ANÁLISIS DEL ESTADO DE LA SEGURIDAD DIGITAL DE LA ASOCIACIÓN SCOUTS DE COLOMBIA A TRAVÉS DEL USO DEL MARCO DE CIBERSEGURIDAD DEL NIST

ING. JAVIER MAURICIO ROMERO ROMERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2021

ANÁLISIS DEL ESTADO DE LA SEGURIDAD DIGITAL DE LA ASOCIACIÓN SCOUTS DE COLOMBIA A TRAVÉS DEL USO DEL MARCO DE CIBERSEGURIDAD DEL NIST

ING. JAVIER MAURICIO ROMERO ROMERO

Proyecto de Grado presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMATICA

Director de Proyecto
ING. ESP. EDGAR MAURICIO LÓPEZ ROJAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2021

NOTA DE ACEPTACIÓN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá., Fecha sustentación

DEDICATORIA

Este trabajo está dedicado con mucho amor a mi esposa y mi hijo quienes me han acompañado en el camino y han sabido soportar las ausencias en las largas noches de dedicación al estudio; también lo dedico a mi madre que siempre me protege con su bendición y a mi papá que desde la eternidad sigue a mi lado.

AGRADECIMIENTOS

Agradezco al Maestro Danny León y al Ingeniero Fernando Zambrano por su acompañamiento y dedicación en el desarrollo del trabajo y al Ingeniero Edgar López por su aporte y visión profesional en la estrategia de creación de contenido; a la Asociación Scouts de Colombia por permitirme desarrollar el proyecto y de esta forma aportar mi grano de arena a la construcción de un mundo mejor y a los Scouters Kenny Pua y Herbert Baquero por su dedicación y apoyo.

CONTENIDO

Pág.

LISTA DE TABLAS

LISTA DE FIGURAS

Pág.

-LISTA DE ANEXOS

GLOSARIO

ACTIVO DE INFORMACIÓN: Es cualquier elemento de hardware, software, comunicaciones, datos o personas que tiene un valor para una organización y por lo tanto es susceptible de ser protegido.

AMENAZA: Es la acción que emplea una vulnerabilidad para realizar una acción negativa contra un activo de información, se considera que las amenazas siempre son externas.

ANTIVIRUS: Software de propósito desarrollado para detectar y mitigar malware en equipos de cómputo.

CIBERATAQUE: Es un ataque con el cuál se vulneran al menos uno de los principios de la triada de seguridad, causando afectaciones a infraestructuras y sistemas de información.

CIBERSEGURIDAD: Es el desarrollo de capacidades empresariales para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar los datos, sistemas y aplicaciones en el ciberespacio.

CIBERDELINCUENTE: Es una persona que utiliza el internet para ejecutar acciones ilegales como robo de información o suplantaciones de identidad.

CONTROL: Es una salvaguarda implementada después de un análisis de riesgos que busca minimizar el impacto de la materialización de incidentes de seguridad.

HACKER: Es una persona con conocimientos avanzados en temas de tecnología, que los utiliza para acceder de manera no autorizada a un sistema de información con distintos fines como pueden ser explotar vulnerabilidad o reportarlas a los desarrolladores.

IMPACTO: Se refiere al conjunto de secuelas derivadas de la materialización de un riesgo.

NIST: Es el National Institute of Standards and Technology, una entidad del Gobierno Estadounidense que busca la promoción y la innovación industrial a través del uso de la tecnología.

PROBABILIDAD: Es la posibilidad de ocurrencia de un incidente adverso en un determinado espacio de tiempo.

RIESGO: Es la combinación entre el impacto y la probabilidad de que una amenaza pueda afectar negativamente el desarrollo de objetivos organizacionales.

SCORE DE SEGURIDAD: Es la calificación que entrega un software o un perito especializado y que muestra el nivel de madurez en seguridad de una aplicación.

SEGURIDAD DE LA INFORMACIÓN: La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información, buscando mantener los pilares de la seguridad de la información que son la confidencialidad, la disponibilidad e integridad de esta.

SEGURIDAD INFORMÁTICA: La seguridad informática, es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con ésta (incluyendo la información contenida). Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura.

VULNERABILIDAD: Es cualquier defecto que puede tener una aplicación y que permite que un atacante acceda de manera no autorizada causando afectación a la integridad de esta.

RESUMEN

Las Organizaciones sin ánimo de lucro por la naturaleza propia de su misión tienen las TIC como instrumentos de apoyo pero la gran mayoría no ha podido fomentar iniciativas de seguridad por falta de presupuesto o de expertos en la materia e incluso porque aún no lo han visto como una necesidad; sin embargo los ciberdelincuentes están al acecho y no se detienen a la hora de atacar y su blanco puede ser cualquier tipo de organización, es más, se han acercado a estas empresas del tercer sector de la economía pues manejan información bastante llamativa para sus malas intenciones.

Este es el caso de la Asociación Scouts de Colombia, una entidad que presenta una necesidad en temas de protección de seguridad digital a causa del proyecto de modernización tecnológica que se inició recientemente; para determinar las mejoras requeridas se realizará un análisis de la situación actual y se propondrán acciones de mejora que permitan aumentar los niveles de seguridad corporativa.

Para el desarrollo del proyecto aplicado que busca proteger los activos de información de la Asociación, se utilizará el marco del NIST; aplicando las 5 fases de este, realizando un análisis de riesgos de las diferentes plataformas e implementando los controles y procedimientos que surjan como parte del plan de tratamiento.

Palabras Clave: Ciberseguridad, NIST, Política de Seguridad, Controles de Seguridad, Riesgo Tecnológico.

ABSTRACT

Due to the nature of their mission, non-profit organizations have ICT as support instruments, but most have not been able to promote security initiatives due to lack of budget or of experts in the field and even because they have not yet seen it as a need; However, cybercriminals are on the lookout and are not selective when it comes to attacking and their target can be any type of organization, in fact they have approached these companies from the third sector of the economy because they handle information that is quite striking for their malicious intentions.

This is the case of the Scouts Association of Colombia, an entity that presents a need in digital security protection issues due to the technology modernization project that began recently; To determine the required improvements, an analysis of the current situation will be carried out and improvement actions will be proposed that allow increasing levels of corporate security.

