UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

FACULTAD DE INGENIERÍA Y GESTIÓN

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

"DISEÑO DE UN PLAN DE SEGURIDAD DE LA INFORMACIÓN PARA OPTIMIZAR LA PROTECCIÓN DE LOS ACTIVOS INFORMACIONALES DE LA ASOCIACIÓN CIVIL CENTRO CULTURAL DEPORTIVO, LIMA"

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de

INGENIERO DE SISTEMAS

PRESENTADO POR EL BACHILLER

ACERO PICÓN, CRISTIAN ERNESTO

Villa El Salvador
2018

DEDICATORIA

Quiero dedicar este proyecto a mi familia y amigos, especialmente a mi madre y hermanos, que con su amor, paciencia y apoyo me guiaron a seguir y culminar mis estudios. Gracias mamá por nunca dejar de confiar en mí, por el esfuerzo y sacrificio, por darme el empuje para volver a empezar y ver ahora como culmino lo que hace mucho tiempo empecé.

A mi incondicional compañera que gracias a su paciencia y ánimos me alentaron a culminar este proyecto.

A mis dos motores y motivo, Luz Tatiana y Juan Manuel, que gracias a ustedes hijos pude llegar hasta donde estoy, por ser la razón de mí vivir, por darme los mejores momentos de mi vida y darme ese empuje para salir adelante.

AGRADECIMIENTOS

Quiero agradecer en primer lugar a Dios, por estar siempre a mi lado y por su bendición.

Al Dr. Ing. Frank Escobedo, por su paciencia y asesoría, sin su apoyo no hubiera podido realizar correctamente este proyecto.

A mis profesores que estuvieron a lo largo de mi carrera, que me compartieron sus conocimientos para convertirme en un profesional.

Y a todas las personas que llegaron a mi vida, porque guardo las enseñanzas que alguna vez me dieron.

ÍNDICE

Página

LISTADO DE FIGURAS

LISTADO DE TABLAS

INTRODUCCIÓN

En el presente trabajo, se diseña y desarrolla un Plan de Seguridad de la Información para el club Asociación Civil Centro Cultural Deportivo Lima, cuyo rubro es el esparcimiento, fundado en el año 1966. La oportunidad de laborar en esta institución me permitirá el acceso al levantamiento de la información, seguido del análisis del estado situacional, definición de procedimientos y políticas de seguridad de la información, identificación y análisis de riesgos.

La seguridad de información, en términos generales es entendida como todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información, buscando de esta manera mantener la confidencialidad, la disponibilidad e integridad de la misma. Un activo de información es un activo que tiene un determinado valor para la organización, sus operaciones comerciales y su continuidad.

La característica principal de un sistema de gestión de seguridad de información es resguardar la integridad, confidencialidad e integridad de los activos de información en una empresa u organización; lo cual se logra a través de un minucioso análisis de los riesgos a los que están expuestos los activos de información para luego implementar los controles necesarios que ayudaran a proteger estos activos.

La problemática principal actual de la institución es la falta de seguridad y la poca previsión respecto a los riesgos con la que cuentan sus activos de información. El resultado de no tener las medidas necesarias para mitigar estos riesgos puede llevar a la organización a pérdidas no solo de información, sino también económica.

Es por ello, que la Asociación Civil Centro Cultural Deportivo Lima se ve en la necesidad de implementar un conjunto de herramientas, procedimientos, controles y políticas que aseguren la confidencialidad, disponibilidad e integridad de la información, con ello garantizar a que accedan a la información sólo quienes estén designados para su uso, que esté disponible cuando requieran los que estén autorizados y permanezca tal y como fue creada por sus propietarios, y asegurar así también la actualización de la misma.

El presente trabajo consta de los siguientes componentes básicos:

En el capítulo I, revisaremos el planteamiento del problema, la realidad problemática de la institución, la justificación, la formulación del problema, los objetivos, las limitaciones y la viabilidad del proyecto.

En el capítulo II, nombraremos el marco teórico, en el que están planteadas las bases teóricas relacionadas con un Sistema de Gestión de Seguridad de la Información (SGSI) definiciones de términos básicos que sustentan el desarrollo adecuado del trabajo y antecedentes de la investigación.

El capítulo III contiene la etapa de desarrollo del proyecto, donde se define los métodos y herramientas utilizadas para la realización del trabajo y solución del problema. Incluye la metodología a emplear, la cual es la resultante de un estudio de distintas metodologías y aporte de distintas investigaciones.

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA

1.1 Descripción de la Realidad Problemática

Las organizaciones públicas y privadas día a día generan conocimientos, datos, reportes, actas y material de diferente índole de suma importancia para ellas, lo cual representa toda la información que requieren para su funcionalidad. Esta información en la mayoría de los casos, es almacenada en diferentes medios tanto físicos como electrónicos, además es puesta a disposición del personal que requiere hacer uso de esta información para toma de decisiones, realización de planes, reportes, inventarios, entre otros.

El acceso no autorizado a la información se ha vuelto más fácil debido a los tantos métodos existentes y nuevos para extraer información, esto ha permitido que sea más difícil salvaguardar la información y sus modos de transmisión; ya sean estos comunicados verbales, archivos, documentos, comprobantes de pago, registros de compras y ventas, base de datos, entre otros.

Debido a la situación en que se gobierna la Asociación Civil Centro Cultural Deportivo Lima, por medio de directivas que son elegidas cada 02 años a través de elecciones convocadas por la asamblea general de asociados, cuya lucha por el poder ha puesto en peligro los activos de información del Club, la misma que pueda ser utilizada para crear zozobra entre los mismos socios, con el fin de causar inestabilidad. Lo cual resulta peligroso para la institución, ya que mucha de la información fundamental e importante para la realización de los diversos proyectos pueda ser vulnerada y amenazada ocasionando la interrupción de estos procesos, que conllevan, de esta manera, a una pérdida no solo de información, sino también financiera.

Sumado al fraude informático, a fines del año 2017, causado por el ex trabajador encargado del Área de Sistemas, quien eliminó el sistema de cobranzas y la base de datos causando un perjuicio económico para la institución. Dejándose de cobrar en ese mes la suma de S/ 120,000.00 SOLES.

Los accesos y privilegios a la información estuvieron centrados hacia una única persona, lo que generó una dependencia y posteriormente la pérdida del sistema y la base de datos, debido a que la institución no contó ni cuenta con herramientas, procedimientos, controles y políticas que aseguren la confidencialidad, disponibilidad e integridad de la información.

Los documentos que ingresan al club: cartas, oficios, solicitudes, recibos, notificaciones y correos, no son registrados ni distribuidos correctamente, lo que ha generado demora en la ejecución de los trámites correspondientes por posibles pérdidas o traspapelados de los documentos. Esto debido a la inexperiencia y falta de capacitación del personal. EL 90% de los trabajadores tienen conocimiento vano sobre seguridad de la información.

1.2 Justificación del Problema

Debido a los riesgos a los que están expuestos los activos de información de la Asociación Civil Centro Cultural Deportivo Lima, y el impacto que estos puedan causar en el funcionamiento de la organización. Es preponderante la definición de una metodología que nos permita reducir y mitigar estos riesgos.

Es por ello que, se propone Diseñar un Plan de Seguridad de Información, el cual nos brindará los procedimientos y lineamientos necesarios para identificar y evaluar los riesgos, las amenazas, las vulnerabilidades de los activos de información, implantar controles necesarios que ayudarán a salvaguardar los activos de información de los procesos tecnológicos, alineándolo de esta manera a los objetivos estratégicos de la institución.

El desarrollo e implementación de un Plan de Contingencias aumentará la confianza por parte de los asociados, proveedores y dirigentes. Así mismo, habrá mayores garantías de continuidad del negocio.

La implementación de un Plan de Seguridad de Información en la Asociación Civil Centro Cultural Deportivo Lima permitirá un mejor funcionamiento, agilidad y confianza en la realización de los procesos de tecnología, apoyará a la toma de decisiones gracias a la confidencialidad y buen manejo de los activos de información.

La implementación de un Plan de Seguridad de la Información y sus buenas prácticas mejorará la imagen de la Institución y aumentará su valor comercial.

Por lo tanto, habrá un aumento del presupuesto institucional gracias a la buena gestión debido al cuidado, preservación y buena interpretación de sus

activos de información. Lo que permitirá un mejor desarrollo de la asociación y aumento de confianza por parte de la actual directiva.

Otra de las ventajas que se tendrá al desarrollar un Plan de Seguridad de la Información, a través de la gestión de riesgos son las evidencias, lo cual para casos de fraudes internos o externos, nos permitirá entregar al área legal información válida para afrontar posibles procesos administrativos internos o judiciales, para lo cual es conveniente que esta recopilación de información se realice cumpliendo las normas legales para este procedimiento.

La implementación de un Plan de Seguridad de la Información en la Asociación Civil Centro Cultural Deportivo Lima, a través de la gestión de riesgos, permitirá identificar, analizar y evaluar las posibles amenazas a las que están expuestos los activos informacionales, definiendo así un Plan de Mitigación de Riesgos, el cual reducirá el impacto de las amenazas, y posteriormente el control de los mismos. Asegurando la integridad, disponibilidad, confiabilidad y confidencialidad de la información, coadyuvando en todos los procesos administrativos y operacionales liderados por la actual gestión, mostrando ante los asociados, transparencia y confianza, ganándose el respaldo y reconocimiento del entorno.

1.3 Delimitación del Proyecto

1.3.1 Delimitación Teórica

- **Activos informacionales:** Son los bienes que tienen valor o utilidad para una empresa, los mismos que aseguran la continuidad del negocio y permiten alcanzar los objetivos estratégicos que propone su alta dirección. Pueden estar de distintas formas, sea físicamente en documentos

impresos o escritos, y en dispositivos de almacenamiento electrónico como correos o grabaciones. (Leyva, 2016)

- **Plan de seguridad de la información:** Es el documento donde se definen las medidas preventivas y reactivas que se deben cumplir en una organización para proteger la información asegurando la confidencialidad, disponibilidad e integridad de la misma. (Leyva, 2016)
- **SGSI (Sistema de Gestión de Seguridad de la Información):** Es el diseño, implantación y mantenimiento de un conjunto de procedimientos para gestionar eficientemente la accesibilidad de la información, minimizando a la vez los riesgos de seguridad a los que están expuestos los activos informacionales. (ISO27000.es)

1.3.2 Delimitación Temporal

Inicio: 12 de Febrero de 2018

Término: 15 de Junio de 2018.

1.3.3 Delimitación Espacial

El presente trabajo se desarrolla en el club Asociación Civil Centro Cultural Deportivo Lima cuyo rubro es el esparcimiento, fundado en el año 1966. Su ubicación actual es en Av. Alameda Sur 1530, Distrito Chorrillos, Región Lima, Perú.

1.4 Formulación del Problema

1.4.1 Problema General

¿De qué manera el Diseño de un Plan de Seguridad de la Información optimizará la protección de los activos informacionales de la Asociación Civil Centro Cultural Deportivo Lima?

1.4.2 Problemas Específicos

- ¿De qué manera la implementación de políticas, normativas y procedimientos optimizará la protección de los activos informacionales de la Asociación Civil Centro Cultural Deportivo Lima?
- ¿De qué manera la identificación y evaluación de los riesgos de seguridad de la información optimizará la protección de los activos informacionales de la Asociación Civil Centro Cultural Deportivo Lima?
- ¿De qué manera la prevención, el control y/o mitigación de los riesgos identificados optimizará la protección de los activos informacionales de la Asociación Civil Centro Cultural Deportivo Lima?

1.5 Definición de los Objetivos

1.5.1 Objetivo general

Diseñar un plan de seguridad de la información para optimizar la protección de los activos informacionales de la Asociación Civil Centro Cultural Deportivo Lima.

1.5.2 Objetivos específicos

- Implementar políticas, normativas y procedimientos para optimizar la protección de los activos informacionales de la Asociación Civil Centro Cultural Deportivo Lima.
- Identificar y evaluar los riesgos de seguridad de la información para optimizar la protección de los activos informacionales de la Asociación Civil Centro Cultural Deportivo Lima.
- Prevenir, controlar y/o mitigar los riesgos identificados para optimizar la protección de los activos informacionales de la Asociación Civil Centro Cultural Deportivo Lima.

CAPÍTULO II

MARCO TEÓRICO

2.1 Antecedentes

A continuación se listan los siguientes antecedentes sobre Seguridad de la Información:

- En el 2011, Carlos Ampuero C. de Lima - Perú, alumno de la Universidad Católica del Perú perteneciente a la Facultad de Ciencias e Ingeniería, realizó la investigación con el tema “Diseño de un Sistema de Gestión de Seguridad de Información para una compañía de seguros”, en donde se concluyó: “Es importante contar con un Sistema de Gestión de Seguridad de la Información (SGSI) para poder asegurar, a un nivel aceptable, la información de la compañía y poder cumplir con las regulaciones de la Superintendencia de Banca y Seguros (SBS) y evitar así que la compañía incumpla con las regulaciones de la superintendencia. Para poder brindar un nivel aceptable de seguridad a la compañía, todo SGSI se debe basar en estándares y buenas prácticas orientadas a seguridad de la información que nos indican las consideraciones que debemos de tener en diferentes aspectos”. Esto sirve para corroborar la importancia de un SGSI y tener como referencia base los

estándares y buenas prácticas orientadas a la seguridad de la información. (Ampuero, 2011)

- En el 2008, J. Vásquez y C. De la Cruz de Chiclayo - Perú, alumnos de la Universidad Católica Santo Toribio de Mogrovejo pertenecientes a la Facultad de Ingeniería, realizaron la investigación con el tema “Elaboración y aplicación de un Sistema de Gestión de la Seguridad de la Información (SGSI) para la realidad tecnológica de la USAT”, en donde concluyeron que adquirir nuevos conocimientos sobre seguridad de la información permitirá fijar los mecanismos y procedimientos que deben adaptar las organizaciones para salvaguardar sus activos de información, y a su vez servirá de mucho para futuras investigaciones acerca de la seguridad de información. Esto sirve para resaltar la importancia del aprendizaje de mecanismos y procedimientos que se debe tener en cuenta para salvaguardar los activos de información y a la vez aportar los conceptos y teorías que servirán de apoyo al desarrollo de la presente investigación. (Vásquez y De la Cruz, 2008)

- En el 2016, Ronald Leyva P. de Lambayeque – Perú, alumno de la Universidad Nacional Pedro Ruiz Gallo perteneciente a la facultad de Ciencias Físicas y Matemáticas escuela profesional de Ingeniería de Computación e Informática, realizó la investigación con el tema “Diseño de un Sistema de Gestión de Seguridad de la Información basado en las Normas ISO/IEC 27001 e ISO/IEC 27002 para proteger los activos de información en el proceso de suministros de medicamentos de la Red de Salud de Lambayeque 2015”, en donde se concluyó: “Que trabajar con una metodología (PDCA) y seguir paso a paso las recomendaciones que nos

brinda una norma ISO, permitirán identificar dentro de los procesos de negocio, cuales son las dificultades por las que atraviesa la seguridad de los sistemas y de los activos en general que se encuentran dentro de la organización, que al no contar con controles de seguridad pueden terminar ocasionando un gran riesgo en la continuidad de negocio de cualquier entidad". Esto sirve para entender y comprender la importancia del uso de las metodologías y recomendaciones de los estándares de seguridad, que nos permitirá realizar el diseño e implementación de un Sistema de Gestión de Seguridad de la Información, cumpliendo con los procedimientos necesarios y adecuados como son: levantamiento de información, análisis de situación de los activos, gestión de los riesgos, implementación de políticas de seguridad y los controles que la misma norma recomienda, para así, garantizar la continuidad del negocio. (Leyva, 2016)

- En el 2014, Robín Salcedo B. de Barcelona – España, alumno de la Universidad Oberta Catalunya, realizó la investigación con el tema "Plan de implementación del SGSI basado en la norma ISO 27001:2013 para ISAGXXX", en donde se concluyó: "La cultura organizacional a nivel de seguridad de la información se ha incrementado en un 40%, debido a las actividades desarrolladas por el proyecto. El apoyo de la dirección es un factor clave en el gobierno del SGSI y en la madurez de la organización. La gestión de riesgos, debe involucrar a todos los niveles de la organización y a la alta dirección. Se deben incrementar las pruebas de seguridad de forma periódica". Esto sirve para conocer la importancia del apoyo de la alta dirección dentro de cualquier organización, así como la cultura organizacional

aumenta a nivel de seguridad de la información y que la gestión de riesgos debe estar involucrada en todos los niveles de la organización para poder actuar y realizar los debidos planes de contingencia y mitigación ante las posibles amenazas. (Salcedo, 2014)

- En el 2009, Gustavo Pallas M. de Montevideo - Uruguay, alumno de la Universidad de la Republica perteneciente a la Facultad de Ingeniería Instituto de Computación – CPAP, realizó la investigación con el tema: "Metodología de Implantación de un SGSI en un grupo empresarial jerárquico", en donde se concluyó: "En cada etapa del ciclo PDCA del SGSI cada una de las empresas del grupo debería tener la mayor información posible a efectos de aplicar criterios y lineamientos corporativos o ajustar los parámetros adecuados para la percepción y estimación de riesgos, y permitir escalar riesgos locales percibidos así como heredar los riesgos percibidos y priorizados desde los estratos superiores, buscando alinear los planes de gestión de seguridad al negocio de la forma más conveniente, en función de los recursos, objetivos concretos y condicionantes". Esto sirve para entender la importancia de disponer de la mayor información posible en cada etapa del Ciclo Deming (PDCA) para así definir y aplicar los criterios con mayor precisión con la finalidad de atenuar el impacto de los riesgos, buscando alinear la gestión de seguridad con los objetivos de la organización. (Pallas, 2009)

