISO 27,000 y a COBIT.

Del 100 % de las organizaciones encuestadas, el 83% manifestó estar interesados en implementar políticas y procedimientos de seguridad de la información con el apoyo y guía de las normas ISO.

Relación entre pregunta 17 y 18:

PREGUNTA	CRITERIO	RESPUESTA	FRECUENCIA	
			ABSOLUTA	RELATIVA
17	Identificar si las ONG`S aplican medidas de seguridad a la instalaciones	Extintores de fuego	28	48%
		Salidas de emergencia	23	40%
		Cámaras de video	18	31%
		Dispositivos Biométricos	6	10%
18	Conocer qué tipo de dispositivos biométricos utilizan las ONG´S, como medida de seguridad en las instalaciones	Contraseñas Numéricas	11	19%
		Huella Digital	9	16%

Proteger las instalaciones de la entidad es parte de las medidas que se deben de aplicar para garantizar la seguridad de la información, es por ello que se consideró importante

conocer si las entidades aplican este tipo de medidas, en la pregunta 17, se determinó que el uso de extintores de fuego es la más utilizada con el 48% , identificación de salidas de emergencia con el 40% y la instalación de cámaras de video con el 31%, pero también se considera importante que existan medidas que incluyan el uso de dispositivos biométricos, pero lastimosamente solo el 10% de las 58 ONG´S encuestadas aplican esta medida, por lo que se interesó también indagar de este 10% que tipo de dispositivos son los más utilizados, dando como resultado en la pregunta 18, las contraseñas numéricas y la huella digital con el 19% y el 16% respectivamente.

CAPITULO III: PROPUESTA DE SISTEMA DE SEGURIDAD DE LA INFORMACION EN BASE A LA ISO 27000, APLICADO A LA ORGANIZACIONES NO GUBERNAMENTALES

3.1 Planteamiento del caso

3.1.1. Generalidades

En este capítulo se presenta la propuesta del trabajo realizado para desarrollar un sistema de seguridad de información aplicado a las Organizaciones no Gubernamentales de El Salvador, con el objetivo de elaborar una herramienta útil que ayude a garantizar y proteger los datos procesados dentro de las organizaciones desde la dirección ejecutiva hasta los niveles operativos, se trabajará bajo los requerimientos del estándar internacional ISO 27000, esta es una guía que permite establecer, implementar, operar, revisar, mantener y mejorar la gestión de la seguridad de la información; utilizando el enfoque PDCA(Planear, Hacer, Chequear, Actuar) que establece la ISO 27001.

3.2.1 Estructura y forma de desarrollo del sistema de seguridad de información.

Para la elaboración del sistema de seguridad se considerarán los requerimientos que la organización necesita mejorar dentro de los procesos administrativos.

A continuación se presenta la estructura del desarrollo del sistema de seguridad para la Fundación “Un Futuro Mejor” que no cuenta con procedimientos documentados para garantizar la protección de los activos que posee dicha organización.

3.2.1.1 Requerimiento de los estándares de seguridad

En esta primera fase se idéntica lo que la institución desea mejorar y el compromiso de la Dirección Ejecutiva para poner en marcha dicho sistema, así mismo establecerá la planificación con fechas y responsables para iniciar el proceso y desarrollo de la normativa internacional.

En la siguiente Tabla se muestra lo que la organización requiere para garantizar que los activos cumplan los tres elementos fundamentales que son disponibilidad, confidencialidad e integridad.

Tabla 13

Detalle de requerimientos de seguridad para los activos

Requerimiento de seguridad que deben de cumplir los activos críticos				
Activo Critico	**Descripción**	**Disponibilidad**	**Confidencialidad**	**Integridad**
Sistema SAF	Contiene el registro histórico de la contabilidad desde el 2006, cada proyecto que se encuentre en ejecución posee su contabilidad individual, también tiene la capacidad de consolidar la información de todos los proyectos y operaciones normales de la institución**.**	a) Requiere que la información esté disponible en el momento en que cada usuario la necesite. b) La información debe procesarse de forma adecuada y eficiente.	a) Cada usuario debe tener una contraseña de acceso, lo cual debe ser asignado de acuerdo a los niveles de autorizaciones que posea. b) Autenticación de la contraseña de cada uno de los usuarios. c) advertencia de finalización de sesión.	Notificación de advertencia si ocurre modi ficación de la información por usuarios no autorizados.

Servicio de Internet	El servicio es proporcionado por un proveedor externo, distribuidos a los empleados y clientes externos, para poder alcanzar los objetivos de la organización.	a) Realizar monitoreo permanente del servicio con el proveedor. b) Que esté disponible el servicio para todos los usuarios.	a) Asignación de usuarios con contraseña para el acceso al correo institucional. b) Realizar cambio de contraseña cada 3 meses.	a) Proporciona políticas de restricción para el acceso al correo institucional. b)Utilizar aplicativos como es el SSL(security socket layer) para transferir la información del sistema contable y el correo electrónico.
Infraestructura de red	Parte esencial para la transmisión de la información ya que son todos los dispositivos de almacenamiento y trasmisión como son los servidores, Reuter entre otros.	Todos los puntos de accesos deben de estar abiertos para comunicar la información a los usuarios que la requieren.	a) Cada acceso debe de contener restricciones para su uso. b) Para evitar la manipulación de los accesos no autorizados, se debe de establecer protocolos de seguridad, donde solo el personal de soporte técnico pueda tener acceso.	a) Establecer políticas de respaldos de la información. b) Políticas para proteger los activos.

Recurso humano	El personal es la pieza fundamental para el cumplimiento de los objetivos de la fundación.	El personal debe estar preparado para desarrollar todas las funciones asignadas en su puesto de trabajo, deberá de recibir capacitación de concientización en el uso de la información que procesa y transfiere.	El acceso de la información debe de estar restringida de acuerdo a los permisos de cada usuario, y contratos de confidencialidad.	Elaboración de política para el acceso a la información, cumpliendo los protocolos de seguridad.
Infraestructura física	Posee amplias instalaciones para el desarrollo de las actividades.	El uso y acceso a las instalaciones de be contener un registro de los visitantes y personal de la institución.	Elaboración de políticas para controlar los accesos a las instalaciones.	Política para proteger los accesos a las instalaciones.
Personal de soporte técnico	Equipo de trabajo que está capacitado para responder a los incidentes Ocurridos en el proceso del manejo de la información.	El equipo debe de estar disponible en el momento que los usuarios lo requieran.	Aplicación de normativas y políticas para el manejo de la información.	El personal debe estar autorizado para realizar procedimientos de seguridad en todas las áreas.

Fuente elaboración propia en base a entrevista realizada al personal de la Fundación un Fututo Mejor

3.2.1.2 Definición del alcance del SGSI

El SGSI se aplicará en todas las áreas de la Fundación un Futuro Mejor ya que el proceso de la información está compuesto por una cadena de comunicación, que cualquier cambio realizado erróneamente puede generar pérdidas significativas como ocurrió en el año 2011; cuando se perdió la información contable del 25 de octubre al 31 de diciembre 2011, lo cual no se logró recuperar, debido a que no se realizaron copias de respaldos.

Este sistema ayudará a fortalecer las áreas de la institución y a establecer medidas preventivas que garanticen la seguridad de la información.

3.2.1.3 Definir las políticas de la seguridad de la información.

Las políticas se documentaran de acuerdo a las directrices de la Dirección Ejecutiva y el compromiso adquirido para que se cumplan en cada área dicho documento deberá de ser aprobado por la Junta directiva de la Fundación un Futuro Mejor.

3.2.1.4 Metodología de evaluación del riesgo

Para determinar los riesgos que están inherentes a la información se ha realizado una entrevista bajo el análisis de para evaluar cuáles son las áreas más vulnerables dentro la Fundación un Futuro Mejor lo cual se detalla en la siguiente tabla:

Tabla 14

Análisis de riesgos en base a la escala de Likert

No	Pregunta	Escala de Likert				
		1	2	3	4	5
	DIRECCION EJECUTIVA	Muy en acuerdo	En desacuerdo	Indeciso	De acuerdo	Muy de acuerdo
1	¿La organización tiene controles de seguridad para el acceso a la información?			√		
2	¿Obtendría beneficios la organización con la implementación de un Sistema de Seguridad de la información?				√	
3	¿Cuenta la organización con instalaciones físicas y tecnológicas que garanticen la protección de la información?		√			
4	¿La organización tiene un compromiso con relación a la seguridad de la información?			√		
5	¿La Dirección ha tomado acciones en función de la seguridad de la información?			√		
6	¿Se verifico el cumplimiento de políticas y la divulgación a los empleados de la fundación?			√		
7	¿Cuenta la organización con los recursos necesarios para la implementación de un sistema de seguridad?			√		
8	¿Se definieron los riesgos asociados a la falta de protección de los activos?		√			
9	¿Se ha realizado evaluación general de la seguridad de la información?				√	
GERENCIA DE FINANZAS Y RECAUDACIÓN DE FONDOS						
10	¿Se lleva un control de los activos y un registro actualizado?				√	

11	¿Cada activo cuenta con su propietario identificado?				√	
12	¿Existe un documento que regule el uso adecuado de los activos y de la información que se procesa?			√		
13	¿Se han implementado medidas que garanticen la protección de la información, ya sea que estén documentadas o no?		√			
14	¿Cuenta con una clasificación para la información, de acuerdo al valor, requerimientos legales o confidencialidad de la misma?		√			
RECURSOS HUMANOS						
15	¿Existen asignación de roles y responsabilidades de seguridad definidas y documentadas previo a la contratación?			√		
16	¿Existe reglamento o procedimiento que rige la evaluación de antecedentes de los candidatos al empleo?			√		
17	¿Los empleados firman un acuerdo de confidencialidad o no divulgación como parte de los términos del contrato?			√		
18	¿Cuenta la organización con un programa de capacitación relacionado con el resguardo de los datos?			√		
19	¿Existe un proceso disciplinario documentado para los empleados que han cometido una infracción de seguridad?			√		
20	¿Al finalizar el contrato o por despido justificado, se realiza un inventario de los activos que los empleados tenían en su poder, incluyendo revisión de la información que administraba?				√	

21	¿Al finalizar el contrato o por despido, se eliminan los accesos a las instalaciones de la organización?				√	
GERENCIA DE TECNOLOGÍA E INNOVACIÓN						
22	¿Existen políticas para la seguridad de la información establecidas?		√			
23	¿La Gerencia de Tecnología e Innovación cuenta con procesos documentados?			√		
24	¿En la Fundación existe un responsable de gestionar la política de seguridad de la información?		√			
25	¿Existe un procedimiento para la autorización de nuevos medios de procesamiento de información como: software, hardware?				√	
26	¿Se implementan medidas de seguridad previo al otorgamiento de accesos a los usuarios?			√		
27	¿Para las cuentas inactivas, se aplica procedimiento para el bloqueo o eliminación?				√	
28	¿Se han realizado auditorías a nivel de sistemas?		√			
29	¿Cuenta con procedimientos de trabajo documentados y están a disposición de todos los usuarios?			√		
30	¿Cuenta con instalaciones adecuadas para los sistemas?			√		
31	¿Se establecen criterios de aceptación para los sistemas de información nuevos o actualización de los que tiene la organización?				√	
32	¿Son implementados de forma adecuada las alertas de detección, prevención y				√	

	recuperación de la información, en caso de que se presente un código malicioso?					
33	¿Se realizan pruebas al sistema antes de ser implementado?				√	
34	¿Toda la información confidencial y los software utilizados en la organización se pueden recuperar en caso de algún incidente o mal funcionamiento de los medios de almacenamiento?			√		
35	¿La organización lleva control de la administración de dispositivos extraíbles como memorias, USB, discos duros externos y tarjetas de memoria?			√		
36	¿La información que se envía o recibe por medio de correo electrónico está protegida?			√		
37	¿Las transacciones realizadas en línea están protegidas para prevenir transmisión incompleta o accesos no autorizados?				√	
38	¿Se ha informado a los usuarios y proveedores de servicios los requerimientos de seguridad para el control de accesos?			√		
39	¿El uso de privilegios respecto al acceso a los sistemas de información está restringido o controlado?				√	
40	¿Se lleva control de la asignación y cambios de contraseñas por área de trabajo?			√		
41	¿Se solicita a los usuarios firmar documento de confidencialidad de contraseñas?			√		
42	¿Cuenta con procedimientos de seguridad para el acceso al				√	

	sistema operativo al iniciar sesión?					
43	¿Se ha asignado a los usuarios un ID de usuario para el uso personal y exclusivo dentro de la organización?				√	
44	¿La organización cuenta con controles criptográficos para la protección de la información?				√	
45	¿Se proporciona información oportuna sobre las vulnerabilidades técnicas de los sistemas de que se utilizan?			√		
46	¿Existen planes de contingencia para asegurar la disponibilidad de la información después de una falla o interrupción en los procesos?			√		
47	¿Los registros confidenciales están protegidos ante destrucción, pérdida o falsificación, según lo establece el requisito legal, reglamentario o contractual de la fundación?		√			
AUDITORÍA INTERNA						
48	¿Cuenta la organización con revisiones internas respecto a la información que se procesa y los requerimientos técnicos y legales?			√		
GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN						
49	¿Es importante para la fundación conocer, identificar y enfrentar los riesgos asociados a la información?				√	
50	¿En las reuniones ordinarias que tiene la dirección ejecutiva, es frecuente tratar temas relacionados con los riesgos que afectan a la organización?			√		

51	¿La fundación ha identificado fallas de seguridad como: • Violaciones de seguridad que involucra al personal de la fundación. • Errores u omisiones por parte de los usuarios. • Abusos por parte de los encargados de los sistemas de información.			√		
52	¿La fundación cuenta con un plan para tratar el impacto de los riesgos asociados a la información?			√		
	Total		14	81	64	
	Promedio		2.80	16.20	12.80	

Con base al análisis Likert se observa que existe un alto índice de riesgo en el área Tecnología e Innovación, se considera el área más sensible ya que son los responsables de garantizar que la información que se procese dentro la Fundación se mantenga integra, pero a consecuencia de la ausencia de no tener políticas debidamente documentadas y aplicadas en todas las áreas eleva el nivel de riesgo en toda la organización; así mismo la falta de capacitación del personal en la prevención del riesgo. Para controlar los riesgos identificados anteriormente, se detalla la estructura que recomienda la ISO 31000 para establecer un marco de referencia que ayude a mitigar los riesgos.

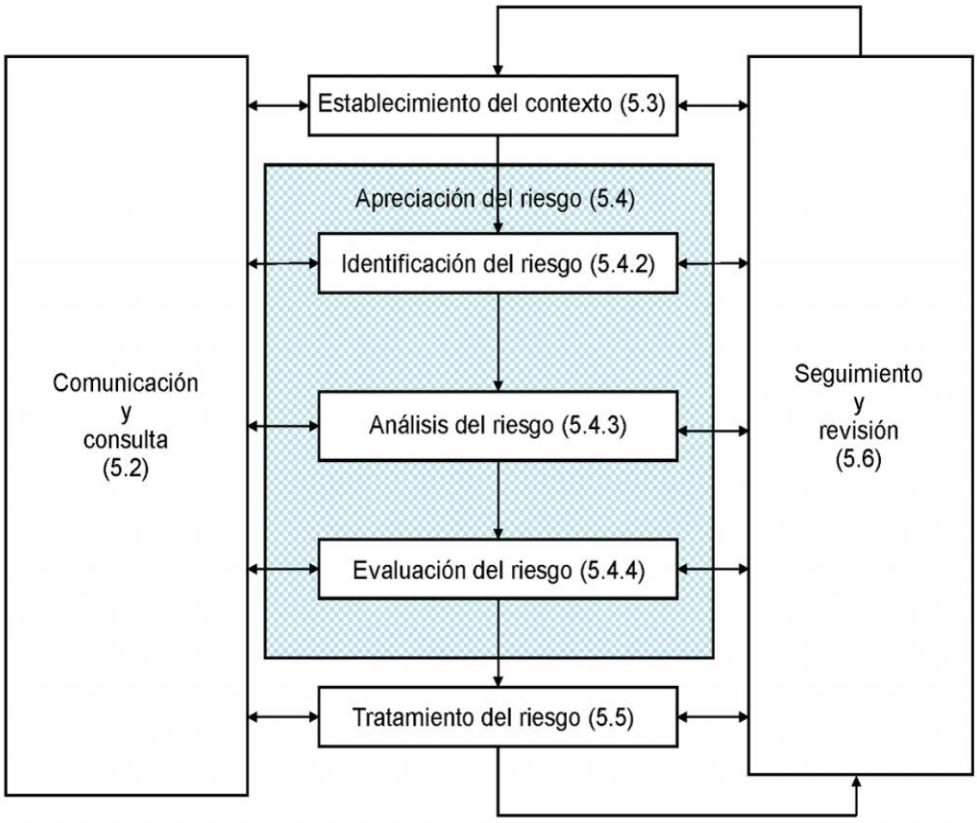


Figura 5 Estructura del marco de referencia para el tratamiento del riesgo

Fuente: ISO 31000

3.2.1.5 Inventarios de activos

La Fundación un Futuro Mejor cuenta con un inventario detallado de los activos que posee y que serán incorporados al SGSI, para determinar los riesgos de cada uno y controlarlos según el marco de referencia de los riesgos.

Tabla 15

Inventario de activos

Categoría	**Tipos de activos**
Sistemas	• Correo Institucional por medio de Office 365. • Página Web Hosting Externo. • Sistema Administrativo Financiero. (SAF) • Sistema de Recursos Humanos.
Información	• Base de Datos Institucional. (SIIDB) • Sistema de Intermediación Laboral. • Sistema de Fomento al Emprendedurismo
Software	• 300 Licencias Windows XP. • .
Hardware	Infraestructura de red: • 4 Switch 3Com 2250 sfp • 3 Switch 3Com 2226 sfp • 1 Switch Allied Telesis • 7 Switch 3Com 4226T • 2 Router Cisco 2600 • 4 Media Converter • 2 Firewall WacthGuard 55e • 1 Firewall WacthGuard 550e • 4 Cisco Linksys 300n Servidores: • 5 Servidores de red HP / LIEBERT 2KVA l) 20 Computadoras Notebook (PC Portátil) m) 183 Computadoras desktop, monitor, teclado, mouse, cpu. • 33 Impresores • 6 Scanner • 50 UPS • 15 Webcam • 1 Equipo de diseño gráfico: PC, UPS, monitor y periféricos. • 6 Monitores • 8 CPU • 3Fotocopiadora multifuncional

Fuente de elaboración: Inventario proporcionado por la Fundación un Futuro Mejor

3.2.1.6 Identificación de activos críticos, vulnerabilidades, valorización del riesgo y amenazas.

Con base a la identificación de los activos que posee la institución, se consideran como críticos aquellos que son estratégicos para su mejoramiento y que utilizaran como parte fundamental para el desarrollo de los objetivos de la institución.

En la siguiente tabla se presentan los activos críticos, así como su vulnerabilidad, la valorización del riesgo y las amenazas que poseen dichos activos.

Tabla 16

Detalle de activos críticos

Activos críticos	Vulnerabilidad	Valorización de riesgo	Amenazas
Sistema contable SAF	Este sistema está distribuido para usarlo por niveles de accesos, el contador general posee la categoría de administrador, y es el que da acceso a los usuarios y auxiliares quienes procesan la información. El mantenimiento del sistema es externo ya que no se cuenta con los permisos, para modificar la base de datos, en el 2011 hubo pérdida de la información contable de 3 meses, el origen de esta pérdida fue por falta de capacidad del servidor y por no	El riesgo en el uso del sistema es muy alto.	El acceso físico y el uso de la red sin autorización puede ocasionar graves problemas a la institución.

	realizar copias de respaldo, además del uso inadecuado de los usuarios.		
Servicio de internet	En la medida que la institución ha ido creciendo se ha visto en la necesidad de incrementar el ancho de banda del internet, para cubrir las necesidades de todas las áreas involucradas para trasmitir y comunicar la información que se procesa y que necesita transferir a clientes internos y externos, donantes, proveedores. Algunos usuarios tienen restringidos ciertos sitios web.	En este activo el riesgo es alto debido a que es la principal herramienta de trabajo.	El ingreso de correos no deseados que contengan virus puede ingresar a la base de datos del sistema, ya que la ingeniería social manipula a los empleados a través de correos electrónicos que se consideran seguros, pero que contienen virus.
Infraestructura de red	La institución cuenta con el cableado necesario para que la comunicación de la red sea efectiva, pero no cumple con los protocolos de seguridad.	EL riesgo es Alto no se cuenta con planes de contingencia.	Las acciones humanas pueden ocasionar graves problemas en la manipulación errónea de la red, así mismo el no tener planes de contingencias para enfrentarlos.
Personal de soporte técnico	Personal asignado para el área está capacitado para atender todas las necesidades, aunque no cuenta con suficiente personal para cubrir toda la institución.	El riesgo es medio debido a que el personal no alcanza a cubrir todas las necesidades.	a) No tener un registro de incidentes no permitirá tener control de los problemas que tienen mayor ocurrencia. b) La falta de personal no permite solventar de inmediato los incidentes ocurridos en los tres polideportivos

Recurso humano	El personal con el que cuenta actualmente es de 150 empleados, a la fecha no se brinda capacitación sobre la seguridad de la información, aunque se tiene conocimiento de que el personal es la parte más vulnerable dentro de cualquier organización ya que puede ser manipulado o engañado.	Se considera alto este riesgo debido que al personal no se concientiza sobre la importancia de tener una cultura de seguridad.	a) El personal es la parte más sensible en cualquier organización debido a que posee los conocimientos y puede manipular la información, por lo que un empleado insatisfecho puede ocasionar graves problemas. b) La falta de capacitación a los empleados no le permite tener una cultura de seguridad de la información.
Infraestructura física	Posee espacio suficiente en la ubicación de los servicios tecnológicos, se cuenta con cámara de seguridad en algunos sectores, aunque no las suficientes, y lamentablemente no cuenta con protocolos de seguridad que ayude a garantizar la seguridad en los accesos a las instalaciones.	Se evalúa el riesgo como medio, debido a que es necesario procesos de control para los accesos a terceros a las instalaciones.	El acceso de proveedores, clientes, beneficiarios de los programas puede generar pérdida de equipo, por robo, si no se cuenta con los protocolos de seguridad debidamente documentados para ejecutarse, en los procesos.

Fuente: Elaboración propia en base a la información proporcionada de la Fundación Un Futuro

3.2.1.7 Determinación del diagnóstico en base a los controles de la ISO 27001

En la siguiente tabla se determina cuáles son los controles que la organización está aplicando y los que no utiliza. Esto permitirá poder evaluar la importancia de trabajar bajo los estándares internacionales.

Tabla 17

Diagnóstico de la organización versus controles de la ISO 27001

Controles	Diagnóstico de la organización	Resultado del diagnostico
5. Políticas de Seguridad	• La organización no posee un conjunto de políticas que estén documentadas, ni en proceso de elaboración	No cumple con este dominio
6.Organizacion de la seguridad de la información	• Actualmente posee un área de soporte técnico que es quien controla los procedimientos que se han establecido para brindar los servicios de información a todas la áreas de la fundación, pero no se ha establecido quienes son responsables de resguardar la información	La administración no ha asignado responsable para organizar la seguridad de la información
7.Gestión de Activos	• Se ha realizado un levantamiento de inventario; se cuenta con un listado de asignación de los mismos al personal, pero no se cuenta con un reglamento.	En esto dominio no se cumple en su totalidad debido a que no existe un reglamento de aplicación.
8. Seguridad de recursos humanos	• La organización posee el departamento de recursos humanos, que es quien realiza el trabajo de reclutamiento de nuevos empleados, ellos investigan al postulante antes de su contratación, no cuenta con contratos de confidencialidad de la información, aunque el contrato individual de trabajo si contempla la cláusula de confidencialidad.	La administración no cumple con este dominio en su totalidad.

	• No cuenta con acciones disciplinarias para los empleados que infringen la seguridad de la información. • No cuenta con un programa de capacitación en el ámbito de la seguridad de información	
9. Seguridad física y ambiental	• El área más sensible es donde se encuentran los servidores, y para ingresar a ese espacio físico la organización cuenta con un sistema de cerradura digital donde solo tiene acceso el personal de soporte técnico. • A la fecha no está preparado para los desastres naturales como son inundaciones, algunas áreas de las instalaciones cuenta con extintores en caso de incendios.	La administración no aplica todos los dominios y es necesario identificar los riesgos naturales para mitigar los incidentes
10. Gestión de las comunicaciones y operaciones	• No se cuenta con procedimientos documentados, aunque se elabora bitácoras de servicios efectuados al cliente interno. • No se realizan revisiones de auditorías a nivel de sistemas • Se cuenta con el administrador de accesos firewall • Se realizan copias de seguridad semanalmente, aunque no existe ninguna política por escrito. • El uso de dispositivos extraíbles como memoria USB, se usan libremente en los equipos, sin ninguna medida de seguridad. • La divulgación de la información a externos por medio de correo electrónico, no cuenta con políticas documentadas. • Solo se realiza monitoreo al sistema contable, ya que se considera como el más importante dentro de la ONG, los demás programas no tienen ningún tipo de supervisión.	Faltan las políticas documentadas

11. Control de acceso	• No posee políticas documentadas. • Para la asignación de contraseñas para los usuarios existen procedimientos para su inscripción y desactivación de los mismos, este procedimiento no está documentado como política. • Se han realizado recomendaciones a los usuarios en el uso del equipo, pero no hay nada por escrito. • Los usuarios tienen restricciones en el uso de las redes sociales. • Realiza el proceso de autentificación de contraseñas • No aplica con políticas de control de accesos, solamente con medidas de restricción de acuerdo a las funciones de cada usuario. • La telefonía móvil solo se podrá conectar a la red si está autorizado de lo contrario está restringido. • El acceso a la red de internet por terceras personas solo se brinda a través del área de soporte técnico.	No aplican este dominio en su totalidad
12. Adquisición, desarrollo y mantenimiento de sistemas	• La fundación no utiliza mecanismos de validación de nuevos sistemas. • No se cuenta con políticas de criptografía, pero si se protege la información en los servidores con este lenguaje.	No implementa este dominio
13. Gestión de incidentes en la seguridad de la información.	• El área de soporte técnico de informática no posee los procedimientos formales para reportar los incidentes ocurridos a los usuarios. • No se realiza un programa de mantenimiento preventivo a los equipos.	No existe políticas ni herramientas para ejecutar este dominio

14. Gestión de la continuidad comercial	• No tiene un plan de contingencia de reacción ante el paro de actividades que afecte la continuidad de las operaciones.	Posee plan de contingencias
15. Cumplimiento con requerimientos Legales.	• No se realiza revisión de auditoría a nivel informática. • La administración es la responsable de cumplir con todas las políticas y procedimientos establecidos para la seguridad de la información.	No cumple con este dominio

Fuente: Elaboración con base a la ISO 27001 y entrevista realizada al personal de la Fundación un Futuro Mejor

3.2.1.8 Implementación

En esta fase se establecen los requisitos generales y los criterios para aplicar el sistema de seguridad de información en la Fundación un Futuro Mejor, para luego realizar la ejecución del sistema. A continuación se detalla en la siguiente Tabla:

Tabla 18 *Requerimientos de la norma técnica según la ISO 27001*

Requisitos de la Norma	1 Procedimiento / documentado	2 Definir/ Documentar/ acción	3 Medición / Revisar	4 Método o metodología	5 Registro	6 Controles a implementar	7 Planificar	Comentarios Generales
Requerimientos generales	Trabajar bajo los lineamientos de la ISO 27001, permite Establecer, implementar, operar, monitorear, mantener y mejorar los procesos dentro de las ONGs.	Permite documentar todos los procedimientos y las actividades de las ONGs, creando un marco de referencia normativo.		PDCA		Todas las áreas de la Fundación.		Elaborar un marco de referencia para su aplicación.

Establecer y manejar el SGSI								
Establecer el SGSI	Documentar los procedimientos	-Establecer el límite y alcance del sistema de información -Elaboración de políticas -Asignación de responsabilidades de la organización	Aceptación del riesgo. Análisis y Probabilidad de ocurrencia del riesgo. Evaluación del impacto del riesgo en la ONG.	En este proceso se establece un marco de referencia de evaluación de riesgo en base la ISO 31000		Detección de vulnerabilidades y amenazas Previsión del riesgo.		
Implementar y operar el SGSI		Formulación del tratamiento del riesgo Asignación de responsabilidades. Medición de matrices Desarrollo de capacitación.	Efectividad de los controle en su aplicación.		Bitácoras de incidentes ocurridos.	Detección y respuesta a los incidentes.		

Monitorear y revisar	Monitoreo de los procedimientos y su cumplimiento.	Definir Lineamientos de revisión. Determinar si son efectivas las acciones tomadas.	Medir la efectividad de los controles.		Revisar los registros de incidentes ocurridos durante la ejecución los controles.			
Mantener y mejorar	Aplicación de acciones preventivas y correctivas.		Evaluación de acciones aplicadas.		Eventos ocurridos durante la aplicación de los controles.			
Requerimientos de documentación								
General	Enunciar las políticas. Establece procedimientos y controles. Responsable de aplicar los controles.		Evaluación de riesgo.		Decisiones gerenciales	Planeación, operación, y procesos de seguridad de la información.		

Control de documentos	Establecer un Sistema de seguridad de información donde se documente todos los procesos.					Aprobación del sistema.	Protección y control de los procedimientos documentados.	
Control de registros	Establecer evidencias y registros que estén acordes a los requerimientos de la ISO.	Implementar los controles.			Registro de evidencias Desempeño del sistema de seguridad y de los incidentes ocurridos.			