For the development of the applied project that seeks to protect the information assets of the Association, the NIST framework will be used; applying the 5 phases of this, carrying out a risk analysis of the different platforms and implementing the controls and procedures that arise as part of the treatment plan.

Keywords: Cybersecurity, NIST, Security Policy, Security Controls, Technological Risk.

INTRODUCCIÓN

La Asociación Scouts de Colombia es una organización sin ánimo de lucro que tiene como misión complementar la formación escolar a través del desarrollo de actividades al aire libre; en medio de esas labores recolecta información de menores de edad y adicionalmente funciona como una empresa con procesos administrativos, financieros y operativos que manejan información que debe ser protegida. Como consecuencia se hace vital el desarrollo de capacidades en los aspectos de seguridad de la información y ciberseguridad que permitan a la entidad proteger adecuadamente sus activos de información y blindarse legalmente frente a la legislación en la materia.

Para poder aumentar el score de seguridad se hace necesario evaluar la situación actual, estableciendo el apetito de riesgo que tiene la entidad y definiendo las políticas y buenas prácticas que se han de implementar, así como los controles que permitirán mantener los niveles de seguridad en niveles tolerables.

Se escogió el marco de Ciberseguridad del NIST para el desarrollo del presente trabajo ya que es versátil y puede ser aplicado en todo tipo de organizaciones a través de la comprensión y tratamiento adecuado del riesgo tecnológico.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

La Asociación Scouts de Colombia es una entidad sin ánimo de lucro que cuenta con operaciones de programa de jóvenes en todo el país y con oficinas centrales en la ciudad de Bogotá desde donde se desarrolla toda la parte administrativa y financiera; se ha designado un rol específico para la Gestión del Desarrollo Institucional, quien dentro de sus iniciativas ha promovido el uso de las TICs en las áreas administrativas , entre los cuales se identifica con la adquisición de software de propósito específico para la administración de la membresía institucional y para la gestión del talento humano de los adultos voluntarios en la Asociación; así como la compra de licenciamiento de Office 365 para comunicación a nivel nacional.

La entidad no cuenta con un área dedicada a la gestión de las TICs pues sus empleados a tiempo completo se dedican a tareas relacionadas con la administración y las finanzas, es por esto que la implementación de estas soluciones se ha desarrollado por parte de los proveedores de las aplicaciones en compañía de voluntarios de la asociación que aportan un poco de su tiempo libre en estas actividades; lastimosamente la falta de experticia en temas de seguridad digital de estos voluntarios no ha permitido que los niveles de protección sean los adecuados pues se han configurado las aplicaciones con los niveles que traen por defecto dejando un nivel de riesgo de exposición elevado y sin controles para mitigar establecidos.

Adicionalmente no se ha establecido ninguna política de seguridad digital que permita establecer unos requisitos mínimos para futuras implementaciones de sistemas de información ni para garantizar la preservación de la integridad, disponibilidad y confidencialidad de la información de la entidad y sus asociados.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo lograr a través de la implementación del marco de ciberseguridad del NIST, una mejora en los niveles de seguridad de la Asociación Scouts de Colombia?

JUSTIFICACIÓN

Un estudio de la Cámara Colombiana de Informática y Telecomunicaciones en conjunto con la Policía Nacional de Colombia denominado “Tendencias de Cibercrimen en Colombia 2019-2020”[1] reveló que en 2019 se reportaron 28.827 incidentes de seguridad digital a las autoridades nacionales, con una tendencia en el crecimiento año por año desde 2015; por lo tanto, la implementación de salvaguardas en los activos de información es una necesidad para todas las organizaciones. El tercer sector de la economía compuesto por asociaciones y entidades sin ánimo de lucro está ante una transformación en sus actividades tradicionales migrando hacia ambientes digitales, a estos cambios no es ajena la Asociación Scouts de Colombia que maneja información de un poco más de 10 mil niñas, niños y adolescentes en sus sistemas de información. Se hace necesario implementar mecanismos de protección para los datos que trata la Asociación por la naturaleza sensible de la misma y por la responsabilidad de la entidad en el cumplimiento de lo estipulado por la Ley 1581 de 2012 que en su artículo séptimo aboga por los derechos de la población menor de edad con respecto al tratamiento de sus datos personales.

Para el desarrollo del presente proyecto se pretende utilizar el marco de ciberseguridad del NIST, el cual es empleado por muchas organizaciones alrededor del mundo por su versatilidad y aplicabilidad; tal como lo afirman la OEA y AWS en su documento “Marco NIST – Un abordaje integral de la Ciberseguridad” la metodología ha tomado como base varios estándares de la industria haciendo que la gobernanza de ciberseguridad permee todas las estructuras de las organizaciones llevando los conceptos técnicos hacia la estrategia corporativa.

En el informe Global State of Information Security Survey de la PwC en el año 2017, se logró establecer que los incidentes de seguridad ocurridos en las ONG y otras organizaciones de este sector, causaron pérdidas cercanas a los U$ 100.000 en promedio para cada entidad[2]; por lo tanto abordar la protección digital de la organización propuesta para este proyecto aplicado supone un ejercicio de responsabilidad financiera y ayuda a destacar la labor de los especialistas en Seguridad Informática como asesores de la alta gerencia y generadores de información de valor para la toma de decisiones.

[1] CCIT – POLICIA NACIONAL DE COLOMBIA – CISCO. (2020). Informe de las tendencias del cibercrimen en Colombia 2019-2020. Disponible en: https://www.ccit.org.co/wpcontent/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

[2] Castelli, Christopher – Gabriel, Barbara (2017). Global State of Information Security Survey. Disponible en https://www.pwc.com/us/en/cybersecurity/assets/pwc-strengthening-digital-society-against-cyber-shocks.pdf

OBJETIVOS

1.3 OBJETIVO GENERAL

Analizar el estado actual de la seguridad digital de la Asociación Scouts de Colombia a través del uso de las diferentes herramientas del marco de ciberseguridad del NIST, que aporte en la toma de decisión para la mejora continua de su estructura TI.

1.4 OBJETIVOS ESPECÍFICOS

- Realizar un análisis de riesgos de seguridad de la información a la estructura de TI de la Asociación scouts de Colombia usando la metodología SP 800-30 del NIST, con el fin de determinar el grado de exposición que esta presenta.