- En el 2008, Harrison Velasco H. de Medellín – Colombia, alumno de la Universidad Pontificia Bolivariana perteneciente a la facultad de Ingeniería

Informática, realizó la investigación con el tema “Diseño del Sistema de Gestión de Seguridad de la Información que permita apoyar a la Subgerencia de Informática y Tecnología de la empresa de telecomunicaciones de Bucaramanga Telebucaramanga S.A – E.S.P en el proceso de Certificación en ISO 27000”, en donde se concluyó: “La Subgerencia de Informática y Tecnología no cuenta con un comité responsable de seguridad de la información, no cuenta con el personal suficiente para realizar labores de administración de red, no cuenta con servidores de respaldo para los servicios de red, correo corporativo, intranet y conexiones remotas, que generan desconfianza a la hora de proteger los activos de información por lo que ponen en peligro la continuidad del negocio”. Esto sirve como modelo de auditoría y así realizar la debida documentación, el conocimiento y las herramientas básicas para llevar a cabo la implementación de la norma ISO 27000, incluyendo en la culminación de esta etapa los controles que la misma norma recomienda para lograr la certificación, sin dejar de lado los diseños e investigaciones de otras normas que las auditorias tanto externas como internas proponen. (Velasco, 2008)

- En el 2013, Hans Espinoza A. de Lima – Perú, alumno de la Universidad Católica del Perú perteneciente a la Facultad de Ciencias e Ingeniería, realizó la investigación con el tema “Análisis y Diseño de un Sistema de Gestión de Seguridad de Información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo”, en donde se concluyó: “La Gestión de Seguridad de la Información debería estar incluida en la cultura organizacional de las empresas, apoyada

de la alta gerencia como promotor de seguridad de los activos en la empresa. El diseño de SGSI presentado se adapta a los objetivos actuales del proceso de producción, el cual podría variar ya que los objetivos estratégicos y de gobierno de la empresa pueden cambiar y por ello algunos sub procesos que forman parte del alcance del proyecto, también lo harán. Se debe establecer que los dueños de cada uno de los procesos analizados para el diseño del SGSI, le den mayor importancia a la seguridad de la información, y que velen para que de alguna manera disminuyan los riesgos encontrados dentro de sus actividades". Esto nos muestra la importancia que tiene la protección de los activos informacionales y que la misma debería estar incluida en la cultura organizacional de las empresas, apoyada por la alta dirección; los objetivos estratégicos deberían estar alineados con el SGSI y así facilitar la adaptación ante cualquier cambio. Por último, todos los involucrados de los procesos del SGSI deben estar comprometidos y prestar mayor importancia al cuidado de los activos de información, apoyando a disminuir el impacto de los riesgos y amenazas. (Espinoza, 2013)

2.2 Bases Teóricas

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

Es el diseño, implantación y mantenimiento de un conjunto de procedimientos para gestionar eficientemente la accesibilidad de la información, minimizando a la vez los riesgos de seguridad a los que están expuestos los activos informacionales. (ISO27000.es)

2.2.1.1 Fundamentos:

Para asegurar el éxito en la gestión de seguridad de la información, lo primero es identificar su ciclo de vida y los aspectos relevantes adoptados para garantizar su C-I-D:

- **Confidencialidad:** la información no se revela ni se pone a disposición de individuos, entidades o procesos no autorizados.
- **Integridad:** la información se mantiene tal y como se creó, manteniendo su exactitud y veracidad en todos los procesos que sea requerido.
- **Disponibilidad:** la información está disponible a todo aquel individuo, entidad o proceso autorizado a su acceso cuando este lo requiera. (ISO2700.es)

La implementación de un SGSI es recomendado para las organizaciones y debe ser incluido en la estrategia de negocio, este debe ser diseñado teniendo en cuenta los objetivos, estrategias y direccionamiento de la empresa, sus alcances deben estar acordes con los requisitos de seguridad, los procesos empleados y la magnitud de la estructura organizacional, de esta manera se espera que un SGSI de soluciones acordes con la inversión realizada y que sea coherente con el tamaño del negocio. (Velasco, 2008, p.31)

2.2.1.2 Uso del SGSI

La información en conjunto con los procesos y sistemas son muy importantes para la organización, ya que juntas forman un activo muy

valioso. La confidencialidad, integridad y disponibilidad de los activos son fundamentales para alcanzar niveles altos de competitividad y rentabilidad necesarios para alcanzar los objetivos de la institución y así generar beneficios económicos. Las organizaciones y sus activos están cada vez más expuestos a un número elevado de amenazas (fraude, espionaje, sabotaje o vandalismo) que ponen en riesgo la continuidad de negocio de la organización.

Los virus informáticos o “hacking” son algunos ejemplos comunes y conocidos, pero también se deben considerar los incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización o aquellos provocados por desastres naturales y fallos técnicos.

El cumplimiento de las normas legales, la adaptación al entorno variable, la protección adecuada de los objetivos de negocio para asegurar el máximo beneficio o aprovechar nuevas oportunidades de negocio, son algunos de los aspectos fundamentales que muestran la gran utilidad e importancia de un SGSI para la gestión de las organizaciones. (ISO2700.es)

2.2.1.3 Beneficios del Uso de SGSI:

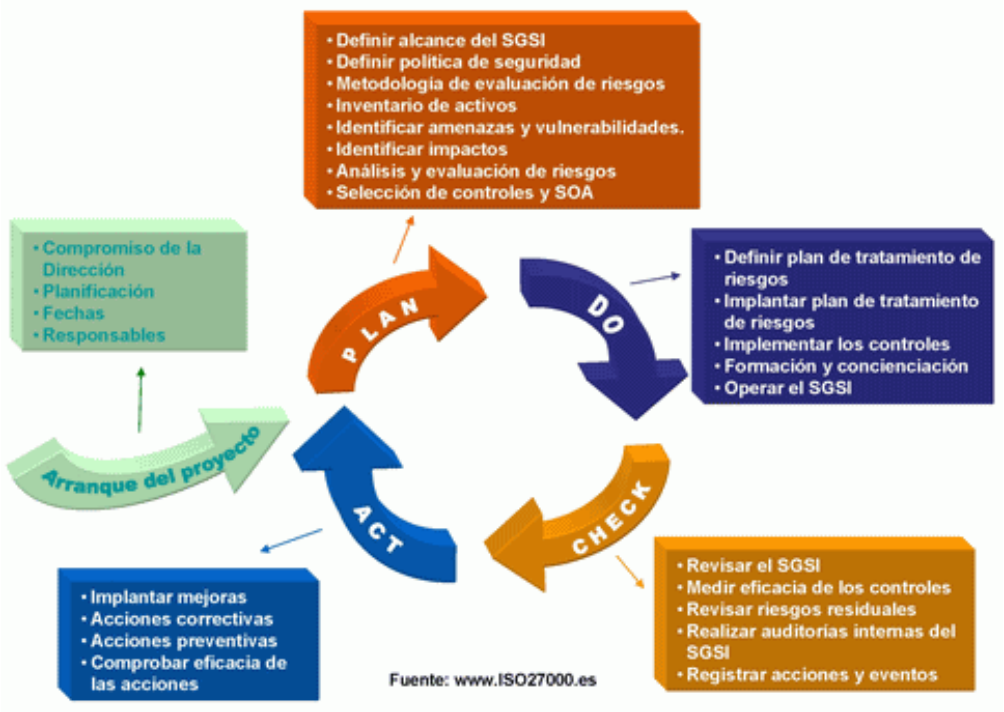
- Establecimiento de una metodología de gestión de la seguridad clara y estructurada.
- Reducción del riesgo de pérdida, robo o corrupción de información.

- Los usuarios tienen acceso a la información a través de programas con 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.
- Posibilidad de integrarse con otras normas (ISO 9001, ISO 14001, OHSAS 1800).
- Continuidad de las operaciones necesarias de negocio tras incidentes de gravedad.
- Imagen de empresa a nivel internacional y elemento diferenciador de la competencia.
- Confianza y reglas claras para las personas de la organización.
- Reducción de costes y mejora de los procesos y servicio.
- Aumento de la seguridad en base a la gestión de procesos en vez de la compra sistemática de productos y tecnologías. (Vásquez y De la Cruz, 2008)

2.2.2 ISO27001

Es un estándar internacional que proporciona un modelo para establecer, implementar, utilizar, monitorizar, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Se basa en un ciclo de vida PDCA de mejora continua o también llamado “Ciclo Deming”: PDCA – acrónimo de Plan, Do, Check, Act, que en español significa Planificar, Hacer, Verificar, Actuar. (ISO27000.es)

Figura N° 01: Ciclo Deming



Fuente: (ISO2700.es)

2.2.2.1 ISO 27001:2013

Esta versión en comparación a la 2005 ha tenido diversos cambios. Entre ellos destacan:

- Se deja de lado el "enfoque a procesos" para dar mayor énfasis a la elección de metodologías de trabajo de análisis de riesgos.
- La identificación de los activos, amenazas y vulnerabilidades ya no son requisitos previos para la identificación de los riesgos de seguridad de la información.
- Aumenta los requisitos de 102 a 130.
- Cambia su estructura conforme al anexo SL común al resto de estándares de la ISO.
- Considerables cambios en los controles, incrementando el número de dominios a 14 y disminuyendo el número de controles a 114. Incluyendo un nuevo dominio sobre "Relaciones con el Proveedor" por las crecientes relaciones entre ambas partes. (Leyva, 2016)

2.2.2.2 Beneficios que aporta a la organización

- Cumple los requisitos de gestión corporativa y de continuidad de negocio.
- Verifica el cumplimiento de las leyes y normativas que resulten de la aplicación del SGSI.
- Garantiza una ventaja competitiva cumpliendo con los requisitos contractuales y demostrando a los clientes que la seguridad de su información es fundamental.
- Verifica que los riesgos de la organización estén correctamente identificados, evaluados y tratados al mismo tiempo que formaliza los procesos y procedimientos de seguridad de la información.
- Demuestra el compromiso de la alta dirección con la seguridad de la información.

- Las constantes evaluaciones ayudan a supervisar continuamente el rendimiento y la mejora. (Leyva, 2016)

2.2.2.3 Implantación

La implantación de la norma ISO 27001 en una organización es un proyecto que suele durar entre 6 y 12 meses, según el grado de madurez en seguridad de la información y el alcance. Por lo general, es recomendable el apoyo de consultores externos. Aquellas organizaciones que hayan adecuado sus sistemas de información y procesos de trabajo a las exigencias de las normativas legales de protección de datos o que hayan realizado un acercamiento progresivo a la seguridad de la información mediante la aplicación de las buenas prácticas de ISO 27002, partirán con ventaja a la hora de implantar ISO 27001. (Leyva, 2016)

El equipo de proyecto de implantación debe estar conformado por los jefes de áreas de la organización que intervengan en los procesos del SGSI, comandado por la alta dirección y asesorado por especialistas en seguridad de la información.

2.2.2.4 Certificación

Cualquier organización que tenga implementado un SGSI según este modelo puede solicitar una auditoría externa por parte de una entidad acreditada y una vez aprobada la misma, recibir la certificación en ISO 27001. (ISO2700.es)

2.2.3 ISO 27002

Este estándar brinda la guía de implementación de la lista de las mejores prácticas y los más aceptados objetivos de control presentados como anexo en la ISO 27001, con el objetivo de facilitar la elección de controles para garantizar la seguridad de los activos de información. (Aguirre, 2014)

Un Sistema de Gestión de Seguridad de la información se logra mediante la implementación de un conjunto adecuado de controles, políticas, procesos, procedimientos, apoyados y liderados por la alta dirección. Estos controles se deben establecer, implementar, supervisar, revisar y mejorar, en forma constante para asegurar el cumplimiento de los objetivos de seguridad y de continuidad de negocio de la organización. Un SGSI según la norma ISO 27001 tiene una visión amplia y coordinada de los riesgos de seguridad de la información de la organización con el fin de poner en práctica un conjunto completo de controles de seguridad.

2.2.3.1.- Alcance

> Las normas ISO 27001, ISO 27002 están enfocadas a todo tipo de organizaciones (empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro), cualquier tamaño (pequeña, mediana o gran empresa), tipo o naturaleza. (ISO 27000.es)
>
> Este estándar proporciona directrices para las normas y prácticas de gestión de seguridad de la información, incluyendo la selección, implementación y gestión de los controles, teniendo en cuenta el entorno del riesgo de seguridad de los activos de la organización.

Esta Norma está diseñada para ser implementada por las organizaciones que tengan la necesidad de:

- Implementar controles seleccionados dentro del proceso de implantación de un Sistema de Gestión de Seguridad de la Información basado en ISO 27001.
- Desarrollar sus propias directivas de gestión de seguridad de la información. (Leyva, 2016)

2.2.3.2.- Estructura

Está organizado en base a 14 dominios, 35 objetivos de control y 114 controles de ISO 27002:2013. (Ver anexo 01).

2.2.4 ISO 27003:2010

Esta norma no es certificable. Se centra en los aspectos críticos necesarios para diseñar e implementar con éxito un Plan de Seguridad de la Información de acuerdo a la norma ISO27001. Describe los procesos de especificación y diseño desde su inicio hasta la ejecución de planes de implementación, de cómo obtener la aprobación de la gerencia para implementar un SGSI y define el procedimiento a seguir para la planificación e implementación del proyecto de Gestión de Seguridad de la Información. (ISO27000.es)

2.2.4.1.- Alcance.

Esta Norma es aplicable a cualquier tipo de organización (empresas privadas, agencias públicas, organizaciones sin fines de lucro) de cualquier tamaño. La complejidad de cada organización y sus necesidades en cuanto a la seguridad de sus activos impulsarán a la implementación de un SGSI.

Proporciona recomendaciones y explicaciones, mas no especifica los requisitos. Es utilizada en conjunto con las normas ISO / IEC 27001: 2005 y la ISO / IEC 27002: 2005, pero no tiene la intención de modificar o reducir los requisitos especificados en la norma ISO / IEC 27001: 2005 ni las recomendaciones de norma ISO / IEC 27002: 2005. (Leyva, 2016)

2.5.- ISO 27005:2011

Esta norma no es certificable. Proporciona directrices para la gestión de riesgos en la seguridad de la información, apoyando con la exigencia de los términos de la norma ISO 27001:2005 y está enfocada a la de gestión de riesgos como apoyo a la aplicación con éxito de los sistemas de seguridad de la información. (ISO27000.es)

No proporciona ningún método para gestionar los riesgos de seguridad de la información. Corresponde a la organización definir un enfoque de gestión de riesgos, en función tal vez al alcance del SGSI, al contexto de la gestión de riesgos, o al rubro de la organización. Existen diversas metodologías que

pueden ser utilizadas bajo el marco descrito en esta norma internacional, unas de ellas es Magerit. (Leyva, 2016)

4.2.5.1.- Alcance

Esta Norma es aplicable a cualquier tipo de organización (empresas privadas, agencias públicas, organizaciones sin fines de lucro) de cualquier tamaño, que tengan la intención de gestionar los riesgos que puedan comprometer la seguridad de sus activos de información.

Proporciona directivas para la gestión de riesgos de seguridad de la información. Guarda compatibilidad con los conceptos generales especificados en la norma ISO 27001 y está diseñado como soporte para la ejecución satisfactoria del SGSI basado en un enfoque de gestión de riesgos. (Leyva, 2016)

2.3 Definición de Términos Básicos

- **Aceptación del riesgo:** Acción de aceptar el riesgo. (Leyva, 2016)

- **Activo de información:** Todo elemento, proceso, sistema o información que tenga valor o utilidad para la organización. (Leyva, 2016)

- **Administración de continuidad de negocios:** En esta sección se señala las acciones correctivas y preventivas que deben tomarse en cuenta para hacer frente a interrupciones que afecten las actividades de negocio y para proteger los procesos críticos de negocio de los efectos, fallas o desastres mayores. (Villena, 2006)

- **Amenaza:** Causa potencial de un incidente no deseado, que puede causar daño a la organización. (Leyva, 2016)

- **Certificación ISO:** Un certificado ISO es un documento que indica que un producto, servicio o proceso cumple con los estándares internacionales, definidos por la Organización Internacional de Normalización (ISO). Trabajando en redes en 161 países de todo el mundo, la ISO es el mayor desarrollador y editor de normas internacionales; la organización cuenta con un miembro por país, y el sistema se coordina en Secretaría Central de Ginebra. Aunque ISO por sí misma es una organización no gubernamental, los institutos que son miembros pueden ser tanto organizaciones públicas como privadas, una disposición que permite a ISO desarrollar normas que beneficien a todos los sectores de la sociedad. (Shoaib, 2018)

- **Confiabilidad de la información:** Se refiere a que tanto se puede creer en la información que nos brinda una fuente de información. Que tan cierta pueda ser o que tan confiable pueda resultar. (Martínez, Cruz, Rodríguez, et al., 2013).