3.2.1.9 Selección de los controles de cumplimiento de los objetivos para establecer los procedimientos.

Según lo establece la ISO 27001, se diseñara el sistema de seguridad de la información para establecer los procedimientos que conlleven el fiel complemento de los mismos dentro de la organización

Tabla 19

Normativa de cumplimiento de la ISO 27001

Apartado	Procedimiento
5. RESPONSABILIDAD DE LA DIRECCION.	
5.1 Compromiso de la dirección	**Documentar la evidencia del compromiso de la dirección** • Establecer política • Establecer objetivos • Asignación de roles y responsabilidades para control interno • Comunicar importancia del objetivo de seguridad y cumplir la política • Proporcionar recursos para desarrollar, implementar, monitorear, revisar, mantener y mejorar el sistema • Decidir el criterio para la aceptación del riesgo y niveles aceptado • Asegurar que se realicen las auditorías • Realizar revisiones generales
5.2 Gestión de recursos	La administración debe determinar y proporcionar los recursos necesarios • Establecer, implementar, operar, monitorear, revisar, mantener y mejorar el sistema de seguridad.

	• Asegurar que los procedimientos de seguridad de la información respalden los procedimientos comerciales • Identificar y tratar los requerimientos legales y reguladores y las obligaciones de seguridad contractuales • Mantener una seguridad adecuada mediante la correcta aplicación de todos los controles implementados • Llevar a cabo revisiones cuando sea necesario y reaccionar apropiadamente ante los resultados de estas revisiones • Donde se quiera mejorar la seguridad del sistema Determinar que el personal posea las competencias para asumir las responsabilidades asignadas se requiere que el personal cumpla con el siguiente listado de conocimientos : Determinar capacidades necesarias para el personal que realice el trabajo que afecta el sistema de seguridad • Proporcionar capacitación o realizar otras acciones (emplear personal competente) para satisfacer estas necesidades • Evaluar actividades de las acciones tomadas • Mantener registros de educación, capacitación, capacidades, experiencia y calificaciones Es importante que el personal clave este consiente de la relevancia e importancia de sus actividades de seguridad de información y como debe contribuir al logro de los objetivos del sistema de seguridad de la información.
6.AUDITORÍAS INTERNAS	• Realizar auditoría interna. • Cumplir con requerimientos de la ISO 27000 • Cumplir con requerimientos de seguridad identificados • Implementar y mantener de manera efectiva: • Un programa de revisión de auditoría. • Definir claramente el criterio, alcance, frecuencia y métodos a utilizar. • Asegurar la objetividad e imparcialidad en el proceso de auditoría.

7.REVISIÒN GERENCIAL	
7.1 General	La administración debe revisar el sistema de seguridad en intervalos de 1 año, y verificar que su cumplimiento es idóneo y efectivo.
7.2 Insumo de la revisión	En insumos de revisión incluir: • Resultados de auditorías • Retroalimentación de las partes interesadas • Técnicas, productos o procedimientos a usar • Estatus de acciones preventivas y correctivas • Vulnerabilidades o amenazas no tratadas • Resultados de mediciones de efectividad • Acciones de seguimiento • Cualquier cambio que afecta los procedimientos y políticas establecidas • Recomendaciones para mejoramiento
7.3 Resultado de la revisión	Del resultado de las revisiones permitirá realizar cambios que pueden ser significativos e incluir las siguientes líneas: • Incluir mejoramiento de actividad del sistema de seguridad • Actualización de la evaluación del riesgo • Modificación de procedimientos y controles que afectan la seguridad de información • Necesidades de recursos • Mejoramiento de cómo se mide la efectividad en los procesos
8 MEJORAMIENTO DEL SGSI	
8.1.Mejoramiento continuo	• Mejorar continuamente la efectividad del sistema de seguridad de información y las políticas
8.2 Acción correctiva	Realizar acciones para eliminar causas de no conformidades: • Identificar no conformidades • Determinar las causas de no conformidades

	• Evaluar la necesidad de acciones para no repetirlas • Determinar e implementar la acción correctiva • Registrar los resultados de la acción tomada • Revisar la acción correctiva
8.3 Acción preventiva	Determinar la acción para eliminar la causa de la no conformidad potencial • Identificar las no conformidades potenciales • Evaluar la necesidad para accionar y evitar ocurrencia • Determinar e implementar la acción preventiva • Registrar los resultados de acción tomada • Revisar la acción preventiva tomada Identificar riesgos cambiados en gestión y requerimientos de acción preventiva Determinar con base a resultados de la evaluación del riesgo, las acciones preventivas

Fuente: Elaboración en base la ISO 27001

3.3 Monitoreo y evaluación:

Se realizará revisión de los procesos y políticas establecidas, se utilizará la metodología PDCA (Planear, Hacer, Chequear, Actuar) para garantizar la mejora continua del sistema.

3.4 Desarrollo del caso práctico

3.4.1 Conocimiento de la organización

La Fundación un Futuro Mejor es una organización sin fines de lucro no gubernamental, apolítica, que nace como una alternativa de solución a la problemática de la niñez y juventud en zonas de alto riesgo de violencia, brinda apoyo en la

formación profesional complementaria en el tiempo libre a través del Programa Integral Juvenil Don Bosco de la cual cuenta con 4 componentes: Computación, Valores, Deportes y Medio Ambiente, dicho programa está dirigido a estudiantes desde sexto a noveno grado, se ha atendido a más de 55,000.00 estudiantes de un aproximado de 60 centros escolares, siendo el Ministerio de Educación y los Directores de centros escolares un apoyo fundamental para el fortalecimiento de dicho programa.

La Fundación Un Futuro Mejor nace el 17 de agosto de 2001, como iniciativa de la Institución Salesiana a través de un alianza público privado con los Gobiernos de España y de El Salvador proporcionando los fondos para la construcción y equipamiento del polideportivo en las zonas de Soyapango, San Miguel y Santa Ana siendo el primero el administrador de los polideportivos.

Desde sus instalaciones brinda oportunidades de desarrollo integral al joven ofreciendo una casa de puertas abiertas que acoge a una comunidad creyente que comunica la fe, escuela que encamina hacia la vida, patio donde se comparte la amistad. Se caracteriza por desarrollar torneos deportivos a través de la coordinación de oratorio, también se desarrollan proyectos en el ámbito de la prevención de la violencia a través de los diferentes proyectos como son la gestión socio laboral, Centro de Atención Familiar, Coordinación de pastoral y el Programa Integral Juvenil; también se gestionan proyectos con diferentes organizaciones con responsabilidad social y comprometidos con la juventud. Dentro de las diferentes organizaciones podemos mencionar, la Cooperación Estadunidense USAID, Cooperación Española AECID,

Fondos de cooperación Suiza, Fondos de la Unión Europea, Fondo de las Naciones Unidas UNICEF, UNFPA.

Misión

Construir una educación integral liberadora e innovadora con Carisma Salesiano en niño(a) s jóvenes de escasos recursos y/o condición de riesgo en su entorno familiar.

Visión

La Fundación Un Futuro mejor es un referente nacional y regional en el desarrollo integral de jóvenes con perspectivas nuevas y distintas hacia la construcción de un proyecto de vida trascendente

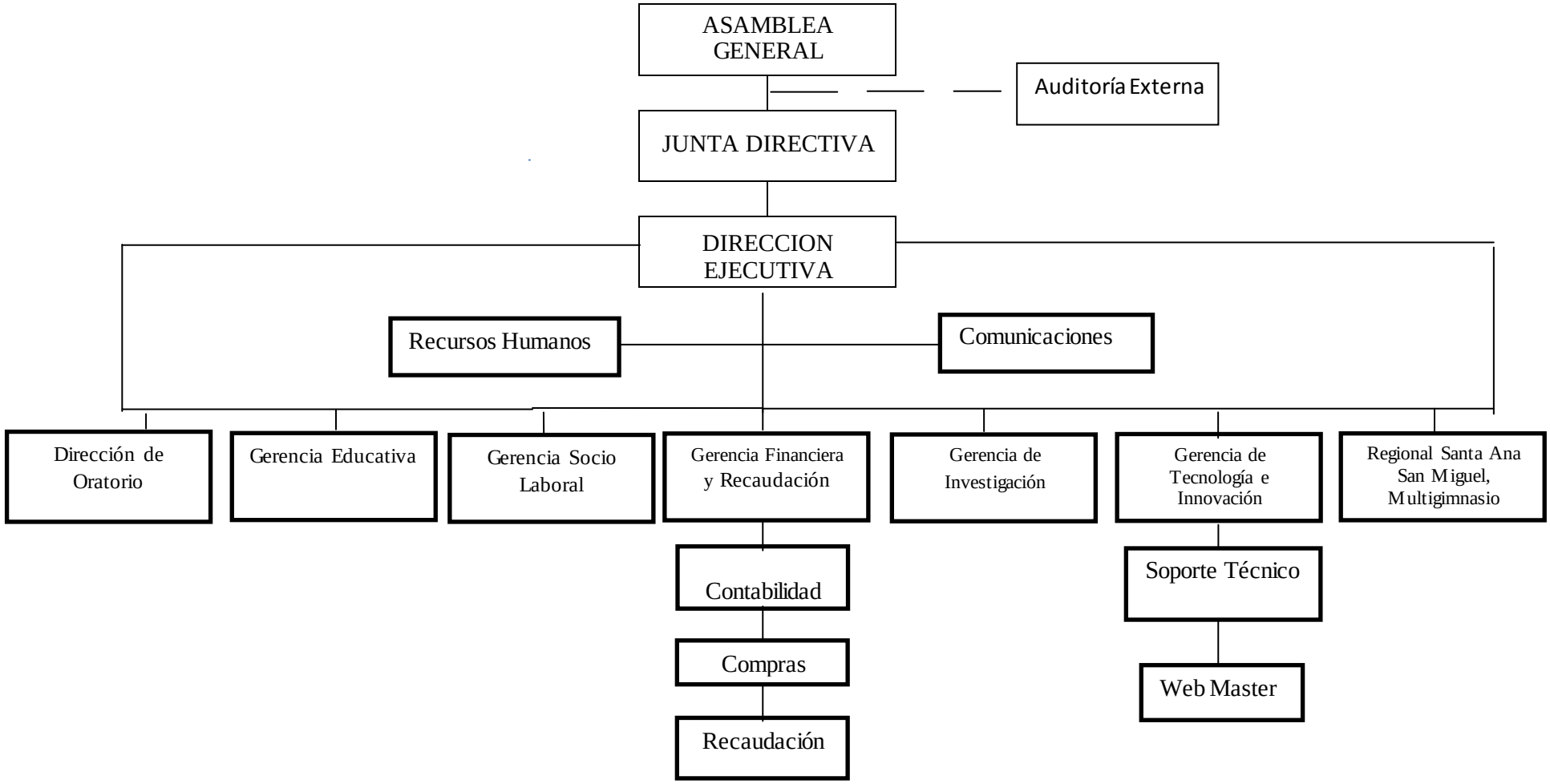
Valores Institucionales

- Amabilidad
- Espíritu de familia
- Apertura
- Solidaridad
- Testimonio
- Transparencia
- Eficiencia
- Efectividad

- Auto sostenibilidad
- Osadía pastoral

La fundación cuenta con la estructura organizativa según lo exigen la normativa legal, a continuación se presenta la Junta Directiva vigente en este periodo.

Figura 6 Organigrama de la Fundación Un Futuro Mejor



A continuación se presentan el detalle de proyectos que tiene en ejecución de los cuales debe rendir cuenta mediante informes financieros y cumplimiento de indicadores.

Tabla 20

Proyectos en ejecución a la fecha

Fundación un Futuro Mejor
Informe de proyectos en Ejecución

N°	MONBRE DEL PROYECTO	NOMBRE DEL COOPERANTE	PRESUPUESTO	EJECUTADO A JUNIO 2016
1	Educación para la Niñez y Juventud	USAID	$ 5,933,925.00	$ 2,407,450.88
2	PROYECTO JOVENES	AECID-Cesal	$ 469,440.00	$ 58,619.94
3	Jóvenes Creando Futuro	Brucke Le Pont	$ 321,280.00	$ 83,298.42
4	EDYTRA	Union Europea	$ 195,027.29	$ 176,014.01
5	Escuela Emprende	Dona tu Cora	$ 13,745.75	$ 12,666.20
6	CCPVJ.	Union Europea	$ 1,657,650.00	$ 306,757.29
7	Fortalecimiento de desarrollo académico,	RTI	$ 82,103.84	$ 26,393.80
8	Jóvenes Emprendedores en TI	Silicon Valley Community Foundation	$ 15,000.00	$ 2,722.41
9	Embajadores Digitales	Telemovil de El Salvador	$ 14,300.00	
10	CISCO It Essentials	Colegio Liceo San Miguel	$ 10,500.00	$ 230.56
11	CISCO It Essentials	Colegio Espíritu Santo	$ 1,808.00	$ 148.37
12	COMPUMOVIL	Fundación Simán	$ 23,921.10	$ 11,502.69
13	Aldeas Infantiles SOS-Tecnología	Telemovil de El Salvador	$ 13,450.00	$ 10,343.37
14	Aldeas Infantiles SOS-Ingles	Telemovil de El Salvador	$ 12,000.00	$ 8,674.11
			$ 8,764,150.98	**$ 3,104,822.05**

Fuente: Información proporcionada por la administración de la Fundación un Futuro Mejor

3.4.2 Determinación de los activos

Para realizar la evaluación del riesgo se ha determinado el marco de referencia de la ISO 31000 que permite tener un esquema de evaluación y tratamiento del riesgo.

A continuación se presenta el listado de los activos que posee la Fundación según la siguiente tabla:

Tabla 21

Detalle de Inventario

SISTEMA DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA ISO 27000

Nombre de la Organización : Fundacion un Futuro Mejor

Criterio de Valorizacion de riesgo : Disponibilidad

Corr	Activos	Evaluacion del riesgo		
		Bajo	Medio	Alto
1	Correo Institucional por medio de Office 365.			X
2	Página Web Hosting Externo.			X
3	Sistema Administrativo Financiero. (SAF)			X
4	Sistema de Recursos Humanos.		X	
5	Base de Datos Institucional. (SIIDB)			X
6	Sistema de Intermediación Laboral.			X
7	Sistema de Fomento al Emprendedurismo			X
8	300 Licencias Windows XP.	X		
9	2 Router Cisco 2600			X
10	2 Firewall WacthGuard 55e		X	
11	1 Firewall WacthGuard 550e		X	
12	4 Cisco Linksys 300n		X	
13	5 Servidores de red HP / LIEBERT 2KVA			X
14	20 Computadoras Notebook (PC Portátil)			X
15	183 Computadoras desktop, monitor, teclado, mouse, cpu.			X

3.4.3 Establecimiento de contexto

La administración de los riegos es una parte integral de las buenas prácticas y que consta de pasos sistemáticos que permite identificar, analizar, evaluar tratar y monitorear seguir este proceso posibilita la mejora continua ya que ayuda a evitar y mitigar perdidas.

3.4.4 Identificación de los riesgos de la Fundación "Un Futuro Mejor"

En el siguiente procedimiento se identificaran los factores internos y externos de riesgos que permite determinar las fuentes y características para posteriormente evaluar de forma acertada los riesgos, según se detalla en la siguiente tabla:

Tabla 22

Definición y clasificación de riesgos

Nº	FACTORES DE RIESGOS	AREAS DE IMPACTO PROCESOS ESTRATEGICOS								
		Direccion Ejecutiva	Recuros Humanos	Comunicaciones	Gerencia finanicera y Recaudacion de fondos	Gerencia educativa	Gerencia socio laboral	Gerencia de investigación	Gerencia de tecnologia e inmovación	Instalaciones Regionales, Santa Ana , San Miguel
1	RIESGO DE INCUMPLIMIENTO LEGAL	X	X		X					
2	RIESGOS FINANCIEROS	X	X		X					
3	DAÑOS O DESTRUCCIÓN DE ACTIVOS	X	X	X	X	X	X	X	X	X
4	RIESGOS DE RECURSOS DE TI	X	X	X	X	X	X	X	X	X
5	RIESGOS AMBIENTALES	X	X	X	X	X	X	X	X	X
6	DECISIONES ERRÓNEAS	X	X		X				X	
7	PÉRDIDA DE IMAGEN	X	X	X	X	X	X	X	X	X
8	COMPORTAMIENTO HUMANO	X	X	X	X	X	X	X	X	X

3.4.5 Análisis de riesgos

Según la ISO 31000 recomienda calificar los riesgos a partir de las variables que están asociadas a la probabilidad de ocurrencia y el impacto que está asociado a los riesgos y para ello se utilizara el mapa de calor para medir los riesgos inherentes a los activos de la institución como se muestra en la siguiente tabla:

Criterio de medición de riesgo

La magnitud del riesgo se mide de acuerdo a la fórmula siguiente:

Magnitud= Probabilidad x impacto

En base a esta fórmula se establece el mapa de calor para cuantificar el riesgo:

Tabla 23

Magnitud de Medición según la probabilidad e impacto

Probabilidad: Frecuencia de que ocurra el riesgo	**Impacto:** La manera en que afecta el resultado en los procesos de la institución
Alto: Es muy factible de que se presente el riesgo	**Alto**: Porcentaje que afectara los resultado del proceso y la disponibilidad el servicio
Medio: Es la factibilidad que ocurra el riesgo	**Medio:** El porcentaje es medio y el efecto en los resultado
Bajo: Es poco factible que se presente el riesgo	**Baja:** el efecto de este porcentaje es bajo

Tabla 24 *Detalle priorización*

Probabilidad	Alta	B	A	A
	Media	B	B	A
	Baja	C	B	B
		Bajo	Medio	Alto
		Impacto		

A continuación se presenta la siguiente tabla donde se detalla calificación, valorización y la evaluación de los riesgos:

Tabla 25

Matriz de calificación, valoración y evaluación

ACTIVOS CRITICOS	RIESGOS	CAUSA	EFECTO	CALFICACION Y VALORIZACION						PRIORIDAD
				PROBABILIDAD			IMPACTO			
				BAJO	MEDIO	ALTO	BAJO	MEDIO	ALTO	(A+B+C)
Sistema SAF	Pérdida de información no procesada en los servidores	No se realizan copia de respaldo en tiempo programado	Pedida de integridad de los datos		X				X	A
	Manipulación errónea de los empleados	Registros contables mal efectuados, Modificaciones sin autorización			X				X	A
	Falta de respaldos de seguridad.	Descuido del personal responsable			X				X	A
	Accesos no autorizados	Falta medidas de seguridad		X				X		B
	Infección de virus.	No aplica medidas de protección			X				X	A
	Modificación no intencionada de información.	Errores involuntarios		X			X			C
	Ataques externos.	Manipulación y engaño de agentes externos a la institución			X				X	A
Servicio de internet	Falta de capacidad del ancho de banda y saturación no disponibilidad del servicio de internet	Falta de capacidad económica para adquirir mayor capacidad de ancho de manda	Afecta la disponibilidad de la información	X				X		B
	Falta de conexión..	No poseer el equipo para establecer conexión			X			X		B
	Saturar los enlaces de la red.	Los usuarios accedan a paginas y redes sociales que no están autorizadas			X			X		B
	Acceso no autorizado a la red	Utilizar las claves de la red wifi		X			X			C
	Problemas en los equipos de conectividad	Equipos obsoletos			X			X		B
	Fallo de equipo de proveedor	Falta de capacidad de brindar los servicios oportunos		X			X			C
	Acceso a información no autorizada desde la red	Ataques externos			X				X	A
	Accesos móviles	Saturan la red el ancho de banda		x			x			C

Infraestructura de red	Fallo el equipo y mantenimiento de la red.	Falta de mantenimiento al equipo	Afecta la disponibilidad de la información		X				X	A
	Falta de conectividad a los dispositivos de la red	Falla de Switch por equipos en mal funcionamiento		X				X		B
	Mal uso de los administradores de la red	Desgastes de los conectores de la red			X				X	A
	Falla de licencias	Vencimiento de licencias		X			X			C
	Colapso en equipo por desastres naturales	No posee planes de contingencias para evitar perdidas de equipos		X				X		B
	Acceso no controlado a los equipos	No hay control en las aula de equipo informático		X				X		B
	Instalaciones no seguras para los activos de red.	Mala instalación		X			X			C
	Revelación de información crítica al no haber políticas de acceso a la red	Falta de restricción de en el manejo la información			X				X	A
	Destrucción de red o equipo	Accidentes ocurridos por mal uso del equipo		X				X		B
Estructura física	Falta de registros de acceso a las instalaciones	Falta de control de las entradas y salidas de visitantes	Pedida de la condifencialidad de la informacion	X				X		B
	Cámaras insuficientes para todas las áreas	Espacio sin control de vigilancia			X				X	A
	Inundaciones y terremotos	Falta de planes de contingencias para desastres naturales		X				X		B
	Falta de identificación a terceros proveedores	Accesos de entradas sin control de registros a proveedores		X			X			C
	Corte de energía eléctrica	No se aplica mantenimiento a las conexiones eléctricas				X			X	A
Recursos humanos	Falta de conocimiento en uso de los equipos	Mal uso de parte de los empleados para el manejo del equipo informático		X			X			C
	Personal insatisfecho	Falta de estimulo por su trabajo			X				X	A
	Personal no capacitado	No se concientiza sobre el la importancia del manejo de la información		X				X		B
	Divulgación de información clasificada	Manipulación y engaño de agentes externos a la institución			X				X	A
	Falta de acuerdo de confidencialidad	No se cuenta con acuerdos de confidencialidad			X				X	A
	Rotación del personal	Inestabilidad laboral		X				X		º

Para este proceso se determina la gravedad del riesgo los cuales se pueden clasificar de la siguiente manera:

Tabla 26

Clasificación del riesgo

A	Inaceptable: Riesgo alto	Se requiere acciones inmediatas y tratamiento del riesgo
B	Grave: Riesgo medio	Atención a los procesos y determinar planes de tratamientos , reportarlos a la gerencias
C	Aceptable: Riesgo bajo	Mitigar el riesgo con procesos administrativos

3.4.6 Tratamiento del riesgo

De acuerdo a la evaluación del riesgo cada una de las áreas debe implementar la forma de mitigar el riesgo y como controlarlo, esto implica establecer medidas de tratamiento para cada incidente ocurrido en las la operaciones diarias de la organización.

La ISO 27005 proporciona una guía para el tratamiento del riesgo, como se muestra en la siguiente tabla:

Tabla 27

Guía de tratamiento del riesgo

Reducción del riesgo	Para los riesgos identificados se deben establecer los controles adecuados para reducir y evaluar como aceptado el riesgo residual , lo cual será aceptado por la Dirección Ejecutiva
Retención del riesgo	Dependerá de cómo se evalúa el riesgo cuando se considera alto, medio, o bajo y el impacto que este genera y la probabilidad de ocurrencia.
Evitación del riesgo	Cuando se considere muy alto el riesgo y el costo el muy elevado y no se obtiene beneficio se evitara el riesgo , retirando las actividades de mitigación y control-
Transferir el riesgo	Se involucrará la participación de terceros como son las aseguradoras, cuando ya se tenga identificado el riesgo.
Aceptación del riesgos	Elaboración del plan donde se establece el porcentaje de aceptación riesgo,

Fuente: Elaboración en base la ISO 27005

3.4.7 Desarrollo del Sistema de Seguridad de la Información

Actividad a desarrollar	Responsable	Objetivo	Estrategia a utilizar	Documentos a utilizar
Fase 1: Presentación de la propuesta del SGSI				
Presentación de propuesta a la Dirección Ejecutiva y a la Gerencia de Tecnología e Innovación	Equipo que ha realizado la investigación	Dar a conocer los resultados obtenidos en la investigación y concientizar la necesidad de tener documentado las políticas mediante una normativa	Convocatoria de reunión para la presentación del SGSI	Propuesta de : Sistema de seguridad de información basado en la ISO 27000
Fase 2: Establecer el comité de seguridad de información				
Definir el área y el personal que conformara el comité para la seguridad información	Dirección Ejecutiva y Gerencia de Tecnología de Innovación	Delegar responsabilidades para la implementación del SGSI y el seguimiento , monitoreo del mismo	Programación de reuniones con el comité seguridad	Conocimiento de la propuesta de : Sistema de seguridad de información basado en la ISO 27000
Capacitación de comité	Gerencia de Tecnología de Innovación	Enseñar la metodología del SGSI	Reunión con el comité	Utilización del SGSI
Fase 3: Implementación del SGSI				
Desarrollo de programa de capacitación al personal	Comité de seguridad de información	Concientizar a todo el personal sobre las nuevas políticas y la importancia en el cumplimiento de las mismas	Reunión con todo el personal y las jefaturas	Divulgación del Sistema de seguridad de información basado en la ISO 27000
Elaboración de procedimientos y registros ya existentes	Comité de seguridad de información	Consolidar las funciones ya existentes de los empleados	Revisión de los procedimientos y adaptarlos a las ISO	Procesos y registros adaptados al SGSI
Fase 4: Desarrollo y Evaluación				
Programación de auditoria internas para la ejecución y planificación del SGSI	Gerencia de Tecnología de Innovación y comité de seguridad de información	Revisar el cumplimentó de la mejora continua	Supervisión de la auditoria	Desarrollo del procedimiento y programas de auditoria
Desarrollo de la ejecución de acciones correctiva y preventivas	Comité de seguridad de información		Revisión de la auditoria	Procedimiento de las acciones correctiva y preventivas
Identificación e implementación de mejora continua	Gerencia de Tecnología de Innovación y comité de seguridad de información		Evaluación de las mejoras	Conocimiento de la propuesta de : Sistema de seguridad de información

3.4.8 Sistema de seguridad de la información basado en la ISO 27000

A continuación se presenta el sistema de seguridad de información basado en la ISO 27000, lo cual podrá ser aplicado por todas las Organizaciones no Gubernamentales de El Salvador, ya que no importara el tamaño o naturaleza de sus actividades.

SISTEMA DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA ISO 27000

SEPTIEMBRE 2016
SAN SALVADOR, CENTRO AMÉRICA

INTRODUCCIÓN

Para la Fundación Un Futuro Mejor la información es considerada como un recurso que, como el resto de los activos que posee tiene valor y por consiguiente debe ser protegida de forma adecuada.

La información puede existir en muchas formas, impresa o escrita en papel, almacenada electrónicamente, transmitida por un medio electrónico, presentada en imágenes, o expuesta en una conversación; independientemente cual sea la forma que adquiere o los medios por los cuales se distribuye o almacena, el objetivo principal de la organización es proteger y evitar o minimizar las amenazas que ponen en riesgo la confidencialidad, integridad y disponibilidad de la misma.

Este sistema detalla las políticas de seguridad de la información y la forma como deben implementarse para dar cumplimiento a los controles y procedimientos establecidos, tomando como base la regulación técnica ISO/IEC 27001 que se refiere a los requisitos que debe contener un Sistema de gestión de seguridad de la información. La Organización se compromete a dar a conocer a todos sus miembros lo establecido en este sistema con el propósito de cuidar y garantizar las buenas prácticas para la protección de los datos.

OBJETIVOS

Objetivo General

- Proporcionar una herramienta que facilite la protección de los activos relacionados con el procesamiento de la información.

Objetivos Específicos:

- Identificar los riesgos asociados a la pérdida de confidencialidad, integridad y disponibilidad de la información y proporcionar tratamiento para contrarrestarlos.

- Asumir responsabilidad por parte de la organización en el cumplimiento de normas y estándares relacionados con la seguridad de la información, que permitan una mejora continúa de las actividades realizadas por cada miembro.

ALCANCE

La seguridad informática es de gran importancia para todas las organizaciones y es responsabilidad de cada uno de los colaboradores. Es fundamental identificar los requerimientos de seguridad y evaluar periódicamente los riesgos asociados al manejo de la información.

Las políticas de seguridad establecidas en este sistema, comprende todos los aspectos relacionados con la administración y control de la información, el cumplimiento va dirigido a todo el personal que desempeña funciones dentro de la organización como; la dirección, administración, los empleados permanentes y temporales, así como terceros instituciones nacionales y extranjeras que apoyan con donaciones a la organización.

A.1. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

REF.: Dominio 5.1. ISO/IEC27002:2005

Alcance: Determinar la dirección de la política en coordinación con los objetivos operacionales de la organización.
Objetivo: Proporcionar a la Dirección Ejecutiva una herramienta que permita establecer, implementar, monitorear y revisar controles que contribuyan en los procesos establecidos para el procesamiento de la información y el cumplimiento de las obligaciones legales y contractuales que está sujeta la organización.

Controles:

A.1.1.Política de Seguridad de la información

A.1.1.1. Documento de la política de seguridad de la información

Se debe emitir un documento que contenga el compromiso por parte de la Junta Directiva de la organización respecto a la seguridad de la información y la asignación de responsabilidades.

El encargado de aprobar las políticas de seguridad es la Junta Directiva es el ente que acepte y apruebe el sistema de seguridad de información

La Dirección Ejecutiva demuestra su apoyo mediante lo siguiente:

- Revisión y aprobación de las políticas de seguridad establecidas en este sistema.
- Difundir a todo el personal de la fundación que está directamente involucrado con el manejo de la información.

- Sancionar las violaciones realizadas a los lineamientos establecidos que afecten el cumplimiento de los objetivos. (Ver formulario de aplicación sanciones y medidas correctivas Anexo No 4.)
- Realizar reuniones periódicas para revisión y mejoramiento de las políticas.
- Establecer roles y responsabilidades para asegurar que las actividades se están realizando en el tiempo y forma establecida previamente.

A.1.1.2. Revisión de la política de seguridad de la información

Control:

Es responsabilidad de la organización, elegir un Comité de Seguridad de la Información que colabore con la definición, actualización y mantenimiento del sistema, realizando periódicamente según lo establezcan, revisiones en el control de documentos y registros.

Se recomienda un periodo de 3 años para la revisión y actualización del sistema, si la organización realiza revisiones antes de este periodo deberá ser por las siguientes causas:

- Se ha generado incidentes que requieren atención y respuesta.
- Identificación de nuevos riesgos asociados a la información.
- Surgimiento de cambios tecnológicos o en la organización que afectan directamente las actividades diarias.
- Se requiere mejorar los procesos ya establecidos.