- Planear el tratamiento del riesgo a partir de las necesidades legales, contractuales y emanadas por el análisis, que sirva como insumo para mejorar el entorno digital de la organizacional.

- Presentar el estado actual de la seguridad digital y las oportunidades de mejora detectadas en el análisis realizado que aporte a la mejora continua de la seguridad de la información.

- Proponer los controles necesarios que permitan garantizar los niveles de seguridad mínimos para la operación de la asociación, estableciendo salvaguardas para cada una de las fases de la metodología del NIST.

MARCO REFERENCIAL

1.5 MARCO TEÓRICO

Teniendo en cuenta el planteamiento del problema del presente estudio y las necesidades particulares que llevaron al diseño de los objetivos, los siguientes son los componentes de programas de seguridad digital que se ejecutarán durante el proyecto:

Política de Seguridad: El Ministerio de Tecnologías de la Información y Comunicaciones de Colombia en su guía "Elaboración de la política general de seguridad y privacidad de la información"[3] establece los lineamientos para la materia en las entidades públicas y define la Política de Seguridad como "Una declaración general que representa la posición de la administración de una entidad respecto a la protección de los activos de información que soportan los procesos de la organización y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información".

Hardening: El Centro de Innovación y Soluciones Empresariales y Tecnológicas de España en una reciente publicación de su blog define el Hardening o Endurecimiento como "el proceso de reducción de vulnerabilidades en el sistema"[4]. Para lograr esto se establecen unas medidas de seguridad con el objetivo de estar preparados ante un ataque informático.

El hardening se basa en el supuesto que los sistemas que cumplen menos funciones son más seguros, esto se logra con unas consideraciones básicas entre las que se destacan: Cambiar todas las claves que existan por default, desinstalación de todo el software que no sea necesario, dar de baja a los usuarios que no sean requeridos, deshabilitación de todos los servicios que no se están utilizado, cerrar los puertos que se no se encuentren en uso, realizar copias de seguridad, preferir el uso de firewall si lo tiene el sistema y actualizar los sistemas operativos con frecuencia.

Controles de Seguridad: Son las medidas implementadas para proteger los activos de información. Para seleccionar estas salvaguardas el Instituto Nacional de Ciberseguridad de España en su documento "Protección de la Información" propone primero que todo determinar la importancia de la data que se maneja, luego identificar, clasificar y valorar la información y determinar el costo.

---

[3] MINTIC (2016). Elaboración de la política general de seguridad y privacidad de la información. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

[4] CISET. (2020). ¿Qué es el hardening de sistemas operativos? Disponible en: https://www.ciset.es/publicaciones/blog/746-hardening

Los controles se pueden clasificar según su naturaleza en 3 categorías:

- Técnicos: Son medidas que requieren la intervención de soluciones tecnológicas como los antivirus, firewall, DLP, IPS, entre otros.
- Organizacionales: Cuando el control se enfoca en aumentar la seguridad con enfoque en las personas como la capacitación, el manejo de usuarios y la asignación de responsabilidades.
- Físicos: Que implican el acondicionamiento de instalaciones para minimizar los riesgos propios del sitio.

Análisis de Riesgos de Seguridad: La Norma IS0 31000 define el Riesgo como el "Efecto de la Incertidumbre sobre los objetivos" y el análisis como el "proceso para comprender la naturaleza del riesgo y determinar el nivel del mismo"[5].

Cualquier iniciativa de seguridad digital debe tener el análisis de riesgos como su génesis, los cambios en la normatividad, en los procesos y la evolución propia de la tecnología exigen que las organizaciones realicen este proceso al menos una vez cada año con las fases que sugieren las principales metodologías y que incluyen en líneas generales al menos estos pasos:

- Caracterización del sistema
- Identificación de amenazas
- Identificación de vulnerabilidades
- Análisis de controles
- Determinación de la probabilidad
- Análisis de impacto
- Determinación del riesgo
- Recomendaciones de control
- Documentación de resultados
- Establecimiento de parámetros
- Necesidades de Seguridad

Adicionalmente es importante tener presente para el desarrollo del proyecto, los siguientes conceptos:

Seguridad de la Información: Es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información, buscando mantener los pilares de la seguridad de la información que son la confidencialidad, la disponibilidad e integridad de esta. Fuente: Pago Simple.

Seguridad Informática: Es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con ésta (incluyendo la

[5] Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC). (2013). Norma Técnica Colombiana ISO 31000. GESTIÓN DEL RIESGO. PRINCIPIOS Y DIRECTRICES. Requisitos

información contenida). Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura. Fuente: Nedetel.

SGSI: Un Sistema de Gestión de la seguridad de la Información es un conjunto de políticas de administración adecuada de los activos de información de una organización. Fuente: Consultora Firma-E

Confidencialidad: Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados**.** Fuente: NTC ISO/IEC 27000:2018.

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos. Fuente: NTC ISO/IEC 27000:2018.

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera. Fuente: NTC ISO/IEC 27000:2018.