- **Confidencialidad:** La confidencialidad es una propiedad de la información mediante la cual se garantizará el acceso a la misma solo por parte de las personas que estén autorizadas. Es de alguna manera lo que se dice o hace en confianza y con seguridad recíproca entre dos o más individuos. (Barrantes y Hugo 2012)

- **Control:** Medios para contrarrestar o atenuar los riesgos, implica procedimientos, políticas, lineamientos y buenas practicas, que pueden ser de

naturaleza legal, administrativa o de gestión propia de la organización. (Leyva, 2016)

- **Cumplimiento:** Se refiere al cumplimiento de aquellas leyes, regulaciones y acuerdos contractuales a los que el proceso de negocios está sujeto, por ejemplo, criterios de negocio impuestos externamente. (Velasco, 2008)

- **Cumplimiento de requerimientos legales:** En esta sección se busca reducir las brechas que pudieran existir en cuanto a obligaciones contractuales y regulatorias. Así mismo se busca cumplir con las políticas y estándares previamente establecidos por el ente regulador. (Villena, 2006)

- **Disponibilidad de la información:** La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. A groso modo, la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran. (Barrantes y Hugo 2012)

- **Efectividad:** Se denomina efectividad a la capacidad o facultad para lograr un objetivo o fin deseado, que se han definido previamente, y para el cual se han desplegado acciones estratégicas para llegar a él. (Velasco, 2008)

- **Eficiencia:** Capacidad para lograr un fin empleando los mejores medios posibles, no siempre eficacia es sinónimo de eficiencia. (González, 2002)

- **Evaluación del riesgo:** Proceso de comparar el nivel de riesgo estimado durante el proceso de análisis de riesgo con los criterios para determinar la importancia e impacto del riesgo. (Leyva, 2016)

- **Información:** La información es un activo que brinda valor al negocio; por ello, se necesita tener una adecuada protección frente a la constante exposición a distintas amenazas y vulnerabilidades. (Aguirre, 2014)

- **Integridad de la información:** Permite asegurar que no se ha falseado la información, es decir, que los datos recibidos o recuperados son exactamente los que fueron enviados o almacenados, sin que se haya producido ninguna modificación. (Barrantes y Hugo, 2012)

- **Riesgo:** Es la probabilidad de que una amenaza se convierta en un desastre. (Leyva, 2016)

- **Seguridad de la información:** Es la protección de la confidencialidad, integridad y disponibilidad de la información; es decir, es asegurarse que esta sea accesible solo a las personas autorizadas, sea exacta sin modificaciones no deseadas y que sea accesible a los usuarios cuando lo requieran. (Aguirre, 2014)

- **Sistema de Gestión:** Es una estructura probada para la gestión y mejora continua de políticas, procedimientos y procesos de una organización. Su implementación ayuda a mejorar la efectividad operativa, optimizar beneficios, lograr mejoras continuas, aumentar la calidad y renovar constantemente las estrategias de la organización. (Aguirre, 2014)

- **Tratamiento del riesgo:** Proceso de selección e implementación de controles para disminuir o mitigar el riesgo. (Leyva, 2016)

- **Vulnerabilidad:** Es la debilidad de un activo o grupo de activos a ser atacadas y vulneradas por una o más amenazas. (Leyva, 2016)

CAPÍTULO III

DESARROLLO DEL TRABAJO DE SUFICIENCIA PROFESIONAL

3.1. Modelo de solución propuesto

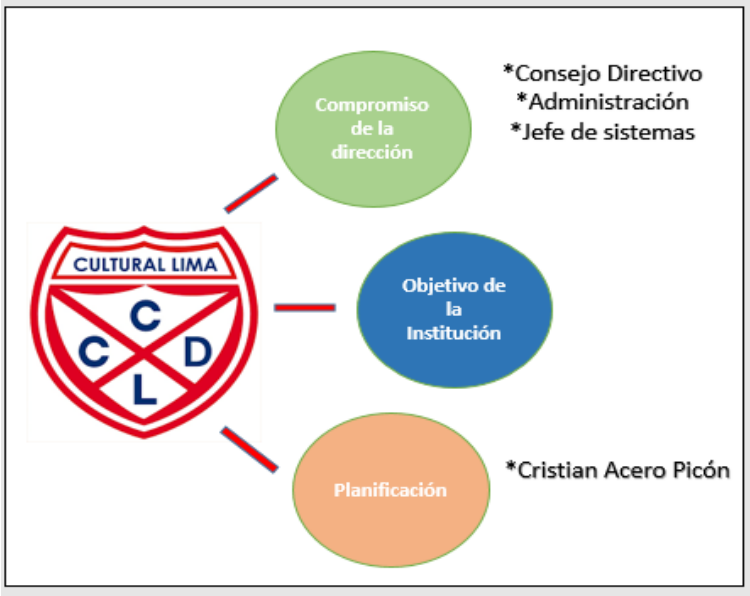
Para el desarrollo del presente proyecto “Plan de Seguridad de la Información para la Asociación Civil Centro Cultural Deportivo Lima” se utilizó la metodología del ciclo de mejora continua o también llamado Ciclo Deming o PDCA, que comprende cuatro etapas: Planear, Hacer, Verificar y Actuar. El mismo que se alinea con la norma ISO 27001 para la implementación de un adecuado Sistema de Gestión de Seguridad de la Información. Para el levantamiento de información haremos uso de herramientas como son: entrevistas, encuestas y observación. Los que se adjuntan en el anexo del presente trabajo.

A continuación, se procede con el desarrollo del proyecto (Según análisis de alternativas detallado en el Anexo N°04). **La vigencia del SGSI será de un año.**

3.1.1 Inicio del proyecto

Para el inicio de un proyecto es importante asegurar el compromiso de la dirección y determinar sobre qué objetivo se va a partir.

Figura N° 02: Inicio del proyecto



Fuente: Elaboración propia

3.1.1.1. Compromiso de la Dirección

Para el desarrollo del Plan de Seguridad de la Información en el club Asociación Civil Centro Cultural Deportivo Lima se vio en la necesidad de realizar el proyecto para su evaluación y aprobación ante el Consejo Directivo del club. Se levantó la información del estado situacional en cuanto a la seguridad de la información, conjuntamente con el jefe de sistemas, ya que el desarrollo del presente plan implica que todos los colaboradores estén involucrados con la política de seguridad de información.

3.1.1.2. Objetivos de negocio de la Institución

- OE 1. Incrementar el número de asociados.
- OE 2. Disminuir la tasa de morosidad del pago de cotizaciones.
- OE 3. Mejorar la atención al asociado en cuanto a servicios.

3.1.1.3. Responsables

Hoy, 12 de febrero de 2018, se constituye el Equipo Implementador SGSI conformado por:

Cargo	Dependencia	Firma
Jefe de Proyecto	Gerencia de Administración	
Jefe de Sistemas	Gerencia de Administración	

Mediante la presente, el equipo implementador asume la responsabilidad directa de implementación del proyecto.

3.1.2. Planificación del Proyecto

3.1.2.1. Alcance del Proyecto

El plan de seguridad de la Información de la Asociación Civil Centro Cultural Deportivo Lima abarcará las áreas de Informática, Recepción, Tesorería y Contabilidad, dirigido a los Jefes de dichas áreas y sus colaboradores.

Figura N° 03: Alcance del proyecto

Fuente: Elaboración propia

3.1.2.2 Cronograma del Proyecto

A continuación, se muestra el cronograma de actividades del Proyecto:

Figura N° 04: Cronograma del Proyecto

	Modo de	Nombre de tarea	Duración	Comienzo	Fin	Predecesora	Nombres de los recursos
1		**DISEÑO DE UN PLAN DE SEGURIDAD DE LA INFORMACIÓN PARA OPTIMIZAR LA PROTECCIÓN DE LOS ACTIVOS INFORMACIONALES DE LA ASOCIACIÓN CIVIL CENTRO CULTURAL DEPORTIVO LIMA**	**90 días**	**lun 12/02/18**	**vie 15/06/18**		
2		**Gestion del proyecto**	**90 días**	**lun 12/02/18**	**vie 15/06/18**		
3		**Iniciacion**	**1 día**	**lun 12/02/18**	**lun 12/02/18**		
4		Elaborar el acta de constitucion del proyecto	1 día	lun 12/02/18	lun 12/02/18		Acero
5		**Planificacion del proyecto**	**6 días**	**mar 13/02/18**	**mar 20/02/18**		
6		Elaboracion alcance del proyecto	1 día	mar 13/02/18	mar 13/02/18	4	Acero
7		Aprobacion del alcance del proyecto (reunion)	1 día	mié 14/02/18	mié 14/02/18	6	Acero
8		Identificar entregables según alcance del proyecto	1 día	jue 15/02/18	jue 15/02/18	7	Acero
9		Elaborar EDT	1 día	jue 15/02/18	jue 15/02/18		Acero
10		Estructurar cronograma del proyecto	1 día	vie 16/02/18	vie 16/02/18	8	Acero
11		Elaborar analisis costo/beneficio	1 día	lun 19/02/18	lun 19/02/18	10	Acero
12		Identificar los riesgos que afectan al proyecto	1 día	mar 13/02/18	mar 13/02/18		Acero
13		Identificar un plan de tratamiento de riesgos	1 día	mié 14/02/18	mié 14/02/18	12	Acero
14		**Ejecucion del Proyecto**	**83 días**	**mié 21/02/18**	**vie 15/06/18**		
15		Estructurar propuesta de politica del SGSI	2 días	mié 21/02/18	jue 22/02/18	13	Acero
16		Diseño del plan de seguridad	2 días	vie 23/02/18	lun 26/02/18	15	Acero
17		**Analisis y Evaluacion de riesgos**	**47 días**	**mié 21/02/18**	**jue 26/04/18**		
18		Elaborar diagrama de identificacion de procesos del area de informatica	6 días	mié 21/02/18	mié 28/02/18		Acero
19		Identificar los procesos / sistemas	3 días	mié 21/02/18	vie 23/02/18		Acero
20		Identificacion de activos por procesos / sistemas	4 días	lun 26/02/18	jue 01/03/18	19	Acero
21		Valoracion e inventario de activos identificados	2 días	vie 02/03/18	lun 05/03/18	20	Acero
22		Identificar y evaluar amenazas por activos identificados	3 días	mar 06/03/18	jue 08/03/18	21	Acero
23		Identificar y evaluar riesgos por activos identificados	3 días	vie 09/03/18	mar 13/03/18	22	Acero
24		Hallar el riesgo efectivo por amenaza de un activo	2 días	mié 14/03/18	jue 15/03/18	23	Acero
25		Definir controles de implementacion	6 días	vie 16/03/18	vie 23/03/18	24	Acero
26		Revisiones de controles propuestos	2 días	lun 26/03/18	mar 27/03/18	25	Acero
27		Definir plan de accion de tratamiento del riesgo	2 días	mié 28/03/18	jue 29/03/18	26	Acero
28		Implementacion de politicas de seguridad	20 días	vie 30/03/18	jue 26/04/18	27	Acero
29		Implementacion del plan de tratamiento de riesgos	20 días	vie 30/03/18	jue 26/04/18	27	Acero
30		Elaborar programa de capacitacion y concientizacion	1 día	mié 21/02/18	mié 21/02/18		Acero
31		Coordinar fechas para la capacitacion y concientizacion	1 día	jue 22/02/18	jue 22/02/18	30	Acero
32		Ejecutar capacitacion y concientizacion al personal involucrado	3 días	vie 23/02/18	mar 27/02/18	31	Acero
33		Evaluar y calificar a los participantes de la capacitacion y concientizacion	2 días	mié 28/02/18	jue 01/03/18	32	Acero
34		Presentar resultados de capacitacion y concientizacion al Consejo Directivo	1 día	vie 02/03/18	vie 02/03/18	33	Acero
35		Resultado y analisis de indicadores	1 día	mié 21/02/18	mié 21/02/18		Acero
36		Presentar resultados finales al consejo directivo	1 día	mié 21/02/18	mié 21/02/18		Acero
37		**Seguimiento y control**	**30 días**	**vie 27/04/18**	**jue 07/06/18**		
38		Registro de avances mensuales	30 días	vie 27/04/18	jue 07/06/18		Acero
39		Registro de cambios del proyecto	23 días	mar 08/05/18	jue 07/06/18		Acero
40		**Cierre**	**1 día**	**vie 15/06/18**	**vie 15/06/18**		
41		Elaborar el acta de cierre del proyecto	1 día	vie 15/06/18	vie 15/06/18	39	Acero

Fuente: Elaboración Propia

3.1.2.3 Análisis Costo / Beneficio

Tabla N°01. Costos de implementación de Proyecto

Descripción	Precio (S/)	Tiempo de vida (años)
Jefe de Proyecto	9000	1
Licencia de ESET Endpoit antivirus	2000	1
Licencia completa software de copia de seguridad	300	1
Software de monitoreo de red	100	1
Servicios básicos, teléfono e internet	2500	1
Papel bond A4	80	1
Conectores RJ45	40	3
Cable UTP categoría 6	200	3
Canaleta	200	3
Detector de fuego	1500	3
Aire Acondicionado	2000	5
Muebles con seguridad	1000	5
Deshumedesedor	500	5
Software especializado para el control de accesos	500	1
Firewall Fortinet	800	1
UPS CDP R-UPR508i de 500VA, 240W	1450	
Mantenimiento de pozo de tierra	1200	1
Costo total	23,370.00	

Fuente: Elaboración propia

Tabla N°02. Ahorro supuesto anual por contar con un SGSI

Descripción	Ahorro
Pérdida de información accidental	20,000.00
Pérdida de información por desastres naturales y/o provocados	60,000.00
Pérdida o robo de información por problemas de comunicación	20,000.00
Interrupción del sistema de cobranza	100,000.00
Robo de información de los clientes, personal interno, contratistas y/o proveedores	20,000.00
Total ahorro supuesto anual (S/)	220,000.00
Ingresos del Club 2017	2,500,000.00
	2,720,000.00

Fuente: Elaboración propia

El tiempo de recuperación de la inversión del Proyecto SGSI puede variar dependiendo de cuantos incidentes reales sucedan al año. En este supuesto, se consideró que ocurrió una vez al año cada uno de los incidentes.

Dando como resultado:

B/C = Beneficio / Costo = 220000 / 23370 = 9.4138

Meses: 12

B/C = 12 / 9.4138 = 1.2747

Tiempo de recuperación: Aproximadamente 1 mes.

3.1.2.4 Riesgos del Proyecto

Tabla N°03. Valoración para determinar tipo de Riesgo

Probabilidad	Valor numérico	Impacto	Valor numérico	Tipo de riesgo	Probabilidad x Impacto
Muy improbable	1	Muy bajo	1	Muy alto	Mayor a 49
Relativamente probable	2	Bajo	2	Alto	30 - 49
Probable	3	Moderado	3	Moderado	20 - 29
Muy probable	4	Alto	4	Bajo	10 - 19
Casi cierto	5	Muy alto	5	Muy bajo	Menor a 10

Fuente: Elaboración propia

Tabla N°04. Evaluación de Riesgos del Proyecto

Riesgos	Descripción del riesgo	Estimación de probabilidad	Objetivo afectado	Estimación de impacto	Prob. x impacto	Tipo de riesgo
R01	Incumplimiento de las actividades del cronograma de proyecto.	5	Alcance	1	5	Alto
			Tiempo	4	20	
			Costo	1	5	
			Calidad	2	10	
			Total probabilidad x impacto		40	
R02	Trabajos no programados.	3	Alcance	2	6	Alto
			Tiempo	5	15	
			Costo	2	6	
			Calidad	3	9	
			Total probabilidad x impacto		36	
R03	Cambios en el alcance del proyecto.	2	Alcance	5	10	Moderado
			Tiempo	5	10	
			Costo	2	4	
			Calidad	2	4	
			Total probabilidad x impacto		28	
R04	Modificación del cronograma de proyecto.	3	Alcance	1	3	Moderado
			Tiempo	3	9	
			Costo	2	6	
			Calidad	2	6	
			Total probabilidad x impacto		24	
R05	Falta temporal de personal clave.	3	Alcance	1	3	Moderado
			Tiempo	3	9	
			Costo	2	6	
			Calidad	2	6	
			Total probabilidad x impacto		24	

R06	Perdida de personal clave.	2	Alcance	1	2	Bajo
			Tiempo	3	6	
			Costo	2	4	
			Calidad	2	4	
			Total probabilidad x impacto		16	
R07	Restructuración Organizacional.	2	Alcance	2	4	Moderado
			Tiempo	4	8	
			Costo	3	6	
			Calidad	3	6	
			Total probabilidad x impacto		24	
R08	Procesos de tecnología definidos incorrectamente.	4	Alcance	5	20	Muy Alto
			Tiempo	3	12	
			Costo	1	4	
			Calidad	4	16	
			Total probabilidad x impacto		52	
R09	Desconocimiento del plan de continuidad por parte del implementador.	4	Alcance	3	12	Alto
			Tiempo	3	12	
			Costo	1	4	
			Calidad	3	12	
			Total probabilidad x impacto		40	
R10	Incorrecta definición de los activos de información.	3	Alcance	2	6	Alto
			Tiempo	5	15	
			Costo	1	3	
			Calidad	4	12	
			Total probabilidad x impacto		36	
R11	Incorrecta identificación de los riesgos en los activos de información.	3	Alcance	2	6	Alto
			Tiempo	5	15	
			Costo	1	3	
			Calidad	4	12	

			Total probabilidad x impacto		36	
R12	Incorrecta definición de controles para los riesgos.	3	Alcance	2	6	Alto
			Tiempo	5	15	
			Costo	1	3	
			Calidad	4	12	
			Total probabilidad x impacto		36	
R13	El equipo implementador SGSI no se encuentra comprometido con el proyecto.	3	Alcance	1	3	Alto
			Tiempo	5	15	
			Costo	1	3	
			Calidad	5	15	
			Total probabilidad x impacto		36	
R14	Personal de Informática no se encuentra capacitado para la implementación de un SGSI.	4	Alcance	1	4	Muy alto
			Tiempo	5	20	
			Costo	1	4	
			Calidad	5	20	
			Total probabilidad x impacto		48	
R15	Personal de Informática no cumple con los controles definidos en la implementación.	3	Alcance	1	3	Moderado
			Tiempo	1	3	
			Costo	2	6	
			Calidad	5	15	
			Total probabilidad x impacto		27	
R16	Elaboración del plan de tratamiento de riesgos en fecha equivoca.	2	Alcance	1	2	Moderado
			Tiempo	5	10	
			Costo	1	2	
			Calidad	5	10	
			Total probabilidad x impacto		24	
R17	Formatos inadecuados		Alcance	1	2	
			Tiempo	4	8	

	para el análisis y evaluación de riesgos.	2	Costo	1	2	Moderado
			Calidad	5	10	
			Total probabilidad x impacto		22	
R18	Incumplimiento de los programas de auditorías internas.	2	Alcance	1	2	Bajo
			Tiempo	3	6	
			Costo	2	4	
			Calidad	**3**	6	
			Total probabilidad x impacto		18	

Fuente: Elaboración propia

3.1.2.5 Plan de tratamiento de riesgos del proyecto

Luego de haber evaluado los riesgos del proyecto, según la probabilidad e impacto que estos puedan causar, procederemos a listar un plan de tratamiento de los mismos.