Para llevar un control de las revisiones o modificaciones al sistema, se deberá utilizar el formulario detallado en el anexo No 5.

Cuando se solicite revisión o cambios al sistema, se deberá complementar toda la información que contiene este formulario y se colocará como anexo al final del documento. El encargado del área de Seguridad de la información evaluará las revisiones y cambios solicitados antes de pasar el informe a Junta Directiva para aprobación, en caso de ser denegada, se le informará al Departamento que realizó la solicitud y se dará a conocer los motivos por los cuales no fue aprobada.

Para identificar las revisiones emitidas al documento, se colocará al inicio de la página, fecha de aprobación, número de revisión y el motivo del cambio, además de añadir los cambios en hojas nuevas sin modificar el sistema. Todas las solicitudes aprobadas y rechazadas, serán conservadas por un periodo de tres meses a partir de la fecha de entrega.

B.2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

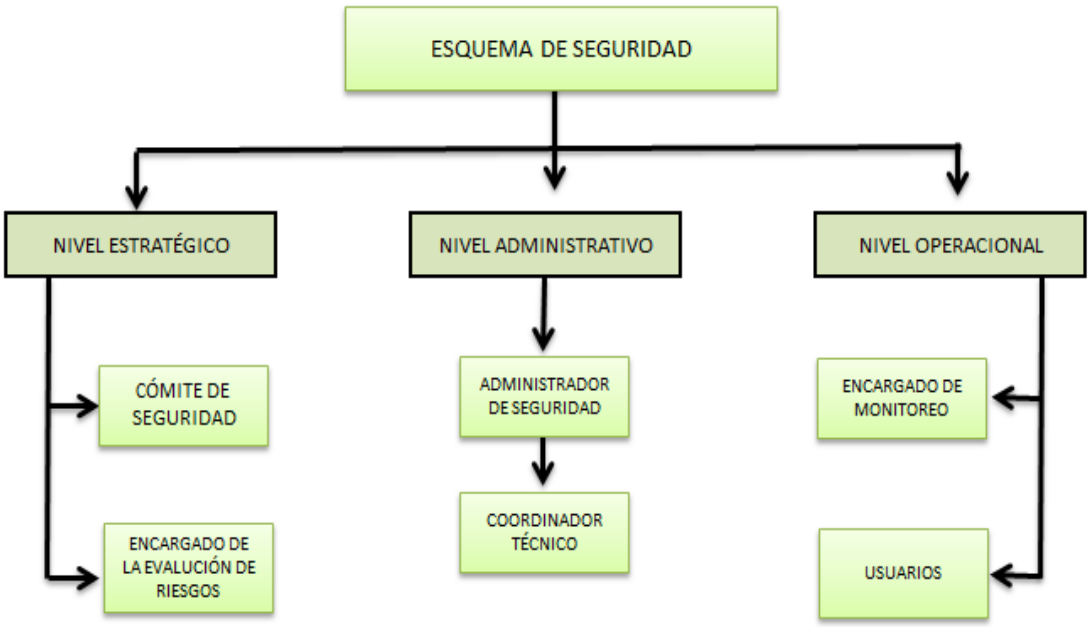
REF.: Dominio 6. ISO/IEC27002:2005

Alcance: La Dirección ejecutiva debe establecer un marco de referencia para iniciar e implementar la seguridad de la información dentro de la organización.
Objetivo: Tratar la seguridad de la información como parte importante de la estructura organizativa dentro de la institución.

Controles:

B.2.1. Organización interna

La organización establecerá un organigrama que representará la estructura de seguridad de la información, como se muestra en la siguiente figura:



- Nivel estratégico: En este nivel se encuentra el comité de seguridad, que es el principal responsable de velar por el cumplimiento de las políticas establecidas en el sistema, de su actualización y presentación ante la Junta Directiva, en apoyo del encargado de evaluación de riesgos, cuya labor es identificar las amenazas y elaborar un perfil del riesgo para orientar al comité cómo se debe proceder ante determinado evento.

- Nivel administrativo: Este nivel comprende las actividades desarrolladas por el administrador de seguridad que es el encargado de definir los roles y responsabilidades de cada usuario, con ayuda de un coordinador técnico que brinda soporte a todas las áreas de la organización.

- Nivel operacional: Este nivel está constituido por el encargado de monitoreo que da seguimiento a la aplicación del sistema y los objetivos trazados por el comité de seguridad, además es el responsable de guiar a los usuarios para el cumplimiento de las políticas establecidas en el sistema.

B.2.1.1. Compromiso de la Gerencia con la seguridad de la información

Control:

La Dirección ejecutiva debe apoyar de forma constante la seguridad de todas las áreas dentro de la organización, comprometiéndose y asignando responsabilidades de protección de los activos para mejorar de forma continua sus operaciones.

Para llevar a cabo esta actividad deberá:

- Verificar que las metas de seguridad sean identificadas y proveer los recursos necesarios para su cumplimiento.
- Crear, analizar y aprobar la política de seguridad de la información.
- Fomentar conciencia de seguridad a todos los empleados de la organización por medio de planes o programas que contribuyan a la formación de un ambiente seguro.

B.2.1.2. Coordinación de la seguridad de la información

Control:

La organización debe cuidar que todas las actividades relacionadas a la seguridad sean coordinadas por representantes de diferentes áreas como gerentes, usuarios, administradores entre otros, que posean un perfil adecuado para desempeñar sus funciones.

Los encargados de coordinar la seguridad deberán tener algunas de las siguientes características:

a) Disciplina para desarrollar su trabajo
b) Conocimiento de las operaciones de la organización
c) Confidencialidad
d) Habilidades personales
e) Responsable

Y deberán:

- Lograr que las actividades relacionadas a la seguridad se elaboren conforme a la política establecida.
- Aprobar metodologías como clasificación de la información, evaluación de riesgos, respuesta a los riesgos, identificación de amenazas, entre otros.
- Monitorear la información recibida y revisar los incidentes de seguridad.

Para llevar a cabo esta acción puede hacer uso de un cronograma, que permitirá llevar un control de las actividades realizadas durante las fechas establecidas previamente, para verificar su cumplimiento. (Ver anexo No 6 formato de cronograma de actividades)

B.2.1.3. Asignación de responsabilidades de la Seguridad de la Información

Control:

Se debe definir la asignación de responsabilidades para la protección de los activos y los encargados de llevar a cabo los procesos de seguridad específicos. (Ver anexo 7 matriz de asignación de responsabilidades)

- Revisar la estructura organizativa y las responsabilidades que cada empleado desempeña en el área
- Verificar si está documentado los niveles de autorización dentro de la organización
- Identificar los activos y determinar los procesos de seguridad a implementar para su protección.

B.2.1.4. Acuerdos de confidencialidad

Control:

Todos los empleados, miembros y terceras personas que tienen relación directa con las actividades de la organización deben aceptar los acuerdos de confidencialidad y no divulgación de la información, dicho acuerdo debe estar incluido ya sea en un documento independiente o como una cláusula anexa a los contratos de trabajo de los empleados o los acuerdos de servicios que prestan terceros. La información mínima que debe contener el documento se encuentra en el anexo No 8.

C.3. GESTIÓN DE ACTIVOS

REF.: Dominio 7. ISO/IEC27002:2005

Alcance: La organización debe identificar e inventariar sus activos y designar responsables del mantenimiento y cumplimiento de los controles aplicables a los mismos.
Objetivo: Proteger apropiadamente los activos de la organización.

C.3.1. Responsabilidad de los activos

C.3.1.1. Inventario de los activos

Control:

Cada área y sus colaboradores deben garantizar el uso y protección adecuada de los activos, además de realizar periódicamente un inventario que permita llevar un registro actualizado y evitar riesgos en las operaciones de la organización.

Se puede hacer uso de una bitácora que facilite la identificación y el control de los activos, como se muestra en el anexo No 9.

C.3.1.2. Propiedad de los activos

Control:

El encargado de la custodia de los activos consolidados será el comité de seguridad de la información, sin embargo cada área y empleado de la organización será responsable del equipo y los datos procesados.

Se consideran activos propiedad de la organización: la información, sistemas, archivos físicos, equipos (escritorios, portátiles, impresoras, redes, internet, correo electrónico, teléfonos, fax, entre otros).

C.3.2. Clasificación de la información

C.3.2.1. Lineamientos de clasificación

Control:

La información se deberá clasificar en función de su valor, requisitos legales, sensibilidad y criticidad para la organización.

Las actividades a realizar para llevar a cabo una adecuada clasificación son las siguientes:

- Definir la clasificación de un activo
- Revisión periódica
- Actualización de la información

C.3.2.2. Etiquetado y manejo de la información

Control:

Desarrollar procedimientos para el procesamiento, resguardo, transferencia, clasificación y destrucción de la información.

- El etiquetado se realizará a todos los activos que contenga información en formato físico o electrónico.
- Los sistemas que contenga información clasificada como sensible o crítica, debe llevar una etiqueta de clasificación apropiada que permita identificar su clasificación.

Para el tratamiento de la información según su clasificación se podrá utilizar un historial de revisiones según el contenido en el anexo 10.

D.4. SEGURIDAD DE RECURSOS HUMANOS

REF.: Dominio 8. ISO/IEC27002:2005

Alcance: Que la organización implemente medidas para la selección de los empleados, contratistas y terceros.
Objetivo: Definir lineamientos que permitan dar a conocer a los empleados, contratistas y terceros, los roles y responsabilidades para los cuales se han seleccionado y reducir el riesgo de robo, fraude o mal uso de los recursos de la organización.

Controles:

D.4.1. Antes del empleo

La selección del personal se regirá por las leyes vigentes en la República de El Salvador, Ley de equiparación de oportunidades y lo dispuesto en el Código de Trabajo, además del Reglamento Interno de Trabajo. Se verificará la información

proporcionada por el solicitante y se realizará investigación de los antecedentes. Cuando se haya finalizado el proceso de selección, se procederá a la inducción, información de actividades laborales, horarios, entre otros.

D.4.1.1. Roles y responsabilidades

- Se debe definir y documentar los roles y responsabilidades que cada empleado está obligado a cumplir de acuerdo con las medidas de seguridad de la información que la organización ha implementado.
- Investigación de antecedentes por medio de una lista de chequeo de cada candidato, de acuerdo a las leyes y regulaciones vigentes en el país. En este control se solicita como mínimo:
  a) Dos cartas de referencia, una personal y otra emitida por el jefe inmediato del último empleo.
  b) Revisión del curriculum vitae del aspirante.
  c) Confirmación de calificaciones académicas y profesionales.
- Definir documento que contenga los compromisos y responsabilidades que acepta a partir del momento en que es contratado. (Ver anexo No 11 Documento de Carta compromiso)

D.4.1.2. Durante el empleo

- Términos y condiciones del empleo: Todos los empleados de la Fundación tienen la responsabilidad de aceptar y adoptar las políticas de seguridad de

la información, así como el uso adecuado de los recursos de la organización que son entregados al momento de su contratación.

- Capacitación y entrenamiento en seguridad de la información: Es responsabilidad de la Dirección brindar capacitaciones, actualización de políticas y los procedimientos para desempeñar las funciones.
- Procesos Disciplinarios: En caso de incumplimiento o identificación de incidentes de seguridad, éste se debe registrar e investigar con el objetivo de determinar las posibles causas que lo generaron y los responsables, para tomar las medidas correctivas.

D.4.1.3. Terminación o cambio de empleo

El encargado de Recursos Humanos de la Fundación en conjunto con el jefe inmediato, son los responsables de finalizar el contrato laboral. En este proceso se debe:

- Verificar y documentar la devolución de los activos propios de la Fundación.
- Verificar que los accesos físicos y lógicos sean eliminados
- Realizar back up de toda la información, esta actividad debe realizarla el encargado de Tecnología e Innovación de la fundación.

E.5. SEGURIDAD FÍSICA Y SU ENTORNO

REF.: Dominio 9. ISO/IEC27002:2005

Alcance: Los medios de procesamiento de información deben estar físicamente protegidos de acceso no autorizado, daño intencional por parte de los empleados de la organización y terceras personas.
Objetivo: Resguardar el acceso físico a los activos de la organización y proteger la información de pérdida, daño y robo.

Controles:

E.5.1. Seguridad física y control de acceso físico

E.5.1.1. Perímetros de seguridad física

Las áreas donde se encuentran los equipos e infraestructura de soporte a los sistemas de información deben estar protegidas por medio de controles de acceso solo a personal autorizado.

- Se debe llevar un registro de la fecha y hora de entrada y salida de los visitantes.
- Videocámaras
- Una persona (Recepcionista) encargada de controlar el acceso a las salas u oficinas donde se encuentran los equipos informáticos.
- El centro de cómputo, cableado y áreas técnicas de las oficinas deben contar con mecanismos que cumplan con los requerimientos ambientales, ante desastre naturales.

E.5.1.2. Ubicación y protección del equipo

La ubicación de los equipos es fundamental para garantizar la protección y reducir los riesgos asociados al uso inadecuado de los mismos. Para disminuir las amenazas y peligros ambientales se debe:

- No situar equipos en sitios altos para evitar caídas.
- Separar los equipos cercanos a las ventanas para evitar caídas o que objetos lanzados desde el exterior de la organización los dañen.
- Antes de una tormenta desconectar los equipos para evitar daños.
- Evitar comer o beber cerca de los medios de procesamiento de la información.
- Alejar los equipos de lugares que pueden ocasionar un riesgo ambiental, como incendios, explosiones, agua polvo, entre otros.
- Suministrar soporte adecuado a los servidores donde se encuentra la información, para evitar fallas y pérdidas de la información.
- Seguridad en el cableado de energía, utilizando tubos que ayuden a evitar daños y que las líneas no estén expuestas.
- Mantenimiento de los equipos para asegurar la disponibilidad e integridad de la información que se almacena.

E.5.1.3. Protección de las tecnologías de información

La organización debe llevar un control que incluya:

- Registro actualizado del software instalado en cada equipo.

- Realizar copias de respaldo por equipo y por área, antes y después de las actualizaciones a los sistemas.
- Registro de cambios realizados al software.

F.6. GESTIÓN DE LAS COMUNICACIONES Y OPERACIONES

REF.: Dominio 10. ISO/IEC27002:2005

Alcance: La organización debe establecer responsabilidades para el procesamiento de la información y segregación de funciones para minimizar el riesgo ya sea por negligencia por parte de los empleados o el uso incorrecto del sistema.
Objetivo: proteger los medios de procesamiento de la información

Controles:

F.6.1. Procedimientos y responsabilidades operacionales

F.6.1.1. Procedimientos de operaciones documentados

Es responsabilidad de la fundación crear y documentar procedimientos que faciliten a los usuarios las actividades a realizar en el sistema. Dentro de las principales instrucciones que se deben establecer se encuentran:

- Procedimientos para encender y apagar la computadora
- Copias de seguridad de la información almacenada
- Mantenimiento de los equipos
- Manejo de correo y seguridad, entre otros.

F.6.1.2. Gestión del cambio

Se debe controlar los cambios realizados a la infraestructura tecnológica para el procesamiento de la información, esto debe ser autorizado y evaluado con el propósito de identificar posibles riesgos que pueden afectar la operación de la fundación. Es responsabilidad del Comité de Seguridad revisar los cambios y los requerimientos de protección.

F.6.1.3. Segregación de funciones

Cada área debe contar con segregación de funciones que permita delegar responsabilidades y reducir los riesgos de modificaciones o mal uso de los activos y la información con la que cuenta la organización. Es importante crear reglas de acceso a los sistemas, definiendo los encargados de administrar, operar, mantener y auditar los procesos.

F.6.1.4. Gestión de la capacidad

La organización debe llevar un control que le permita identificar cuál es el consumo de sus recursos y la capacidad de la infraestructura tecnológica para el procesamiento de la información. Para dar cumplimiento a este proceso, la fundación deberá:

- Monitorear el sistema para mejorar la disponibilidad y eficacia.
- Designar personal calificado para detectar problemas en el momento oportuno.
- Realizar proyecciones de los requerimientos de capacidad futura de los sistemas.

F.6.1.5. Aceptación de Sistemas

Para que la Gerencia de Tecnología e Innovación acepte los requerimientos de un sistema nuevo o nuevas versiones de software, deberá estar aprobado por el Director ejecutivo y documentado, deberá contener los requerimientos técnicos y funcionales claros y específicos. Antes de aceptar formalmente un sistema, se debe realizar una lista de chequeo que contenga como mínimo los siguientes requerimientos:

Criterios	Aplica	No aplica
a) Las computadoras cuentan con el desempeño y requerimientos de capacidad		
b) Cuenta con planes de contingencia		
c) Se han realizado pruebas de los procedimientos de operación rutinarios para estándares definidos		
d) Se cuenta con controles de seguridad acordados y aceptados		
e) Existe evidencia que la instalación de un sistema nuevo o la actualización no afectará el sistema existente		
f) Es fácil de usar y no afectará el desempeño de los usuarios		

F.6.2. Protección contra código malicioso y móvil

F.6.2.1. Controles contra códigos maliciosos

El propósito de implementar este control dentro de la organización, es proteger mediante herramientas como antivirus, anti spam entre otros, la seguridad de la información almacenada.

Para dar cumplimiento a este procedimiento, es necesario:

a) Prohibir al personal de la organización el uso de software no-autorizado
b) Realizar revisiones periódicas al software de la fundación
c) Chequeos preventivos de cualquier archivo recibido en por medio electrónico
d) Chequear las páginas web para detectar códigos maliciosos

F.6.3. Respaldo o Back-up

El objetivo principal de este control es mantener la integridad y disponibilidad de la información, esto es posible a través de procedimientos que permitan proteger y evitar futuras pérdidas.

La organización debe realizar regularmente procedimientos para el resguardo y recuperación de la información, estableciendo:

- Traslado de la información
- Frecuencia e identificación de los datos
- Períodos de retención de la información
- Ubicación segura de las copias de respaldo para evitar daños., entre otros.

Ver anexo No 12.

F.6.4. Gestión de seguridad

Se debe designar un encargado de manejar y controlar las redes para proteger la información que se transmite por medio de ellas y así mantener seguros los sistemas y aplicaciones de la fundación.

- Se debe llevar un control de las personas que se conectan a la red
- Verificar que recursos son compartidos con los usuarios internos y externos
- Restringir acceso a dispositivos como USB
- Autenticar e identificar accesos de usuarios que no cumplan con la política de seguridad establecida por la fundación.

F.6.5. Gestión de medios

Se deben establecer procedimientos apropiados que contribuyan a la protección física de los documentos y equipos de cómputo:

- Gestión de medios removibles: los encargados de la Gerencia de Tecnología e Innovación de la fundación en conjunto con el comité de seguridad, serán los responsables de asegurar que en los sistemas de información solamente el personal autorizado haga uso de medios removibles como; memorias USB, discos duros extraíbles, grabador portátil, CD, DVD, entre otros.
- Seguridad de la documentación del sistema: es necesario que la organización proteja los archivos con accesos no-autorizados e implemente los siguientes lineamientos:
    a) Almacenar de forma segura toda la documentación del sistema

b) La dirección ejecutiva como el principal propietario del sistema, deberá llevar una lista de acceso a la documentación que contenga, nombre del usuario, motivo por el cual requiere la información y autorización.

c) La documentación del sistema ya sea que éste se mantenga o suministre por medio de una red pública debe estar debidamente protegida.

F.6.6. Intercambio de información

Para llevar a cabo un proceso seguro dentro de la organización es importante aplicar controles que contribuyan a un adecuado intercambio de información restringida o confidencial entre los involucrados, ya sean colaboradores de la fundación o personas externas como los donantes. Cuando se utilizan medios de comunicación manual o electrónica para el intercambio de información se debe:

a) Si es por medio de correo electrónico la información enviada deberá ser encriptado para proteger su contenido y deberá incluir en su pie de página un aviso especificando que el uso y autorización de la información queda bajo la responsabilidad de la persona que recibe el mensaje.

b) No se permite intercambio de información vía fax o teléfono para evitar la pérdida o conocimiento de personas no autorizadas

c) Toda información que se transmita a organizaciones externas por cualquier medio magnético, de almacenamiento o papel deberá utilizarse los servicios de correo o personal contratado por la organización como un mensajero para que la información sea entregada personalmente al destinatario. Ver anexo No 13 formulario para el envío y recepción de documentos.

Además de aplicar controles para el intercambio de información, es necesario dejar documentado un acuerdo de intercambio que permita determinar responsabilidades, notificación de la transmisión, despacho y recepción de los documentos (Anexo No 14)

F.6.7. Servicios de comercio electrónico

Se deben establecer los requerimientos necesarios para proporcionar a los usuarios todo lo relacionado con las transacciones en línea y los servicios prestados por medios electrónicos, para ello es indispensable proteger la integridad de la información de actividades fraudulentas efectuando algunos lineamientos como:

- Autenticación de usuario
- Autorización para emitir o firmar documentos de comercialización
- Emisión de reporte, en papel o por medio electrónico, al momento de realizar una transacción
- Verificación apropiada para chequear la información de pago o donación
- Elaboración de contratos para proveedores de servicios que se les realizará pago electrónico
- Utilización de firmas electrónicas para cada una de las partes involucradas en la transacción.

F.6.8. Monitoreo

Este control consiste en descubrir toda actividad de procesamiento de información no autorizada que afecte la protección de los datos. Para lograr el objetivo es necesario llevar a cabo las siguientes medidas:

- **Registro de auditoría:** se debe llevar un registro de auditoría en relación a los incidentes de seguridad que se consideren relevantes; este registro debe contener como mínimo, fecha, hora y detalle del evento ocurrido, identidad o ubicación, registro de intentos fallidos al sistema o cambios en la configuración del sistema, archivos a los cuales se tuvo acceso, alarmas activadas por el sistema al momento de un acceso no autorizado, entre otros.
- **Uso del sistema de monitoreo:** es importante determinar las áreas que requieren revisión continua por el riesgo que representan, entre las que se deben considerar;
  - **a)** Acceso autorizado
  - **b)** Todas las operaciones privilegiadas como uso de cuentas, inicio y apagado del sistema, dispositivos para adjuntar o eliminar archivos
  - **c)** Intentos de accesos no autorizados
  - **d)** Alertas o fallas del sistema
- **Registro de fallas:** es necesario llevar un control de fallas reportadas por cada usuario y por los operadores del sistema con el propósito de implementar medidas que disminuyan el riesgo de daños en los sistemas y pérdida de información.

G.7. CONTROL DE ACCESOS

REF.: Dominio 11. ISO/IEC27002:2005

Alcance: Controlar el acceso a la información y los medios de procesamiento de la misma, aplicando políticas para su divulgación y autorización.
Objetivo: Controlar los accesos a la información que se procesa dentro de la organización

Controles:

G.7.1. Política de control de accesos

Se debe establecer y documentar quien será el responsable de controlar los accesos a las plataformas, aplicaciones y recursos que contengan información, que en todo caso será la Gerencia de Tecnología e Innovación junto con el comité de seguridad de la información, como parte de esta política el personal de la organización deberá cumplir con las siguientes medidas:

- Todo acceso a la red como a la plataforma de la organización será autorizada por el encargado de Tecnología e Innovación, quien definirá los permisos adecuados según el tipo de usuario y la información que procesa.
- Todo usuario interno o externo que requiera acceso remoto a la red de la organización deberá estar autenticado y sus conexiones deberán utilizar cifrado de datos, ya sea que el acceso sea por internet, telefónico o por otro medio.
- Se debe establecer perfiles de acceso de cada usuario y por cada puesto de trabajo.

- En caso de cometer algún error significativo o atentar contra la seguridad, se revocaran los derechos de acceso.

G.7.2. Gestión de acceso del usuario

Los procedimientos que se determinaran en esta etapa, son un detalle cronológico que comprende desde el registro inicial de los usuarios hasta el personal que requiera acceso a los sistemas y servicios de información, para este cumplimiento se deberá:

a) Realizar el registro de los usuarios que se les otorgará acceso a los sistemas de información, por medio de ID único que permitirá vincular y responsabilizar las acciones realizadas con cada perfil, dicha autorización la realizará la Gerencia de Tecnología e Innovación quienes serán los únicos responsables de la creación, modificación y eliminación de cada usuario y contraseña.

b) Se deberá restringir y controlar la asignación y uso de privilegios a los sistemas de información, base de datos y aplicaciones que solo los encargados de tecnología e innovación deben tener permiso, se le debe asignar a cada usuario "solo lo que necesitan saber y utilizar para desarrollar su trabajo"

c) Se asignará a cada usuario una clave secreta, seguido de un requerimiento que deberá firmar cada uno para mantener la confidencialidad dentro y fuera de la organización, esto permitirá verificar la identidad de cada empleado.

G.7.3. Responsabilidades del usuario

Todo el personal de la organización debe estar consciente de las responsabilidades que cada uno posee para contribuir al cumplimiento efectivo de los controles establecidos, entre ellas:

- Se debe requerir a cada usuario buenas prácticas para mantener la confidencialidad de las claves asignadas, evitar mantenerla en un papel o dispositivo manual y realizar cambios periódicos cuando tenga conocimiento de un posible peligro o como una medida preventiva.
- Las claves deben ser fáciles de recordar, pero que no sean vulnerables a los ataques, se puede utilizar nombres, números o fechas en diferente orden que no tenga una secuencia lógica o idénticos.
- No compartir las claves individuales (esto forma parte del acuerdo de confidencialidad) y no utilizar la misma clave para todas los accesos autorizados.
- Todos los empleados de la organización deben mantener su espacio de trabajo limpio y ordenado, para evitar pérdidas o daños al equipo y a los datos contenidos en los mismos. Esta medida aplica para toda documentación impresa, equipo de cómputo y todo archivo enviado a impresión. Cada usuario, al momento de levantarse debe bloquear la sesión de la computadora y al finalizar su trabajo cerrar todos los archivos y aplicaciones utilizadas.
- Está autorizado utilizar protector de pantalla institucional en los equipos informáticos, el cual será programado por la gerencia de tecnología e

innovación y se activará automáticamente después de cinco minutos de estar inactivo el escritorio.

G.7.4. Control de acceso a la red

Para evitar el acceso a las redes internas por personas no autorizadas, es necesario aplicar las siguientes políticas:

- Se realizará segregación de redes, esto consiste en separar en segmentos la red física y lógica con independencia de la red a la que tendrá acceso cada usuario de la organización.
- Se establecerán unidades de identificación automática de los equipos en red.
- Los encargados de tecnología e innovación son los responsables de que los puertos lógicos y físicos estén restringidos y monitoreados de forma permanente.

G.7.5. Control de acceso al sistema operativo

Para proteger el sistema operativo es importante evitar que personas no autorizadas ingresen o lo manipulen a su conveniencia, para evitar este tipo de riesgo se debe:

- Realizar un registro seguro que muestre una advertencia a la computadora que controla los demás equipos en línea, los intentos no autorizados de acceder al sistema.
- Establecer un ID de usuario para identificar las actividades hasta la persona responsable.
- Asignación de claves secretas solo a personal autorizado

- Los tiempos de conexión serán en horario laboral, solo con autorización de la Dirección Ejecutiva se extenderá el tiempo, por motivos estrictamente de trabajo.

G.7.6. Control de acceso a la aplicación y a la información

- Computación móvil: Los equipos no pueden ser utilizados fuera de las instalaciones de la organización sin previa autorización y por motivos laborales, si la Dirección ejecutiva y la Gerencia de Tecnología e innovación lo autorizan, los equipos deben ir protegidos por controles tecnológicos como:
  a) Antivirus
  b) Cifrado de datos
  c) Restricciones en la ejecución de aplicaciones

- Teletrabajo: Se podrá acceder a la información de la organización utilizando redes externas, previa autorización de la Dirección ejecutiva, siempre que las conexiones que se utilicen sean seguras y mediante autenticación de usuario.

H.8. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

REF.: Dominio 12. ISO/IEC27002:2005

Alcance: Identificar los requerimientos de seguridad antes de adquirir o desarrollar un sistema de información.

Objetivo: Garantizar la seguridad de los sistemas de información y prevenir el uso inadecuado de las aplicaciones de la organización.

Controles:

H.8.1. Identificación de los requerimientos de seguridad

Si la organización adquiere un software nuevo, se debe realizar un proceso de prueba paralelo con el que se maneja actualmente, para evitar riesgos de perdida de información.

La Gerencia de tecnología e innovación es la responsable de definir y dar cumplimiento a los requerimientos de seguridad y establecer dichos aspectos en los contratos con las instituciones que venden el producto o prestan el servicio.

H.8.2. Controles criptográficos

El objetivo principal de este control es proteger la integridad, confidencialidad y disponibilidad de la información, por medio de protocolos criptográficos para el uso de las aplicaciones y transferencia de información.

- Los correos enviados fuera de la organización que contengan información confidencial, llevaran un cifrado que solamente el destinatario que tenga una clave privada podrá recibir y leer el mensaje.
- El uso de firmas digitales, considerando las leyes vigentes que sean aplicables.

H.8.3. Seguridad de los archivos del sistema

- Sólo el personal de la Gerencia de Tecnología e innovación de la organización tendrá acceso al código fuente de los programas y a los archivos del sistema.
- La actualización de software, aplicaciones o programas la podrá realizar el personal capacitado previa autorización de la Dirección ejecutiva.
- Se debe llevar un registro de las actualizaciones realizadas, detallando fecha y periodo de realización, e incluir un archivo con las versiones antiguas del software y los motivos por los cuales se realizó el cambio.
- Los proveedores de nuevos software no deben tener acceso directo a los sistemas de información, un representante autorizado por la fundación estará permanentemente durante el proceso de implementación.

H.8.4. Filtración de la información

- Controlar cualquier tipo de malware que pueda obtener información importante de los equipos, como contraseñas, cuentas de usuarios entre otros.