1.6 MARCO CONCEPTUAL

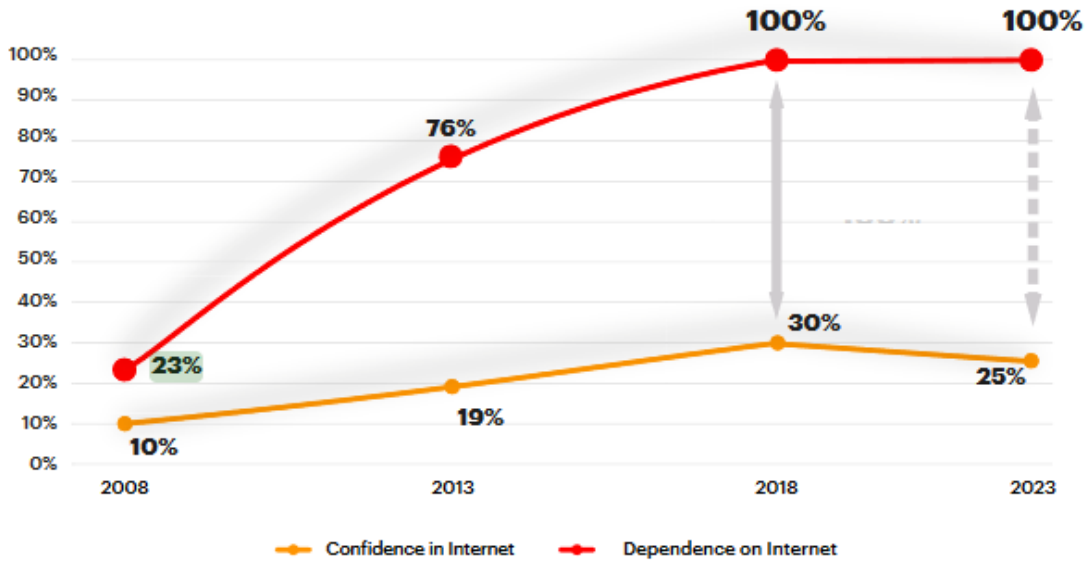
La necesidad por proteger los sistemas de información en su conjunto (Hardware, Software y Datos) ha estado presente desde el inicio mismo de la informática; de acuerdo con la firma Sofistic que en una entrada de su blog de Ciberseguridad titulada "¡Empieza la informática! Y el malware…"[6] reporta el nacimiento del primer virus a principio de los años 70 que recibió por nombre "Creeper" y la respuesta inmediata con una solución llamada "Reaper", lo que nos ubica en una carrera de casi 50 años en los que la protección ha pasado de medidas básicas a convertir la seguridad digital en una corriente de la informática con especialistas dedicados a la materia y nuevos hallazgos permanentes.

La Seguridad Digital o Ciberseguridad entendida como el conjunto de técnicas, procesos y esfuerzos que realizan las organizaciones para proteger los activos de información expuestos hacia el ciberespacio se ha convertido en una necesidad empresarial, un análisis realizado por Accenture en el documento "Securing the digital Economy" afirma que la dependencia que tenemos sobre el internet como se puede apreciar en la figura 1, aumento del 23% al 100% en solo 10 años (De 2008 a 2018), mientras que la confianza en la herramienta solo paso del 10% al 30% en el mismo lapso de tiempo y con tendencia a disminuir en los siguientes años. Ese bajo nivel de confianza es el que da campo para que la Ciberseguridad surja como

[6] Sofistic Cybersecurity. (2019). La breve historia de la ciberseguridad. Disponible en: https://www.sofistic.com/blog-ciberseguridad/la-breve-historia-de-la-ciberseguridad/

una disciplina valiosa y cada vez más cercana al común de las personas; el impacto de la tecnología en nuestras vidas ha sido tal que se puede afirmar sin temor a equivocarse que todas las actividades a nivel mundial dependen en alguna medida de servicios de T.I y por consiguiente la protección y la higiene digital deben permear a más sectores de la economía.

Figura 1 Índices de Confianza y Dependencia de Internet



Fuente:https://www.accenture.com/_acnmedia/thought-leadership-assets/pdf/accenture-securing-the-digital-economy-reinventing-the-internet-for-trust.pdf

La evolución de la Seguridad de la Información y la Ciberseguridad ha llevado a los organismos internacionales de normalización y a entidades públicas y privadas a desarrollar marcos de trabajo para aumentar los niveles de confianza digital, entre estos se destacan:

- Norma técnica ISO:27032/2012: La cual según sus autores "proporciona orientación para mejorar el estado de la ciberseguridad, destacando los aspectos únicos de esa actividad y sus dependencias en otros dominios de seguridad" (Definición traducida al español de la encontrada en el sitio web de la International Organization for Standardization).

- COBIT 5 para Seguridad de la Información: Que en su documentación se presenta como una "ayuda a las empresas para crear el valor óptimo desde la tecnología de la información (TI) manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos."

- Framework NIST: Que es un marco de trabajo para la gestión de riesgos de ciberseguridad diseñado por el Instituto Nacional de Estándares y Tecnología de los Estados Unidos y que pretende establecer la gestión coordinada de los controles de seguridad de forma óptima, escalable e integrable.

Y es precisamente el marco del NIST el que se utilizará en este proyecto. Para su desarrollo, el marco contiene 5 funciones continuas y simultaneas: Identificar, Proteger, Detectar, Responder y Recuperar. La "Federal Trade Commision" explica en su documento "ciberseguridad para pequeños negocios"[7] como implementar de manera sencilla las 5 fases:

1- Identificar: Inventariando activos, escribiendo políticas, definiendo responsabilidades y estableciendo los pasos para detener un ciberataque.
2- Proteger: Controlando los accesos a los sistemas, usando software de seguridad, haciendo backups, parchando hardware y software constantemente y capacitando al usuario final.
3- Detectar: Monitoreando la red, revisando conexiones poco usuales e investigando cada incidente de seguridad.
4- Responder: Implementando planes para mantener funcionando el negocio y notificando a los stakeholders las novedades en caso de incidente.
5- Recuperar: Restaurando la infraestructura afectada y manteniendo informado a los interesados sobre las actividades de las fases 4 y 5.

La forma en la que se implementa el estándar NIST se especifica en el documento oficial "Marco para la mejora de la seguridad cibernética en infraestructuras críticas" que indica que una organización puede establecer o mejorar un programa de seguridad cibernética siguiendo 7 pasos descritos a continuación:

- ✓ Paso 1 – Priorización y definición de alcance.
- ✓ Paso 2 – Orientación.
- ✓ Paso 3 – Crear un perfil.
- ✓ Paso 4 – Ejecutar un análisis de riesgos.
- ✓ Paso 5 – Crear un perfil objetivo.
- ✓ Paso 6 – Determinar, analizar y priorizar las brechas detectadas.
- ✓ Paso 7 – Implementar el plan de acción.

[7] Federal Trade Commision. (Sin fecha establecida – Consultado en Marzo de 2021). CIBERSEGURIDAD PARA PEQUEÑOS NEGOCIOS. Disponible en: https://www.ftc.gov/es/system/files/attachments/understanding-nistcybersecurity-framework/cybersecurity_sb_nist-cyber-framework-es.pdf

1.7 MARCO TECNOLÓGICO

Para el cumplimiento de las actividades que propone el marco de ciberseguridad del NIST se emplean equipos de cómputo con software de ofimática para el desarrollo la parte teórica y las herramientas tecnológicas relacionadas en la tabla 1para las revisiones técnicas:

Tabla 1 Herramientas de T.I.