Cabe mencionar que se escogieron los riesgos de criticidad: Muy alto, alto y moderado, de la tabla anterior (tabla N°04).

Tabla N°05. Plan de tratamiento de riesgos del proyecto

Riesgos	Responsable de tratamiento	Plan de mitigación	Plan de contingencia
R01	- Implementador SGSI - Jefe de sistemas	- Aprobación del cronograma por el Consejo Directivo, previa revisión de los involucrados.	- Personal de apoyo para los recursos responsables de actividades del proyecto.
R02	- Implementador SGSI	- Aprobación del cronograma por el Consejo Directivo, previa revisión de los involucrados.	- Rápida adaptación del cronograma del proyecto. - Asignación de recursos a los nuevos trabajos.
R03	- Implementador SGSI	- Revisión y aprobación del alcance del SGSI por el Consejo Directivo y las áreas afectadas.	- Reunión con la gerencia. - Adaptación del alcance, política y cronograma. - Ajustes en los recursos sujetos al nuevo alcance.
R04	- Implementador SGSI	- Aprobación del cronograma por el Consejo Directivo,	- Rápida adaptación del cronograma del proyecto, previa

		previa revisión de los involucrados.	coordinación con los involucrados.
R05	- Jefe de sistemas	- Revisión del rol de vacaciones. - Realizar ajustes al cronograma y aprobarlo por el consejo directivo.	- Sustitución temporal del personal por un perfil similar.
R07	- Implementador SGSI	- Aprobación del proyecto SGSI mediante Sesión de Consejo y publicarlo en asamblea general de asociados.	- Reunión con el nuevo consejo directivo si fuera el caso, explicando la importancia de la implementación SGSI.
R08	- Implementador SGSI - Jefe de sistemas	- Los jefes de cada área deben reunirse con el personal a su cargo para la definición de todos los procesos ejecutados.	- El jefe de cada área debe solicitar apoyo al área de sistemas para re-definir los procesos.
R09	- Implementador SGSI - Jefe de sistemas	- Capacitación en la elaboración de un plan de continuidad de tecnología.	- Sub contratar una capacitación externa. - Sub contratar un tercero para la elaboración del plan de continuidad.
R10	- Implementador SGSI - Jefe de sistemas	- Realizar presentaciones con metodologías para la identificación de activos.	- Participar de reuniones con los responsables para la definición de los activos de información a cargo.
R11	- Implementador SGSI - Jefe de sistemas	- Realizar presentaciones con metodologías para la identificación de riesgos.	- Participar de reuniones con los responsables para la identificación de los riesgos.
R12	- Implementador SGSI - Jefe de sistemas	- Realizar presentaciones con metodologías para la definición de controles aplicables. - Facilitar formato con todos los controles aplicables.	- Participar de reuniones con los responsables para la definición de controles aplicables.
R13	- Implementador SGSI - Jefe de sistemas	- Realizar presentación de concientización al equipo implementador.	- Coordinar reunión con el área de sistemas para revisar avance del proyecto.
R14	- Implementador SGSI - Jefe de sistemas	- Capacitar al personal de las áreas involucradas para implementar un SGSI.	- Sub contratar una capacitación externa. - Sub contratar un tercero para la implementación del SGSI.
R15	- Implementador SGSI - Jefe de sistemas	- Capacitar al personal de las áreas involucradas para cumplir con los controles definidos	- Coordinar reunión con el área de sistemas y áreas responsables para revisar avance del proyecto.
R16	- Implementador SGSI - Jefe de sistemas	- Aprobación del plan de tratamiento de riesgos previa revisión por los involucrados.	- Rápida adaptación al nuevo plan de tratamiento de riesgos. - Concientización de los involucrados.
R17	- Implementador SGSI - Jefe de sistemas	- Aprobación y revisión de todos los formatos a usar, por las jefaturas y alta dirección.	- Re definir los formatos en reunión con el equipo implementador SGSI.

Fuente: Elaboración propia

3.1.3 Ejecución del Proyecto

3.1.3.1 Política de Seguridad

A. Generalidades

La definición de la política de seguridad de la información garantiza un compromiso con la protección de los activos frente a las distintas amenazas, con la finalidad de asegurar la continuidad de los sistemas de información, minimizando los riesgos y garantizando el cumplimiento de los objetivos del plan. Es importante que estas políticas sean parte de la cultura del club. Para ello, se debe garantizar un compromiso con la alta Dirección del club para la propagación y cumplimiento de la presente.

B. Objetivo principal

Establecer directivas que orienten la protección de la información en el club Asociación Civil Centro Cultural Deportivo Lima, visualizando el compromiso, fomento y desarrollo de la cultura de seguridad de la información en todo el ámbito de la institución.

C. Objetivo secundario

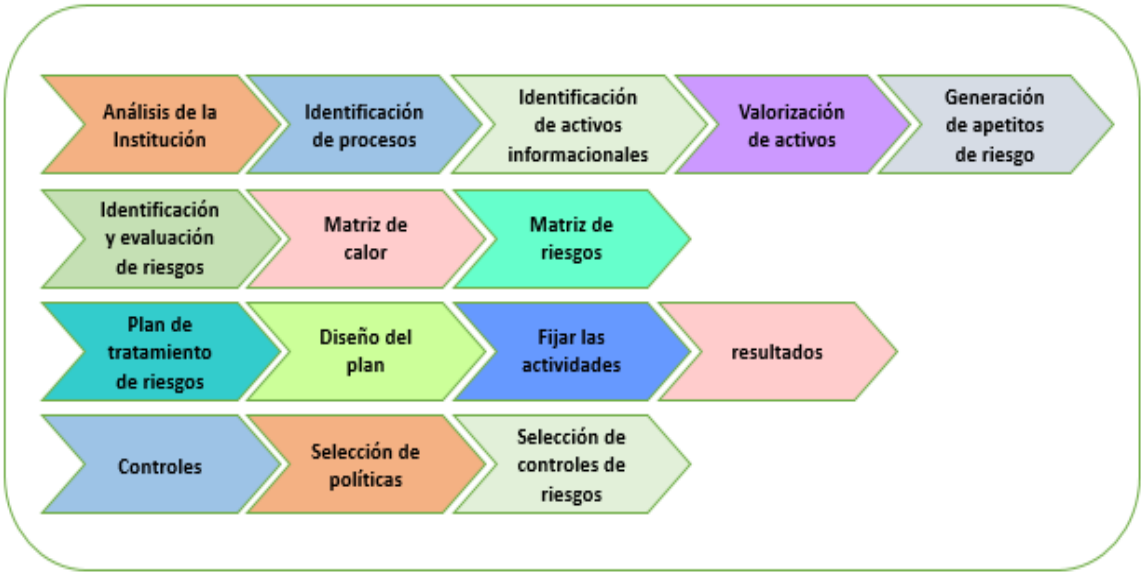
- Salvaguardar los activos informacionales del club Asociación Civil Centro Cultural Deportivo Lima, frente amenazas internas o externas, asegurando el cumplimiento de la confidencialidad, disponibilidad e integridad de la información.
- Afianzar la implementación de las normas procedimientos y políticas de seguridad comprendidas en esta política.

- Actualizar constantemente la política de seguridad de la información a implementar en la Asociación Civil Centro Cultural Deportivo Lima, con la finalidad de asegurar su vigencia, eficiencia y eficacia a lo largo de su práctica.

3.1.3.2 Diseño del Plan de Seguridad

El diseño del presente trabajo se desarrolló en 4 etapas, que describen desde el análisis de la institución (estado situacional) hasta finalizar con la definición de controles de riesgos, para lo cual se muestra en la siguiente figura.

Figura N° 05: Diseño del Plan de Seguridad



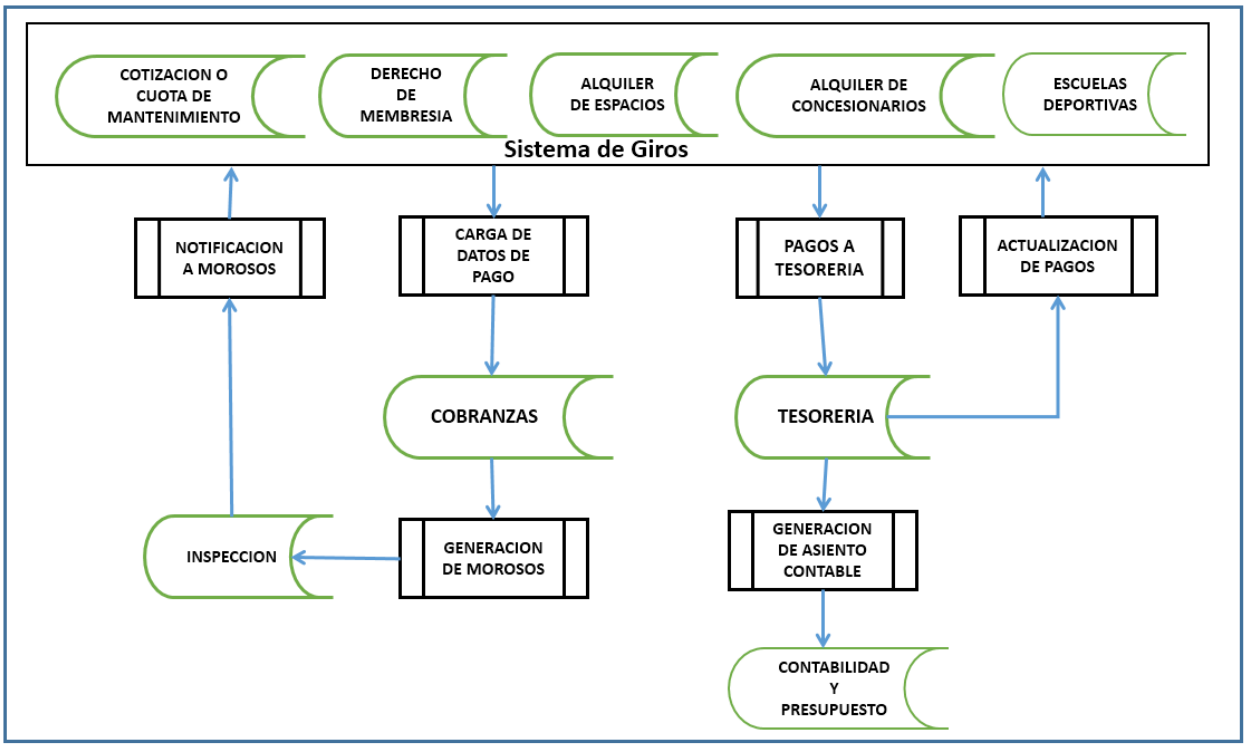
Fuente: Elaboración propia

3.1.3.2.1 Análisis de la Institución

A. Identificación de Procesos de la Institución

Se desarrollará un modelado del proceso principal que permitirá visualizar detalladamente el flujo del trabajo.

Figura N° 05: Diagrama de Sistema de Cobranzas



Fuente: Elaboración propia

Proceso Sistema de Cobranzas

Objetivo:

Brindar una herramienta de gestión dinámica que permita de manera ordenada implantar procedimientos que faciliten el proceso de cobro, manteniendo actualizado el sistema de cobranza, lo que permitirá

analizar de manera confiable los activos de información para la toma de decisiones.

Descripción:

- Generación del listado de cuentas por cobrar del sistema.
- Se comunica a todos los asociados, concesionarios realizar los pagos correspondientes.
- Generación de penalidades por incumplimiento de pago.
- Administración inspecciona los incumplimientos y realiza las gestiones correspondientes.
- Se notifica a los morosos.
- Se carga la información al sistema para generar el cobro de las penalidades.
- Los asociados realizan los pagos en caja del club.
- Actualización de pagos en el sistema.
- Caja entrega reporte diario de los ingresos a contabilidad y tesorería.
- Contabilidad genera el asiento contable y resguarda los comprobantes.
- La información es cargada al Presupuesto.

B. Identificación de los activos de información

Se identificarán los activos que están relacionados en cada proceso descrito anteriormente. Existen dos tipos de activos: primarios y los de soporte.

- **Dato:** Es toda aquella información que se genera, envía, recibe y se gestiona dentro de la institución.
- **Aplicación:** Software que se utiliza como soporte en los procesos.

- **Personal**: Son todas aquellas personas que se ven involucradas en el acceso y manejo de los activos informacionales de la institución.
- **Servicio:** Son los servicios que alguna área de la organización suministra a otra área o identidad externa.
- **Tecnología:** Hardware donde se maneja la información y las comunicaciones.
- **Instalación**: Es el espacio donde se almacena o alojan los activos informacionales. Este ambiente puede estar dentro o fuera de la institución.
- **Equipamiento auxiliar:** son los activos que no se hallan definido en ninguno de los anteriores.

Se pueden observar los activos de información identificados en el club Asociación Civil Centro Cultural Deportivo Lima, en la siguiente tabla:

Tabla N° 06. Inventario de activos

ID	ACTIVO	TANGIBLE	TIPO DE ACTIVO
1	Computadora de escritorio	SI	Tecnología
2	Licencia de Microsoft Windows 7	NO	Aplicación
3	Licencia de Microsoft office 2013	NO	Aplicación
4	Antivirus	NO	Aplicación
5	Email (Outlook)	NO	Aplicación
6	Página web del club	NO	Aplicación
7	Sistema de cobranzas	NO	Aplicación
8	Teléfono	SI	Tecnología
9	Impresoras	SI	Tecnología
10	Fotocopiadora	SI	Tecnología

11	Scanner	SI	Tecnología
12	Cableado ethernet	SI	Tecnología
13	Red de informática (carpeta compartidas)	NO	Aplicación
14	Firewall de Windows	NO	Aplicación
15	Archivadores para documentos	SI	Equipamiento auxiliar
16	Llave de ingreso	SI	Equipamiento auxiliar
17	Jefe de Sistemas	SI	Personal
18	Jefe de Tesorería	SI	Personal
19	Administrador	SI	Personal
20	Comprobantes de ingreso de caja (boletas, facturas, etc).	SI	Dato
21	Cartas de solicitud de suspensión de cotización	SI	Dato
22	Cartas de solicitud de usufructos	SI	Dato
23	Carta de solicitud de transferencia	SI	Dato
24	Carta de solicitud de socio vitalicio	SI	Dato
25	Fichas de socios	SI	Dato
26	Oficios de distintas identidades judiciales, laborales, etc. que ingresan por mesa de partes al club.	SI	Dato
27	Base de datos (SQL)	NO	Aplicación
28	Cámaras de seguridad	SI	Tecnología

Fuente: Elaboración propia

C. Valorización de los activos de información

Luego de haber identificado los activos informacionales que se encuentran comprendidos en los procesos de la Asociación Civil Centro Cultural Deportivo Lima, pasamos a determinar el valor que cada activo tiene para la institución y el impacto que tendría si llegara a faltar o fallar en algún momento.

Para esta etapa se determinó una escala cualitativa, la cual se muestra en la siguiente tabla, según criterios analizados para realizar la correcta valorización, que nos permitirá clasificarlos.

Tabla N° 07. Criterios de valorización de activos

Criterio	Valor	Descripción
Disponibilidad	0	No aplica / no es relevante
	1	Debe estar disponible al menos el 10% del tiempo
	2	Debe estar disponible al menos el 50% del tiempo
	3	Debe estar disponible siempre
Integridad	0	No aplica / no es relevante
	1	No son relevantes los errores que tenga o la información faltante.
	2	Tiene que estar correcto y completo al menos un 50%.
	3	Tiene que estar correcto y completo en un 100%
	0	No aplica / no relevante
	1	Daños muy bajos, el incidente no transcendería del área afectada
	2	Seria relevante, el incidente implicaría a

Confidencialidad		otras áreas
	3	Los daños serian catastróficos, la reputación y la imagen de la institución se verían comprometidas

Fuente: (Leyva, 2016)

Para hallar el valor final del activo, se sumarán los valores de los distintos criterios. Este resultado se ubicará en un rango de valores de 0 a 9, lo que representará un nivel de criticidad para cada valor. Mientras más alto sea el valor final de la suma, más alta será su criticidad.

Para este trabajo se definieron cuatro niveles de criticidad, los cuales se muestran en la siguiente tabla.

Tabla N°08. Valores según nivel de criticidad

Valor	Nivel de criticidad
0	No aplica
1	Baja
2	Baja
3	Baja
4	Media
5	Media
6	Media
7	Alta
8	Alta
9	Alta

Fuente: Elaboración propia

Apetito de Riesgo:

Se definió que los activos de criticidad “Alta” son con los que trabajaremos para la identificación y análisis de riesgo de los activos informacionales. Los activos de criticidad “Media” y “Baja” no se tomarán como activos críticos para la Asociación Civil Centro Cultural Deportivo Lima. Por lo tanto, no estarán dentro del análisis.

Procedemos a mostrar todos los activos identificados con sus respectivos valores.