- Cifrado de la información, implementando este control se puede asegurar que solo las personas autorizadas con claves y contraseñas tendrá acceso a la información.
- Evitar que los usuarios accedan a sitios inseguros o utilicen unidades extraíbles.
- Controlar el acceso a servicios en la nube, en caso de que la Dirección ejecutiva autorice subir información confidencial, ésta debe ir cifrada para evitar el riesgo de fuga de datos.
- Determinar el contenido que se quiere controlar como, números de tarjetas, cuentas bancarias, contratos con las organizaciones donantes, información financiera, entre otros.

H.8.5. Control de las vulnerabilidades Técnicas

Es responsabilidad de la Gerencia de Tecnología e Innovación identificar las vulnerabilidades técnicas de las plataformas y sistemas de información, para dar cumplimiento a esta medida se debe:

- Realizar un inventario completo de los activos con los que cuenta la organización.
- El persona de tecnología e innovación debe generar un reporte de las vulnerabilidades detectadas al momento de realizar el inventario físico.
- Se debe realizar por lo menos una vez al año pruebas de vulnerabilidad para las plataformas más expuestas, esto debe realizarlo personal especializado en el área e independiente a la organización.

- La Gerencia de Tecnología e Innovación será la responsable de implementar las medidas correctivas, después del diagnóstico proporcionado por el especialista.

I.9. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN

REF.: Dominio 13. ISO/IEC27002:2005

Alcance: Establecer procedimientos que permitan identificar los eventos y debilidades que pueden afectar la protección de los activos de la organización.

Objetivo: Asegurar que los riegos y debilidades asociados a los sistemas de información sean notificados de manera oportuna para realizar las acciones correctivas.

Control:

I.9.1. Comunicación de incidentes y eventos de seguridad

Un evento de seguridad es la posibilidad de ocurrencia de una situación que afecte las políticas de la información o genere falla en los controles implementados por la organización. Un incidente de seguridad es el acto intencional o no intencional que tiene una alta probabilidad de afectar las operaciones de la fundación. Por tanto para mitigar este tipo de situaciones es necesario que:

- Los responsables de la seguridad lleven un reporte de todos los eventos o incidentes como los siguientes:
  a) Violaciones de los acuerdos de seguridad
  b) Mal funcionamiento del software

c) Violaciones de accesos

d) Mal funcionamiento o sobre carga del sistema

e) Pérdida de servicio o equipos

- Aplicar un proceso disciplinario cuando los usuarios o empleados hayan cometido violaciones a la seguridad.
- Cada usuario o empleado de la organización debe tomar nota y reportar cualquier debilidad que observe en el sistema que ponga en riesgo la protección del equipo y los datos.

H.9.2. Gestión de incidentes y mejoras en la seguridad de la información

- El comité de seguridad de la organización será el responsable de llevar un registro de los incidentes e implementar las acciones correctivas que se requieran. Para llevar a cabo esta labor se debe tomar en cuenta las causas, impacto y frecuencia de los eventos, con el propósito de llevar una estadística del comportamiento y responder de forma rápida para evitar más daños.(Ver anexo No 14)
- Implementar un plan de contingencia que incluya análisis e identificación de la causa del incidente, comunicación con los afectados o involucrados, reporte de las acciones a la Dirección ejecutiva.
- Recolectar evidencia para analizar el problema y brindar una solución apropiada.
- Evaluar los incidentes ocurridos ya sea para incrementar o fortalecer los controles establecidos y evitar que ocurran en un futuro.

J.10. GESTIÓN DE CONTINUIDAD DEL NEGOCIO

REF.: Dominio 14. ISO/IEC27002:2005

Alcance: Implementar procesos de gestión de continuidad del negocio para disminuir el impacto sobre la organización en caso de existir pérdida de información.

Objetivo: Desarrollar controles que contribuyan a identificar y minimizar los riesgos que afecten las operaciones de la organización

Controles:

- En caso que ocurran desastres naturales, accidentes, fallas en el equipo entre otras amenazas, se debe establecer un plan de recuperación y restablecimiento de los servicios de tecnología así como los responsables de garantizar la continuidad de las operaciones.
- La Dirección de Tecnología e Innovación en conjunto con la Dirección Ejecutiva deben realizar una evaluación del riesgo que permita identificar y cuantificar las consecuencias que afectarían a la organización.
- En caso de pérdida de activos o información confidencial, se debe definir los responsables de comunicar a los involucrados el desastre ocurrido y las actividades que se efectuaran para mantener en orden y con normalidad las actividades diarias de la organización.
- Es importante brindar entrenamiento al personal de la organización en cuanto a los roles y responsabilidades que cada uno desarrollará para contribuir a la normalidad de las actividades.

- Se deben realizar pruebas y mantenimiento de continuidad de la organización, por lo que se definirá el responsable de coordinar periódicamente un plan para cubrir las necesidades y requerimientos de la fundación.

K.11. CUMPLIMIENTO

REF.: Dominio 15. ISO/IEC27002:2005

Alcance: Implementar un sistema de seguridad que contribuya a la seguridad de los sistemas de información. **Objetivo:** Evitar incumplimiento a los requerimientos legales y a las políticas y estándares de seguridad aplicables a las tecnologías de información.

Controles:

- La organización debe cumplir con la legislación aplicable en el Salvador y las obligaciones contractuales con terceros.
- Se dará cumplimiento a lo que establece la propiedad intelectual vigente en el país y se realizaran revisiones por lo menos una vez al año para garantizar que se estén respetando los derechos sobre licencias, información publicitaria y comercial relacionada con la imagen de la fundación.
- La Gerencia de Tecnología e Innovación será la responsable de administrar el inventario y control de licencias de software y aplicaciones utilizadas en la organización.
- Queda prohibido el uso ilegal de software por los empleados de la organización, se podrá adquirir licencias solo por fuentes conocidas y acreditadas para asegurar que no sean violados los derechos de autor.

- No se permite duplicar, copiar o extraer registros contables, bases de datos, registros de transacciones entre otros considerados como confidenciales dentro de la organización.

CAPITULO IV: CONCLUSIONES Y RECOMENDACIONES

Una vez finalizado el trabajo de investigación y la información obtenida, concluimos que:

4.1. Conclusiones

- Las organizaciones No Gubernamentales no cuentan con un sistema de seguridad de la información desarrollado bajo un estándar internacional.

- Las Organizaciones No Gubernamentales no contemplan dentro de su presupuesto anual, financiamiento para el estudio y evaluación de los riesgos relacionados con la seguridad de la información.

- En su mayoría, las Organizaciones No Gubernamentales, no poseen auditoría interna ni de sistemas, ya que los requerimientos de los organismos internacionales solo se provee la revisión externa de auditoria a nivel financiero y económico.

- Los empleados forman parte de los activos valiosos dentro una organizaciones es la parte más sensible y vulnerable debido a que un empleado insatisfecho puedo ocasionar grandes pérdidas significativas, ya que es el quien conoce la información que se procesa, administra y transfiere información que se considera confidencial.

- Es necesario mantener un estado de alerta y actualización permanente sobre nuevos métodos de seguridad de la información, ya que la seguridad es un proceso continuo que exige aprender diariamente y más aún sobre las propias experiencias.

- No cuentan con un programa de capacitación sobre la seguridad informática y no se socializan las políticas y procedimientos ya existentes.

- No se ha incorporado dentro de la carga académica de la Licenciatura de contaduría pública materias relacionadas a la actualización tecnológica y seguridad de la informática dentro de las organizaciones para proteger la información y los sistemas.

- Los avances tecnológicos han crecido significativamente a lo largo de la historia lo cual comprende un sinfín de procesos y equipos como lo es el hardware, aplicaciones, bases de datos, infraestructura, el personal, todo constituye información en procesos lo cual debe ser protegida, como el componente más valioso dentro la organización.

4.2. Recomendaciones

- Que las Organizaciones No Gubernamentales implementen un sistema de seguridad de la información basado en la ISO 27000, que contribuya al control y protección de los recursos y la información que se procesa.

- Asignar un porcentaje del presupuesto para la contratación de personal técnico debidamente calificado para llevar a cabo un control y monitoreo de las vulnerabilidades e incidentes que perjudiquen a los activos

- La creación del área de auditoría interna y que cumplan con el perfil sistemas que permita detectar las áreas vulnerables de la organización y proporcione un aporte para conservar la confidencialidad, integridad y disponibilidad de la información.

- Establecer dentro de los objetivo de trabajo un excelente ambiente laboral para los empleados , generando actividades de auto cuido, trabajo en equipo , cuidando el entorno laboral , respetando la dignidad de cada persona desde los altos mando hacia todos los empleados .

- Se recomienda establecer programas de mejora continua para mantener en constante actualización al personal de las organizaciones sobre los diferentes métodos para la seguridad de la información, que a diario van cambiando y proponiendo mejores resultados.

- Elaborar un plan de capacitación continua para los empleados sobre la seguridad informática, esto ayudara a conocer la importancia de proteger los activos.

- El perfil académico del profesional de la contaduría pública ha crecido significa ya que las nuevas tecnologías han creado oportunidades para los servicios ofrecidos, como auditoria de sistemas, sitios web, pero para ello es necesario invertir en la formación continua como lo recomienda IFAC en su guía curricular de Tecnología de Información en el Currículo de Contaduría.

- Conocer la importancia y proteger los activos ayudara a las ONG a proteger minimizar los riesgos, controlarlos y sobre el buen funcionamiento de los mismos. Ya que cada día sale al mercado nuevos ataque que afectan la información, pero así mismo nuevos avances para su protección, lo que se debe de esta en continua formación.

BIBLIOGRAFÍA

Asamblea Legislativa de la República de El Salvador. (Decreto No 894, 1992). *Ley de Asociaciones y Fundaciones Sin Fines de Lucro.* San Salvador, El Salvador.

Asamblea Legislativa de la Republica de El Salvador . (Decreto 150, Tomo 320, 1993). *Ley de Propiedad Intelectual.* San Salvador, El Salvador.

Asamblea Legislativa de la Republica de El Salvador . (Decreto No 868, Tomo No 356, 2002). *Ley de Marcas y Otros Signos Distintivos.* San Salvador, El Salvador.

Asamblea Legislativa de la Republica de El Salvador . (Decreto No 86, Tomo No 313, 1991). *Ley General Tributaria Municipal.* San Salvador, El Salvador.

Asamblea Legislativa de la Republica de El Salvador . (Decreto 894,21 de Noviembre de 1996). *Ley de Asociaciones y Fundaciones Sin Fines de Lucro.* San Salvador.

Asamblea Legislativa de la Republica de El Salvador . (Decreto No 134, Tomo No 313, 1991). *Ley de Impuesto sobre la Renta.* San Salvador, El Salvador.

Asamblea Legislativa de la Republica de El Salvador . (Decreto No 230,Tomo No 349,2000). *Código Tributario.* San Salvador, El Salvador.

Asamblea Legislativa de la Republica de El Salvador . (Decreto No296,Tomo No 316, 1992). *Ley de Impuestos a la Transferencia de Bienes Muebles y a la Prestación de Servicios.* San Salvador, El Salvador.

Asamblea Legislativa de la Republica de El Salvador. (Decreto No133, Tomo 409, 2015). *Ley de Firma Electrónica.* San Salvador, El Salvador.

Asamblea Legislativa. (Deccreto No101, 1991). *Reglamento de la Ley de Impuesto sobre la Renta.* San Salvador, El Salvador.

Blandón Morales, D. J., Córdova Santamaria, C. P., & Juárez Rivera, L. Y. (2000). *www.ufg.edu.sv.* Recuperado el 10 de 05 de 2016, de http://wwwisis.ufg.edu.sv/wwwisis/documentos/TE/361.763-M672p/361.763-M672p-CAPITULO%20I.pdf

Cornejo Perez, M. H. (2008). Tecnologia de Informacion en el contexto Profesional del Contador Publico . *ABACO CONTABLE* , 3.

definicionabc. (12 de 09 de 2016). Recuperado el 12 de 09 de 2016, de http://www.definicionabc.com/

enter.co. (s.f.). Recuperado el 15 de 05 de 2016, de http://www.enter.co/chips-bits/seguridad/conozca-las-amenazas-informaticas-mas-comunes-disi2010/

Gomez Vieties, A. (2007). *Enciclopedia de la seguridad informatica.* Mexico: Alfaomega.

Guia para la formulacion de procedimientos de seguridad. (s.f.). *Guia para la formulacion de procedimientos de seguridad*.

htt://wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n. (s.f.).

http://www.microsoft.com/business/smb.es/guia_lopf/medidas_seguridad.mspx. (s.f.).

ICETEX. (Octubre 2014). Manual de Politicas de Seguridad de la Información.

ISO 27000. es . (s.f.). Recuperado el 12 de 09 de 2016, de ISO 27000. es: http://www.iso27000.es/

ISO/IEC 27001, Sistema de Gestion de Seguridad. (15 de 10 de 2005).

Portillo, S. (15 de 05 de 2016). *Historia de la seguridad informatica.* Obtenido de Historia de la seguridad informatica: https://prezi.com/vnbaj88nuq0p/historia-de-la-seguridad-informatica/

protejete.wordpress.com. (s.f.). Recuperado el 23 de 06 de 2016, de Gestión de Riesgo en la Seguridad Informatica : https://protejete.wordpress.com/gdr_principal/elementos_informacion/

Servicio TIC. (04 de 11 de 2015). Recuperado el 04 de 11 de 2015, de Servicio TIC: http://www.serviciostic.com/las-tic/definicion-de-tic.html

Tobar, V. H. (23 de 01 de 1998). *vrijmetselaarsgilde.eu.* Recuperado el 10 de 05 de 2016, de http://www.vrijmetselaarsgilde.eu/Maconnieke%20Encyclopedie/FMAP~1/REFORM/reform3/cap41.htm

Universia.net . (s.f.). Recuperado el 23 de 06 de 2016, de fundacionuniversia.net: http://universitarios.universia.es/voluntariado/ongs-fundaciones/historia-ongs/breve-historia-ong-s.html

Weblog Blog Calidad ISO. (s.f.). Recuperado el 12 de 09 de 2016, de WeblogBlog Calidad ISO: http://blogdecalidadiso.es/historia-de-la-iso/

WWW.2 FUSALMO . (08 de 11 de 2015). Recuperado el 08 de 11 de 2015, de WWW.2 FUSALMO : http://www5.fusalmo.org/index.php?option=com_content&view=featured&Itemid=378

www.auritam.blogspot.com/2008/10. (07 de 11 de 2015). Recuperado el 07 de 11 de 2015, de www.auritam.blogspot.com/2008/10: http://auritam.blogspot.com/2008/10/definicin-de-procedimientos-de.html

www.microsoft.com. (07 de 11 de 2015). Obtenido de www.microsoft.com: http://www.microsoft.com/business/smb.es/guia_lopf/medidas_seguridad.mspx

www.sgsi-iso27001. (07 de 11 de 2015). Obtenido de www.sgsi-iso27001: http://sgsi-iso27001.blogspot.com/2008/07/como-resumen-al-documento-que-ya-indiqu.html

ANEXOS

ANEXO No 1

UNIVERSIDAD DE EL SALVADOR

FACULTAD DE CIENCIAS ECONOMICAS

ESCUELA DE CONTADURÍA PÚBLICA

(Encuesta de uso didáctico)

Proyecto de Investigación: Sistema de Seguridad de la Información Basado en la ISO 27000, aplicado a las Organizaciones no Gubernamentales de El Salvador

Dirigido a: El personal Técnico o jefe de sistemas de las Organizaciones no Gubernamentales de El Salvador

Objetivo: Obtener información relevante de cómo el personal encargado del área de informática responde ante los riesgos que enfrentan los sistemas y la información que se procesa dentro de la organización.

Indicaciones: Favor de contestar las preguntas de acuerdo a sus conocimiento y marque con una X las preguntas de opción múltiple

1. ¿Cuál es la forma que se suministra el soporte técnico al equipo informático en su organización? (selecciones cualquiera de la opciones que posee)

   a) Departamento de informática ☐
   b) Mantenimiento y monitoreo externo del equipo ☐
   c) Contabilidad ☐
   d) No posee ☐

Objetivo: Conocer la forma que se brinda soporte al equipo informático

2. ¿Posee un programa anual de soporte y mantenimiento de los sistemas de seguridad informática que garantice la seguridad de la información?

   a) Si ☐ b) No ☐

Objetivo: Conocer si cuentas con programa de mantenimiento anual

3. ¿Si cuenta el con programa de soporte y mantenimiento, cada cuanto tiempo lo ejecuta (Seleccione la opción de acuerdo al programa de realiza?

a) Mensualmente ☐
b) Trimestralmente ☐
c) Semestralmente ☐
d) Anualmente ☐

Objetivo: Conocer la forma de como ejecuta el programa anual de mantenimiento

4. ¿Cuáles son las actividades principales que desarrolla el encargado de la seguridad informática de su institución?

a) Mantenimiento y soporte de equipo informático ☐
b) Desarrollo de programas de información ☐
c) Mantenimiento de sitio Web ☐
d) Administra, configura e instala las red las computadoras ☐
e) Administra los sistemas de información ☐

Objetivo: Conocer las actividades asignadas al personal a cargo del área

5. ¿De las siguientes vulnerabilidades que afectan la organización cuales ha identificado dentro de sus instalaciones?

a) Mala ubicación de los centros de computo ☐
b) Software mal configurado ☐
c) Software desactualizado ☐
d) Falta de hardware ☐
e) Ausencia de copias de seguridad o copia incompleta ☐
f) Falta de seguridad para archivos digitales ☐
g) Falta de socialización de normas y políticas ☐
h) Cuenta de usuarios mal configurados ☐
i) Ausencia de manuales de aplicaciones ☐
j) Dependencia de proveedor externo de mantenimiento ☐
Informáticos

Objetivo: Determinar las principales vulnerabilidades de las organizaciones

6. ¿Del siguiente listado cual o cual son las medidas preventivas que aplica en su organización para garantizar la seguridad de la información?

a) Autentificación de usuarios (Contraseñas) ☐
b) Control de acceso a los datos ☐
c) Encriptación de datos sensibles o confidencial ☐
d) Socialización a los usuarias de normas o políticas de seguridad informática ☐
e) Actualización de Software ☐
f) Instalación de disco espejo ☐
g) UPS ☐
h) Validación de datos ☐
i) Implementación de sistemas de acceso CPD ☐
j) No aplica ninguna medida ☐

Objetivo: Determinar cuáles son las medidas que aplican las organizaciones

7. ¿Cuál de las siguientes características utiliza su organización para autentificar las contraseñas? (Puede seleccionar más de una opción)

a) Asignación de ID únicos para establecer responsabilidades ☐
b) Técnicas de cifrado ☐
c) Bloqueo de accesos por intentos fallidos ☐
d) Cambio de contraseña cada determinado periodo ☐
e) No utiliza ninguno ☐

Objetivo: Identificar si la organización utiliza medidas para autentificar las Contraseñas

8. ¿Su organización cuenta con medidas de seguridad que detecten los ataques a los sistemas informáticos?

a) Si ☐ b) No ☐

Objetivo: Conocer si cuenta con medidas detección de ataques a los sistemas informático

9. ¿Si su respuesta fue positiva del siguiente listado cuales son los equipos o sistemas que posee para detectar los ataques?

   a) Sistema de detección de intrusos ☐
   b) Procedimientos para analizar los log ☐
   c) Antivirus ☐
   d) Antispyware ☐
   e) Firewalls o contra fuegos ☐
   c) No posee ☐

   Objetivo: Identificar si cuentan con las medidas de detección para la seguridad informática

10. ¿Del siguiente listado cuales son ataques que han sufrido los sistemas de informáticos en su organización?

    a) Enmascaramiento ☐
    b) Reenvió de paquete ☐
    c) Modificación de mensajes ☐
    d) Acceso no autorizados ☐
    e) Correo spoofing ☐
    f) Ataque de fuerza –Bruta ☐
    g) Ataque interno de empleados ☐
    h) Puertos abiertos ☐
    i) Ninguno ☐

Objetivo: Conocer si han sufridos ataque a los sistemas de seguridad

11. ¿Cómo considera la probabilidad de amenazas dentro de su organización?

    a) Baja: ☐
    b) Mediana: ☐
    c) Alta: ☐

Objetivo: Conocer los niveles de amenazas dentro de las instituciones

12. ¿Su organización realiza capacitación sobre prevenir los ataques de la ingeniería social?

a) Si ☐ b) No ☐

Objetivo: Conocer si existe concientización sobre los ataques de ingeniería social

13. ¿Existen políticas y procedimientos para los usuarios de los sistemas de informáticos y encargado de TI?

Usuarios a) Si ☐ b) No ☐

Encargado de TI a) Si ☐ b) No ☐

Objetivo: Conocer si la organización cuenta con manuales para los usuarios de los Sistemas y los responsables de los mismos.

14. ¿Si cuenta con políticas y procedimiento para la seguridad informática cual o cuales normas técnicas aplica para la protección de la información?

a) COBIT ☐

b) ISO 27000 ☐

c) COSO ☐

d) Entrada, soporte y servicio (DSS) ☐

e) ITIL ☐

f) Ninguna ☐

Objetivo: Conocer si las organizaciones cuentas con políticas y procedimientos Para la seguridad de la información

15. ¿Del siguiente listado cual o cuales considera usted que afectaría la continuidad o funcionamiento de su organización?

a) Pérdida de privacidad ☐
b) Divulgación de información sensitiva ☐
c) Afectación de las operaciones de la entidad ☐
d) Pérdida de credibilidad ☐
e) Pérdidas financieras ☐
f) Consecuencias legales y obligatorias ☐
g) No considera que le afecta ☐

Objetivo: Identificar las causas que pueden afectar a la organización en su Funcionamiento

16. ¿Del siguiente listado de contingencias ¿Para cual no está preparada su organización para proteger la seguridad de los equipos y su mantenimiento?

a) Incendio ☐
b) Inundación ☐
c) Terremoto ☐
d) Si está preparado ☐

Objetivo: Conocer si están preparados para enfrentar contingencias que ponen en riesgos la información.

17. ¿Seleccione cuál de las siguientes medidas de seguridad se encuentran en las instalaciones de su organización (Seleccione las que poseen)

a) Cámaras de vigilancia y video ☐

b) Extintores de fuego ☐

c) Caseta de vigilancia ☐

d) Detector de humo ☐

e) Sensores de movimiento ☐

f) Barandas de seguridad en gradas, niveles y ventanas ☐

g) Dispositivos biométricos ☐

h) Salidas de emergencia ☐

i) Prohibido comer, beber y fumar ☐

j) Protector de voltaje ☐

k) Cableado, panales y conductos a prueba de juego ☐

l) Ninguna medida ☐

Objetivo: Identificar qué medidas de seguridad física cuenta la organización dentro de sus instalaciones.

18. ¿Si dentro de su respuesta anterior cuenta con dispositivos biométricos, señale cual o cuales del siguiente listado tiene su organización?

a) Huella digital ☐

b) Cerradura electrónica ☐

c) Contraseñas numéricas ☐

d) Reconocimiento de la firma ☐

e) Reconocimiento de la voz ☐

f) Autentificación Tokens ☐

g) Geometría de dedos y manos ☐

h) Ninguna de las anteriores ☐

Objetivos: Identificar qué tipo de dispositivo biométrico posee la organización.

19. ¿Del siguiente listado determine si se cumplen las condiciones idóneas de los equipos dentro y fuera del área informática para su funcionamiento?

a) Iluminación suficiente y adecuada ☐
b) Espacios amplios y ergonomía dentro de la unidad de informática ☐
c) Uso seguro de redes y dispositivos eléctricos ☐
d) Ductos de aire acondicionado con buena ubicación ☐
e) Disponibilidad de planos de instalaciones eléctricas ☐
f) Interruptores de apagado en caso de emergencia en lugares visibles ☐
g) Cables eléctricos y cajas térmicas en óptimas condiciones ☐
h) Señalizaciones idóneas para advertencia de voltajes y evacuación ☐
i) Vigilancia continua por parte de guardias ☐
j) No posee las condiciones idóneas ☐

Objetivo: Determinar si los equipos cuentan con condiciones adecuadas para su funcionamiento dentro y fuera de la organización

20. ¿Cuenta con un inventario de todos los activos que posee la organización?

a) Si ☐ b) No ☐

Objetivo: Conocer si la organización tiene definido un inventario de activos que le permita tener control de los mismos

21. ¿Su organización estaría interesado en aplicar un sistema de seguridad de la información en base a la normativa técnica ISO 27000?

a) Si ☐ b) No ☐

Objetivo: Conocer si están interesados en aplicar un sistema de SI.

ANEXO No 2

UNIVERSIDAD DE EL SALVADOR

FACULTAD DE CIENCIAS ECONOMICAS

ESCUELA DE CONTADURÍA PÚBLICA

(Encuesta de uso didáctico)

Proyecto de Investigación: Sistema de Seguridad de la Información Basado en la ISO 27000, aplicado a las Organizaciones no Gubernamentales de El Salvador

Dirigida al: Personal clave de las Organizaciones no Gubernamentales de El Salvador

Objetivo de la encuesta:
Conocer si las Instituciones no Gubernamentales poseen un Sistema de Seguridad de la información y su aplicación, con el fin de proporcionar una herramienta para aquellas que no aplican procedimientos.

Indicaciones: Favor de contestar las preguntas de acuerdo a sus conocimiento y marque con una X las preguntas de opción múltiple

1. ¿Posee conocimiento de lo que significa la seguridad informática?

   a. Si ☐ b. No ☐

   Objetivo: Conocer si el personal de las ONG´S poseen conocimiento sobre el tema de seguridad de la información.

2. ¿Si su respuesta a la pregunta anterior fue negativa, Cual o cuales son las causas que ocasionan la falta de conocimiento sobre la seguridad informática?

   a. La organización no proporciona capacitaciones sobre el tema ☐

   b. No considero que existan riesgos por falta de conocimiento ☐

c. No estoy interesado/a en ese tipo de información ☐

d. No corresponde a mi área de trabajo ☐

Objetivo: Identificar las causas por las cuales los usuarios no tienen conocimiento sobre la seguridad de la información

3. ¿Dónde adquirió los conocimientos sobre la seguridad informática ? (Selecciones una o más alternativas de respuesta)

a. Capacitación ☐

b. Concientización de políticas de seguridad informática impartido por la institución ☐

c. Plan de educación continua ☐

d. Autodidacta ☐

e. Libros ☐

f. Documentos informáticos ☐

g. Ninguno ☐

Objetivo: Identificar a través de qué medios obtiene conocimiento sobre la seguridad de la información el personal de las ONG´S

4. ¿De las siguientes medidas de seguridad informática cuales son las que aplica en su puesto de trabajo?

a. Análisis de antivirus a las de USB ☐

b. Análisis de antivirus de archivos adjuntos en correos electrónico ☐

c. Realiza copias de seguridad de la información que procesa ☐

d. Reporta los incidentes por amenazas externas ☐

e. Bloquea su computadora al levantarse de su escritorio ☐

f. Cambia periódicamente la contraseña de su computadora ☐

g. Ninguna de las anteriores ☐

Objetivo: Analizar las diferentes medidas que implementan el personal de las ONG para proteger su información.

5. ¿En su institución existen restricciones para el acceso a internet para el personal? Del siguiente listado selecciones cuales son los accesos restringidos.

   a. Facebook ☐
   b. YouTube ☐
   c. Correo electrónico personal ☐
   d. Descargar programas e instalarlos ☐
   e. Totas las anteriores ☐
   f. Ninguno ☐

Objetivo: Conocer si las ONG´S aplican al personal medidas de seguridad para la restricción del uso de internet.

6. ¿La institución le autoriza a llevarse información para trabajar a su casa?

   a. Si ☐ b. No ☐

Objetivo: Identificar si los empleados tienen permisos para llevar información fue de la Organización

7. ¿Si su respuesta fue positiva, del siguiente listado cual es la forma más común que utiliza para llevarse la información? (puede seleccionar más de una opción)

    a. Información procesada y almacena en USD ☐
    b. Documentación física ☐
    c. Computadora móvil (laptop) ☐
    d. Todas las anteriores ☐
    e. No hay autorización ☐

    Objetivo: Descubrir si en las ONG´S les permite a los empleados sacar información o activos físicos de la institución.

8. ¿Posee su institución políticas y procedimientos para la seguridad informática que garantice la protección de la información que se procesa (si su respuesta es negativa pase a la siguiente pregunta 9)

    a. Si ☐ b. No ☐

    Objetivo: Determinar si las ONG´S tienen políticas y procedimientos definidos que garanticen la seguridad de la información.

9. ¿Del siguiente listado cuales cree que son las razones de no contar con políticas de seguridad informática?

    a. Por falta de recursos ☐
    b. No lo considera necesario ☐
    c. Costo elevado ☐
    d. Por ser una organización pequeña ☐
    e. Falta de conocimiento de los riesgos y amenazas ☐

Objetivo: Analizar las posibles causas por las que las ONG´S no aplican políticas de seguridad para la información.

10. ¿Le exigen los organismos donantes contar con una estructura organizacional?

    a. Si ☐ b. No ☐

    Objetivo: Identificar si los organismos que realizan donaciones requieren que las ONGs tengan una estructura organizativo

11. ¿Si su respuesta a la pregunta anterior fue positiva, indique cuales son con los que cuenta su institución?

    a. Estructura organización definida ☐
    b. Sistema contable ☐
    c. Policías y procedimientos de control interno ☐
    d. Políticas y procedimientos de contratación del personal ☐
    e. Sistema de seguridad informática ☐

    Objetivo: Identificar qué tipo de exigencias piden los donantes a las ONG´S para proteger la información.

12. ¿Se realizan capacitaciones al personal para concientizar lo importante que es la seguridad informática?

    a. Si ☐ b. No ☐

    Objetivo: Conocer si las ONG´S brindan información suficiente al personal, para asegurarse que conozcan de la importancia de la seguridad de la información.