Nombre de la Herramienta	Descripción de la herramienta
Kali Linux	Sistema Operativo Linux basado en Debian que contiene diversas herramientas de seguridad informática.
OWASP	Software de propósito, diseñado para la evaluación de aplicaciones y sitios web con el que se analizan las vulnerabilidades en desarrollo.
Tenant de Office 365	Interfaz administrativa de la suite de Office 365 de Microsoft ® con la que se accede a las configuraciones de seguridad y cumplimiento.
Wireshark	Es un software open-source diseñado para el análisis de tráfico de red a través de la captura de paquetes.

Fuente: Elaboración Propia

1.8 MARCO LEGAL

Marco Legal Colombiano

La siguiente es la legislación vigente que desde el Gobierno Nacional se ha decretado en materia de seguridad de la información y ciberseguridad que puede afectar el proyecto:

Ley 1273 de 2009 – LEY DE DELITOS INFORMÁTICOS

Esta ley modificó el Código Penal definiendo una serie de tipos penales para castigar todo atentado contra la disponibilidad, confidencialidad o integridad de sistemas de información y datos. Las principales consideraciones de la Ley son las siguientes:

- Acceso abusivo a un sistema informático con penas entre los 4 y 8 años y multas hasta los 1.000 SMLV.
- Obstaculización ilegítima de sistema informático o red de telecomunicación con penas entre los 4 y 8 años y multas hasta los 1.000 SMLV.

- Interceptación de datos informáticos con penas entre los 3 y 6 años.
- Daño informático con penas entre los 4 y 8 años y multas hasta los 1.000 SMLV.
- Uso de software malicioso con penas entre los 4 y 8 años y multas hasta los 1.000 SMLV.
- Violación de datos personales con penas entre los 4 y 8 años y multas hasta los 1.000 SMLV.
- Suplantación de sitios web para capturar datos personales con penas entre los 4 y 8 años y multas hasta los 1.000 SMLV.

La ley también establece que el hurto por medios informáticos y la transferencia no autorizada de activos serán sancionados

Ley 1581 de 2012 – LEY DE PROTECCIÓN DE DATOS PERSONALES
Esta ley y su decreto reglamentario el 1377 de 2013, establecen las reglas de juego con respecto al tratamiento de los datos personales de los ciudadanos colombianos; definiendo primero los tipos de datos personales en 4 categorías (público, semiprivado, privado y sensible) y precisando igualmente los deberes de los responsables del tratamiento y los derechos que los ciudadanos tiene con respecto a su información personal.

En su parte sancionatoria la ley faculta a la Superintendencia de Industria y Comercio para establecer multas hasta por los 2.000 SMLV y la suspensión de las actividades comerciales de los infractores. El artículo 7 de esta Ley incluye algunas reglas especiales para el tratamiento de los datos sensibles de niñas, niños y adolescentes; aspecto que tiene influencia directa sobre la data que se maneja en la organización sujeto de este proyecto aplicado.

Otra legislación sobre la materia:

- Decreto 1078 de 2015 - Por medio del cual se expide el decreto único reglamentario del sector de tecnologías de la información y las comunicaciones
- Ley 1978 de 2019 - Por la cual se moderniza el sector de las tecnologías de la información y las comunicaciones.
- Ley 1928 de 2018 - Por medio de la cual se aprueba el "convenio sobre la ciberdelincuencia", adoptado el 23 de noviembre de 2001, en Budapest
- Ley 1712 de 2014 - Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones

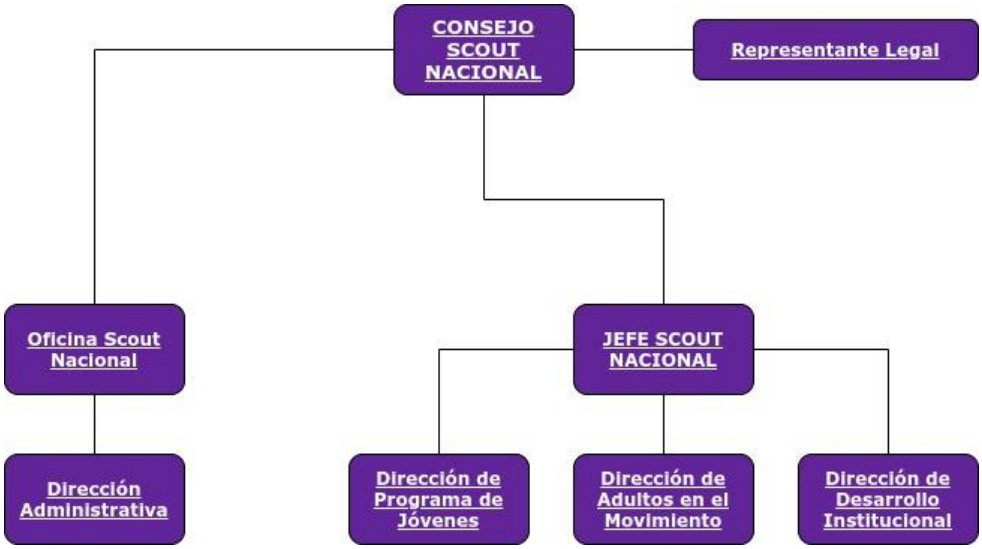
Por su parte la Asociación Scouts de Colombia está protegida en sus actividades operativas y administrativas por el Decreto 1786 de 1954.

1.9 MARCO CONTEXTUAL

La Asociación Scouts de Colombia es una entidad sin ánimo de lucro que empezó sus actividades en el país en 1913 y que está protegida en su objeto social, uniformes, insignias y distintivos por el Decreto 1786 de 1954; esta entidad se dedica a la contribuir a la educación de los niños y jóvenes, a través de un sistema de valores basados en la Promesa y la Ley Scout, para ayudar a construir un mundo mejor donde las personas son autosuficientes como individuos y juegan un papel constructivo en la sociedad. Esta organización maneja información de niños, niñas y adolescentes y cuenta en sus registros con algo más de 10 mil asociados en todo el país.