Tabla N°09. Valorización de los activos de la información

ID	ACTIVO	Criterio de valorización			Valor total	criticidad
		integridad	disponibilidad	confidencialidad		
1	Computadora de escritorio	3	3	3	9	Alta
2	Licencia de Microsoft Windows 7	3	3	1	7	Alta
3	Licencia de Microsoft office 2013	3	3	1	7	Alta
4	Antivirus	3	3	2	8	Alta
5	Email (Outlook)	2	3	2	7	Alta
6	Página web del club	2	3	2	7	Alta
7	Sistema de cobranzas	3	3	3	9	Alta
8	Teléfono	3	3	0	6	Media
9	impresoras	3	2	0	5	media
10	fotocopiadora	3	2	0	5	Media
11	Scanner	3	2	0	5	Media
12	Cableado ethernet	3	3	2	8	Alta
13	red de informática (carpeta compartidas)	3	3	3	9	Alta
14	Firewall de Windows	2	3	1	6	Media
15	Archivadores para documentos	2	1	2	5	Media

16	Llave de ingreso	3	3	3	9	Alta
17	Jefe de Sistemas	3	2	0	5	Media
18	Jefe de Tesorería	3	2	0	5	Media
19	Administrador	3	2	0	5	Media
20	Comprobantes de ingreso de caja (boletas, facturas, etc).	3	3	2	8	Alta
21	Cartas de solicitud de suspensión de cotización	2	2	0	4	Media
22	Cartas de solicitud de usufructos	2	2	0	4	Media
23	Carta de solicitud de transferencia	2	2	0	4	Media
24	Carta de solicitud de socio vitalicio	2	2	0	4	Media
25	Fichas de socios	3	2	2	7	Alta
26	Oficios de distintas identidades judiciales, laborales, etc. que ingresan por mesa de partes al club.	3	1	1	5	Media
27	Base de datos (SQL)	3	3	3	9	Alta
28	Cámaras de seguridad	3	3	0	6	Media

Fuente: Elaboración propia

Seguido de haber realizado la valorización de los activos de información, se encontraron 13 activos con criticidad alta, los que mostramos a continuación.

Tabla N° 10. Activos con criticidad alta

ID	ACTIVO	VALOR
1	Computadora de escritorio	9
2	Licencia de Microsoft Windows 7	7
3	Licencia de Microsoft office 2013	7
4	Antivirus	8
5	Email (Outlook)	7
6	Página web del club	7
7	Sistema de cobranzas	9
8	Cableado ethernet	8
9	Red de informática (carpeta compartidas)	9
10	Llave de ingreso	9
11	Comprobantes de ingreso de caja (boletas, facturas, etc).	8
12	Fichas de socios	7
13	Base de datos SQL	9

Fuente: Elaboración propia

3.1.3.2.2 Identificación y evaluación de riesgos

Mapa de riesgos

Luego de haber realizado la valorización en detalle de los riesgos seleccionados del apetito de riesgos previamente definido. Procederemos a hallar las vulnerabilidades y amenazas a los que están expuestos estos activos.

Para determinar dicha valorización se determinó utilizar una matriz de calor, la cual posee como criterios la probabilidad que cierta amenaza explote

cierta vulnerabilidad y el impacto estimado al negocio que el riesgo pueda ocasionar.

Tabla N° 11. Matriz de calor

Impacto en el negocio	Probabilidad de afectación				
	Muy Baja	**Baja**	**Media**	**Alta**	**Muy Alta**
Muy Alto	Relevante	Relevante	Alto	Extremo	Extremo
Alto	Relevante	Relevante	Alto	Alto	Extremo
Medio	Moderado	Moderado	Relevante	Alto	Extremo
Bajo	Bajo	Bajo	Bajo	Moderado	Relevante
Muy Bajo	Bajo	Bajo	Bajo	Bajo	Moderado

Fuente: Elaboración propia

El significado al respecto de los criterios de probabilidad de afectación se describe en la siguiente tabla:

Tabla N° 12. Descripción de los niveles de la probabilidad de afectación

Probabilidad de Afectación	Interpretación
Muy Alta	Es casi seguro que la amenaza afectara la vulnerabilidad.
Alta	Es probable que la amenaza afectara la vulnerabilidad
Media	Es posible que la amenaza afectara la vulnerabilidad
Baja	Es improbable que la amenaza afectara la vulnerabilidad
Muy Baja	Es impensable que la amenaza afectara la vulnerabilidad

Fuente: Elaboración propia

El significado respecto a los criterios de impacto en el negocio se detalla en la siguiente tabla:

Tabla N° 13. Descripción de los niveles de impacto en el negocio

Impacto en el Negocio	Interpretación
Muy Alto	Afecta por más de un mes las operaciones del club.
Alto	Afecta hasta en 15 días las operaciones del club.
Medio	Afecta hasta en 7 días las operaciones del club.
Bajo	Afecta hasta 48 horas las operaciones del club.
Muy Bajo	Tiene un efecto nulo o muy pequeño en las operaciones del club.

Fuente: Elaboración propia

Luego de describir los niveles de impacto y probabilidad en el negocio que pueda ocasionar la materialización de los riesgos obtendremos el nivel de dichos riesgos. Como se detalla en la tabla N° 06 (mapa de calor) obtuvimos 5 valores de riesgos: extremo, alto, relevante, moderado y bajo.

A continuación, mostramos matriz completa de riesgos de los activos con criticidad alta que se obtuvieron del análisis, según el apetito de riesgo analizado y desarrollado previamente.

Tabla N° 14. Materiales de riesgos

MATRIZ DE RIESGO						
ID de riesgo	ACTIVO	VULNERABILIDAD	AMENAZA	Posibilidad de que la amenaza explote la vulnerabilidad	Impacto estimado en la Institución	Nivel de Riesgo
R1	Computadora de escritorio	Mala seguridad de contraseñas	Divulgación de la información	Muy alto	Muy alto	Extremo
R2		Sensibilidad de golpes o caídas	Destrucción de equipos	Bajo	Muy alto	Relevante
R3		Falta de backups	Sustracción de la información o equipo	Muy alto	Muy alto	Extremo
R4		Falta de cierre de sección al dejar el trabajo	Manipulación de información	Muy alto	Alto	Extremo
R5		Sensibilidad a la humedad, polvo o calor	Polvo, corrosión, congelamiento	Muy alto	Muy alto	Extremo
R6		Susceptibilidad a variaciones de energía	Perdida de suministro de energía	alto	Muy alto	Extremo
R7	Licencia de Microsoft Windows 7	Falta de mecanismo de autenticación e identificación de usuarios	Abuso o forzado de derechos	alto	Muy alto	Extremo
R8		Mala gestión de contraseña	Abuso o forzado de derechos	Bajo	Muy alto	Relevante
R9		Servicios	Procesamiento	Alto	Muy alto	Alto

		innecesarios para el usuario	ilegal de los datos			
R10	Licencia de Microsoft office 2013	Falta de mecanismo de autenticación e identificación de usuarios	Abuso o forzado de derechos	Alto	Muy alto	Extremo
R11		Mala gestión de contraseña	Abuso o forzado de derechos	Bajo	Muy alto	Relevante
R12		Servicios innecesarios para el usuario	Procesamiento ilegal de los datos	Alto	Muy alto	Alto
R13	Antivirus	Interfaz de usuario complicado	Error en el uso del software	Alto	Alto	Alto
R14		Configuración incorrecta de parámetros	Error en el uso del software	Medio	Medio	Relevante
R15		Funciones del antivirus obsoletas	Licencia caducada	Alto	Medio	Alto
R16	Email (Outlook)	Falta de mecanismo de autenticación e identificación de usuarios	Abuso de derechos	bajo	bajo	Bajo
R17		Falta de backup	Manipulación de información	Alto	alto	Alto
R18		Efectos en el funcionamiento del software	Abuso de derechos	alto	alto	Alto
R19		Mala gestión de	divulgación de	Muy alto	alto	Extremo

	Página web del club	contraseña	la información			
R20		Falta de documentación	Error en el uso del software	Medio	medio	Relevante
R21	Sistema de cobranzas	Mala gestión de usuarios del sistema	Adulteración de la información	alto	Muy alto	Extremo
R22		Falta de backup	Robo de información o del sistema	alto	Muy alto	Extremo
R23		Defectos en el funcionamiento del software	Abuso de derechos	Alto	Alto	Alto
R24	Cableado ethernet	Trafico de información desprotegido	Escuchar información ilegalmente	Alto	alto	Alto
R25		Cableado desprotegido	Falla en los equipos de red	Alto	Muy Alto	Extremo
R26		Arquitectura de red insegura	Espionaje remoto	Bajo	Alto	Relevante
R27		Gestión inadecuado de la red	Saturación de los sistemas de información	Alto	Alto	Alto
R28	Red de informática (carpeta compartidas)	Falta de controles en el traspaso de información	Robo de documentos o de equipos tecnológicos	Alto	Muy alto	Extremo
R29		Falta de privilegios en los permisos	Manipulación de información	Muy alto	Muy alto	Extremo
R30		Mala seguridad de contraseñas	Manipulación de información	Alto	Alto	Alto
R31		Gestión inadecuado de	Saturación de los sistemas	Alto	Alto	Alto

		la red	de información			
R32		Conexiones de red desprotegidas	Uso no autorizado de los equipos de red	Alto	Alto	Alto
R33	Llave de ingreso	Acceso a instalaciones sin permisos	Destrucción o robos de equipos o medios de comunicación	Alto	Muy alto	Extremo
R34	Comprobante de ingreso de caja (boletas, facturas, etc)	Falta de mecanismo de backup	Robo o manipulación del activo	Alto	Alto	Alto
R35		Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	media	Alto	Alto
R36		Pocos o nulos controles de acceso	Robo o manipulación del activo	Media	Alto	Alto
R37	Fichas de socios	Falta de mecanismo de backup	Robo o manipulación del activo	Alto	Alto	Alto
R38		Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	media	Alto	Alto
R39		Pocos o nulos controles de acceso	Robo o manipulación del activo	Media	Alto	Alto
R40		Mala gestión de acceso a la BD	Adulteración de la información	alto	Muy alto	Extremo

R41	Base de datos SQL	Falta de backup	Robo o manipulación de la información	alto	Muy alto	Extremo
R42		Defectos en el funcionamiento del software	Abuso de derechos	medio	Alto	Alto

Fuente: Elaboración propia

3.1.3.2.3 Plan de Tratamientos de riesgos

En este punto procederemos a definir un criterio de aceptación de riesgo el cual definirá si es aceptable o si requiere algún tratamiento. Posteriormente definiremos el plan de tratamiento de los riesgos identificados previamente.

En el siguiente cuadro se presenta el plan de tratamiento de los riesgos:

Tabla N° 15. Plan de tratamiento de riesgo

Nivel de Riesgos	Política para la toma de acciones
Extremo	Riesgo no aceptable
Alto	Riesgo no deseable
Relevante	Riesgo aceptable
Moderado	Riesgo aceptable
Bajo	Riesgo aceptable

Fuente: Elaboración propia

En el siguiente cuadro se listan las actividades del plan de tratamiento de riesgo:

Tabla N°16. Actividades de plan de tratamiento de riegos

Actividades	Recursos generales y financieros	Responsabilidades
Reunión con el consejo directivo para la aprobación del plan de seguridad de la información	Oficina Presidencia del club	Consejo directivo y bachiller encargado del desarrollo del proyecto.
Reunión para implementar el tratamiento de los riesgos a mitigar.	Oficina Presidencia del club	Jefe de sistemas, bachiller encargado del proyecto
Reuniones del comité de seguridad de la información	Oficina de administración del club	Jefe de sistemas, bachiller encargado del proyecto.

Fuente: Elaboración propia

A continuación, listamos los 30 riesgos que se tomaran en cuentan para el tratamiento de riesgos, cabe mencionar que seleccionamos los riesgos de valor “Alto” y “Extremo”.

Tabla N° 17. Lista de riesgos no aceptables

MATRIZ DE RIESGO						
ID de riesgo	ACTIVO	VULNERABILIDAD	AMENAZA	Posibilidad de la que la amenaza explote la vulnerabilidad	Impacto estimado en la Institución	Nivel de Riesgo
R1	Computadora de escritorio	Mala seguridad de contraseñas	Divulgación de la información	Muy alto	Muy alto	Extremo
R3	Computadora de escritorio	Falta de backups	Sustracción de la información o equipo	Muy alto	Muy alto	Extremo
R4	Computadora de escritorio	Falta de cierre de sección al dejar el trabajo	Manipulación de información	Muy alto	Alto	Extremo
R5	Computadora de escritorio	Sensibilidad a la humedad,	Polvo, corrosión,	Muy alto	Muy alto	Extremo

		polvo o calor	congelamiento			
R6	Computadora de escritorio	Susceptibilidad a variaciones de energía	Perdida de suministro de energía	Alto	Muy alto	Extremo
R7	Licencia de Microsoft Windows 7	Falta de mecanismo de autenticación e identificación de usuarios	Abuso o forzado de derechos	Alto	Muy alto	Extremo
R9	Licencia de Microsoft Windows 7	Servicios innecesarios para el usuario	Procesamiento ilegal de los datos	Alto	Muy alto	Alto
R10	Licencia de Microsoft office 2013	Falta de mecanismo de autenticación e identificación de usuarios	Abuso o forzado de derechos	Alto	Muy alto	Extremo
R12	Licencia de Microsoft office 2013	Servicios innecesarios para el usuario	Procesamiento ilegal de los datos	Alto	Muy alto	Alto
R13	Antivirus	Interfaz de usuario complicado	Error en el uso del software	Alto	Alto	Alto
R15	Antivirus	Funciones del antivirus obsoletas	Licencia caducada	Alto	Medio	Alto
R17	Email (Outlook)	Falta de backup	Manipulación de información	Alto	Alto	Alto
R18	Email (Outlook)	Defectos en el funcionamiento del software	Abuso de derechos	Alto	Alto	Alto
R19	Página web del club	Mala gestión de contraseña	divulgación de la información	Muy alto	Alto	Extremo
R21	Sistema de cobranzas	Mala gestión de usuarios del sistema	Adulteración de la información	Alto	Muy alto	Extremo
R22	Sistema de cobranzas	Falta de backup	Robo de información o del sistema	Alto	Muy alto	Extremo

R23	Sistema de cobranzas	Defectos en el funcionamiento del software	Abuso de derechos	Alto	Alto	Alto
R24	Cableado ethernet	Trafico de información desprotegido	Escuchar información ilegalmente	Alto	Alto	Alto
R25	Cableado ethernet	Cableado desprotegido	Falla en los equipos de red	Alto	Muy Alto	Extremo
R27	Cableado ethernet	Gestión inadecuado de la red	Saturación de los sistemas de información	Alto	Alto	Alto
R28	red de informática (carpeta compartidas)	Falta de controles en el traspaso de información	Robo de documentos o de equipos tecnológicos	Alto	Muy alto	Extremo
R29	red de informática (carpeta compartidas)	Falta de privilegios en los permisos	Manipulación de información	Muy alto	Muy alto	Extremo
R30	red de informática (carpeta compartidas)	Mala seguridad de contraseñas	Manipulación de información	Alto	Alto	Alto
R31	red de informática (carpeta compartidas)	Gestión inadecuado de la red	Saturación de los sistemas de información	Alto	Alto	Alto
R32	red de informática (carpeta compartidas)	Conexiones de red desprotegidas	Uso no autorizado de los equipos de red	Alto	Alto	Alto
R33	Llave de ingreso	Acceso a instalaciones sin permisos	Destrucción o robos de equipos o medios de comunicación	Alto	Muy alto	Extremo
R34	Comprobante de ingreso de caja (boletas, facturas, etc)	Falta de mecanismo de backup	Robo o manipulación del activo	Alto	Alto	Alto
R35	Comprobante de ingreso de caja (boletas,	Falta de cuidado en el transporte o en	Robo o manipulación del activo	media	Alto	Alto

	facturas, etc)	su transferencia				
R36	Comprobante de ingreso de caja (boletas, facturas, etc)	Pocos o nulos controles de acceso	Robo o manipulación del activo	Media	Alto	Alto
R37	Fichas de socios	Falta de mecanismo de backup	Robo o manipulación del activo	Alto	Alto	Alto
R38	Fichas de socios	Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	media	Alto	Alto
R39	Fichas de socios	Pocos o nulos controles de acceso	Robo o manipulación del activo	Media	Alto	Alto
R40	Base de datos SQL	Mala gestión de acceso a la BD	Adulteración de la información	alto	Muy alto	Extremo
R41	Base de datos SQL	Falta de backup	Robo o manipulación de la información	alto	Muy alto	extremo
R42	Base de datos SQL	Defectos en el funcionamiento del software	Abuso de derechos	medio	Alto	Alto

Fuente: Elaboración propia

3.1.3.2.4. Controles para el Tratamiento de riesgos

Procedemos a definir las políticas de seguridad para el tratamiento de riesgos que se identificaron anteriormente, en la siguiente tabla:

Tabla N° 18. Políticas de seguridad

DOMINIOS	CATEGORIA DE SEGURIDAD	NOMBRE DEL CONTROL	DESCRIPCION
Políticas de seguridad	**Directrices de la dirección en seguridad de la información**	**Conjunto de políticas para la seguridad de la información**	Se debe definir un conjunto de políticas para la seguridad de la información, aprobado por el consejo directivo mediante sesión de consejo, difundido a todos los jefes de área y sus colaboradores, asociados.
		Revisión de las políticas para la seguridad de información	Se debe planificar la revisión de las políticas de seguridad de información en forma constante para garantizar su efectividad.
Aspectos organizativos de seguridad de la información	**Organización interna**	**Asignación de responsabilidades para asegurar la información**	Se debe definir y asignar detalladamente todas las responsabilidades para el cumplimiento de las normas de seguridad de la información.
		Segregación de tareas	Se debe separar las tareas y áreas de responsabilidad para que trabajen con independencia ante posibles conflictos de interés, con la finalidad de minimizar las oportunidades de modificaciones no autorizadas o el de un mal uso de los activos de la institución.
		Seguridad en la información en la gestión de	Toda planificación de proyectos de la institución debe estar enfocada en la

		proyectos	seguridad de la información con el fin de garantizar la confidencialidad e integridad del proyecto.
Gestión de activos	**Responsabilidad sobre los activos**	**Inventario de activos**	Todos los activos deben estar claramente identificados, relevando un inventario con lo más importante.
		Propiedades de los activos	Todos los activos de información de la institución deben ser controlados y resguardados por un área designada en la institución.
		Uso aceptable de los activos	Se deben implantar mecanismos de regulación para el uso adecuado de la información.
		Devolución de activos	Todo los empleados, colaboradores, asociado, terceras partes deberían devolver todo activo de información que este en su poder, una vez finalizado el contrato, acuerdo o actividades relacionadas con la institución.
	Clasificación de la información	**Directrices de la información**	Los activos de información se deben clasificar en cuanto a su valor, sensibilidad y criticidad para la institución,
		Etiquetado y manipulación de	Se debería desarrollar e implantar conjunto de procedimientos para el

		la información.	etiquetado y uso de la información, de acuerdo al esquema de clasificación adoptado por la institución.
		Manipulación de activos	Se deberían desarrollar e implementar procedimientos para la manipulación de los activos de acuerdo al esquema de clasificación adoptado por la institución.
Gestión de incidentes	**Gestión de incidentes de seguridad de la información y**	**Responsabilidad y procedimientos**	Se debe definir las responsabilidades y procedimientos de gestión para asegurar una respuesta ágil, eficaz y ordenada ante los incidentes de seguridad de la información.
		Notificación de los eventos de seguridad de la información	Los eventos de seguridad de la información deben ser comunicados en el menor tiempo posible utilizando los medios adecuados.
		Notificación de puntos débiles de la seguridad	Se debería comunicar sobre cualquier punto débil en la seguridad de la información a todos los empleados e involucrados que utilizan el sistema y servicios de información de la institución.
		Aprendizaje de los incidentes de seguridad de la	Se debe utilizar el conocimiento adquirido del análisis y la resolución de los

	mejoras	**información**	incidentes de seguridad de la información para reducir la probabilidad en el futuro.
		Recopilación de evidencias	Se debe definir y aplicar los procedimientos para la identificación y preservación de los activos de información que puedan servir de evidencia a posibles estudios.
Cumplimiento	**Cumplimiento de los requisitos legales y contractuales**	**Derechos de propiedad intelectual**	Se debe definir procedimientos que garanticen el cumplimiento de respeto de los derechos de propiedad intelectual. Utilizar software original.
		Protección de los registros de la organización	Todos los registros de información de la institución deben estar protegidos ante cualquier tipo de amenaza
		Protección de datos y privacidad de la información personal	Se debe asegurar la protección y privacidad de la información personal según lo requiere la legislación y las normativas vigentes. Resguardar la información del personal que labora dentro de la institución.
	Revisiones de la seguridad de la información	**Comprobación del cumplimiento**	Los sistemas de información deben ser revisados constantemente para verificar el cumplimiento de la políticas y normas de seguridad dispuestas

			por la institución
Seguridad en la operativa	**Responsabilidades y procedimientos de operación**	**Documentación de procedimiento de operación**	Se debe documentar los procedimientos operativos y dejar a disposición de los usuarios facultados a su uso.
	Protección contra código malicioso	**Controles contra el código malicioso**	Se debe implementar controles para la detección, prevención y recuperación ante cualquier afectación de malware en conjunto con la concientización de los usuarios.
	Copias de seguridad	**Copias de seguridad de la información**	Se debe realizar copias de respaldo periódicamente (backup)
Control de accesos	**Gestión de acceso de usuario**	**Revisión de los derechos de acceso de los usuarios**	Las autoridades responsables de la custodia de los activos deben revisar con frecuencia los derechos de acceso de todos los usuarios.
		Retirada o adaptación de los derechos de acceso	Se deben quitar los accesos a todo los empleados, colaboradores e involucrados a la información que ya no estén laborando en la institución. A si como la restricción a las instalaciones donde se custodian la información.

Fuente: Elaboración propia

Luego de definir las políticas de seguridad, procederemos a realizar un listado de los controles para el tratamiento de riesgos. La elaboración del cuadro de controles para el tratamiento de riesgos se elabora de la siguiente manera, cada columna significa:

- **Clausula**: se refiere al dominio de los controles de la norma ISO 27002.
- **Categoría de seguridad**: es el nombre del objetivo de control de la lista de controles según la norma ISO 27002.
- **Nombre del control**: control de la lista 114 controles de la norma ISO 27002.
- **Descripción**: son las actividades que se realizan en cada control.
- **Riesgos a controlar**: son los riesgos que se van a tratar y está representado por la letra R seguido del número del riesgo según el orden que se le asigno anteriormente. (ver tabla N° 12)

TABLA N° 19. Controles para el tratamiento de riesgos

CLAUSULA	CATEGORIA DE SEGURIDAD	NOMBRE DE CONTROL	DESCRIPCION	RIESGOS A CONTROLAR	ADAPTACION AL CLUB
	Áreas seguras	Seguridad de oficinas, despachos y recursos	Se debe reforzar la seguridad de las oficinas, ambientes e instalaciones de la institución.	R3, R22, R28, R33, R34, R36, R37, R39, R40, R41	Se debería realizar el cambio del sistema de seguridad de las oficinas e instalaciones donde se resguarde información. (Cambio de chapas y lacrado de llaves).
		Instalación de suministros	Los equipos deben estar protegidos contra cortes de luz y otras interrupciones por fallas de suministro de energía	R6	Todos los equipos deben tener estabilizador de energía, para protegerse ante cualquier cambio en el voltaje. El club debe contar con un generador de energía ante cualquier falta de la misma.
			Los cables de		El cableado de red del club

Seguridad física y ambiental	Seguridad de los equipos	Seguridad de cableado	energía y telecomunicaciones que transporta datos o apoyan a los servicios de información deben estar protegidos contra la intercepción o interferencia.	R6, R24, R25, R27	debe ser restructurado y mapeado para el reconocimiento de los puntos de red.
		Mantenimiento de los equipos	Los equipos deberían mantenerse adecuadamente con el fin de garantizar su eficiencia y continuidad	R5, R6, R23	Los equipos del club deben de tener un mantenimiento periódico debido a la humedad que existe por la cercanía al mar.
		Salida de activos fuera de las dependencia de la empresa	Los equipos de información o el software no deben ser retirados del sitio sin autorización.	R3	Los equipos informáticos no deben salir del club sin la autorización de la administración o del consejo directivo.
		Equipo informático de usuario desatendido	Los usuarios se deberían de asegurar que los equipos no supervisados cuenten la protección adecuada.	R4, R5	Los trabajadores del club deben de comunicar al jefe de sistemas o al administrador alguna falla en los equipos informáticos o pedir que sean verificados antes de su uso.
		Política de puesto de trabajo despejado y bloqueo de pantalla	Se debería adoptar una política de puesto de trabajo despejado para documentación de papel y para medios de almacenamiento extraíbles y una política de monitores sin información para las instalaciones.	R4	Se debería de optar en el club una política de puesto de trabajo despejado para la documentación y otra para medios de almacenamiento extraíbles.
	Gestión en la seguridad de redes.	Controles de red	Se deben administrar y controlar las redes para proteger la información	R31	Se deben definir políticas respecto al uso de redes, donde solo las personas autorizadas de la red del club puedan manejar. Se deben crear acceso restringidos para

					las carpetas compartidas.
Seguridad en las telecomunicaciones	Intercambio de información con partes externas	Políticas y procedimientos de intercambio de información	Se deben fijar políticas, procedimientos y controles de transferencia de información para proteger su integridad y confidencialidad.	R21, R23, R18, R28, R31, R35, R38,	Se debe implementar controles y procedimientos que permitan a un usuario de la red del club asegurar la transferencia de información y no falle en ningún momento.
		Mensajería electrónica	Se debería resguardar adecuadamente la información adjunta en la mensajería electrónica.	R22	Los responsables de resguardo de información deben realizar los backup del contenido en los correos electrónicos de manera constante.
		Acuerdos de confidencialidad y secreto	Se debería identificar revisar y documentar los acuerdos de confidencialidad y no divulgación de información de la institución	R1, R2, R22, R28, R34, R37, R41	Se debe firmar documentos donde los usuario que tengan acceso a la información respeten la confidencialidad y no divulguen la información del club
Seguridad en la operativa	Protección contra código malicioso	Controles contra el código malicioso	Se debe implementar controles para la detección, prevención y recuperación ante cualquier afectación de malware en conjunto con la concientización de los usuarios.	R18	La detección del código malicioso en los sistemas de la red del club se debe tratar con la identificación de estos posibles códigos y el uso adecuado de controles para el acceso a los sistemas.
	Copias de seguridad	Copias de seguridad de la información	Se debe realizar copias de respaldo periódicamente (backup)	R3, R17, R22, R34, R37, R41	Se debe realizar backup de información periódicamente, los mismos que deben ser guardados en dispositivos de almacenamiento y custodiados en un lugar distinto al club. Garantizando la total recuperación de la misma ante cualquier tipo de desastre o falla de los medios de almacenamiento.
			Se debe realizar y revisar		

	Registro de actividad y supervisión	Registro y gestión de eventos de actividad	periódicamente los registros relacionados a eventos de actividad del usuario, excepciones, fallas y evento de seguridad de la información.	R21	El club debe promover auditorias y eventos de seguridad de información con el fin de guardar los registros para futuras investigaciones.
	Consideraciones de las auditorias de los sistemas de información	Controles de auditoria de información	Se deben planificar y acordar actividades de auditoria con el fin de evaluar y verificar los sistemas operacionales y así minimizar las interrupciones en los procesos de negocio	R13, R25	Se debe ejecutar las auditorias necesarias para medir la seguridad de los sistemas operacionales del club con la finalidad de no interrumpir los procesos de negocio.
Control de accesos	Requisitos de negocio para el control de acceso	Control de acceso a las redes y servicios a los asociados	Se debe brindar a los usuarios accesos a las redes y los servicios según su rol en la institución.	R32	Se debe definir una política de acceso a los usuarios a la red según las funciones que hayan sido asignadas
	Gestión de acceso de usuario	Gestión de altas bajas en el registro de usuarios	Debe existir un procedimiento formal para dar de alta y baja a los usuarios con el fin de brindarles acceso según su función.	R9, R12, R19, R29, R30, R36, R39	En el club debe aplicar un procedimiento formal para dar de alta y baja a los usuarios con el fin de brindarles acceso según su función.
		Retirada o adaptación de los derechos de acceso	Se deben quitar los accesos a todo los empleados, colaboradores e involucrados a la información que ya no estén laborando en la institución. A si como la restricción a las instalaciones donde se custodian la información.	R1, R29, R33	Se deben quitar los accesos a todo los empleados, colaboradores e involucrados a la información que ya no estén laborando en la institución. A si como la restricción a las instalaciones donde se custodian la información.
			Se debe restringir el acceso de los		Se debe establecer una política de restricción de

	Control de acceso a sistemas y aplicaciones	Restricción del acceso a la información	usuarios y el personal de mantenimiento a la información, en relación a la política de control de acceso definida.	R21	acceso a los usuarios o personal que maneja los sistemas de acuerdo a la función que cumplen dentro del club.
		Gestión de contraseña de usuario	Los sistemas de gestión de contraseñas deberían ser interactivos y asegurar contraseñas de difícil acceso	R1, R19, R30, R40	El jefe de sistemas con conocimiento y aprobación del administrador deberá proporcionar las contraseñas correspondientes para acceder a los sistemas. Este incluye la generación y cambio de las mismas

Fuente: Elaboración propia

3.1.3.2.5 Plan de Comunicaciones

Tabla N° 20. Matriz de comunicaciones del Proyecto

Responsable de la comunicación	Información a comunicar	Medio de comunicación	Idioma	Destinatarios de la comunicación	Frecuencia
- Implementador SGSI (PM)	Iniciación. Acta de constitución del proyecto.	Informe escrito, enviado por correo electrónico y presentado en reunión presencial.	Castellano	Todos los involucrados en los procesos tecnológicos.	Al inicio.
- Implementador SGSI (PM) - Consejo directivo	Aprobación del alcance del proyecto	Informe escrito, enviado por correo electrónico y presentado en reunión presencial.	Castellano	Todos los involucrados en la realización del proyecto.	Al inicio.
- Implementador SGSI (PM)	Estado de avance del proyecto. (alcance, tiempo y coste)	Informe escrito, enviado por correo electrónico y presentado en reunión presencial.	Castellano	Consejo Directivo. Comité de SGSI.	semanal
- Implementador SGSI (PM)	Listado de tareas y recursos necesarios. Estado del proyecto.	Cronograma MS Project enviado por correo electrónico.	Castellano o ingles	Todos los involucrados en la realización del proyecto.	semanal
- Todos los involucrados en	Cambio de	Formulario solicitud	Castellano	Implementador	Siempre

el proyecto	alcance, tiempo o coste	de cambio.		SGSI	que sea necesario
- Implementador SGSI (PM)	Convocatorias reuniones.	Correo electrónico.	Castellano	Todos los involucrados en la realización del proyecto.	Siempre que el PM lo considere necesario
- Implementador SGSI (PM)	Seguimiento del proyecto.	Correo electrónico y reunión presencial.	Castellano	Equipo implementador.	semanal

Fuente: Elaboración propia

3.1.3.2.6 Plan de Continuidad de negocio.

A continuación se lista una serie de pilares que garantizarán la continuidad de las actividades de negocio de la institución.

- **PROCEDIMIENTOS DE BACKUP**

Archivos que deben tener copias de respaldo:

- Backups del Sistema Operativo.
- Backups del Software Aplicativo.
- Backups de los Datos y de estructura de datos.
- Backups de archivos de usuarios (Archivos utilizados por el personal del Club).

Especificaciones y normas para la elaboración de los backups:

Para backups de Sistemas Operativos y Software aplicativos

- Los backups de los Sistemas Operativos deberán estar almacenados en disco duros externos debidamente etiquetados.
- Las claves de instalación de los diferentes Sistemas deberán ser administradas por el Administrador de la Base de Datos y proporcionada

al personal de soporte técnico cada vez que sea necesario manteniendo un registro sobre las instalaciones realizadas.

- La ubicación de resguardo de dichos backups será la oficina de Sistemas de Información que cuenta con las condiciones apropiadas para el mantenimiento de los medios.
- La frecuencia de obtención de estos backups deberá ser semanal o cada vez que se deteriore el medio de almacenamiento de los mismos.

Para Backups de datos

- Los backups de datos y de estructura de las bases de datos deberán realizarse para cada base de datos que se encuentre a cargo del área de Sistemas.
- Los backups de datos deberán elaborarse según su importancia de la siguiente manera:
  - ✓ Backups completos diarios en épocas críticas como inscripciones y backups día por medio en épocas normales y borrado de los backups anteriores semanalmente.
  - ✓ Backups completos semanales y borrado de los backups anteriores mensualmente.
- Los backups se guardan en dos lugares fijos distintos, en el directorio backups del disco donde se halla el motor y en un directorio creado para tal fin, en alguna de las máquinas de la red.
- Para todos los servidores copiar los últimos backups de cada semana y traspasarlos a un dispositivo de almacenamiento; cada mes se debe enviar el último a bóveda.

Backups de archivos de usuarios

- Los archivos de usuarios se almacenarán en un disco duro bajo la responsabilidad del personal de Sistemas y en base a la siguiente configuración de carpetas: [Fecha]/[Nombre Departamento]/[Nombre Usuario].
- La nomenclatura de los subdirectorios del usuario se realizará según la información que almacene el usuario.
- Se obtendrán backups de archivos de usuarios mensualmente para todos los usuarios de la red de la institución.
- Se verificará la información que se almacene, íntegramente, tanto el original como las copias (en caso de encontrarse empaquetada, desempaquetarla como comprobación). Asimismo, debe verificarse que la información no esté contaminada con virus informático.

Medidas de seguridad

- Se grabará el trabajo que se está realizando cada cierto tiempo (10 - 20 minutos aproximadamente).
- Si se está trabajando con USB, antes de hacer uso de otro, se debe cerrar el archivo, de lo contrario perderá la información.
- Si su archivo está en USB y va a trabajar más de una hora, se recomienda copiarlo al disco duro y trabajar en él, una vez concluido el trabajo levante su información al USB y bórrelo del disco duro.
- Se hará un análisis antivirus de los dispositivos de almacenamiento cada vez que se conecten al CPU.

- Para retirar el USB o disco duro externo se debe expulsar el dispositivo de la barra de herramientas.
- Sólo el personal responsable de la seguridad de los archivos tendrá acceso al ambiente donde se encuentren estos medios.
- Antes de descolgar el servidor de la red el Jefe de Sistemas debe enviar con 15 minutos de anticipación un mensaje a los usuarios para que salven su información.

- **BORRADO SEGURO DE LA INFORMACIÓN**

No sólo para cumplir con la Ley será necesario destruir la información de forma segura, sino también cuando queramos borrar datos privados o confidenciales de equipos que ya no se vayan a utilizar más.

Existen múltiples herramientas gratuitas y de pago, para realizar un formateo completo de varias pasadas (2 o 3) que será más que suficientes para eliminar de forma segura la información.

- **RECUPERACIÓN DE DATOS**

El jefe de Sistemas es el responsable de la recuperación de toda la información que pudiera ser almacenada tanto en discos duros como en medios extraíbles y demás soportes, en caso de que se produzca un incidente de seguridad tanto a nivel lógico como a nivel físico.

- **INFRAESTRUCTURAS**

Técnicas y herramientas destinadas a facilitar el despliegue rápido de la infraestructura de la organización, ya que se encuentra respaldada en caso de pérdida.

De esta manera se consigue disminuir el tiempo de interrupción de la actividad de la empresa.

- **VIRTUALIZACIÓN**

Tecnología que engloba diferentes mecanismos que incrementan la seguridad de los sistemas.