13. ¿En el uso del sistema contable se han establecidos categorías de usuarios para procesar la información?

    a. Si ☐ b. No ☐

    Objetivo: Determinar si el sistema contable está programado con categorías para los usuarios

14. ¿Si su respuesta a la pregunta anterior fue positiva, que tipo de categoría posee el sistema que utiliza dentro de su organización?

    a. Administrador del sistema (acceso a todos los módulos ☐
    b. Usuarios Registrados (Identificación por nombre y contraseña) ☐
    c. No posee categorías de usuarios ☐

    Objetivo: Determinar si los sistemas contables poseen permisos de usuarios en función del cargo que desempeña cada empleado.

15. ¿Su organización cuenta con planes y acciones de contingencias que realice en las instalaciones de oficinas, centro de cómputo, área de soporte técnico?(Selecciones con cuales cuenta)

    a. Planes de evacuación en caso de desastres. ☐
    b. Planes de contingencia para salvaguardar los activos de la institución. ☐
    c. Contratos y pólizas de seguros de los edificios ☐
    d. Adiestramiento del personal en primeros auxilios ☐
    e. Adiestramiento del personal en uso de extintores ☐
    f. Capacitaciones del personal para el uso del sistema informático ☐
    g. Capacitaciones en medidas de seguridad y salud ocupacional dentro de la unidad institucional. ☐

h. Simulacros de primeros auxilios, incendios y otros ☐

i. No posee planes ni acciones para mitigar emergencias ☐

Objetivo: Investigar si las ONG´S están debidamente preparadas con planes de contingencias que contribuyan a la protección de la información.

ANEXO No 3

TABULACIÓN Y ANÁLISIS DE LA INFORMACIÓN RECOPILADA

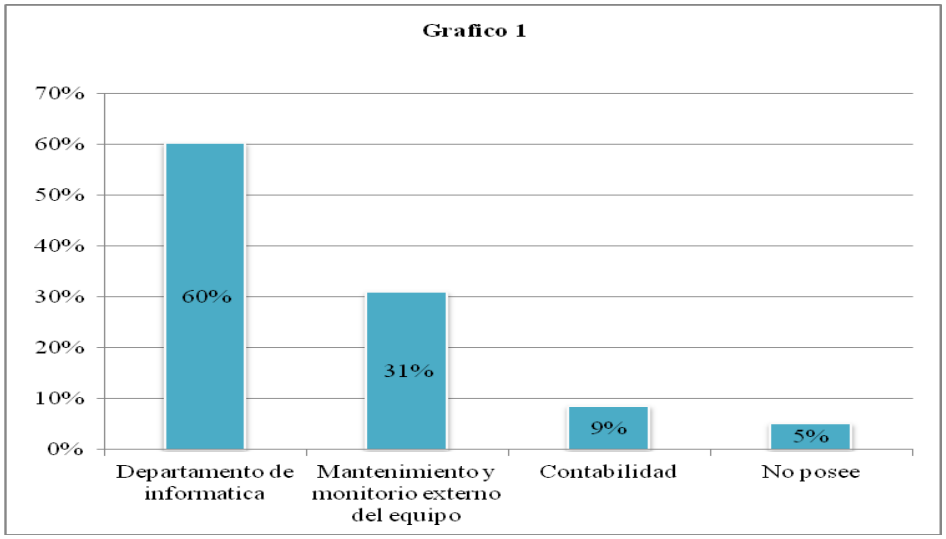
Tabulación y análisis de la información recopilada del personal Técnico o jefe de sistemas de las Organizaciones No Gubernamentales.

PREGUNTA 1:

¿Cuál es la forma que se suministra el soporte técnico al equipo informático en su organización? (seleccione cualquiera de las opciones que posee).

Objetivo: Conocer la forma que se brinda soporte al equipo informático.

RESPUESTA	FRECUENCIA	
	ABSOLUTA	RELATIVA
Departamento de informática	35	60%
Mantenimiento y monitorio externo del equipo	18	31%
Contabilidad	5	9%
No posee	3	5%



Análisis e interpretación:

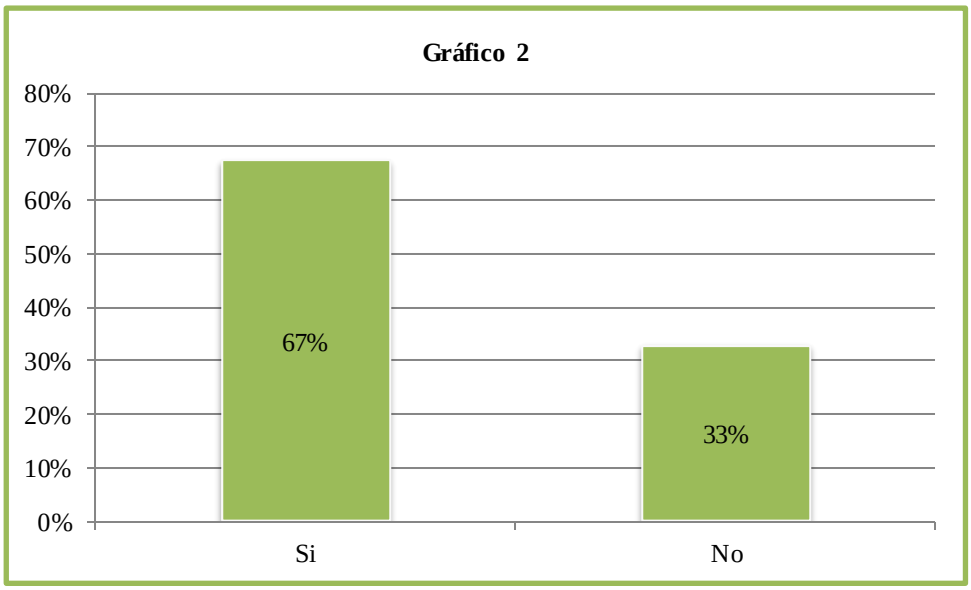
Al investigar si las entidades reciben soporte técnico, solamente el 5% de las encuestadas no lo reciben, siendo el 95% las que tienen este beneficio, el cual en un 60% es proporcionado por un departamento de informática, el 31% brinda este soporte mediante un mantenimiento y monitoreo externo del equipo, y el 9% restante es realizado por el departamento de contabilidad.

PREGUNTA 2:

¿Posee un programa anual de soporte y mantenimiento de los sistemas de seguridad informática que garantice la seguridad de la información?

Objetivo: Conocer si cuentan con programa de mantenimiento anual.

RESPUESTA	FRECUENCIA	
	ABSOLUTA	RELATIVA
Si	39	67%
No	19	33%
Total	**58**	**100%**



Análisis e interpretación:

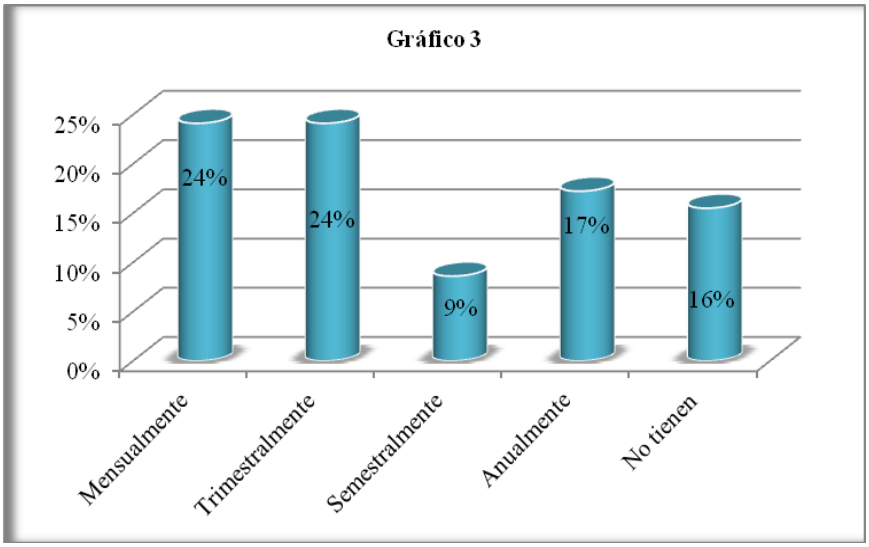
En los resultados de la pregunta anterior se puede ver que el 95% de las ONG´S reciben soporte técnico pero de este 95% solamente el 67% trabaja en base a un programa definido, las demás organizaciones no tiene estructurado un plan de trabajo representado por el 33%.

PREGUNTA 3:

¿Si cuenta el con programa de soporte y mantenimiento, cada cuanto tiempo lo ejecuta? (Seleccione la opción de acuerdo al programa de realización?

Objetivo: Conocer la forma de como ejecuta el programa anual de mantenimiento

RESPUESTA	FRECUENCIA	
	ABSOLUTA	RELATIVA
Mensualmente	14	24%
Trimestralmente	14	24%
Semestralmente	5	9%
Anualmente	10	17%
No tienen	9	16%
Total	**52**	**90%**



Análisis e interpretación:

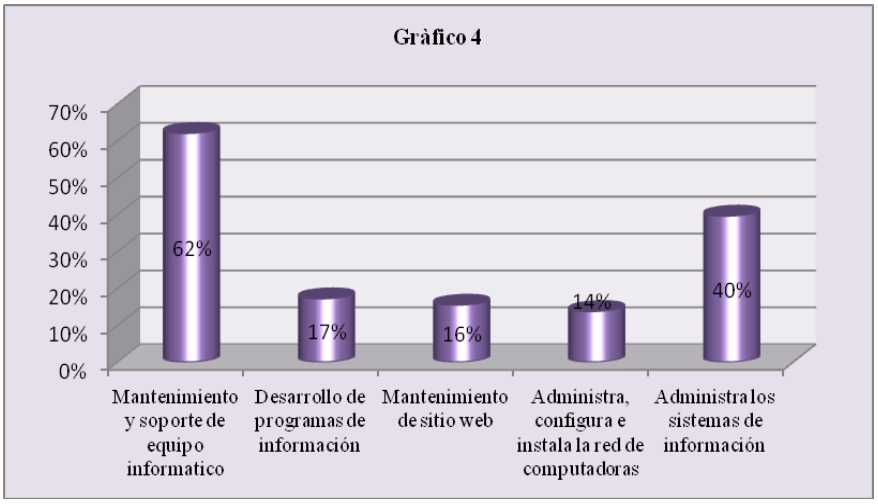
La frecuencia con la que se desarrolla el programa de soporte y mantenimiento en su mayoría de organizaciones las aplican mensual o trimestralmente con el 24% ambas, luego el 17% lo hacen anual, siendo una buena parte de las unidades de análisis los que no implementan ningún plan de mantenimiento con el 16%, y siendo solamente el 6% los que lo aplican de manera semestral, con estos resultados, permite analizar que existe un tiempo razonable para dar dicho mantenimiento.

PREGUNTA 4:

¿Cuáles son las actividades principales que desarrolla el encargado de la seguridad informática de su institución?

Objetivo: Conocer las actividades asignadas al personal a cargo del área

RESPUESTA	FRECUENCIA	
	ABSOLUTA	RELATIVA
Mantenimiento y soporte de equipo informático	36	62%
Desarrollo de programas de información	10	17%
Mantenimiento de sitio web	9	16%
Administra, configura e instala la red de computadoras	8	14%
Administra los sistemas de información	23	40%



Análisis e interpretación:

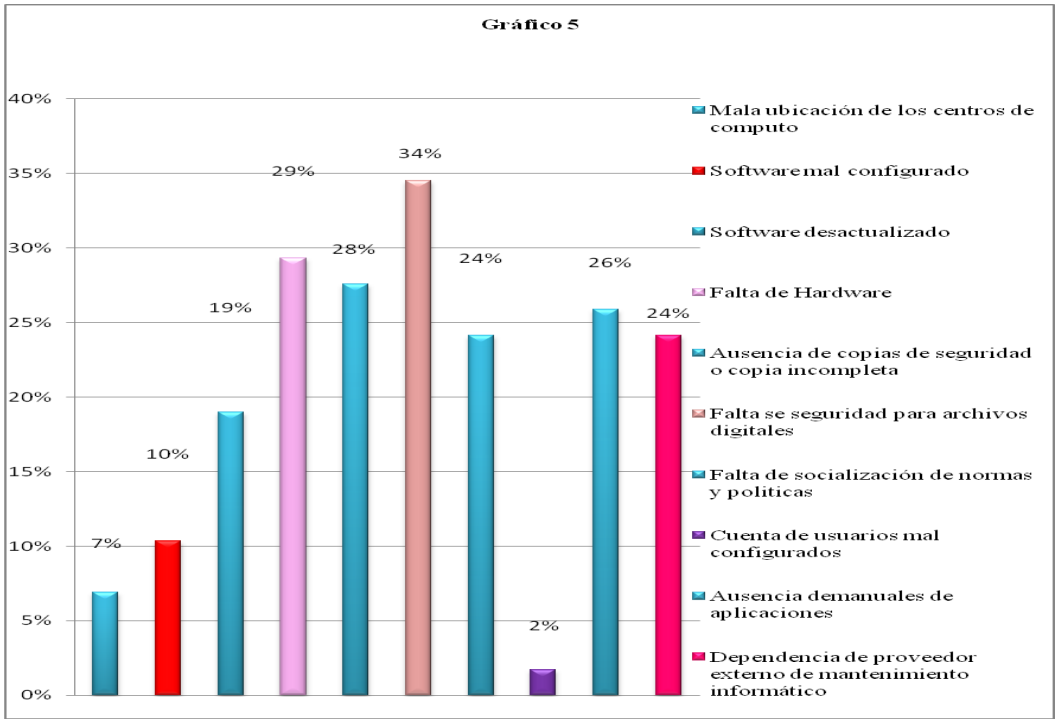
Como es común, el área de soporte técnico no solo se dedica a realizar tareas de mantenimiento, como se puede apreciar en el gráfico, ya que del 100% solamente el 62% realiza estas actividades, el 40% de estos técnicos también realizan trabajo de administración de la información contenida en los sistemas, también un buen porcentaje del personal de soporte técnico encuestado desarrollan programas de información y mantenimientos de sitios web, cada una con el 17% y 16 % respectivamente; y otro 14% realiza funciones de configuración e instalación de redes de computadoras.

PREGUNTA 5:

¿De las siguientes vulnerabilidades que afectan la organización cuales ha identificado dentro de sus instalaciones?

Objetivo: Determinar las principales vulnerabilidades a las cuales están expuestas las organizaciones

RESPUESTA	FRECUENCIA	
	ABSOLUTA	RELATIVA
Mala ubicación de los centros de computo	4	7%
Software mal configurado	6	10%
Software desactualizado	11	19%
Falta de Hardware	17	29%
Ausencia de copias de seguridad o copia incompleta	16	28%
Falta se seguridad para archivos digitales	20	34%
Falta de socialización de normas y políticas	14	24%
Cuenta de usuarios mal configurados	1	2%
Ausencia de manuales de aplicaciones	15	26%
Dependencia de proveedor externo de mantenimiento informático	14	24%



Análisis e interpretación:

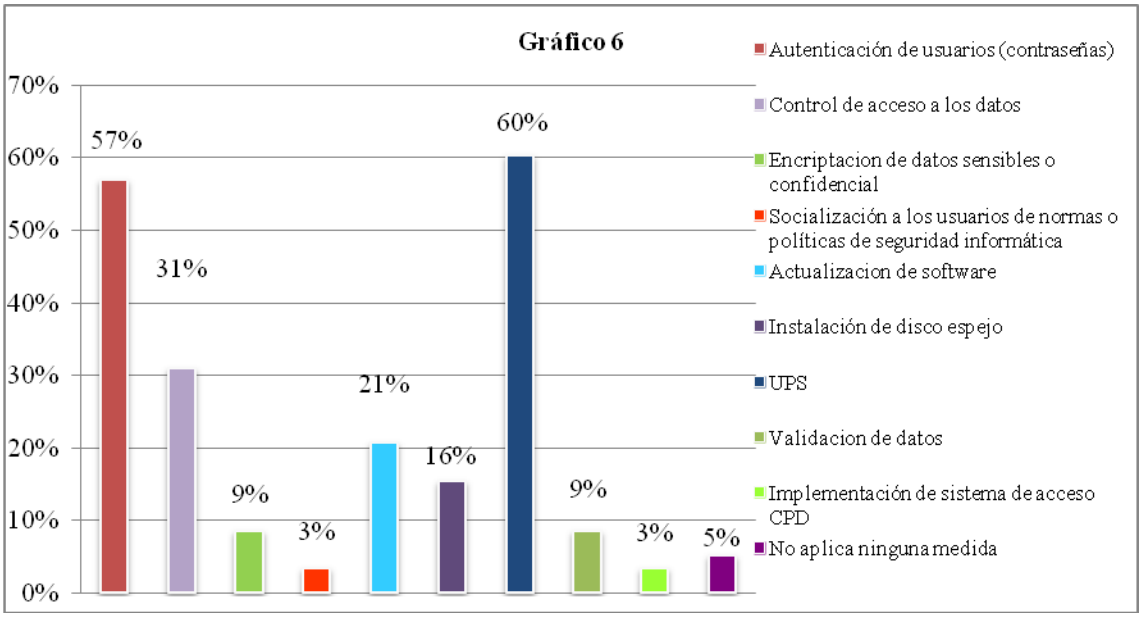
A través de los resultados obtenidos, se ha comprobado que el 100 % de las ONG´S se enfrentan a diferentes tipos de vulnerabilidades, siendo las principales, la falta de seguridad para los archivos digitales, no poseen hardware, ausencia de copias de seguridad y manuales de aplicación, no existe socialización de normas y políticas, dependencia de proveedores externos, con el 34%, 29%, 28%, y 26% y las últimas dos con el 24% ambas, y las que representan una amenaza menor son los software desactualizados, software mal configurados y la mala ubicación de los centros de cómputo, con el 19%, 10% y 7% respectivamente y solamente una mínima parte opinó que la principal vulnerabilidad son las cuentas de usuarios mal configurados con el 2%.

PREGUNTA 6

¿Del siguiente listado cuál o cuáles son las medidas preventivas que aplica en su organización para garantizar la seguridad de la información?

Objetivo: Determinar cuáles son las medidas de prevención que aplican las organizaciones

RESPUESTA	FRECUENCIA	
	ABSOLUTA	RELATIVA
Autenticación de usuarios (contraseñas)	33	57%
Control de acceso a los datos	18	31%
Encriptación de datos sensibles o confidencial	5	9%
Socialización a los usuarios de normas o políticas de seguridad informática	2	3%
Actualización de software	12	21%
Instalación de disco espejo	9	16%
UPS	35	60%
Validación de datos	5	9%
Implementación de sistema de acceso CPD	2	3%
No aplica ninguna medida	3	5%



Análisis e interpretación:

Por los resultados obtenidos en la pregunta anterior, las ONG´S, han tomado a bien implementar medidas de seguridad preventivas, para proteger su información, la más implementada por el 60% de estas ONG´S, son la instalación de UPS a cada computadora,

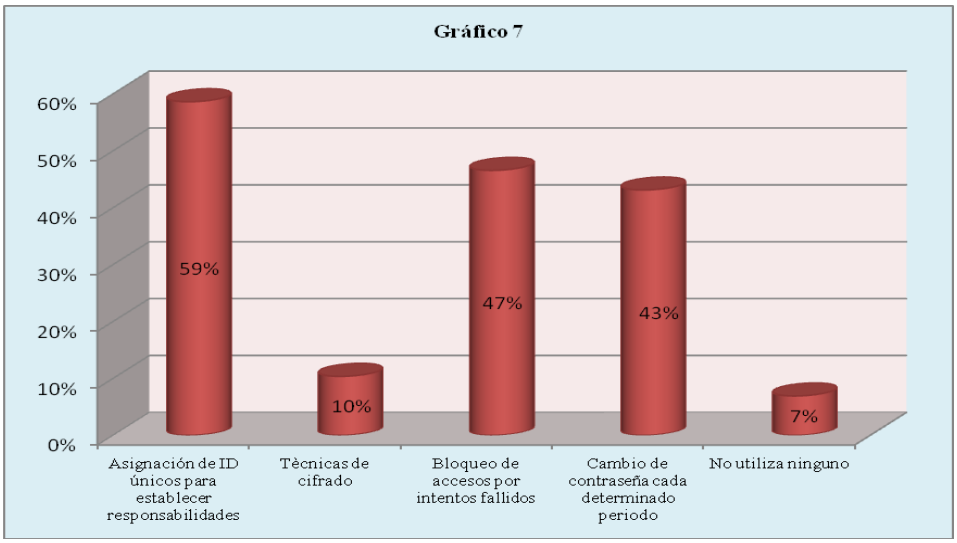
así como también la autenticación de usuarios a través de contraseñas con el 57%, seguido de implementación de control de accesos con el 31%, 21% y 16% aplican medidas de actualización de software y la instalación de discos espejos en las instalaciones, el 9% implementa medidas de encriptación y validación de datos, y el 3% implementa sistemas de acceso CPD y practica la socialización de normas y políticas de seguridad con los usuarios, y por último se puede apreciar que únicamente el 5% no aplica ninguna de las medidas de seguridad mencionadas anteriormente.

PREGUNTA 7:

¿Cuál de las siguientes características utiliza su organización para autentificar las contraseñas? (Puede seleccionar más de una opción)

Objetivo: Identificar si la organización utiliza medidas para autentificar las contraseñas

RESPUESTA	FRECUENCIA	
	ABSOLUTA	RELATIVA
Asignación de ID únicos para establecer responsabilidades	34	59%
Técnicas de cifrado	6	10%
Bloqueo de accesos por intentos fallidos	27	47%
Cambio de contraseña cada determinado periodo	25	43%
No utiliza ninguno	4	7%



Análisis e interpretación:

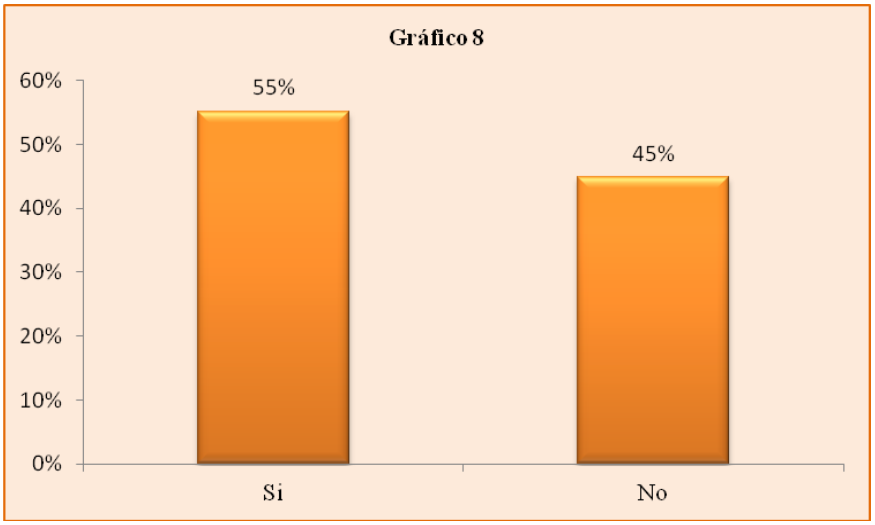
Del 57% de las ONG´S encuestadas que implementan la autenticación de contraseñas, según los resultados de la pregunta 6, se puede visualizar en el gráfico que la principal característica de estas contraseñas es que deben ser únicas para establecer responsabilidades, según el 59% de los resultados, el 47% y el 43% realizan bloqueo de accesos por intentos fallidos y hacen periódicamente cambio de contraseñas, siendo solamente el 10% de las ONG`S las que implementan técnicas de cifrado, y solamente el 7% no hace restricciones a esta medida.

PREGUNTA 8:

¿Su organización cuenta con medidas de seguridad que detecten los ataques a los sistemas informáticos?

Objetivo: Conocer si cuenta con medidas detección de ataques a los sistemas informáticos

RESPUESTA	FRECUENCIA	
	ABSOLUTA	RELATIVA
Si	32	55%
No	26	45%
TOTAL	**58**	**100%**



Análisis e interpretación:

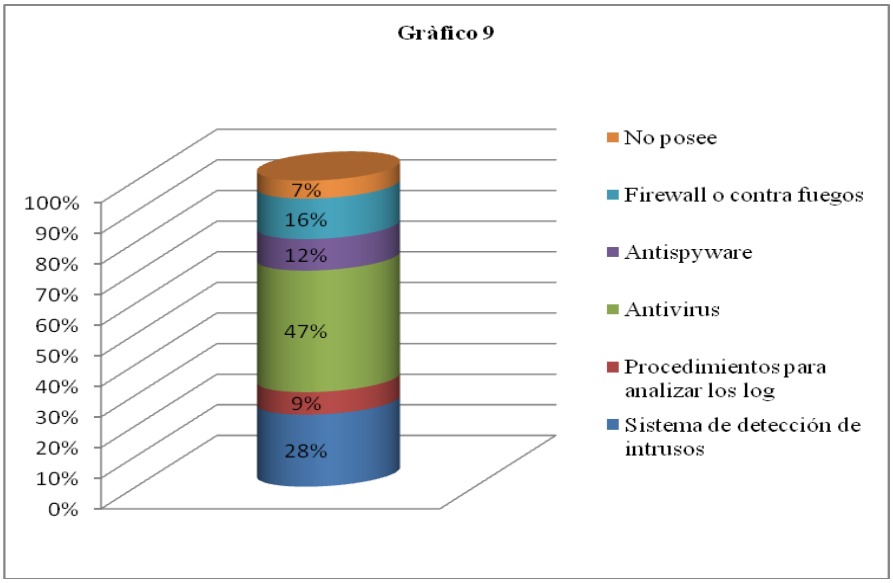
Se observa en el grafico que solamente el 5% separa entre las ONG´S que aplican medidas de seguridad para detectar ataques a la información, es decir el 55% si aplica y el 45% no hace uso de medidas de seguridad para ataques a los sistemas de información.

PREGUNTA 9:

¿Si su respuesta fue positiva, del siguiente listado cuales son los equipos o sistemas que posee para detectar los ataques?

Objetivo: Identificar si cuentan con las medidas de detección para la seguridad informática.

RESPUESTA	FRECUENCIA	
	ABSOLUTA	RELATIVA
Sistema de detección de intrusos	16	28%
Procedimientos para analizar los log	5	9%
Antivirus	27	47%
Antispyware	7	12%
Firewall o contra fuegos	9	16%
No posee	4	7%



Análisis e interpretación:

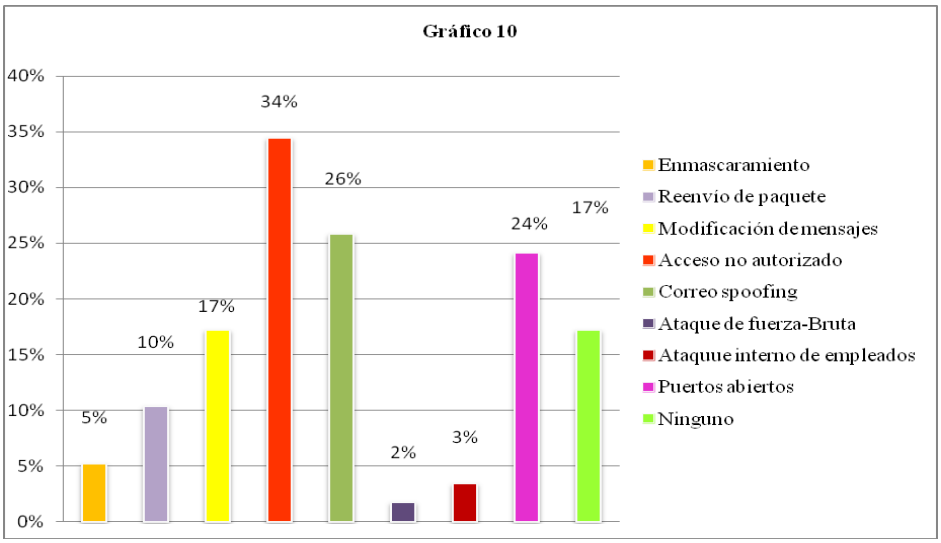
Del 55% de las entidades que aplican medidas para detectar ataques a los sistemas informáticos, lo hacen a través de la instalación de antivirus en las computadoras, ya que es aplicado en un 47% de las ONG´S, seguida de esta con el 28% están los sistemas de detección de intrusos, el 16% firewall y el 12% antispyware, los procedimientos para análisis de log son implementados en el 9% del 100% de la muestra y por último se puede comprobar que el 7% no posee medidas de detección.

PREGUNTA 10:

¿Del siguiente listado, cuales son los ataques que han sufrido los sistemas de informáticos en su organización?

Objetivo: Conocer si han sufrido ataques a los sistemas de seguridad

RESPUESTA	FRECUENCIA	
	ABSOLUTA	RELATIVA
Enmascaramiento	3	5%
Reenvío de paquete	6	10%
Modificación de mensajes	10	17%
Acceso no autorizado	20	34%
Correo spoofing	15	26%
Ataque de fuerza-Bruta	1	2%
Ataque interno de empleados	2	3%
Puertos abiertos	14	24%
Ninguno	10	17%



Análisis e interpretación:

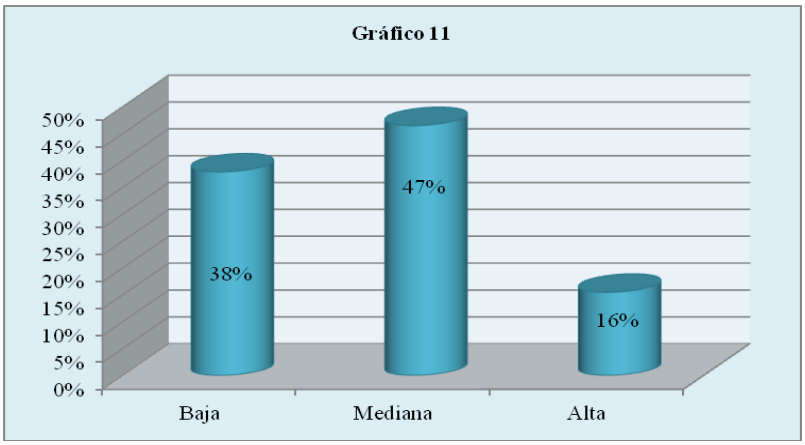
A pesar de todas las medidas que se puedan implementar para proteger la información, siempre existen amenazas diariamente a las que están expuestas estas entidades, y una de las principales es la de los accesos no autorizados a la información, representada del 100% de las organizaciones encuestadas con un 34%, y el menos sufrido es el de ataque de fuerza bruta con un 2%., y el agravio de los propios empleados con el 3%, el 26% se ve afectado con los correos spooning, y el 17% con la modificación de mensajes, el 10% y 5% sufren de reenvío de paquete y enmascaramiento, y por ultimo según estos resultados el 17% de las entidades no han sufrido ningún intento de perjudicar los sistemas de información.