La Asociación Scouts de Colombia desde la parte organizativa depende de un único ente de dirección que es el Consejo Nacional y de este se desprenden funciones para el Programa de Jóvenes, el Desarrollo Institucional y la Administración y Finanzas. La estructura organizacional se puede apreciar en el organigrama de la Figura 2:

Figura 2 Organigrama Asociación Scouts de Colombia



Fuente: Elaboración propia

DISEÑO METODOLÓGICO

Para el caso del estudio se busca indagar la situación actual de la seguridad de la entidad a través de la aplicación de las fases y actividades descritas por el marco de trabajo del NIST, las cuales se pueden observar en la Figura 3: Fases y tareas del marco NIST:

Figura 3 Fases y tareas del marco NIST

FUNCIÓN IDENTIFICADOR ÚNICO	FUNCIONES	CATEGORÍA IDENTIFICADOR ÚNICO	CATEGORIAS
ID	IDENTIFICAR	ID.AM	Gestión de activos
		ID.BE	Ambiente de negocios
		ID.GV	Gobernanza
		ID.RA	Evaluación de riesgos
		ID.RM	Estrategia de gestión de riesgos
		ID.SC	Gestión del riesgo de la cadena de suministro
PR	PROTEGER	PR.AC	Gestión de identidad, autenticación y control de acceso
		PR.AT	Conciencia y capacitación
		PR.DS	Seguridad de datos
		PR.IP	Procesos y procedimientos de protección de la información
		PR.MA	Mantenimiento
		PR.PT	Tecnología de protección
DE	DETECTAR	DE.AE	Anomalías y Eventos
		DE.CM	Monitoreo continuo de seguridad
		DE.DP	Procesos de Detección
RS	RESPONDER	RS.RP	Planificación de respuesta
		RS.CO	Comunicaciones
		RS.AN	Análisis
		RS.MI	Mitigación
		RS.IM	Mejoras
		RS.RP	Planificación de respuesta
RC	RECUPERAR	RC.RP	Planificación de la recuperación
		RC.IM	Mejoras
		RC.CO	Comunicaciones

Fuente: https://www.esan.edu.pe/conexion/actualidad/2019/04/30/que-es-el-cybersecurity-framework-de-nist-de-los-estados-unidos/

Para la fase de Identificación fue necesario realizar una evaluación inicial del estado de la seguridad en la Asociación Scouts de Colombia a través de la aplicación de un cuestionario que mide el GAP frente a lo sugerido por el marco del NIST.

En el Anexo B se encuentran las respuestas conseguidas en entrevista con los voluntarios de la Asociación, el resumen para la Fase 1 del NIST que se encarga de la Identificación arroja que hay aspectos de la ciberseguridad que aún no han sido siquiera contemplados en la dinámica de la organización como se puede apreciar en la figura 4 Valoración del cumplimiento fase 1 NIST, mientras que otros se

apalancan en los procesos ya establecidos; el promedio de cumplimiento de la Asociación en la fase de Identificación apenas alcanza el 44,14%

Figura 4 Valoración del cumplimiento fase 1 NIST

Fuente: Elaboración propia

Las fases de Protección, Detección, Respuesta y Recuperación se abordaron a través de la aplicación de la metodología de riesgos escogida y de los controles a implementar para cada fase que se derivan del análisis de riesgos realizado.

DESARROLLO DE OBJETIVO 1 – ANÁLISIS DE RIESGOS

La calificación de la gestión de riesgo en el GAP llega al 45,71%[8] valor que no es tolerable; si bien hay una Comisión Nacional del Riesgo y unas directivas desde la Oficina Scout Mundial en su documento "PAUTA DE POLÍTICA DE GESTIÓN DE RIESGOS"[9] no se han definido políticas para la gestión del riesgo tecnológico y de seguridad de la información y ciberseguridad a nivel nacional. Y es precisamente el documento del ente superior a nivel mundial el que sugiere hacer tratamiento eficaz del riesgo para abordar situaciones súbitas en pos de una gestión institucional más eficiente.

Para realizar el análisis de riesgos de seguridad de la información en la Asociación Scouts de Colombia se utilizará la metodología SP 800-30[10] del NIST, esta técnica prueba ser eficiente pues además del clásico análisis, desarrolla un plan de actividades que incluye la priorización de las acciones, pasa por el estudio de costo/beneficio de implementación de controles y establece responsables para cada riesgo y control.

La metodología se compone de una serie de pasos que facilitan el análisis:

- Caracterización de sistemas.
- Identificación de las amenazas.
- Identificación de las vulnerabilidades.
- Análisis de Controles.
- Determinación de probabilidades.
- Análisis de impacto.
- Determinación del riesgo.
- Recomendación de controles.
- Documentar Resultados

A continuación, se presentan los hallazgos del análisis realizado:

- **Caracterización de sistemas**
  En este paso se realiza una revisión de los activos de información relacionados con hardware, software y telecomunicaciones empleados en el desarrollo del objeto social de la Asociación, la relación de los mismos se encuentra en la Tabla 2 Caracterización de sistemas.

[8] Promedio obtenido de las respuestas identificadas como ID.RA e ID.RM

[9] World Scout Bureau Inc. (2017). PAUTA DE POLÍTICA DE GESTIÓN DE RIESGOS - Movimiento Scout Seguro. Recuperado de: https://www.scout.org/sites/default/files/library_files/Pauta%20Politica%20de%20gestion%20de%20riesgos%20final%20%28marzoLDM%29.pdf

[10] National Institute of Standards and Technology (2012),«Special Publication 800-30 Rev.1»,Guide for conducting risk assessment, Computer Security Division Information Technology Laboratory, Disponible en: http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

Tabla 2 Caracterización de sistemas

Nombre	Categoría	Descripción
SISCOUT	Software	Plataforma de SaaS que se utiliza para la administración de membresía y programa de jóvenes.
Talento 360	Software	Plataforma de SaaS que se utiliza para la administración de Talento Humano de los adultos voluntarios en el Movimiento Scout.
Office 365	Software	Plataforma de correo, comunicaciones y servicios de ofimática.
www.scout.org.co	Software	Sitio web informativo de la organización, incluye una tienda en línea con acceso a pasarelas de pago.
Equipos de cómputo propios	Hardware	Máquinas propiedad de la asociación que se encuentran en la red corporativa
Equipos de cómputo modalidad BYOD	Hardware	Máquinas propiedad de voluntarios que se conectan ocasionalmente a la red corporativa.
Red LAN	Comunicaciones	Infraestructura de acceso a red cableada y wifi en oficina principal.