La virtualización se puede aplicar a aplicaciones, servidores, almacenamiento y redes, permitiendo un mejor y más rápido aprovisionamiento de aplicaciones y recursos ante desastres, consiguiendo así una mayor eficiencia y reducción de costes gracias también a la escalabilidad que aporta.

- **GESTIÓN Y CONTROL DEL TRÁFICO**

Permitirá al Club tener el control en tiempo real del tráfico saliente y entrante de la red. De esta forma se realiza un control de las infraestructuras de comunicaciones vigilando el correcto uso del ancho de banda basándonos en la política de seguridad establecida.

Mediante herramientas específicas será posible bloquear y limitar el tráfico P2P, mensajería instantánea, VOIP y otras muchas aplicaciones que hacen uso de la red, limitando así el acceso de usuarios a dichos servicios a la vez que se controla la información que se transmite.

- **MONITORIZACIÓN**

Se centra en la vigilancia en tiempo real de las infraestructuras de comunicación, pudiendo detectar una utilización inadecuada de servicios, fallos en el sistema, sobrecargas, averías.

3.1.3.2.7 Gestión del conocimiento

En la siguiente tabla, se lista las experiencias adquiridas en la implementación del presente proyecto.

Tabla N° 21. Experiencias adquiridas en la implementación del proyecto

Experiencias adquiridas en la implementación del Proyecto en el Club
Realización de un proyecto real.
Ampliación de mis conocimientos en Seguridad de la Información.
Experiencia laboral.
Capacidad de investigación y de trabajo individual.
Capacidad de trabajo en equipo y dirección.
Capacidad de análisis de riesgos de activos de información.
Ampliación de conocimientos en metodologías PMI, PMBOK.
Capacidad de realizar cronogramas de trabajo.
Confianza para asumir nuevos retos.
Concientización de la importancia un Plan de Seguridad de la Información.
Satisfacción Personal.

Fuente: Elaboración propia

3.2. Resultados

Como resultado de la implementación del presente Plan de Seguridad de la Información, se obtuvieron políticas de seguridad de la información y controles para el tratamiento de riesgos, como se detallan en las tablas N° 13 y 14 respectivamente. Los cuales fueron definidos según la complejidad del Club Asociación Civil Centro Cultural Deportivo Lima y de acuerdo a sus necesidades y objetivos de negocio.

A continuación se presenta la tabla de Objetivos vs. Indicadores

Tabla N° 22. Objetivos Vs. Indicadores

Objetivos	Indicadores (%)	Formula	Meta
Implementar políticas, normativas y procedimientos para optimizar la protección de los activos informacionales de la Asociación Civil Centro Cultural Deportivo Lima.	Colaboradores que conocen la política de seguridad de información	N° Colabor. conocen / N° Total Colaborador	100%
	Colaboradores que cumplen la política de seguridad de información	N° Colabor. cumplen / N° Total Colaborador	75%
Identificar y evaluar los riesgos de seguridad de la información para optimizar la protección de los activos informacionales de la Asociación Civil Centro Cultural Deportivo Lima	Numero de activos con criticidad alta adecuadamente identificados.	N° de activos con criticidad alta / Total de activos de informacion	46%
Controlar, prevenir y/o mitigar los riesgos identificados para optimizar la protección de los activos informacionales de la Asociación Civil Centro Cultural Deportivo Lima.	Riesgos con nivel de tolerancia “Aceptable”	N° Riesgos Aceptabl / N° Total de riesgos	71%
	Riesgos con nivel de tolerancia “No Aceptable”	N° Riesgos No acept / N° Total de riesgos	29%

Fuente: Elaboración propia

En la siguiente tabla, se presenta el resultado de la medición de los indicadores antes y después de la implementación del proyecto, según información recopilada de a través de las herramientas de recopilación: encuestas, reuniones y observaciones.

Tabla N° 23. Resultado de indicadores antes y después

Indicadores (%)	Antes	Después
Colaboradores que conocen la política de seguridad de información	10%	100%
Colaboradores que cumplen la política de seguridad de información	10%	75%
Numero de activos con criticidad alta adecuadamente identificados.	25%	46%
Riesgos con nivel de tolerancia “Aceptable”	30%	71%
Riesgos con nivel de tolerancia “No Aceptable”	5%	0%

Fuente: Elaboración propia

De la tabla se concluye lo siguiente:

- Se muestra que los trabajadores o colaboradores han tomado conocimiento de la política de Seguridad de la Información.
- La mayoría de los trabajadores cumplen con las políticas definidas de Seguridad de la Información.
- Aumentó la eficiencia en la identificación de amenazas y daños potenciales.
- Los riesgos con nivel de tolerancia aceptable han aumentado, reduciendo los niveles de no aceptación.

Y sobre todo lo más importante el club Asociación Civil Centro Cultural Deportivo Lima, ha adoptado mecanismos de seguridad de la información que le

permitirá accionar flexiblemente ante cualquier tipo de fraude como el sufrido a fines del año 2017, donde se perdió mucho dinero en la recuperación de los sistemas de información sustraídos.

CONCLUSIONES

- La implementación de políticas de seguridad y que los colaboradores o involucrados la conozcan, son de gran utilidad para optimizar la protección de los activos de información, ya que les aporta de conocimientos para el buen manejo y uso de los activos.
- La identificación y evaluación de los riesgos a los que están expuesto los activos de información, sirven para identificar adecuadamente los riesgos de mayor impacto o criticidad, y posteriormente actuar mediante un plan de tratamiento de riesgos asegurando la protección de los activos informacionales.
- El prevenir, controlar y mitigar los riesgos identificados forman parte del plan de tratamiento de riesgos, el cual sirve para reducir a niveles aceptables gran porcentaje de los riesgos que afecten a los activos de información, optimizando la protección de los mismos.
- La identificación de los procesos de negocio de la Organización nos permite establecer el alcance y la delimitación para el desarrollo del Plan de Seguridad de la Información. Alineando las directrices del SGSI con los objetivos estratégicos de la empresa y así asegurar la continuidad del negocio e incremento de la rentabilidad.
- Los recursos humanos son muy importantes para la implementación de cualquier sistema de gestión organizacional, por lo que es indispensable la formación y concientización de los mismos para lograr una implementación exitosa.

RECOMENDACIONES

- Es necesario que la alta dirección no pierda el compromiso de dar seguimiento constante al funcionamiento del SGSI y mantenerlo actualizado con la finalidad de alcanzar la excelencia y a futuro lograr la certificación en Seguridad de la información ISO 27001.
- Es necesario que la institución incluya dentro de su presupuesto anual, la implementación de los controles del SGSI, así como para las capacitaciones y charlas de concientización, los servicios de consultoría y las revisiones anuales que se darán para asegurar la continuidad del sistema.
- Se recomienda que el personal a contratar tenga los conocimientos acerca de SGSI y que se cumpla con las capacitaciones de seguridad de la información ya programadas, para así lograr que todos los involucrados con los activos de información tengan claros los alcances del sistema.
- Es necesario incluir en la agenda de Asamblea General Ordinaria de asociados, la elección de los miembros que conformarán el Comité de Seguridad de la Información con autonomía a la estructura organizacional del Club, el cual sirva como ente regulador y fiscalice el fiel cumplimiento de las normas, políticas y procedimientos de Seguridad de la información.
- Adicionalmente, se recomienda evaluar el uso de COBIT como marco de trabajo para la gestión del SGSI, de igual manera, se podría incluir la gestión de servicios de TI, según el enfoque de ITIL, ambos en sus últimas versiones.

REFERENCIAS BIBLIOGRÁFICAS

- Aguirre, D. (2014). *Diseño de un sistema de gestión de seguridad de información para servicios postales del Perú S.A.* Tesis de licenciatura, Facultad de Ciencias e Ingeniería, Universidad Católica del Perú. Lima, Perú.
- Ampuero, C. (2011). *Diseño de un sistema de gestión de seguridad de información para una compañía de seguros*. Tesis de licenciatura, Facultad de Ciencias e Ingeniería, Universidad Católica del Perú. Lima, Perú.
- Barrantes, C; Hugo, J. (2012). *Diseño e implementación de un Sistema de Gestión de Seguridad de Información en Procesos Tecnológicos.* Facultad de Ingeniería y Arquitectura, Universidad de San Martin de Porres. Lima, Perú.
- González, J. (2002). "La verdad sobre eficiencia, eficacia y efectividad". En *Monografías*. Consultado el 18 de Abril de 2018. Disponible en http://www.monografias.com/trabajos11/veref/veref.shtml.
- ISO 22301. En *ISO27000.es.* Consultado el 15 de Junio de 2018. Disponible en http://www.iso27000.es/.
- ISO 27000 (2012). "Sistema de Gestión de la Seguridad de la Información". En *ISO27000.es.* Consultado el 15 de Marzo de 2018. Disponible en http://www.iso27000.es/.
- ISO 27001. En *ISO27000.es.* Consultado el 15 de Marzo de 2018. Disponible en http://www.iso27000.es/.
- ISO 31001. En *ISO27000.es.* Consultado el 15 de Junio de 2018. Disponible en http://www.iso27000.es/.
- Leyva, R. (2016). *Diseño de un Sistema de Gestión de Seguridad de la Información basado en las Normas ISO/IEC 27001 e ISO/IEC 27002 para*

proteger los activos de información en el proceso de suministros de medicamentos de la Red de Salud de Lambayeque 2015. Facultad de Ciencias Físicas y Matemáticas, Universidad Nacional Pedro Ruiz Gallo. Lambayeque, Perú.

- Martínez, I.; Cruz, Y.; Rodríguez, G., et al. (2013). "Validez y confiabilidad de la información". En *Calameo.* Consultado el 18 de Abril de 2018. Disponible en https://es.calameo.com/read/002592668a91184da7ebd
- Pallas, G. (2009). *Metodología de implantación de un SGSI en un grupo empresarial jerárquico.* Facultad de Ingeniería, Universidad de la Republica. Montevideo, Uruguay.
- Salcedo, R. (2014*). Plan de implementación del SGSI basado en la norma ISO 27001:2013 para ISAGXXX.* Universidad Oberta Catalunya. Barcelona, España.
- Shoaib, K. "Definición de certificación ISO". En *EHOW en español.* Consultado el 17 de Abril de 2018. Disponible en https://www.cuidatudinero.com/13098517/definicion-de-certificacion-iso
- Vásquez, J; De la Cruz, C. (2008). *Elaboración y aplicación de un sistema de gestión de la seguridad de la información (SGSI) para la realidad tecnológica de la USAT.* Facultad de Ingeniería, Universidad Católica Santo Toribio de Mogrovejo. Chiclayo, Perú.
- Velasco, H. (2008). *Diseño del sistema de gestión de seguridad de la información que permita apoyar a la subgerencia de informática y tecnología de la empresa de telecomunicaciones de Bucaramanga Telebucaramanga S.A – E.S.P en el proceso de certificación en ISO 27000.* Tesis de

licenciatura, Facultad de Ingeniería Informática, Universidad Pontificia Bolivariana, Medellín, Colombia.

- Villena, M. (2006). *Sistema de Gestión de Seguridad de Información para una institución financiera.* Tesis de licenciatura, Facultad de Ciencias e Ingeniería, Universidad Católica del Perú. Lima, Perú.

ANEXOS

Anexo 01: Estructura de ISO27002.

Dominios Contemplados:

- Políticas de Seguridad
- Aspectos Organizativos de la Seguridad de la información
- Seguridad ligada a los recursos humanos
- Gestión de activos
- Control de accesos
- Cifrado
- Seguridad Física y Ambiental
- Seguridad en la Operativa
- Seguridad en las Telecomunicaciones
- Adquisición, desarrollo y mantenimiento de los sistemas de información
- Relaciones con Suministradores
- Gestión de incidentes en la Seguridad de la información
- Aspectos de la Seguridad de la Información en la gestión de la continuidad del negocio
- Cumplimiento

Controles:

A. Políticas de Seguridad

5.1 Directrices de la Dirección en seguridad de la información

Actividades de control del riesgo:

5.1.1 Políticas para la seguridad de la información

5.1.2 Revisión de las políticas para la seguridad de la información

B. Aspectos Organizativos de la Seguridad de la información

6.1 Organización Interna

Actividades de control del riesgo:

6.1.1 Asignación de responsabilidades para la seguridad de la información

6.1.2 Segregación de tareas

6.1.3 Contacto con las autoridades

6.1.4 Contacto con grupos de interés especial

6.1.5 Seguridad de la información en la gestión de proyectos

6.2. Dispositivos para movilidad y teletrabajo

Actividades de control del riesgo

6.2.1 Política de uso de dispositivos para movilidad

6.2.2 Teletrabajo

C. Seguridad ligada a los recursos humanos

7.1 Antes de la contratación

Actividades de control del riesgo:

7.1.1 Investigación de antecedentes

7.1.2 Términos y condiciones de contratación

7.2. Durante la contratación

Actividades de control del riego:

7.2.1 Responsabilidades de gestión

7.2.2 Concienciación, educación y capacitación en seguridad de la información

7.2.3 Proceso disciplinario

7.3. Cese o cambio de puesto de trabajo

Actividades de control del riego:

7.3.1. Cese o cambio de puesto de trabajo

D. Gestión de activos

8.1. Responsabilidad sobre los activos

Actividades de control del riesgo:

8.1.1 Inventario de activos

8.1.2 Propiedad de los activos

8.1.3 Uso aceptable de los activos

8.1.4 Devolución de activos

8.2. Clasificación de la información

Actividades de control del riego:

8.2.1 Directrices de clasificación

8.2.2 Etiquetado y manipulado de la información

8.2.3 Manipulación de activos

8.3. Manejo de los soportes de almacenamiento

Actividades de control del riego:

8.3.1 Gestión de soportes extraíbles

8.3.2 Eliminación de soportes

8.3.3 Soportes físicos en tránsito

E. Control de accesos

9.1. Requisitos de negocio para el control de accesos

Actividades de control del riesgo:

9.1.1 Política de control de accesos

9.1.2 Control de acceso a las redes y servicios asociados

9.2. Gestión de acceso de usuario

Actividades de control del riesgo:

9.2.1 Gestión de altas/bajas en el registro de usuarios

9.2.2 Gestión de los derechos de acceso asignados a usuarios

9.2.3 Gestión de los derechos de acceso con privilegios especiales

9.2.4 Gestión de información confidencial de autenticación de usuarios

9.2.5 Revisión de los derechos de acceso de los usuarios

9.2.6 Retirada o adaptación de los derechos de acceso

9.3. Responsabilidades del usuario

Actividades de control del riesgo:

9.3.1 Uso de información confidencial para la autenticación

9.4. Control de acceso a sistemas y aplicaciones

Actividades de control del riesgo:

9.4.1 Restricción del acceso a la información

9.4.2 Procedimientos seguros de inicio de sesión

9.4.3 Gestión de contraseñas de usuario

9.4.4 Uso de herramientas de administración de sistemas

9.4.5 Control de acceso al código fuente de los programas

F. Cifrado

10.1. Controles criptográficos

Actividades de control del riesgo:

10.1.1 Política de uso de los controles criptográficos

10.1.2 Gestión de claves

G. Seguridad Física y Ambiental

11.1. Áreas seguras

Actividades de control del riesgo:

11.1.1 Perímetro de seguridad física

11.1.2 Controles físicos de entrada

11.1.3 Seguridad de oficinas, despachos y recursos

11.1.4 Protección contra las amenazas externas y ambientales

11.1.5 El trabajo en áreas seguras

11.1.6 Áreas de acceso público, carga y descarga

11.2. Seguridad de los equipos

Actividades de control del riesgo:

11.2.1 Emplazamiento y protección de equipos

11.2.2 Instalaciones de suministro

11.2.3 Seguridad del cableado

11.2.4 Mantenimiento de los equipos

11.2.5 Salida de activos fuera de las dependencias de la empresa

11.2.6 Seguridad de los equipos y activos fuera de las instalaciones

11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento

11.2.8 Equipo informático de usuario desatendido

11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla

H. Seguridad en la Operativa

12.1. Responsabilidades y procedimientos de operación

Actividades de control del riesgo:

12.1.1 Documentación de procedimientos de operación

12.1.2 Gestión de cambios

12.1.3 Gestión de capacidades

12.1.4 Separación de entornos de desarrollo, prueba y producción

12.2. Protección contra código malicioso

Actividades de control del riesgo:

12.2.1 Controles contra el código malicioso

12.3. Copias de seguridad

Actividades de control del riesgo:

12.3.1 Copias de seguridad de la información

12.4. Registro de actividad y supervisión

Actividades de control del riesgo:

12.4.1 Registro y gestión de eventos de actividad

12.4.2 Protección de los registros de información

12.4.3 Registros de actividad del administrador y operador del sistema

12.4.4 Sincronización de relojes

12.5 Control del software en explotación

Actividades de control del riesgo:

12.5.1 Instalación del software en sistemas en producción

12.6. Gestión de la vulnerabilidad técnica

Actividades de control del riesgo:

12.6.1 Gestión de las vulnerabilidades técnicas

12.6.2 Restricciones en la instalación de software

12.7. Consideraciones de las auditorías de los sistemas de información

Actividades de control del riesgo:

12.7.1 Controles de auditoría de los sistemas de información

I. Seguridad en las Telecomunicaciones

13.1. Gestión de la seguridad en las redes

Actividades de control del riesgo:

13.1.1 Controles de red

13.1.2 Mecanismos de seguridad asociados a servicios en red

13.1.3 Segregación de redes

13.2. Intercambio de información con partes externas

Actividades de control del riesgo:

13.2.1 Políticas y procedimientos de intercambio de información

13.2.2 Acuerdos de intercambio

13.2.3 Mensajería electrónica

13.2.4 Acuerdos de confidencialidad y secreto

J. Adquisición, desarrollo y mantenimiento de los sistemas de información

14.1. Requisitos de seguridad de los sistemas de información

Actividades de control del riesgo:

14.1.1 Análisis y especificación de los requisitos de seguridad

14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes pública

14.1.3 Protección de las transacciones por redes telemáticas

14.2. Seguridad en los procesos de desarrollo y soporte

Actividades de control del riesgo:

14.2.1 Política de desarrollo seguro de software

14.2.2 Procedimientos de control de cambios en los sistemas

14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo

14.2.4 Restricciones a los cambios en los paquetes de software

14.2.5 Uso de principios de ingeniería en protección de sistemas

14.2.6 Seguridad en entornos de desarrollo

14.2.7 Externalización del desarrollo de software

14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas

14.2.9 Pruebas de aceptación

14.3. Datos de prueba

Actividades de control del riesgo:

14.3.1 Protección de los datos utilizados en prueba

K. Relaciones con Suministradores

15.1. Seguridad de la información en las relaciones con suministradores

Actividades de control del riesgo:

15.1.1 Política de seguridad de la información para suministradores

15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores

15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones

15.2. Gestión de la prestación del servicio por suministradores

Actividades de control del riesgo:

15.2.1 Supervisión y revisión de los servicios prestados por terceros

15.2.2 Gestión de cambios en los servicios prestados por terceros

L. Gestión de incidentes en la Seguridad de la información

16.1. Gestión de incidentes de seguridad de la información y mejoras

Actividades de control del riesgo:

16.1.1 Responsabilidades y procedimientos

16.1.2 Notificación de los eventos de seguridad de la información

16.1.3 Notificación de puntos débiles de la seguridad

16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones

16.1.5 Respuesta a los incidentes de seguridad

16.1.6 Aprendizaje de los incidentes de seguridad de la información

16.1.7 Recopilación de evidencias

M. Aspectos de la Seguridad de la Información en la gestión de la continuidad del negocio

17.1. Continuidad de la seguridad de la información

Actividades de control del riesgo:

17.1.1 Planificación de la continuidad de la seguridad de la información

17.1.2 Implantación de la continuidad de la seguridad de la información

17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información

17.2. Redundancias

Actividades de control del riesgo:

17.2.1 Disponibilidad de instalaciones para el procesamiento de la información

N. Cumplimiento

18.1. Cumplimiento de los requisitos legales y contractuales

Actividades de control del riesgo:

18.1.1 Identificación de la legislación aplicable

18.1.2 Derechos de propiedad intelectual (DPI)

18.1.3 Protección de los registros de la organización

18.1.4 Protección de datos y privacidad de la información personal

18.1.5 Regulación de los controles criptográficos

18.2. Revisiones de la seguridad de la información

Actividades de control del riesgo

18.2.1 Revisión independiente de la seguridad de la información

18.2.2 Cumplimiento de las políticas y normas de seguridad

18.2.3 Comprobación del cumplimiento

Anexo 02: Encuesta al usuario del sistema

ENCUESTA SOBRE SEGURIDAD DE LA INFORMACIÓN

Objetivos:

- Conocer que tan involucrado se encuentra el personal administrativo en el resguardo de la Tecnología de Información.
- Saber si el personal de la institución utiliza de manera óptima las tecnologías de información y de qué manera ayudarían a salvaguardar la misma.

Instrucciones:

Para desarrollar este cuestionario, usted debe leer cada pregunta y escoger una de las alternativas propuestas con una "X" dentro de los paréntesis o llenar dentro de las líneas punteadas según sea su criterio.

---

1. Cargo del informante: **……**

2. A qué área pertenece:**……**

3. Usted apaga los equipos informáticos debidamente después de utilizarlos

SI ( ) NO ( )

Si tu respuesta es **Sí,** Cómo apagas tu equipo después de trabajar

a. Apagando directamente el estabilizador. ( )

b. Desenchufando el cable de energía de la computadora. ( )

c. Manteniendo presionando el botón de apagado del CPU. ( )

d. Haciendo clic en el botón de apagado del menú del sistema operativo. ( )

e. Bajando la llave de energía. ( )

f. Otros, Especificar**……..** ( )

g. Ninguno. ( )

4. Se siente seguro en los ambientes donde se encuentran los equipos informáticos dentro del Club frente a cualquier desastre natural o humano.

SI ( ) NO ( )

5. Ha observado algún extinguidor cerca de los equipos informáticos.

SI ( ) NO ( )

6. Ha observado algún tipo de señalización de emergencia en los ambientes donde existen equipos informáticos.

SI ( ) NO ( )

7. Sabe utilizar de forma adecuada un extintor

SI ( ) NO ( )

8. Ha participado de algún simulacro frente a cualquier desastre natural o humano, especialmente en áreas donde hay equipos informáticos.

SI ( ) NO ( )

Si tu respuesta es **No;**

Como nos sugieres que se realice y cada que tiempo:

……

9. Ha manipulado alguna vez las entradas de corriente al CPU, los cables del teclado, mouse y conexiones de red que conectan al CPU para hacerlos funcionar.

SI ( ) NO ( )

10. Usted cree que debe sentirse responsable e identificarse con el equipo informático que usa o utilizará en algún momento dentro del Club.

SI ( ) NO ( )

11. Si en el transcurso del uso de su equipo informático se detecta alguna actividad sospechosa como ingresando a lugares restringidos, usted sería capaz de afrontarla (por la responsabilidad que asume en ese determinado momento sobre el equipo asignado)

SI ( ) NO ( )

12. Hace usted uso de los antivirus en los equipos informáticos del Club cuando ingresa o saca información en algún dispositivo de almacenamiento.

Si ( ) A veces ( ) Nunca ( )

13. Qué hace cuando detecta un virus en la computadora del Club.

a. Activa el antivirus ( )

b. Activa el antivirus, detecta los virus y los elimina ( )

c. Borra el archivo ( )

d. Formatea el dispositivo de almacenamiento ( )

e. No hago nada (Porque no sé) ( )

f. Otros, Especificar**……..** ( )

14. Usted ha detectado que el antivirus del Club funciona adecuadamente y que se encuentra actualizado.

SI ( ) NO ( )

15. Tu clave de acceso es la misma para todos los servicios y sistemas que operas en el Club.

SI ( ) NO ( )

Normalmente tu clave hace referencia a:

a. Su nombre y apellido ( )

b. Su fecha de nacimiento ( )

c. Teléfono (de casa o móvil) ( )

d. Nombre de su esposo(a) o hijo(a) ( )

e. No comparte con nadie su clave ( )

16. La clave con la cual ingresa a los sistemas del Club es conocida también por:

a. Un compañero de trabajo ( )

b. Mi esposo(a) o hijo(a) ( )

c. Algún amigo ( )

d. Otros, Especifica**……** ( )

17. Cada que tiempo cambia sus claves de acceso a los sistemas.

Cada 7 días ( ) Cada 15 días ( ) Cada 30 días ( ) Cada año ( ) Nunca ( )

18. Utiliza el servicio de correo electrónico que se le asigna en el Club.

SI ( ) NO ( )

Si su respuesta es **Sí**; Con qué frecuencia recibe correos no deseados o spam:

a. De 1 a 10 correos al día ( )

b. De 10 a 20 correos al día ( )

c. De 20 a más correos al día ( )

19. Usted ha utilizado alguna Laptop dentro del Club.

SI ( ) NO ( )

Si su respuesta es **Sí;** Ha recibido algún mensaje en el cual le comunique que su equipo ha sido registrado y puede acceder a la red.

SI ( ) NO ( )

20. Usted recibió alguna capacitación acerca de Seguridad de la Información en el Club.

SI ( ) NO ( )

21. Le interesaría conocer o tener un mayor conocimiento de lo que refiere a Seguridad de la Información.

SI ( ) NO ( )

Si le interesaría conocer más acerca del tema de Seguridad de la Información, a través de que medio te gustaría ser informado:

a. Folletos y boletines ( )

b. Charlas o conferencias ( )

c. Foros a través del portal WEB ( )

d. Como parte de algún curso en tu carrera ( )

e. Otros, Especifique: **……** ( )

22. Usted ha realizado alguna de las siguientes actividades en su PC:

a. Instalando algún software que necesitaba ( )

b. Haciendo limpieza de componente de su PC (teclado, mouse, cpu, etc.) ( )

c. Desarmando el CPU por algún sonido o falla ( )

d. Otros, Especifique**……..** ( )

e. Ninguna ( )

23. ¿Qué hace usted cuando uno de sus componentes o aplicativos no funcionan correctamente en su PC?

a. Intenta arreglarlo ( )

b. Lo arregla mi compañero de trabajo más cercano ( )

c. Llamo a un técnico de taller de computo ( )

d. No sé qué hacer en esos momentos (Pido sugerencias a mi compañero más cercano) ( )

24. ¿Con qué frecuencia solicita usted que se le realice mantenimiento a la PC que se le asigno?

Mensual ( ) Trimestral ( ) Semestral ( ) Anual ( ) Nunca ( )

25. ¿Con qué frecuencia solicita que le revisen su PC frente a cualquier falla?

A veces ( ) Casi Siempre ( ) Nunca ( )

26. Cada vez que sufre algún inconveniente con la PC o aplicación la cual desea trabajar, porque medio informa o reporta el inconveniente:

a. Teléfono (anexo) ( )

b. Correo electrónico al área de cómputo ( )

c. Voy físicamente a buscar algún encargado de cómputo ( )

d. Espero que pasen por mi área de trabajo ( )

e. Otros, Especifique..... ( )

f. Ninguna ( )

(Vásquez y De la Cruz, 2008)

Anexo 03: Entrevista al jefe de la unidad de tecnologías de información

Para saber quiénes son las personas que toman las decisiones con respecto a la seguridad de la información se listó las siguientes preguntas:

¿El Club cuenta con un comité de seguridad de la información?

SI ( )

Las funciones del comité se encuentran detalladas en el manual de funciones y organización u otro documento _____

Quién conforma ese comité _____

Ese comité es plenamente identificable por la comunidad institucional _____

NO ( )

Si no cuentan con ese comité, quienes son los encargados de establecer las políticas de seguridad de la información _____

O, sólo las políticas son establecidas por sí mismo como jefe de área de informatica_____

Estas políticas son conocidas por todos los usuarios _____

A través de que medio se les dio a conocer_____

Preguntas sobre mecanismos de control con respecto a la seguridad de la información

¿Existe algún tipo de manual o documento donde se especifique los controles para la seguridad de la información? _____

¿De qué manera controla a sus trabajadores, con respecto al tema de seguridad de lainformación?_____

¿Cómo se controla la creación de usuarios para acceder al sistema y quién solicita esa creación? _____

¿Quién se encarga de aplicar las restricciones al usuario del sistema?_____

¿Existen bitácoras donde se registran los sucesos de todos los usuarios que ingresan a la red? _____

Detecto en alguna ocasión algo indebido_____

¿Se registran los accesos de personas al área que tiene a cargo?_____

¿Se registran los sucesos o incidentes que suceden dentro del área?_____

¿Cada qué tiempo solicitan que se les de mantenimiento a sus equipos?_____

Preguntas sobre políticas de seguridad

¿Existe un documento donde se especifique las políticas de seguridad de la información?

SI ( )

¿Quién elaboró ese documento y por quién fue aprobado?_____

¿Sus trabajadores y usuarios conocen este documento? _____

¿Se aplican estas políticas a toda la institución? _____

¿Cada qué tiempo se revisan esas políticas? _____

NO ( )

¿Según Usted, a que cree que se deba, que hasta ahora no se implementa las políticas de seguridad de la información en el Club? _____

¿Cree Usted, que es de suma urgencia la elaboración de políticas de seguridad de la información para el Club? _____

Por qué_____

Preguntas sobre el nivel de conocimiento de seguridad de la información por parte de su personal

Frente a cualquier desastre natural, provocado o humano ¿Su personal conoce cuales son los activos más importantes que debe proteger en relación a la información?

SI ( )

¿Para ello existen procedimientos documentados para actuar antes, durante y después del desastre? _____

¿Ha realizado algún simulacro con defensa civil o tiene previsto hacerlo en el futuro? _____

¿Cree necesario hacerlo con esta organización? _____

¿Su área posee algún plan de contingencia, si no lo tiene ha motivado a sus trabajadores para elaborarlo? _____

NO ( )

¿A qué se debe? _____

Anexo N°04: Análisis de alternativas

En el presente anexo se muestra el análisis de alternativas realizado, donde se considera: Implementación de una metodología de riesgos general, Implementación de un Plan de Seguridad de la Información, Certificación de un SGSI enfocado a la norma ISO27001. Para el análisis se realizó una comparación cualitativa y otra comparativa.

En el cuadro de escala de criterios, se observa los valores 1 y 2. Donde el **valor 1** incluye los criterios que son evaluados de forma positiva (competitividad, viabilidad, prioridad, regulatorio) y el **valor 2** incluye los criterios de evaluación negativo (costo, riesgos, tiempo, complejidad).

Tabla N° 24. Escala de criterios

Escala de criterios	Valor 1	Valor 2
Muy bajo	10	50
Bajo	20	40
Medio	30	30
Alto	40	20
Muy alto	50	10

Fuente: Elaboración propia

A continuación se muestra los cuadros de comparación cualitativa y cuantitativa:

Tabla N° 25. Cuadro de comparación cualitativo

Comparación Cualitativa		Alternativas		
		Alternativa 1: Implementación de Metodología de Gestión de Riesgos	Alternativa 2: Implementación de un Plan de Seguridad de la Información	Alternativa 3: Certificación de un SGSI enfocado a la norma ISO27001
Criterio	Costo	Bajo	Alto	Muy alto
	Riesgos	Bajo	Bajo	Medio
	Tiempo	Muy bajo	Bajo	Alto
	Complejidad	Bajo	Medio	Muy alto
	Competitividad	Muy Bajo	Alto	Muy alto
	Viabilidad	Muy alto	Muy alto	Alto
	Prioridad	Alto	Muy alto	Bajo
	Regulatorio	Bajo	Muy alto	Bajo

Fuente: Elaboración propia

Tabla N° 26. Cuadro de comparación cuantitativo

Comparación Cuantitativa			Alternativas		
			Alternativa 1: Implementación de Metodología de Gestión de Riesgos	Alternativa 2: Implementación de un Plan de Seguridad de la Información	Alternativa 3: Certificación de un SGSI enfocado a la norma ISO27001
Criterio	Costo	20%	40	20	10
	Riesgos	10%	40	40	30
	Tiempo	18%	50	40	20
	Complejidad	5%	50	20	10
	Competitividad	12%	10	40	50
	Viabilidad	10%	50	50	40
	Prioridad	10%	40	50	20
	Regulatorio	15%	20	50	20
		100%	**36.7**	**38.5**	**24.1**

Fuente: Elaboración propia

El análisis de alternativas arrojó como resultado la elección de la alternativa 2: Implementación de un Plan de Seguridad de la Información.

Anexo N°05: Plan de capacitación y concientización

Plan de las acciones a desarrollar para capacitar y concientizar al personal del Club, así como también para evaluar si se ha logrado realizar con efectividad.

Acción	Condiciones	Involucrados	Recursos	Tareas	Efectividad	Inicio	Fin
Evaluar el conocimiento del personal.	Se ha aprobado el plan de concientización, capacitación y evaluación.	Responsable: *Implementador del SGSI. Convocado: *Personal que participa del SGSI.	Documentos: *Plan de concientización, capacitación y evaluación *Evaluaciones para el personal	1. Diseñar pruebas para evaluar el conocimiento del personal designado sobre SGSI. 2. Ejecutar la evaluación del personal	Resultado esperado: *Resultado de evaluación de personal	23-feb	26-feb
Charlas de concientización.	Se ha aprobado el plan de concientización, capacitación y evaluación.	Responsable: *Implementador del SGSI. Convocado: *Personal que participa del SGSI.	Documentos: *Plan de concientización, capacitación y evaluación. *Temario de la concientización. Presentación: *Concientización en seguridad de información. Ubicación: *Auditorio del Club. Tecnología: *Laptop y proyector.	1. Ejecutar la charla de concientización - Grupo 1 2. Ejecutar la charla de concientización - Grupo 2 3. Ejecutar la charla de concientización (rezagados)	Resultado esperado: *Listas de asistencia a la presentación. *Personal concientizado.	27 -feb	27-feb
Capacitación para roles específicos.	Se ha aprobado el plan de concientización, capacitación y evaluación.	Responsable: *Implementador del SGSI. Convocado: *Personal que participa del SGSI.	Documentos: *Plan de concientización, capacitación y evaluación. *Evaluaciones para el personal. Presentación: *Roles, responsabilidades y actividades del SGSI. Ubicación: * Auditorio del Club. Tecnología: *Laptop y proyector.	1. Identificar al personal que requiere mejorar o adquirir ciertas competencias, en base a los resultados de las evaluaciones previas. 2. Ejecutar capacitaciones al personal. identificado 3. Ejecutar la reevaluación del personal capacitado.	Resultado esperado: *Listas de asistencia a la presentación. *Personal del sistema competente.	28-feb	29-feb

Contenidos de las charlas de concientización:

- Clasificación de información
- Riesgos y amenazas
- Acceso a áreas seguras
- Ley de transparencia y acceso a la información
- Políticas de seguridad, estándares y procedimientos
- Formas comunes de ataque informático

Ideas clave a reforzar en la campaña:

- No responda a correos de desconocidos que lo invitan a establecer contacto.
- No consulte links en correos sospechosos que lo invitan a actualizar datos o resolver problema que usted no tiene.
- Siempre bloquee su sesión de trabajo cuando deje solo su puesto de trabajo.
- Guarde en lugar seguro documentos en papel cuando no los esté usando.
- Almacene en las carpetas compartidas la información vital de sus procesos
- Adopte la práctica de escritorio despejado.
- Mejore la fortaleza de sus contraseñas.
- Porte su carnet en lugar visible cuando este en las instalaciones del Club.
- Proteja la información reservada con controles de seguridad.