PREGUNTA 11:

¿Cómo considera la probabilidad de amenazas dentro de su organización?

Objetivo: Conocer los niveles de amenazas dentro de las instituciones.

RESPUESTA	FRECUENCIA	
	ABSOLUTA	RELATIVA
Baja	22	38%
Mediana	27	47%
Alta	9	16%
TOTAL	**58**	**100%**



Análisis e interpretación:

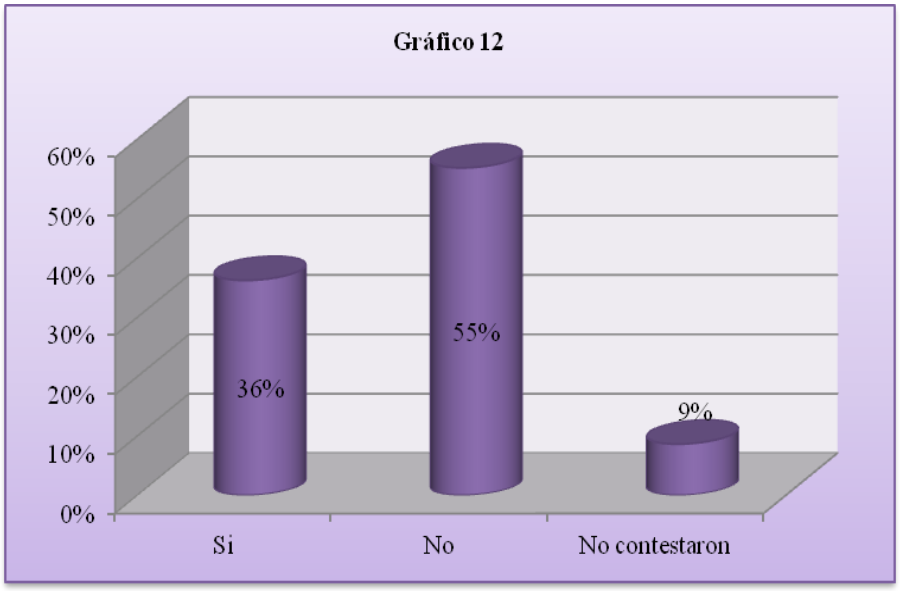
A pesar de que una buena parte de las entidades encuestadas, no poseen medidas de seguridad adecuadas, solamente el 16% se consideran estar en un riesgo alto de probabilidad de amenazas dentro de la organización., siendo en su mayoría de ONG´S con el 47% las que consideran estar entre un nivel intermedio y el 38% con una probabilidad baja.

PREGUNTA 12:

¿Su organización realiza capacitaciones sobre prevenir los ataques de la ingeniería social?

Objetivo: Conocer si existe concientización sobre los ataques de ingeniería social

RESPUESTA	FRECUENCIA	
	ABSOLUTA	RELATIVA
Si	21	36%
No	32	55%
No contestaron	5	9%
TOTAL	**58**	**100%**



Análisis e interpretación:

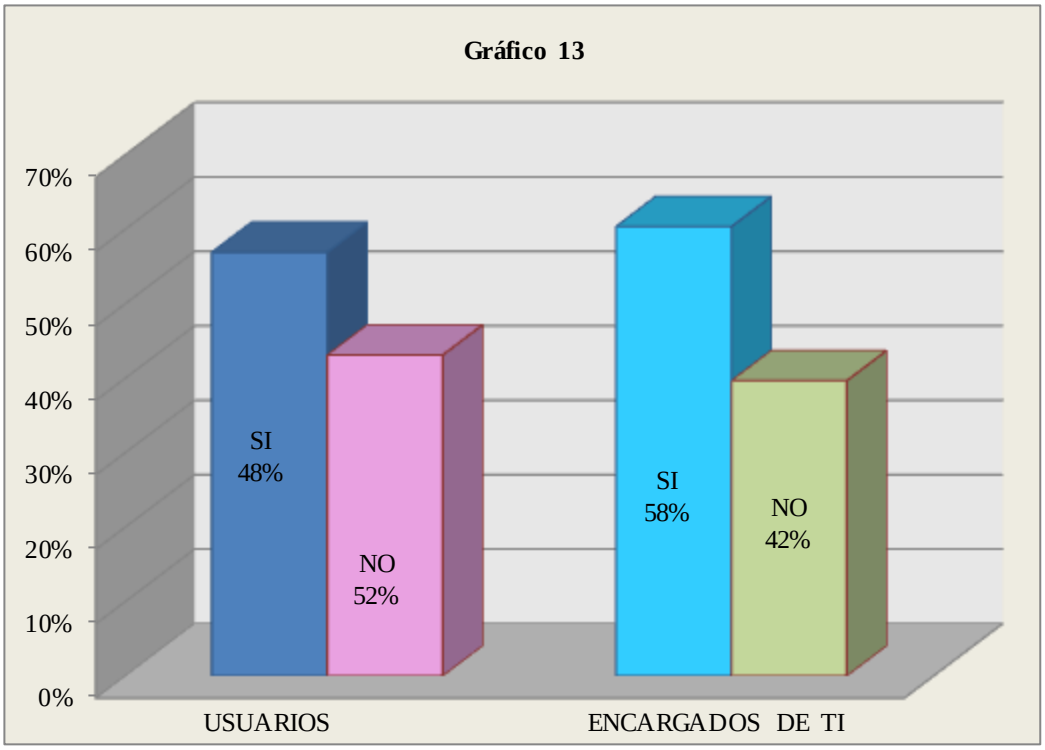
Claramente se puede apreciar, el poco interés que existe por parte de las ONG´S de instruir a sus empleados en el tema de seguridad de la información, ya que solamente el 36% de estas realizan capacitación al personal para darles a conocer las formas en que pueden prevenir posibles ataques a la seguridad de la información, el 55% no consideran que esto sea importante dentro de la ONG´S y el 9% no contestaron a esta interrogante.

PREGUNTA 13:

¿Existen políticas y procedimientos para los usuarios de los sistemas informáticos y encargados de TI?

Objetivo: Conocer si la organización cuenta con manuales para los usuarios de los sistemas y los responsables de los mismos.

REPUESTAS	USUARIOS	ENCARGADOS DE TI	USUARIOS F. RELATIVA	ENCARGADOS TI F. RELATIVA
Si	33	35	57%	60%
No	25	23	43%	40%
	58	**58**	**100%**	**100%**



Análisis e interpretación:

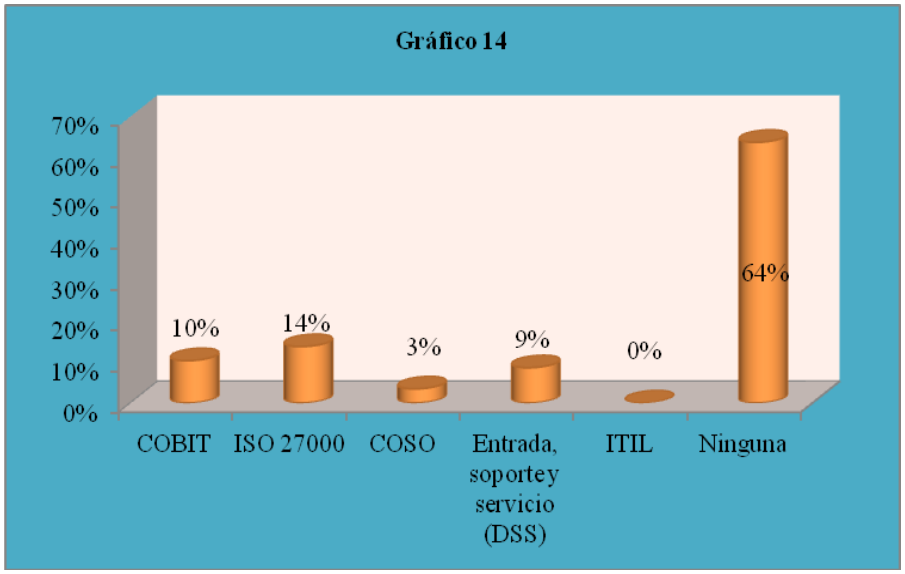
Es importante que tanto los usuarios como los encargados de TI tengan definidos procedimientos de uso en los sistemas informáticos, pero solamente el 48% de usuarios y 58% de encargados de TI tiene procedimientos definidos.

PREGUNTA 14:

¿Si cuenta con políticas y procedimiento para la seguridad informática cual o cuales normas técnicas aplica para la protección de la información?

Objetivo: Conocer si las organizaciones aplican normativa técnica en la implementación de políticas y procedimientos para la seguridad de la información.

RESPUESTA	FRECUENCIA	
	ABSOLUTA	RELATIVA
COBIT	6	10%
ISO 27000	8	14%
COSO	2	3%
Entrada, soporte y servicio (DSS)	5	9%
ITIL	0	0%
Ninguna	37	64%
TOTAL	**58**	**100%**



Análisis e interpretación:

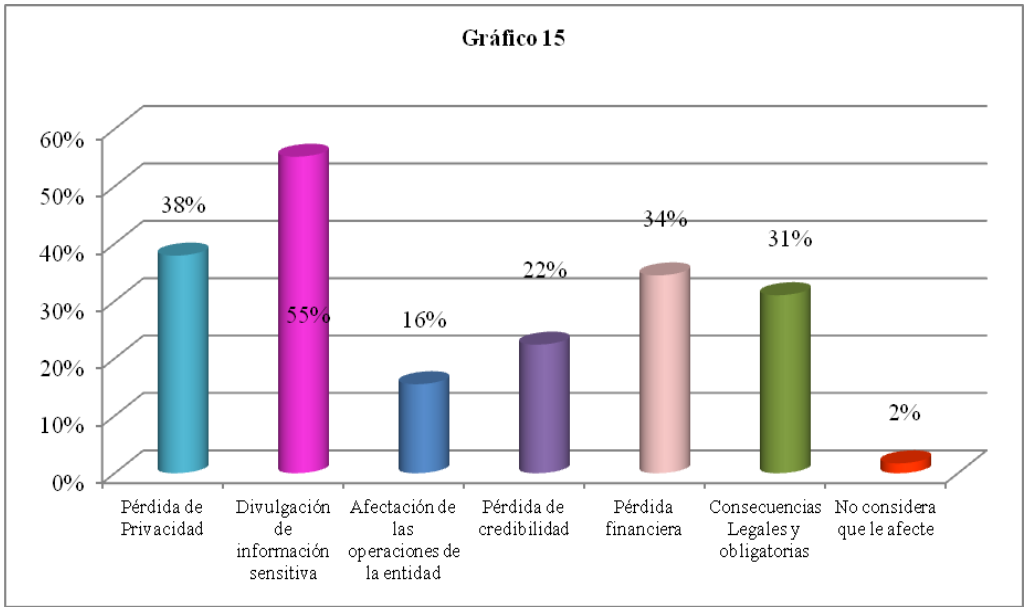
Para poder garantizar mejores resultados en la implementación de políticas y procedimientos de seguridad de información, es necesario que se haga a través de lineamientos técnicos, pero se puede valorar en el grafico que del 100% de las ONG´S encuestadas el 64% no aplica ningún tipo de normativa técnica, el resto está distribuido entre la normativa ISO con el 14%, seguido de COBIT con el 10%, siendo ITIL el único marco técnico que no es aplicado por ninguna entidad, y el 9% y 3% respectivamente aplican COSO y entradas de soporte y servicio DSS.

PREGUNTA 15:

¿Del siguiente listado, cual o cuales considera usted que afectaría la continuidad o funcionamiento de su organización?

Objetivo: Identificar las causas que pueden afectar a la organización en su funcionamiento.

RESPUESTA	FRECUENCIA	
	ABSOLUTA	RELATIVA
Pérdida de Privacidad	22	38%
Divulgación de información sensitiva	32	55%
Afectación de las operaciones de la entidad	9	16%
Pérdida de credibilidad	13	22%
Pérdida financiera	20	34%
Consecuencias Legales y obligatorias	18	31%
No considera que le afecte	1	2%



Análisis e interpretación:

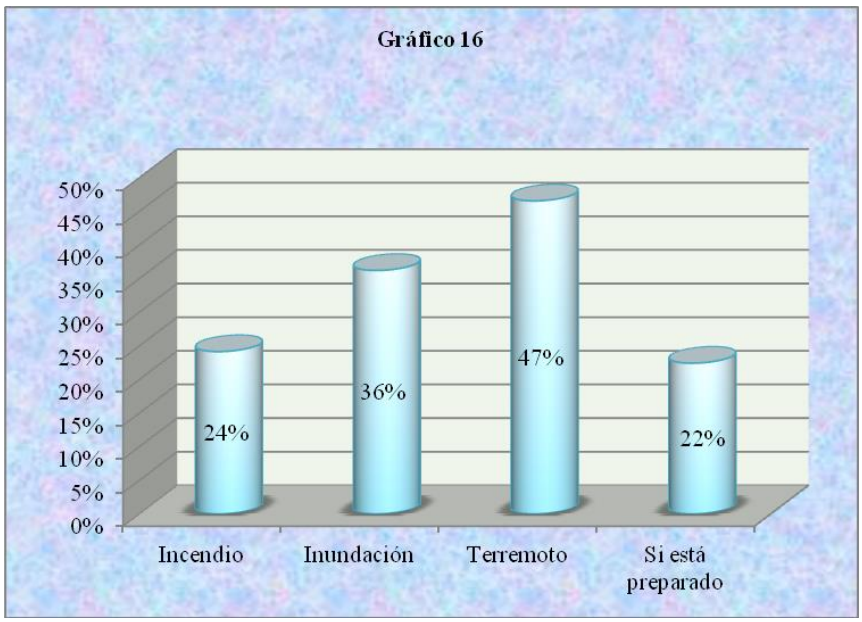
Según la opinión obtenida del personal de soporte técnico de las ONG´S, consideran que la divulgación de información valiosa seria el riesgo más grande a las que se puede enfrentar estas entidades, con un 55%, así como también la pérdida de privacidad y pérdidas financieras, con el 38% y 34%, el 31% considera que el enfrentamiento de consecuencias legales y obligatorias podrían afectar la continuidad de las operaciones, dentro de las opciones están la pérdida de credibilidad y la afectación de las operaciones, para lo cual los resultados obtenidos a estas respuestas fueron del 22% y del 16%, y solamente un mínimo porcentaje del 2% opina que no considera que algunas de las anteriores podrían entorpecer el buen funcionamiento de las actividades de la entidad.

PREGUNTA 16:

¿Del siguiente listado de contingencias ¿ Para cual no está preparada su organización para proteger la seguridad de los equipos y su mantenimiento?

Objetivo: Conocer si están preparados para enfrentar contingencias que ponen en riesgo la información.

RESPUESTA	FRECUENCIA	
	ABSOLUTA	RELATIVA
Incendio	14	24%
Inundación	21	36%
Terremoto	27	47%
Si está preparado	13	22%



Análisis e interpretación:

Claramente se puede apreciar que las ONG´S no están preparadas ante la ocurrencia de algún siniestro o de un desastre natural, ya que solamente el 22% considera tener políticas y procedimientos bien definidos que pueden mitigar este riesgo.

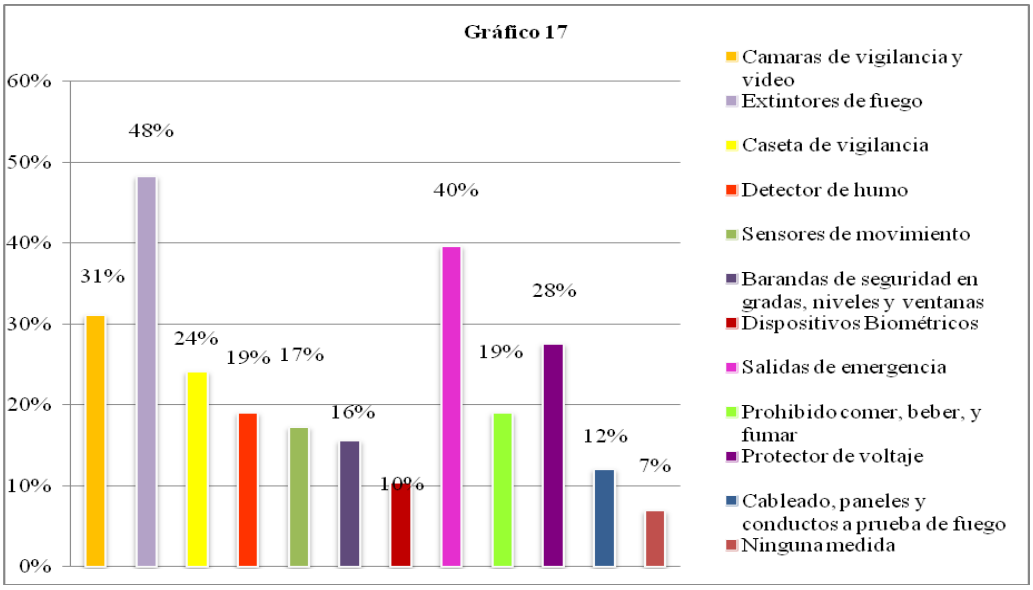
El principal suceso ante los cuales no están preparadas las ONG´S es a un terremoto según lo expresaron el 47% de los encuestados, como segundo lugar con el 36% está la inundación, y opinando el 24% que no están debidamente preparados ante un incendio.

PREGUNTA 17:

¿Seleccione cuál de las siguientes medidas de seguridad se encuentran en las instalaciones de su organización? (Seleccione las que poseen)

Objetivo: Identificar con qué medidas de seguridad física cuenta la organización dentro de sus instalaciones.

RESPUESTA	FRECUENCIA	
	ABSOLUTA	RELATIVA
Cámaras de vigilancia y video	18	31%
Extintores de fuego	28	48%
Caseta de vigilancia	14	24%
Detector de humo	11	19%
Sensores de movimiento	10	17%
Barandas de seguridad en gradas, niveles y ventanas	9	16%
Dispositivos Biométricos	6	10%
Salidas de emergencia	23	40%
Prohibido comer, beber, y fumar	11	19%
Protector de voltaje	16	28%
Cableado, paneles y conductos a prueba de fuego	7	12%
Ninguna medida	4	7%



Análisis e interpretación:

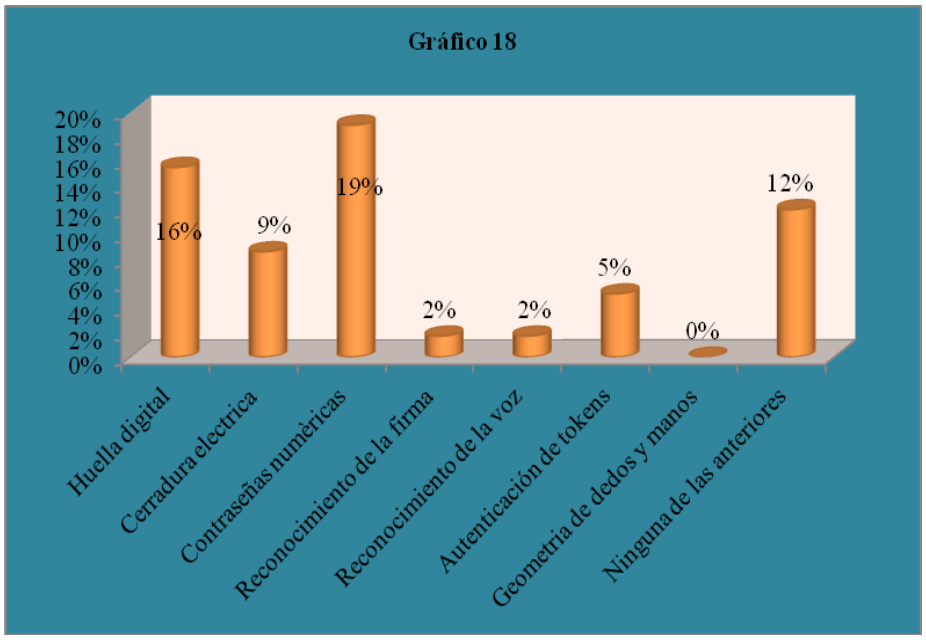
Indudablemente se puede apreciar que casi el 50% de las ONG´S encuestadas poseen dentro de sus instalaciones extintores de fuego así como salidas de emergencia debidamente identificadas, con el 48% y 40% cada una, el 38% posee cámaras de seguridad dentro de las instalaciones, y el 28% protectores de voltaje para las conexiones eléctricas de los equipos, también una muy buena parte del personal técnico manifiestan que poseen caseta de seguridad y detectores de humo, solo un 1% separa las opciones de sensores de movimiento y barandas de seguridad con el 17% y 16% respectivamente, y el resto del 100% de los encuestados manifiestan que el cableado a prueba de fuego y dispositivos biométricos son las medidas de seguridad menos implementadas con el 12% y 10%, y solamente el 7% no cuenta con medidas de seguridad dentro de las instalaciones.

PREGUNTA 18:

¿Si dentro de su respuesta anterior cuenta con dispositivos biométricos, señale cual o cuales del siguiente listado tiene su organización?

Objetivo: Identificar qué tipo de dispositivos biométricos posee la organización

RESPUESTA	FRECUENCIA	
	ABSOLUTA	RELATIVA
Huella digital	9	16%
Cerradura eléctrica	5	9%
Contraseñas numéricas	11	19%
Reconocimiento de la firma	1	2%
Reconocimiento de la voz	1	2%
Autenticación de tokens	3	5%
Geometría de dedos y manos	0	0%
Ninguna de las anteriores	7	12%



Análisis e interpretación:

Según el grafico de la pregunta anterior se puede observar, que el 10% de instituciones cuentan con dispositivos biométricos, para lo cual se indagó que tipos de dispositivos son los que más utilizan, resultando las contraseñas numéricas y la huella digital las más

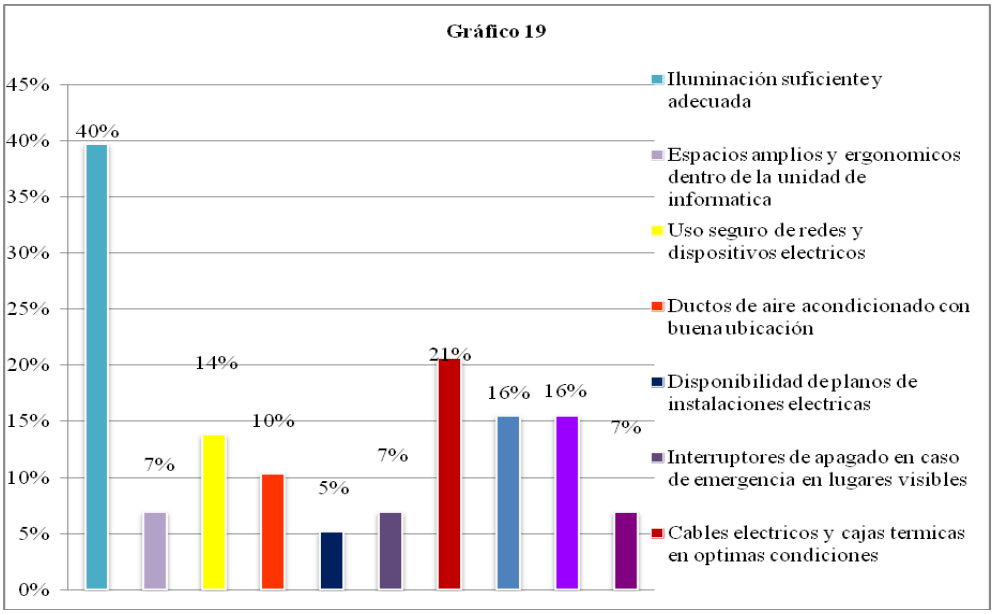
implementadas, con el 19% y el 16%, cada una, el 9% manifiesta utilizar como dispositivo biométrico la cerradura eléctrica, la cual también es considerada como una medida de seguridad para proteger la información, el 12% del personal de soporte técnico encuestado coincidieron que no aplican ninguna de las medidas sugeridas en la pregunta, completando el 100% el reconocimiento de la firma y la voz, y la autenticación de tokens, con el 2% las primeras dos opciones y con el 5% la última opción.

PREGUNTA 19:

¿Del siguiente listado determine si se cumplen las condiciones idóneas de los equipos dentro y fuera del área informática para su funcionamiento?

Objetivo: Determinar si los equipos cuentan con condiciones adecuadas para su funcionamiento dentro y fuera de la organización.

RESPUESTA	FRECUENCIA	
	ABSOLUTA	RELATIVA
Iluminación suficiente y adecuada	23	40%
Espacios amplios y ergonómicos dentro de la unidad de informática	4	7%
Uso seguro de redes y dispositivos eléctricos	8	14%
Ductos de aire acondicionado con buena ubicación	6	10%
Disponibilidad de planos de instalaciones eléctricas	3	5%
Interruptores de apagado en caso de emergencia en lugares visibles	4	7%
Cables eléctricos y cajas térmicas en óptimas condiciones	12	21%
Señalizaciones idóneas para advertencia de voltajes y evacuación	9	16%
Vigilancia continua por parte de guardias	9	16%
No posee las condiciones idóneas	4	7%



Análisis e interpretación:

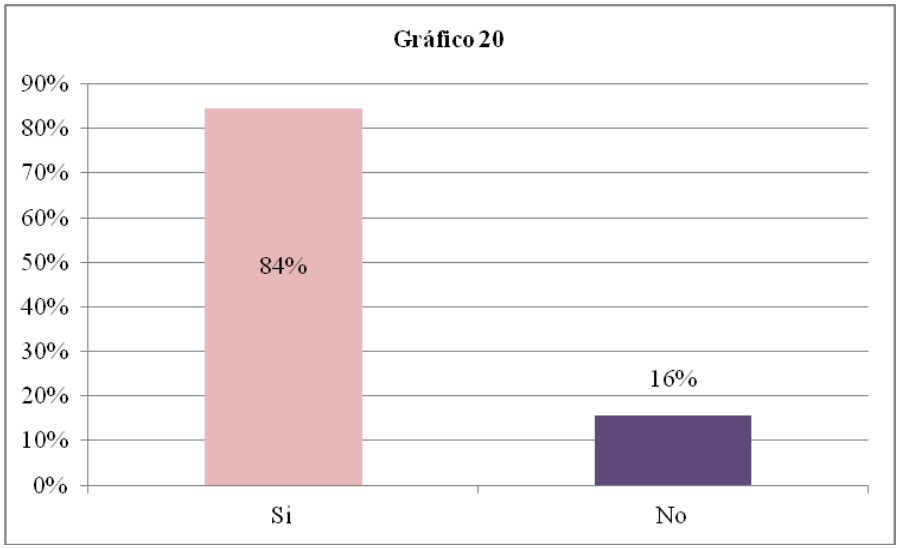
El 40% de encuestados manifiesta que los equipos poseen iluminación adecuada, el 21% respondió tener cables eléctricos en óptimas condiciones, el 16% de las ONG´S sujetas de estudio, manifestaron tener señalizaciones idóneas de advertencia de voltajes y evacuación, también el uso seguro de redes y dispositivos eléctricos así como los ductos de aire acondicionado en buen estado fueron otras dos respuestas con un buen porcentaje de aceptación con el 14% y 10% respectivamente, el 7% lo compone los espacios amplios y los interruptores de apagado en caso de emergencias, y el 5% expreso que no existen planos eléctricos que los guie hacia un buen mantenimiento de los equipos, el 7% indicó que no existen medidas idóneas.

PREGUNTA 20:

¿Cuenta con un inventario de todos los activos que posee la organización?

Objetivo: Conocer si la organización tiene definido un inventario de activos que le permita tener control de los mismos.

RESPUESTA	FRECUENCIA	
	ABSOLUTA	RELATIVA
Si	49	84%
No	9	16%
TOTAL	**58**	**100%**



Análisis e interpretación:

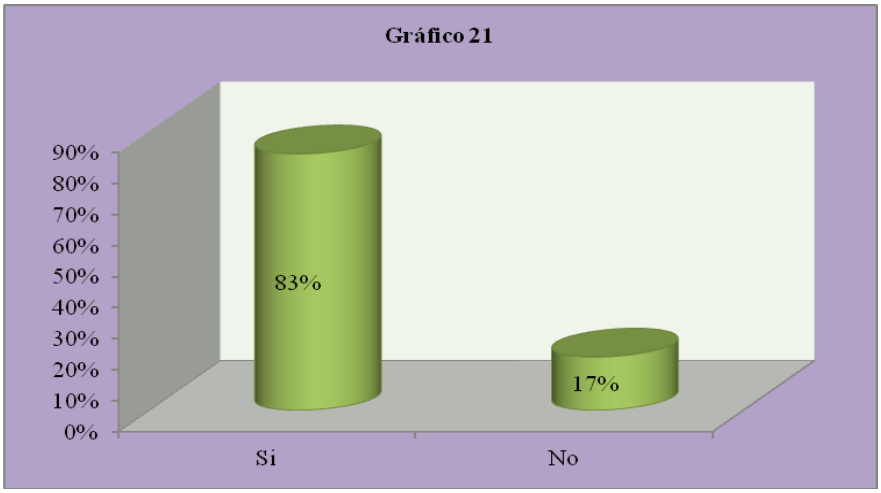
Para poder tener un control adecuado de los activos que posee la entidad, es de mucha importancia que se lleve un inventario, el cual se debe actualizar periódicamente, de las 58 ONG`S encuestadas, 49 manifestaron tener este control, equivalente al 84% y solamente el 16% no cuenta con esta información actualizada.