Fuente: Elaboración propia

Identificación de las amenazas[11] En este paso se revisan las amenazas más populares en el entorno y las que pueden haber afectado a la Organización en algún momento de su historia.

- ✓ Malware en cualquiera de sus categorías.
- ✓ Uso no autorizado de Sistemas de información.
- ✓ Robo de Información sensible.
- ✓ Suplantación de identidad
- ✓ Ataques de denegación de Servicios (DoS)
- ✓ Ataques de Fuerza Bruta
- ✓ Modificaciones no autorizadas de la Información.
- ✓ Divulgación no autorizada de Información sensible.
- ✓ Desastres Naturales
- ✓ Sabotaje interno

- **Identificación de las vulnerabilidades**
  En este paso se incluyen las vulnerabilidades más comunes en el entorno, ya que la entidad está en fases iniciales en materia de Seguridad Digital no hay históricos en informes de análisis de vulnerabilidades; la relación de estas se encuentra en la Tabla 3 Principales Vulnerabilidades.

[11] Lista basada en la propuesta de Tarazona en su documento AMENAZAS INFORMÁTICAS Y SEGURIDAD DE LA INFORMACIÓN. Recuperado de: https://core.ac.uk/download/pdf/230095193.pdf

Tabla 3 Principales vulnerabilidades

Categoría	Nombre
Personas	Falta de personal técnico calificado en seguridad
	Funcionarios sin concientización en materia de ciberseguridad
	Colaboradores inconformes
Físicas y Ambientales	Protección inadecuada de las oficinas
	Controles de acceso débiles
	Equipos protegidos inadecuadamente
	Dificultades con la energía eléctrica
Hardware	Degradación de hardware
	Mala configuración de hardware
	Daño de dispositivos de almacenamiento
	Falta de mantenimiento preventivo
Software	Dejar configuraciones por default
	Contraseñas por defecto
	Programas desactualizados
	Instalaciones no controladas de programas
	Vencimiento de licencias
	Sistemas de información desactualizados
	Presencia de malware en los dispositivos.
Comunicaciones	Degradación de la infraestructura de red
	Control inadecuado o inexistente del tráfico
	Falta de canales alternos de comunicación
Información	Bases de datos no controladas adecuadamente
	Fallas en los backups o ausencia de los mismos
	Repositorios de datos sin contraseñas

Fuente: Elaboración propia

- **Análisis de Controles.**
  Las primeras revisiones sobre los activos de información de la Asociación Scouts de Colombia arrojan controles limitados, básicamente se trata de solicitud de usuario y contraseña para el acceso a los diferentes sistemas de información, equipos de cómputo propios con antivirus licenciado, pero sin monitoreo y mantenimiento preventivo a equipos y red por parte de un tercero.

- **Determinación de probabilidades.**
  INCIBE define la probabilidad como “la posibilidad de ocurrencia de un hecho, suceso o acontecimiento”[12]. Para este ejercicio académico se utilizarán los criterios relacionados en la Tabla 4 Criterios para Probabilidades:

Tabla 4 Criterios para Probabilidades

Calificación	Nombre	Descripción	Frecuencia

[12] INCIBE: Instituto Nacional de Ciberseguridad de España. Definición obtenida de la Guía de Gestión de Riesgos, recuperado de: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestion_riesgos_metad.pdf

1	Raro	La situación puede presentarse sólo en circunstancias excepcionales.	No se ha presentado en los últimos 3 años
2	Improbable	La situación puede presentarse en contadas ocasiones.	Al menos una vez en los últimos 3 años
3	Posible	La situación puede presentarse en algún momento.	Al menos una vez en el último año
4	Probable	La situación se puede presentar en varias ocasiones.	Al menos 2 veces al año
5	Casi seguro	La situación se va a presentar en la mayoría de las ocasiones.	Más de 3 veces al año.

Fuente: Elaboración propia

- **Análisis de impacto.**
  La ISO31000 define el Impacto como "el conjunto de consecuencias que origina un riesgo si llegará a presentarse"[13]. Para este ejercicio académico se utilizarán los criterios relacionados en la Tabla 5 Criterios para Impactos :

Tabla 5 Criterios para Impactos

Calificación	Nombre	Descripción
1	Insignificante	Si se presenta la situación las consecuencias son mínimas para la Asociación.
2	Menor	Si se presenta la situación las consecuencias son bajas para la Asociación.
3	Moderado	Si se presenta la situación las consecuencias son medias para la Asociación.
4	Mayor	Si se presenta la situación las consecuencias son altas para la Asociación.
5	Catastrófico	Si se presenta la situación las consecuencias son catastróficas para la Asociación.

Fuente: Elaboración propia

- **Determinación del riesgo.**
  Teniendo en cuenta que la probabilidad y el impacto se califican de 1 a 5, los riesgos se ubicarán en una matriz de 5x5 con los siguientes valores:

[13] Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC). (2013). Norma Técnica Colombiana ISO 31000. GESTIÓN DEL RIESGO. PRINCIPIOS Y DIRECTRICES. Requisitos.

Figura 5 Modelo Matriz de Riesgos

	IMPACTO				
PROBABILIDAD	**Insignificante 1**	**Menor 2**	**Moderado 3**	**Mayor 4**	**Catastrófico 5**
Casi Seguro 5	5	10	15	20	25
Probable 4	4	8	12	16	20
Posible 3	3	6	9	12	15
Improbable 2	2	4	6	8	10
Raro 1	1	2	3	4	5

Fuente: Elaboración propia

- **Recomendación de controles.**
  Esta fase responde al cumplimiento del Objetivo 4 de este Proyecto Aplicado y se profundizará en el mismo en el capítulo 9 de este documento; sin embargo y con el apetito de riesgo definido por la Organización se establece que se deben implementar controles para minimizar los riesgos que obtuvieron puntajes de 12 a 25 en el cálculo ubicados en la zona de calor naranja y roja del mapa de riesgos.