PREGUNTA 21:

¿Su organización estaría interesada en aplicar un sistema de seguridad de la información en base a la normativa técnica ISO 27000?

Objetivo: Conocer si están interesados en aplicar un sistema de seguridad de la Información en base a la normativa técnica de las ISO.

RESPUESTA	FRECUENCIA	
	ABSOLUTA	RELATIVA
Si	48	83%
No	10	17%
TOTAL	**58**	**100%**



Análisis e interpretación:

Del 67% de las ONG´S que no aplican ninguna normativa técnica para la seguridad de la información, el 83% se mostró interesado en implementar las normas ISO para mejorar sus políticas y procedimientos y para las que no poseen, lo consideran una buena oportunidad comenzar a implementarlas a través de esta normativa, teniendo una negación a esta alternativa un 17%. Equivalente a 10 ONG´S encuestadas.

Además de conocer la opinión del personal técnico que da soporte en el tema de sistemas de información a las ONG´S, es de vital importancia conocer la opinión del personal clave de las mismas entidades, ya que son ellos quienes utilizan en el día a día y de manera directa estos sistemas.

A continuación se presentan los resultados de las respuestas obtenidas por el personal clave de las 58 ONG´S sujetas a estudio.

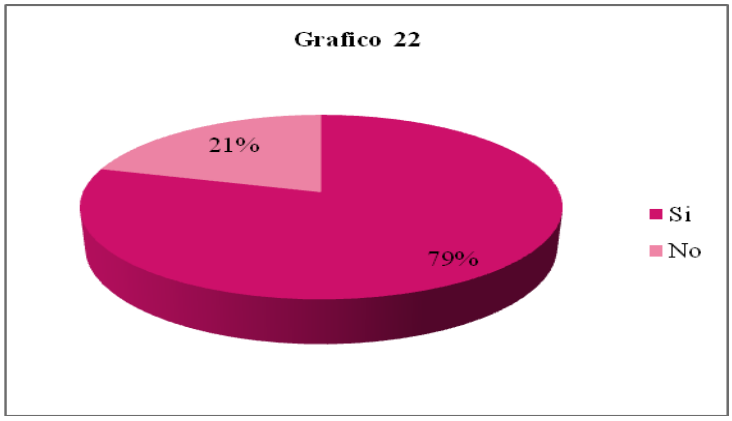
Tabulación y análisis de la información recopilada del personal clave de las Organizaciones No Gubernamentales.

PREGUNTA 1:

¿Posee conocimiento de lo que significa la seguridad informática?

Objetivo: Conocer si el personal de las ONG¨S poseen conocimiento sobre el tema de seguridad de la información.

RESPUESTA	FRECUENCIA	
	ABSOLUTA	RELATIVA
Si	46	79%
No	12	21%
TOTAL	**58**	**100%**



Análisis e interpretación:

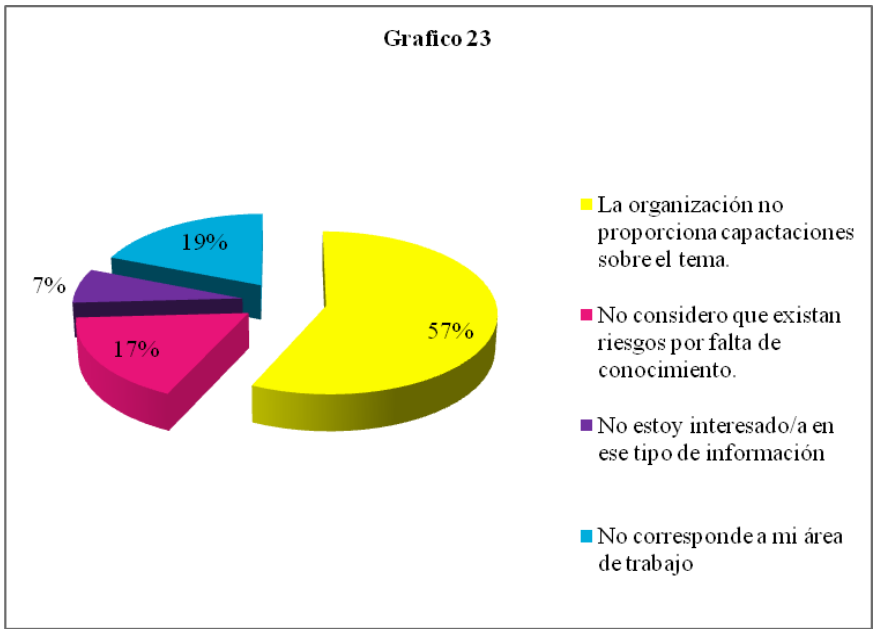
Es alentador ver que el 79% de las personas encuestadas poseen conocimiento sobre lo que es seguridad de la información, y solo una pequeña parte el 21% no tiene idea de este tema.

PREGUNTA 2:

Si su respuesta a la pregunta anterior fue negativa, cuál o cuáles son las causas que ocasionan la falta de conocimiento sobre la seguridad informática?

Objetivo: Identificar las causas por las cuales los usuarios no tienen conocimiento sobre la seguridad de la información.

RESPUESTA	FRECUENCIA	
	ABSOLUTA	RELATIVA
La organización no proporciona capacitaciones sobre el tema.	33	57%
No considero que existan riesgos por falta de conocimiento.	10	17%
No estoy interesado/a en ese tipo de información	4	7%
No corresponde a mi área de trabajo	11	19%



Análisis e interpretación:

Del 21% de los encuestados que manifestaron no poseer conocimiento sobre la seguridad de la información, según la pregunta 1; interesó descubrir, cuales son las

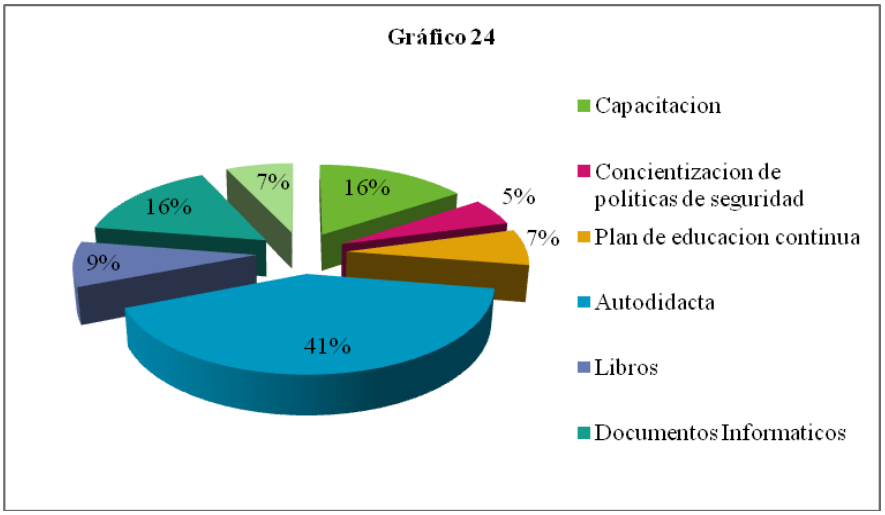
principales causas que han generado este desconocimiento, descubriendo que la principal razón se debe a que las ONG´S no les brindan este tipo de información a los usuarios, según lo manifestó el 57% de las personas, también el 19% consideran que no poseen conocimiento de este tema porque creen que no pertenece a su área de trabajo, por lo que a su criterio está demás esta información, el 17% opinó que según la seguridad de la entidad, no se consideran estar en riesgo ante el desconocimiento de este tema, y por último el 7% manifestó no estar interesado.

PREGUNTA 3:

Donde adquirió los conocimientos sobre la seguridad informática? (Selecciones una o más alternativas de respuesta)

Objetivo: Descubrir los métodos que utilizan las ONG para capacitar a sus empleados en el tema de seguridad de la información

RESPUESTA	FRECUENCIA	
	ABSOLUTA	RELATIVA
Capacitación	9	16%
Concientización de políticas de seguridad	3	5%
Plan de educación continua	4	7%
Autodidacta	24	41%
Libros	5	9%
Documentos Informáticos	9	16%
Ninguno	4	7%
TOTAL	**58**	**100%**



Análisis e interpretación:

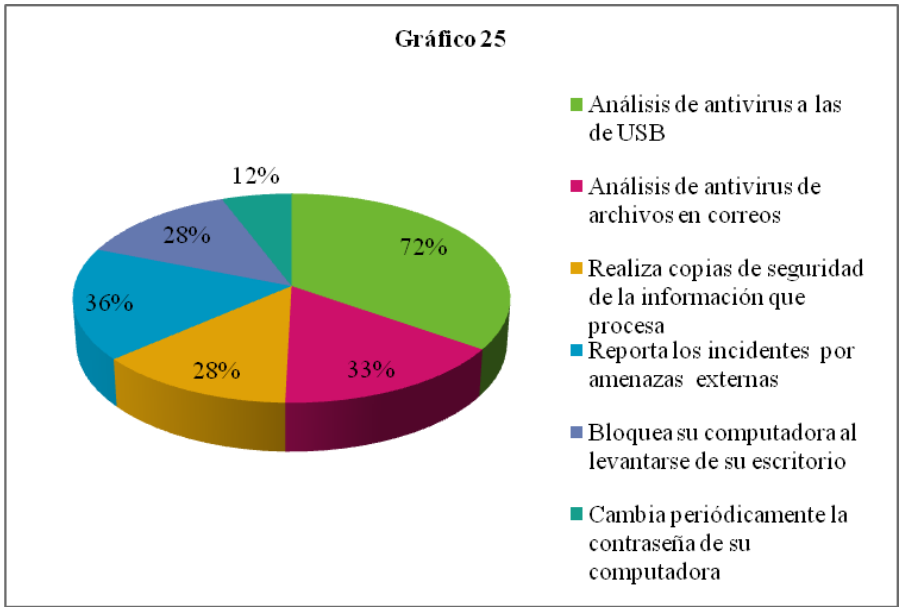
Además de saber qué porcentaje de los encuestados poseen conocimiento sobre la seguridad de la información, interesa saber por qué medios estas personas han adquirido estos conocimientos, descubriendo así que el 41% lo ha hecho bajo sus propios recursos, el 16% se ha auxiliado de documentos informáticos, y ha recibido capacitaciones al respecto, el 9% ha recurrido a libros que hablan de este tema, el 7% manifiesta haber recibido un plan de educación continua, y como último punto, solo una mínima parte del 5% afirma haber recibido capacitaciones sobre concientización de políticas de seguridad informática.

PREGUNTA 4

¿De las siguientes medidas de seguridad informática cuales son las que aplica en su puesto de trabajo?

Objetivo: Analizar las diferentes medidas que implementan el personal de las ONG para proteger su información.

RESPUESTA	FRECUENCIA	
	ABSOLUTA	RELATIVA
Análisis de antivirus a las de USB	42	72%
Análisis de antivirus de archivos en correos	19	33%
Realiza copias de seguridad de la información que procesa	16	28%
Reporta los incidentes por amenazas externas	21	36%
Bloquea su computadora al levantarse de su escritorio	16	28%
Cambia periódicamente la contraseña de su computadora	7	12%



Análisis e interpretación:

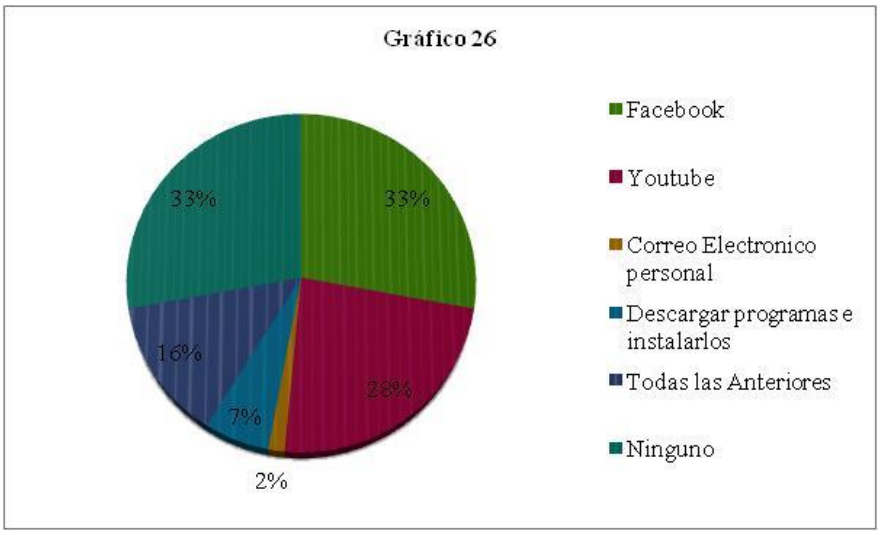
También se consultó con el personal clave cuales son los tipos de medida de seguridad que implementan dentro de sus áreas de trabajo, y se puede observar en el grafico que las más utilizadas son el análisis de antivirus a las USB, el reporte de incidentes por amenazas externas y el análisis de antivirus a los archivo adjuntos provenientes de correos electrónicos, cada una con el 72%, 36%, y 33% respectivamente, el 28% de los encuestados coincidieron que realizan copias de seguridad de la información que procesan y a la vez bloquean su computadora cuando se levantan de sus escritorios, y por último, solo el 12% afirmó que cambia periódicamente sus contraseñas.

PREGUNTA 5

¿En su institución existen restricciones para el acceso a internet para el personal? Del siguiente listado seleccione cuales son los accesos restringidos.

Objetivo: Conocer si las ONG´S aplican al personal medidas de seguridad para la restricción del uso de internet.

RESPUESTA	FRECUENCIA	
	ABSOLUTA	RELATIVA
Facebook	19	33%
YouTube	16	28%
Correo Electrónico personal	1	2%
Descargar programas e instalarlos	4	7%
Todas las Anteriores	9	16%
Ninguno	19	33%



Análisis e interpretación:

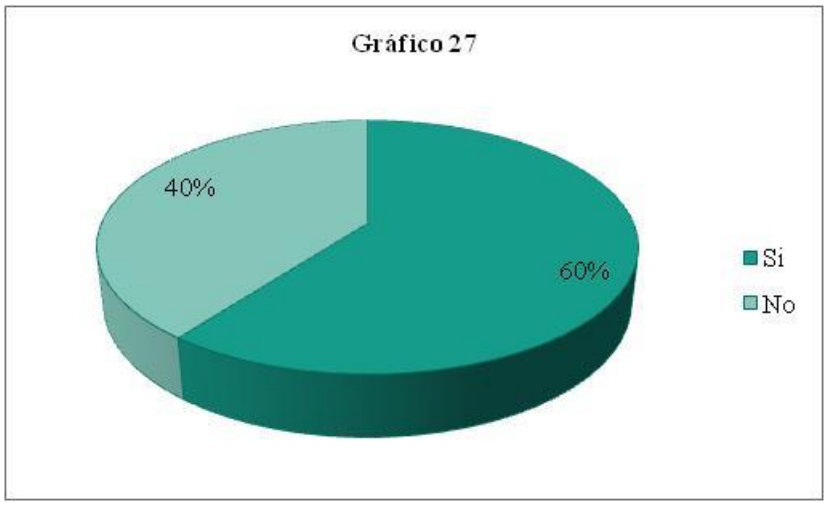
A través de los resultados de esta pregunta, se puede determinar que gran parte de las ONG´S estudiadas, no tienen restricciones al uso de internet, según lo afirmaron el 33%, así como también con este mismo porcentaje manifestaron que la única restricción que tienen es el acceso al Facebook, el 28% confirmó que no pueden acceder a páginas de YouTube, y solamente el 7% de las personas encuestadas informan que lo único que tiene prohibido hacer es descargar e instalar programas, completando el 100% de los encuestados con un 16% que afirman que tienen restringido el usos de todas las opciones mencionadas anteriormente.

PREGUNTA 6

¿La institución le autoriza a llevarse información para trabajar a su casa?

Objetivo: Identificar si los empleados tienen permisos para llevar información fuera de la Organización

RESPUESTA	FRECUENCIA	
	ABSOLUTA	RELATIVA
Si	35	60%
No	23	40%
TOTAL	**58**	**100%**



Análisis e interpretación:

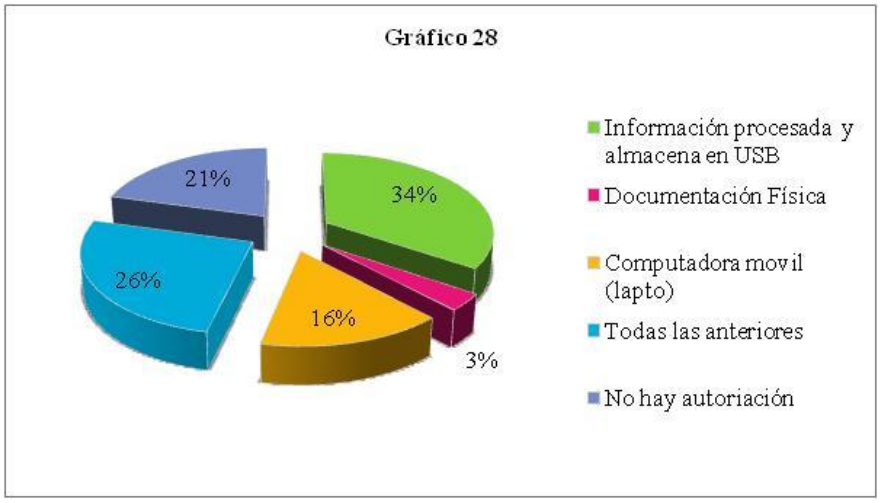
Claramente se puede evidenciar que más del 50% de las ONG´S permiten que sus empleados se lleven información relacionada a la entidad, según lo manifestó el 60% de los encuestados, y solo el 40% indicó que esta práctica no es permitida.

PREGUNTA 7

Si su respuesta fue positiva, del siguiente listado ¿cuál es la forma más común que utiliza para llevarse la información? (puede seleccionar más de una opción)

Objetivo: Descubrir si en las ONG´S les permite a los empleados sacar información o activos físicos de la institución.

RESPUESTA	FRECUENCIA	
	ABSOLUTA	RELATIVA
Información procesada y almacena en USB	20	34%
Documentación Física	2	3%
Computadora móvil (laptop)	9	16%
Todas las anteriores	15	26%
No hay autorización	12	21%
TOTAL	**58**	**100%**



Análisis e interpretación:

Una vez conocido si las ONG´S permiten que los empleados se lleven información confidencial, es importante conocer bajo que medios es sacada esta información, siendo el principal método a través de USB con el 33%, el otro medio mayormente utilizado es a través de laptop con el 16%, solo una pequeña parte del 3% lo hace a través de

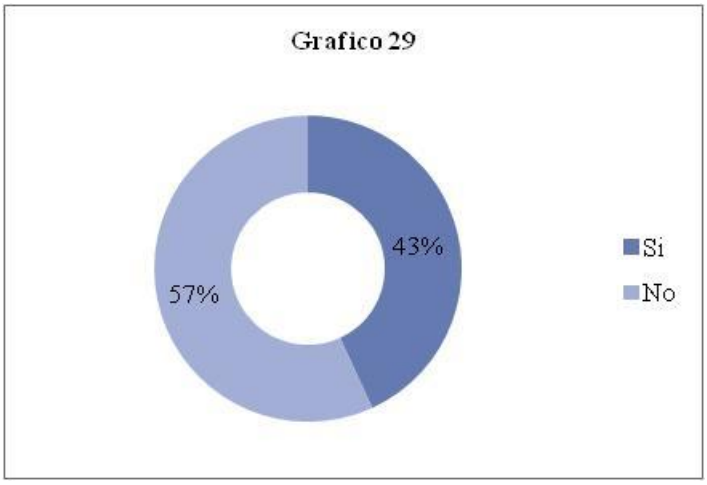
documentos físicos, y el 26% confirmó que utilizan cualquiera de los medios mencionados anteriormente.

PREGUNTA 8

Posee su institución políticas y procedimientos para la seguridad informática que garantice la protección de la información que se procesa (si su respuesta es negativa pase a la pregunta 9)

Objetivo: Determinar si las ONG´S tienen políticas y procedimientos definidos que garanticen la seguridad de la información.

RESPUESTA	FRECUENCIA	
	ABSOLUTA	RELATIVA
Si	25	43%
No	33	57%
TOTAL	**58**	**100%**



Análisis e interpretación:

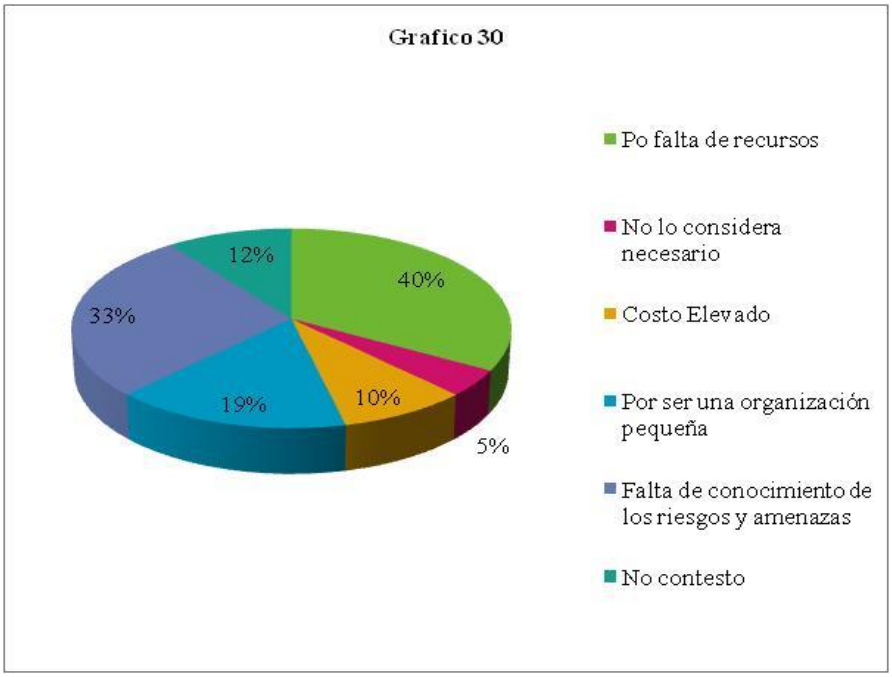
Es importante mencionar que la información que se procesa a diario debe de estar respaldada con políticas y procedimientos, según los resultados obtenidos solo el 57% cumplen con esta característica, y el 43% no implementa políticas ni procedimientos para la información procesada.

PREGUNTA 9

Del siguiente listado ¿Cuáles cree que son las razones de no contar con políticas de seguridad informática?

Objetivo: Analizar las posibles causas por las que las ONG´S no aplican políticas de seguridad para la información.

RESPUESTA	FRECUENCIA	
	ABSOLUTA	RELATIVA
Po falta de recursos	23	40%
No lo considera necesario	3	5%
Costo Elevado	6	10%
Por ser una organización pequeña	11	19%
Falta de conocimiento de los riesgos y amenazas	19	33%
No contesto	7	12%



Análisis e interpretación:

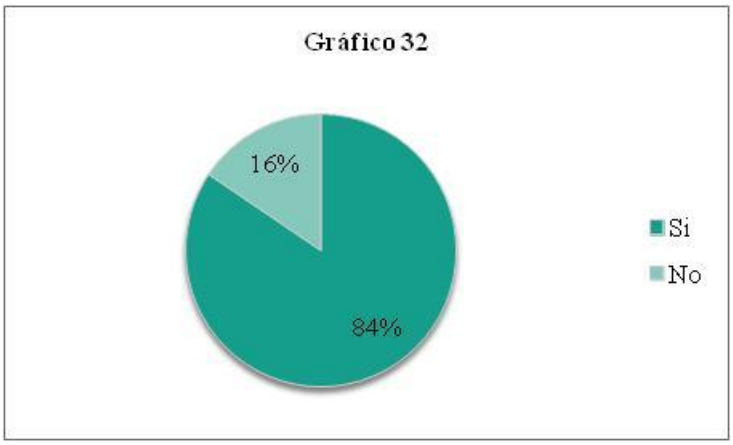
No solo es importante conocer si la entidad cuenta con políticas y procedimientos para la información que se procesa, sino que también se deben conocer las razones ante las faltas de estas, se determinó según los resultados, que el 40% del personal clave encuestado manifiestan que se debe a la falta de recursos que padece la entidad, otro aspecto que influye es la falta de conocimiento de los riesgos y amenazas a los que están expuestos según el 33%, el 19% opinaron que son una entidad pequeña y no necesitan aplicar este tipo de políticas, el 10% mencionaron que se debe al costo elevando que esto representa para la entidad, y solamente el 5% consideran que esta práctica no es necesaria.

PREGUNTA 10

Le exigen los organismos donantes contar con una estructura organizacional e indique con cuales son los que cuenta su institución

Objetivo: Identificar qué tipo de exigencias piden los donantes a las ONG´S para proteger la información.

RESPUESTA	FRECUENCIA	
	ABSOLUTA	RELATIVA
Si	49	84%
No	9	16%
TOTAL	**58**	**100%**



Análisis e interpretación:

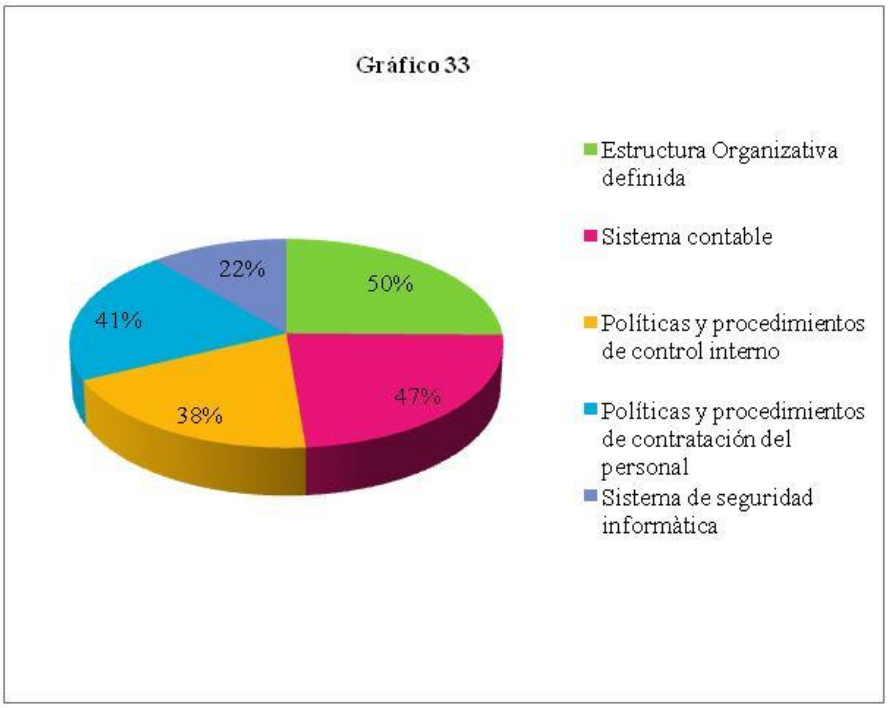
Como es bien conocido, las ONG´S trabajan a base de donaciones por parte de otras instituciones, por lo que es de interés conocer si estas entidades les exigen contar con una estructura organizativa bien definida que les garantice un buen cuidado a la información, teniendo como resultados que el 84% de las ONG´S encuestadas están sometidas ante estas exigencias, y solo al 16% no se les exige este requerimiento.

PREGUNTA 11

¿Si su respuesta a la pregunta anterior fue positiva, indique cuales son con los que cuenta su institución?

Objetivo: Determinar qué tipo de controles son los exigidos por parte de los organismos donantes.

RESPUESTA	FRECUENCIA	
	ABSOLUTA	RELATIVA
Estructura Organizativa definida	29	50%
Sistema contable	27	47%
Políticas y procedimientos de control interno	22	38%
Políticas y procedimientos de contratación del personal	24	41%
Sistema de seguridad informática	13	22%



Análisis e interpretación:

Del 84% de las entidades que están sometidas a grandes exigencias de los donantes, manifiestan que lo principal que deben cumplir es tener una estructura bien definida, y un

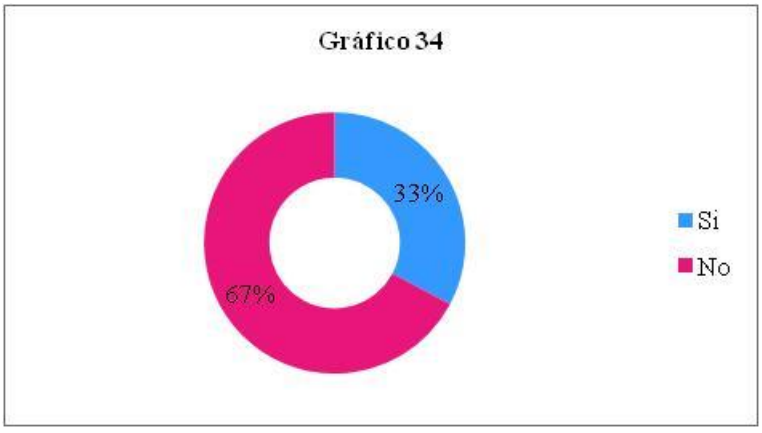
buen sistema contable con el 50% y 47% respectivamente, el 41% les exige tener políticas y procedimientos para la contratación del personal, así como también el 38% exigen políticas de control interno, y únicamente el 22% manifiestan que la principal exigencia es contar con un sistema de seguridad informática.

PREGUNTA 12

¿Se realizan capacitaciones al personal para concientizar lo importante que es la seguridad informática?

Objetivo: Conocer si las ONG´S brindan información suficiente al personal, para asegurarse que conozcan de la importancia de la seguridad de la información.

RESPUESTA	FRECUENCIA	
	ABSOLUTA	RELATIVA
Si	19	33%
No	39	67%
TOTAL	**58**	**100%**



Análisis e interpretación:

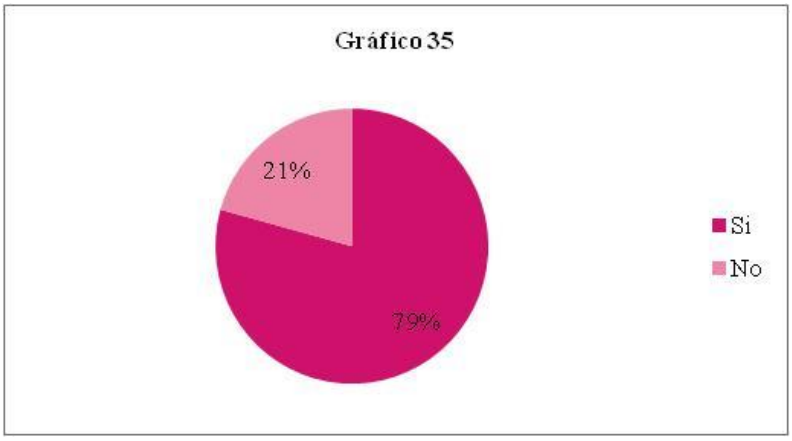
Tal como se vio en los resultados obtenidos del personal de soporte técnico, el personal clave tampoco recibe en su mayoría capacitaciones de concientización de seguridad de la información, ya que el 67% afirmó no recibir este beneficio, solamente el 33% reciben capacitaciones sobre seguridad de la información.

PREGUNTA 13

¿En el uso del sistema contable se han establecidos categorías de usuarios para procesar la información?

Objetivo: Determinar si el sistema contable está programado con categorías para los usuarios.

RESPUESTA	FRECUENCIA	
	ABSOLUTA	RELATIVA
Si	46	79%
No	12	21%
TOTAL	**58**	**100%**



Análisis e interpretación:

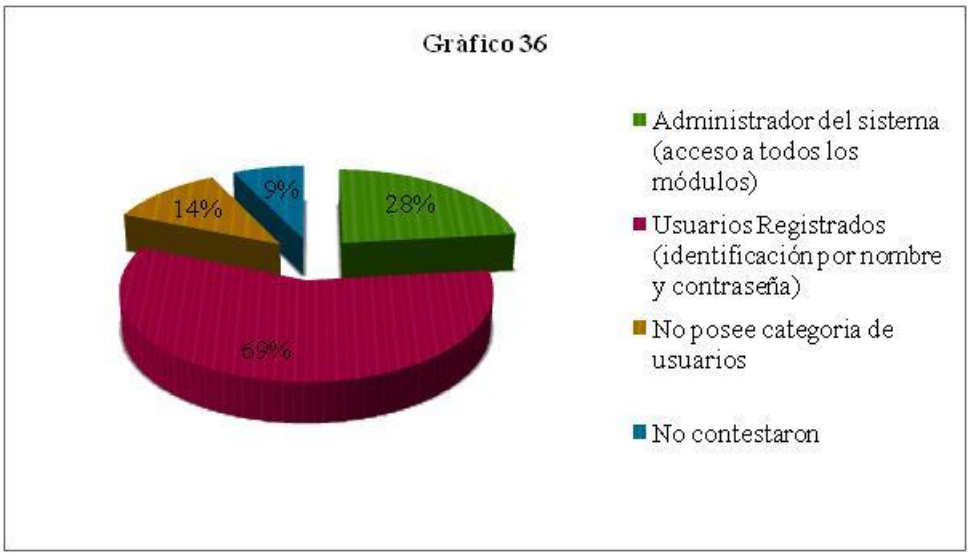
Comúnmente en todas las entidades, se implementan categorías de usuarios en los sistemas, según las funciones de empleado, se puede comprobar que para las ONG´S también es aplicable, del 100% de las personas encuestadas el 79% aseguraron que tiene definidas categorías de usuario en función de sus responsabilidades y actividades desempeñadas, y el 21% informó que no poseen esta característica.

PREGUNTA 14

Si su respuesta a la pregunta anterior fue positiva, que tipo de categoría posee el sistema que utiliza dentro de su organización?

Objetivo: Determinar si los sistemas contables poseen permisos de usuarios en función del cargo que desempeña cada empleado.

RESPUESTA	FRECUENCIA	
	ABSOLUTA	RELATIVA
Administrador del sistema (acceso a todos los módulos)	16	28%
Usuarios Registrados (identificación por nombre y contraseña)	40	69%
No posee categoría de usuarios	8	14%
No contestaron	5	9%



Análisis e interpretación:

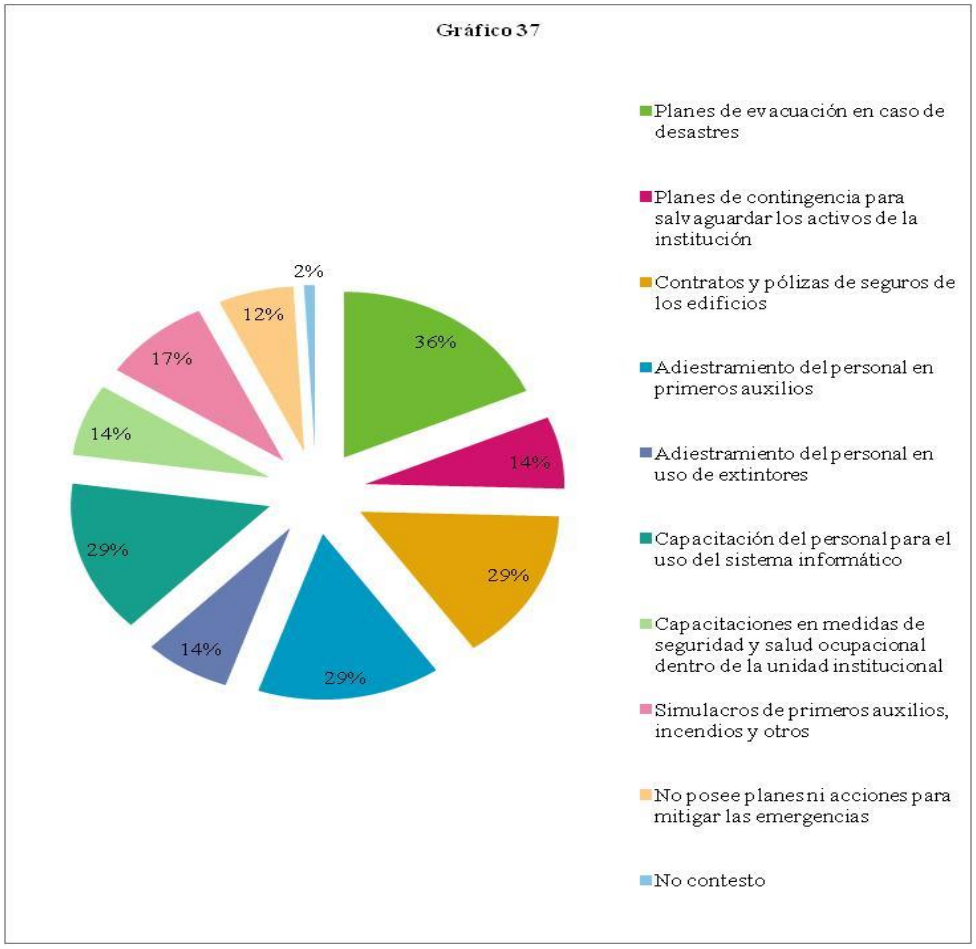
Entre las categorías que se mencionan en la pregunta anterior, claramente se puede ver que la principal son los usuarios registrados a través de su nombre y una contraseña según lo muestran el 69%, el 28% confirmó tener acceso a todos los módulos o campos dentro del sistema informático, y el 14% mencionó que no tiene categorías definidas.

PREGUNTA 15

¿Su organización cuenta con planes y acciones de contingencias que realice en las instalaciones de oficinas, centro de cómputo, área de soporte técnico? (Seleccione con cuales cuenta).

Objetivo: Investigar si las ONG´S están debidamente preparadas con planes de contingencias que contribuyan a la protección de la información.

RESPUESTA	FRECUENCIA	
	ABSOLUTA	RELATIVA
Planes de evacuación en caso de desastres	21	36%
Planes de contingencia para salvaguardar los activos de la institución	8	14%
Contratos y pólizas de seguros de los edificios	17	29%
Adiestramiento del personal en primeros auxilios	17	29%
Adiestramiento del personal en uso de extintores	8	14%
Capacitación del personal para el uso del sistema informático	17	29%
Capacitaciones en medidas de seguridad y salud ocupacional dentro de la unidad institucional	8	14%
Simulacros de primeros auxilios, incendios y otros	10	17%
No posee planes ni acciones para mitigar las emergencias	7	12%
No contesto	1	2%



Análisis e interpretación:

La implementación de planes de contingencia, ayuda en gran medida a mitigar los riesgos, como se puede observar en el gráfico, el plan de contingencia más utilizado dentro de las ONG´S, es: Plan de evacuación en caso de desastres con el 36%, seguido de este con el 29% están los contratos y pólizas de seguro a los edificios, adiestramiento al personal en primeros auxilios y capacitaciones al personal, también un buen porcentaje manifiestan que se realizan simulacros de primeros auxilios con el 17%, así como también la implementación de planes de contingencia para salvaguardar los activos de la entidad, adiestramiento en el uso de extintores y las capacitaciones en medidas de seguridad con el 14% , únicamente el 12% mencionó no tener ningún plan de contingencia.

ANEXO No 4

APLICACIÓN DE SANCIONES

Nombre del Trabajador(a): _____

Cargo que desempeña: _____

Jefe directo: _____

Violaciones al sistema de seguridad de la información

Leve	Grave	Muy Grave

Tipo de Sanción

Administrativa	Disciplinaria	Penal

Medidas correctivas

No	Descripción

_____

Firma del Director Ejecutivo

ANEXO No 5

FORMULARIO DE REVISIÓN Y CAMBIOS AL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

REVISIONES			
No	Fecha de revisión	Párrafo propuesto a revisión	Observaciones

CAMBIOS PRINCIPALES		
Sección	No de Página	Descripción de los cambios

Nombre /Departamento del solicitante: _____

Firma del Jefe de Departamento: _____

Firma del Director de la Organización: _____

ANEXO No 6

CRONOGRAMA DE ACTIVIDADES

FUNDACIÓN UN FUTURO MEJOR

CRONOGRAMA

	Meses	Agosto					Septiembre					Octubre					Noviembre				
Actividades	Semanas	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
Implementación de capacitaciones sobre seguridad de la información a todo el personal de la organización																					
Verificación de las actividades de seguridad																					
Identificación de no-conformidades por parte del personal																					
Evaluación del riesgo																					
Clasificación de la Información																					
Identificación de amenazas																					
Revisión de incidentes de seguridad de la información																					
Respuesta a los incidentes																					
Monitoreo																					

ANEXO No 7

ASIGNACIÓN DE RESPONSABILIDADES				
Actividad	Responsable	Área	Fecha	% de cumplimiento

_____

Firma Director Ejecutivo

ANEXO No 8

CONTRATO DE CONFIDENCIALIDAD

Al objeto de garantizar la confidencialidad del presente [ ], se hace necesario la firma de un acuerdo que garantice unos niveles de confianza entre las partes. El documento se firmará una vez aceptado y firmado por ambas partes.

El contenido del acuerdo es el que figura a continuación.

DE UNA PARTE: **[nombre de la organización]**y en su nombre y representación (con poder suficiente para ello) D/Dña. **[nombre completo],** en calidad de **[cargo, administrador, apoderado,...]**

DE OTRA PARTE: **[nombre de la organización].** y en su nombre y representación **(con poder suficiente para ello)** D/Dña. [nombre completo], en calidad de **[cargo, administrador, apoderado,...]**

Reunidos en **[lugar de la firma del contrato]**, a **[día]** de **[Mes]** de **[Año]**

EXPONEN

I – Que las partes, anteriormente citadas, están interesadas en el desarrollo del presente contrato, para lo cual, aceptaron celebrar el presente Acuerdo de Confidencialidad con el fin de establecer el procedimiento que regirá la custodia y no transmisión a terceros de la información distribuida entre las partes, así como los derechos, responsabilidades y obligaciones inherentes en calidad de remitente, Propietario y «Destinatario» de la referida información.

II – Que las partes, en virtud de lo anteriormente expuesto, convinieron que el presente Acuerdo de Confidencialidad se rija por la normativa aplicable al efecto y, en especial por las siguientes.

CLÁUSULAS

PRIMERA – Definición de la información que se protege

SEGUNDA.- Duración del acuerdo y casos en los que se debe mantener la confidencialidad indefinida

TERCERA.- Acciones requeridas cuando se termine el acuerdo

CUARTA.- Custodia y no divulgación.

QUINTA.- Responsabilidades y acciones de los firmantes para evitar la divulgación de la información no autorizada

SEXTA.- Propiedad de la información

SÉPTIMA.- Uso permitido de la información confidencial y los derechos del firmante para utilizar la información

OCTAVA.- Incumplimiento

NOVENA.- Duración del Acuerdo de Confidencialidad.

DECIMA.- Legislación Aplicable

Nombre de la Organización	Nombre del Empleado/prestador de servicios
_____	_____
Firma representante _____	Firma _____
DUI representante_____	DUI _____

ANEXO No 9

BITACORA

BITACORA DE ACTIVOS					
DATOS INFORMATIVOS					
Fecha:			Área:		
Nombre de responsable:			Firma:		
Tipo de Activo:	Formato	Ubicación	Información de respaldo	Información de licencias	Valor comercial
Información					
Software					
Equipo de computo					
Medios removibles					
Servicios de computación y comunicación					
Intangibles					

ANEXO No 10

HISTORIAL DE REVISIONES A LOS ACTIVOS				Fecha:	
Clasificación	Etiquetado	Elaborado	Revisado	Aprobado	Autorizado

ANEXO No 11

CARTA COMPROMISO

Lugar y Fecha

Nombre del empleado:

Presente.

La dirección ejecutiva de la Fundación un futuro mejor tiene a bien dirigirle la siguiente:

CARTA COMPROMISO

Mediante la cual exponemos los compromisos y responsabilidades que le corresponden y que se llevaran a cabo durante el período para el cual ha sido contratado

1.- Implementar y actuar de acuerdo a las políticas de seguridad de la información de la Fundación.

2.- Proteger los activos asignados para el desarrollo de sus actividades, evitando el acceso, divulgación, modificación o destrucción de los mismos.

3.- Reportar incidentes de seguridad que puedan afectar el desempeño de sus funciones.

Atentamente:

Nombre y Firma del Director Ejecutivo

ANEXO No 12

PROCEDIMIENTO DE RESPALDO DE INFORMACIÓN (Back Up)

Elaborado por: Nombre: Área: Firma: Fecha:	Solicitado por: Nombre: Área: Firma: Fecha:

Autorizado por:

Nombre:

Área:

Firma:

Fecha:

PROCEDIMIENTO DE RESPALDO

No	Responsable	Actividad
1	Gerencia de Tecnología e Innovación	Generar una copia de seguridad de la información contenida en la PC. Se realizará semanalmente programada cada sábado.
2	Gerencia de Tecnología e Innovación	Elegir entre copia completa o parcial, es recomendable seleccionar la primera opción porque

		permite crear un archivo con toda la información y configuraciones del equipo. Se recomienda que sea parcial cuando se requiera resguardar contenido específico como correos electrónicos o una base de datos.
3	Gerencia de Tecnología e Innovación	Descarga de copia de seguridad, puede realizarse en un medio de almacenamiento como USB, Disco duro, entre otros.
4	Gerencia de Tecnología e Innovación	Se debe llevar un registro por cada respaldo realizado en cada equipo informático y notificar vía correo electrónico a la Dirección ejecutiva las actividades realizadas y los inconvenientes encontrados.
5	Gerencia de Tecnología e Innovación	Se realizará entrega física de los respaldos a la Dirección ejecutiva, indicando fecha y hora de realización.

ANEXO No 13

FORMULARIO DE ENVÍO Y RECEPCIÓN DE DOCUMENTOS

Fecha:			
Nombre de la organización			
Dirección:			
Teléfono:			
Nombre y Firma de quien envía:			
Sello:			
Fecha:			
Nombre de la organización			
Dirección:			
Teléfono:			
Nombre y Firma de quien recibe:			
Sello:			

ANEXO No 14

ACUERDO DE INTERCAMBIO DE INFORMACIÒN

El presente acuerdo de intercambio entra en vigencia en [fecha] y se celebra

ENTRE: [Nombre de la organización]

Y: [Nombre de la organización]

El objetivo es garantizar la protección de la información que se transmitirá entre las partes involucradas y determinar responsabilidades en caso de manipulación, pérdida o uso inadecuado de la misma.

En mutuo acuerdo de ambas partes, por medio de la presente las partes acuerdan lo siguiente:

1. Responsabilidades para el control, despacho y recepción de la información.
2. Procedimientos para notificar al remitente la recepción de la información
3. Responsabilidades y obligaciones en caso de ocurrir incidentes de seguridad, como pérdida de documentos.
4. Utilización de un sistema de etiquetado que especifique lo confidencial o crítica que es la información
5. Estándares de identificación de mensajeros

_____	_____
Firma autorizada	Firma autorizada

ANEXO No 15

REPORTE Y SEGUIMIENTO DE INCIDENTES DE SEGURIDAD

Fecha:	Hora:
Datos de la persona que reporta el incidente	
Nombre:	
Puesto:	Área:
Tel:	Correo electrónico:
Información del incidente	
Fecha:	Hora:
Descripción del incidente:	
Área o sistemas afectados:	

ANEXO No 16

ANEXO A

Detalle de dominios de aplicación para el tratamiento y mitigación de los riesgos

Control	Control	Actividades para desarrollar
A.5.1.1	La Dirección debe aprobar un documento de política de seguridad de la información, publicarlo y comunicarlo a todos los empleados y entidades externas afectadas.	• Elaborar una política. • Realizar un documento. • Desarrollar un plan de capacitación.
A.5.1.2	Revisión de la política de seguridad de la información	• Analizar el entorno de forma periódica para determinar si existen cambios. • Realizar un acta de revisión para aprobación de cambios • Documentar el registro de versiones • Actualizar los apartados de las políticas que han sufrido cambios • Comunicar a las partes interesadas
A.6.1.1	Compromiso de la gerencia con la seguridad de la información	• Asistir a reuniones con las partes interesadas • Elaborar de actas de reuniones
A.6.1.2	Coordinación de la seguridad de la información	• Establecer roles y responsabilidades relacionados a la seguridad de información • Comunicar al personal las responsabilidades
A.6.1.3	Asignación de responsabilidades de la seguridad de la información	• Actualizar/ el perfil del descriptor de puestos para personal de seguridad de información • Capacitar y evaluar al personal dedicado a seguridad de información

A.6.1.4	Proceso de autorización para los medios de procesamiento de información	• Documentar procedimiento de autorización
A.6.1.5	Acuerdos de confidencialidad	• Identificar y revisar requerimientos de confidencialidad
A.6.1.7	Contactos con grupos de interés especial	Mantener contacto con los grupos de interés
A.6.1.8	Revisión independiente de la seguridad de la información	• Revisar a intervalos planeados o cuando ocurran cambios significativos el enfoque de la organización para el manejo del sistema de seguridad informático y su implementación.
A.6.2.1	Identificación de riesgos relacionados con entidades externas	• Identificar riesgos de la información y los medios de procesamiento • Implementar controles antes de otorgar accesos
A.6.2.2	Tratamiento de la seguridad cuando trabaja con clientes	• Gestionar los requerimientos de seguridad antes de otorgar accesos a la información
A.6.2.3	Tratamiento de la seguridad en contratos con terceras personas	• Documentar los acuerdos de acceso, procesamiento, comunicación o manejo por parte de terceros • Determinar los requerimientos de seguridad para agregar nuevos productos o servicios
A.7.1.1	Inventarios de activos	• Elaborar y mantener un inventario de los activos
A.7.1.2	Propiedad u uso de los activos	• Determinar la parte de la entidad a que pertenecen los activos • Documentar las políticas de uso para el procesamiento de la información y los activos

		asociados para este fin
A.7.1.3	Lineamientos de clasificación, etiquetado y manejo de la información	• Clasificar la información de acuerdo al valor, requerimientos legales y confidencialidad • Implementar procedimientos para el etiquetado y manejo de la información
A.8.1.1	Antes del empleo Roles y responsabilidades Selección Término y condiciones de empleo	• Definir y documentar roles y responsabilidades del personal • Realizar chequeos de verificación de antecedentes de los empleados de acuerdo a leyes, regulaciones y etiquetas relevantes • Definir documento que establezca compromisos términos y condiciones de las responsabilidades de los empleados que deberán firmar y aceptar
A.8.1.2	Durante el empleo Gestión de responsabilidades Capacitación y educación en seguridad de la información Proceso disciplinario	• Establecer un requerimiento que los empleados cumplen con los procedimientos y políticas de la entidad. • Establecer capacitaciones, actualizaciones de políticas, procedimientos relevantes para las funciones laborales. • Implementar un proceso disciplinario.
A.8.1.3	Responsabilidades de terminación Devolución de activos Eliminación de derechos de accesos	• Definir responsabilidades respecto a la terminación o cambio de empleo. • Documentar la devolución de activos en la terminación del empleo. • Eliminar los derechos de acceso a la información

A.9.1.1	Medidas de seguridad física y acceso físico	• Implementar controles de seguridad para el acceso del personal autorizado. • Diseñar y aplicar la protección física ante un fenómeno natural o provocado.
A.9.2.1	Ubicación y protección del equipo	Proteger los equipos contra riesgos, amenazas y peligros ambientales. • Implementar un sistema de mantenimiento para los equipos. • Implementar un sistema de protección.
A.9.2.2	Políticas y procedimientos para personal contratado y mantenimiento de la infraestructura	• Definir los procesos, organizaciones y relaciones de TI. • Gestionar el ambiento físico
A.9.2.3	Protección de la tecnología de información	• Garantizar la seguridad de los sistemas
A.9.2.4	Gestión de instalaciones físicas	• Gestionar el ambiente físico
A.10.1.1	Procedimientos de operaciones documentados	• Documentar los procedimientos de operación y estar a disposición del usuario.
A.10.1.2	Gestión de cambio	• Proteger y controlar los cambios en los medios y sistemas de procesamiento
A.10.1.3	Segregación de deberes	• Documentar las segregaciones, así como los deberes, y niveles de responsabilidad.
A.10.2.1	Entrega del servicio	• Implementar controles para determinar que terceros cumplan lo incluido en el contrato.
A.10.2.2	Monitoreo y revisión de los servicios de terceros	• Diseñar controles para el monitoreo y revisión de los

		servicios, reportes y registros.
A.10.3.1	Gestión de capacidad	• Gestionar controles para monitorear los recursos del sistema y su desempeño
A.10.3.2	Aceptación de sistemas	• Establecer criterios para la aceptación de un nuevo sistema, actualizaciones o versiones nuevas.
A.10.4.1	Controles sobre software maliciosos	• Implementar controles para la detección, prevención y recuperación para protegerse de códigos maliciosos.
A.10.4.2	Controles contra códigos móviles	• Definir políticas de seguridad para evitar que códigos móviles se ejecuten.
A.10.5.1	Back-up o respaldo de la información	• Realizar copias de respaldo de la información comercial y software.
A.10.6.1	Controles de red	• Implementar controles para el adecuado manejo de las redes y evitar amenazas y mantener la seguridad de los sistemas
A.10.7.1	Gestión de los medio removibles	• Realizar procedimientos para la gestión de medios removibles. • Establecer controles para el manejo y almacenaje de la información
A.10.7.2	Seguridad de la documentación del sistema.	• Proteger la documentación del acceso autorizado.
A.10.8.1	Procedimientos y políticas de información y software	• Establecer políticas, procedimiento y controles para proteger el intercambio de información.
A.10.8.2	Acuerdos de intercambio	• Establecer acuerdos para: • El intercambio de información dentro de la entidad. • Acceso no autorizado para los medios que contiene la información

		• Mensajes electrónicos.
A.10.9.1	Comercio electrónico	• Identificar los riesgos a fin de proteger la información que se trasmite a través de redes públicas.
A.10.9.2	Información disponible públicamente	• Implementar controles para mantener la integridad de la información.
A.10.10.1	Registro de auditoria	• Documentar los registros de las auditoria realizadas
A.10.10.2	Uso del sistema de monitoreo	• Establecer procedimientos para el monitoreo del uso de medios de procesamiento
A.10.10.3	Protección del administrador y operador	• Documentar los registro y actividades del administrador y operador del sistema • Documentar los registros de fallas • Implementar controles de sincronización con una fuente de tiempo
A.11.1.1	Políticas de control de acceso	• Documentar las políticas de control de acceso en base a los requerimientos de seguridad.
A.11.2.1	Gestión de privilegios	• Implementar restricciones en el uso de los privilegios.
A.11.2.2	Gestión de claves de usuario	• Establecer la asignación de claves a través de un proceso de gestión formal.
A.11.3.1	Uso de claves	• Diseñar buenas prácticas de seguridad en el uso de claves
A.11.3.2	Políticas de pantalla y escritorio limpio	• Establecer política de escritorio limpio para los documentos y medios de almacenaje.
A.11.4.1	Política sobre los servicios de uso de red	• Diseñar políticas sobre accesos solo personal autorizado
A.11.4.2	Autenticación de usuario para conexiones externas	• Implementar métodos de autenticación para el control de acceso.

A.11.4.3	Protección del puerto de diagnóstico remoto	• Establecer controles para el acceso físico y lógico
A.11.4.4	Control de conexiones de red	• Restringir la capacidad de conexión de los usuarios de redes compartidas.
A.11.5.1	Procedimiento en la terminal	• Documentar los registros sobre el acceso a los servicios operativos
A.11.5.2	Identificación y autenticación del usuario	• Establecer controles para la identificación para su uso personal y exclusivo.
A.11.5.3	Sistema de gestión de claves	• Diseñar claves que deben ser interactivas y seguras.
A.11.5.4	Limitación de tiempo de conexión	• Establecer restricciones sobre los tiempos de conexión para seguridad de las aplicaciones
A.11.6.1	Restricción al acceso a la información	• Diseñar restricciones al acceso de los usuarios y personal de soporte al sistema de información
A.11.7.1	Computación móvil y comunicaciones	
A.12.1.1	Análisis y especificaciones de los requerimientos de seguridad	• Documentar los requerimientos de los sistemas nuevos o las mejoras de los ya existentes
A.12.2.1	Procesamiento correcto de las aplicaciones	• Realizar chequeos de verificación de las aplicaciones y que la información esté libre de errores de procesamiento o actos deliberados
A.12.3.1	Controles criptográficos	• Diseñar y establecer políticas sobre el uso de controles criptográficos • Establecer controles de gestión de claves para dar soporte a las técnicas criptográficas
A.12.4.1	Control de software operacional	• Implementar controles para: • Instalación de software de sistema. • Selección y protección sobre la

		data de prueba • Restricción al acceso al código fuente
A.12.5.1	Procedimientos del control de cambio	• Diseñar controles para la implementación de cambios del sistema
A.12.5.2	Filtración de información	• Elaborar controles para evitar filtraciones de la información
A.12.6.1	Control de vulnerabilidades técnicas	• Gestionar la protección de las vulnerabilidades técnicas para reducir riesgos en los sistemas de información
A.13.1.1	Reporte de eventos en la seguridad de la información	• Implementar un reporte de eventos de seguridad de la información
A13.1.2	Reporte de debilidades en la seguridad	• Implementar para que los empleados, y otros afines a la entidad reporten debilidades o sospechas de incidentes de seguridad
A.13.2.1	Responsabilidades y procedimientos	• Establecer las responsabilidades y procedimientos gerenciales ante incidentes de seguridad
A.13.2.2	Aprendizaje de los incidentes en la seguridad de la información	• Determinar mecanismos que permitan cuantifiquen y monitoreen los incidentes en la seguridad de la información
A.14.1.1	Seguridad de la información en el proceso de gestión de continuidad comercial	• Desarrollar un proceso gerencial para la continuidad del negocio
A.14.1.2	Implementar planes de continuidad	• Implementar planes para mantener o restaurar las operaciones ante interrupciones o fallas en los procesos críticos
A.14.1.3	Prueba, mantenimiento y re-evaluación de planes de continuidad	• Desarrollar planes de continuidad regularmente
A.15.1.1	Identificación de legislación	• Definir y documentar los

	aplicable	requerimientos estatutarios, reguladores y contractuales
A.15.1.2	Derecho de protección intelectual	• Implementar procedimientos para el cumplimiento sobre el uso del material de software patentado
A.15.1.3	Protección de los registros organizacionales	• Establecer una protección de los registros de incidentes
A.15.1.4	Protección de data y privacidad de la información personal	• Asegurar la protección y privacidad de la información
A.15.1.5	Regulación de controles criptográficos	• Implementar el uso de controles
A.15.1.6	Cumplimientos con las políticas y estándares de seguridad	• Establecer por parte de la gerencia el cumplimiento de los estándares de seguridad • Revisar periódicamente el cumplimiento de dichos estándares
	Controles de auditoría de sistemas de información	• Planear requerimientos y actividades de auditoría relevantes a la información
A.15.1.8	Protección de las herramientas de auditoría	• Establecer un mecanismo de protección del acceso a las herramientas de auditoría

Fuente: Elaboración hecha en base a la ISO 27001