- **Documentar Resultados**
  Para el caso particular de la Asociación Scouts de Colombia se realiza una codificación de cada riesgo, generando su descripción y calificando con base en la fórmula de cálculo del riesgo: Riesgo = Impacto x Probabilidad. Estos resultados se aprecian en la Tabla 6 Calculo del Riesgo antes de controles:

Tabla 6 Calculo del Riesgo antes de controles

ID Riesgo	Descripción Riesgo	Probabilidad	Impacto	Calificación Riesgo
R1	Sistemas de información mal configurados por falta de conocimiento de los implementadores	3	4	12
R2	Usuarios finales sin una adecuada sensibilización en temas de seguridad de la información y ciberseguridad	4	4	16
R3	Afectaciones a los sistemas de información y a la data causados por funcionarios y voluntarios de la Asociación que tengan motivaciones personales en contra de la organización.	1	5	5

R4	Acceso físico no autorizado a las oficinas por fallas en los controles de acceso.	2	5	10
R5	Acceso lógico no autorizado a los sistemas de información por fallas en los controles de acceso.	1	5	5
R6	Equipos de cómputo propios con firmas de antivirus desactualizadas	2	4	8
R7	Equipos de cómputo en modelo BYOD con firmas de antivirus desactualizadas o sin un software de antivirus.	3	4	12
R8	Afectaciones en el servicio de energía eléctrica que provoquen daños en hardware y pérdida de información.	3	4	12
R9	Equipos de cómputo que han superado su vida útil y siguen en uso poniendo en peligro la integridad de la información	3	4	12
R10	Daño físico de discos duros extraíbles y memorias USB generando pérdida de información	2	5	10
R11	Uso no autorizado de dispositivos removibles en los que se pueda extraer información sensible.	3	5	15
R12	Falta de rutinas de mantenimiento de software y hardware que ocasionen daños irreparables	2	5	10
R13	Permitir que en las aplicaciones se utilicen usuarios administradores por default (ej, root, admin, administrador)	1	5	5
R14	Software no actualizado a sus últimas versiones que puede generar vulnerabilidades a toda la red.	3	5	15
R15	Instalación no autorizada de software en equipos corporativos.	4	5	20
R16	Software no licenciado o crackeado que puede generar inconvenientes legales a la Asociación.	2	4	8
R17	Dispositivos de red con altos niveles de desgaste que disminuyan el performance de la red.	1	2	2
R18	Acceso a sitios web desde los que se pueda descargar malware.	5	4	20
R19	Acceso a sitios web que generen alto tráfico generando afectaciones al rendimiento de la red.	5	3	15
R20	Canales de comunicación sin redundancia lo que puede generar afectaciones a la disponibilidad de los servicios.	5	3	15
R21	Bases de datos inadecuadamente protegidas generando posibilidad de robo o pérdida de información sensible.	2	5	10
R22	Datos de niñas, niños y adolescentes protegidos de manera inadecuada, ocasionando faltas a la Ley 1581 de 2012.	1	5	5
R23	Respaldos de información mal ejecutados o ausencia de los mismos.	2	5	10
R24	Repositorios de datos protegidos inadecuadamente	1	5	5

- Fuente: Elaboración propia
-

El análisis de riesgos muestra que la mayoría de estos se encuentran en las zonas más calientes de la matriz, por lo que el perfil de riesgo de la Asociación es alto.

La siguiente es la ubicación de los riesgos en la matriz después de la calificación previa a la implementación de controles:

Figura 6 Matriz de Riesgos de Seguridad Digital

	IMPACTO				
PROBABILIDAD	**Insignificante 1**	**Menor 2**	**Moderado 3**	**Mayor 4**	**Catastrófico 5**
Casi Seguro 5	5	10	15 **R19 - R20**	20 **R18**	25
Probable 4	4	8	12	16 **R2**	20 **R15**
Posible 3	3	6	9	12 **R1 - R7 - R8 - R9**	15 **R11 - R14**
Improbable 2	2	4	6	8 **R6 - R16**	10 **R4 - R10 - R12 - R21 - R23**
Raro 1	1	2 **R17**	3	4	5 **R3 - R5 - R13 - R22 - R24**

Fuente: Elaboración propia

Los riesgos de seguridad de la información y ciberseguridad de la Asociación Scouts de Colombia pueden ser sujeto de diversas opciones de tratamiento que se abordarán en el desarrollo del objetivo 2.

DESARROLLO DE OBJETIVO 2 – PLAN DE TRATAMIENTO DE RIESGOS

Un Plan de Tratamiento del Riesgo debe responder a un compromiso institucional por la mejora y se debe basar en el análisis de riesgos como fuente de recolección principal de información y en una política de gestión del riesgo como soporte procedimental y que debe orientarse en los siguientes aspectos:

a. Establecimiento de variables que puedan afectar los principios de confidencialidad, integridad y disponibilidad de la información, en ese orden de ideas se deben identificar los factores generadores de riesgos, que para el caso de la Asociación Scouts de Colombia se encuentran enmarcados en:

    - Conocimientos en temas de seguridad de parte de los empleados y voluntarios encargados del manejo de data sensible.
    - Conocimientos en temas de protección de datos personales por parte de los empleados y voluntarios encargados del manejo de data sensible.
    - Inexistencia de sistemas de control interno informático, auditorias de T.I o gestión de riesgos digitales.
    - Desarrollo de proyectos de transformación digital.
    - Inexistencia de políticas y procedimientos de seguridad digital.
    - Información de jóvenes y niños, susceptible de ser robada por ciberdelincuentes con destino a pedófilos.
    - Entorno tecnológico en permanente cambio.
    - Gestión de datos personales de sus asociados y las implicaciones que la Ley 1581 de 2012 le da a la entidad como responsable del tratamiento.

b. Selección de la metodología de gestión que para el caso de la Asociación Scouts de Colombia corresponde a la SP 800-30 del NIST, cuyos pasos fueron enumerados en el desarrollo del objetivo 1. El marco de gestión de riesgos del NIST incluye una guía para su aplicación en el documento SP 800-37[14] que considera los siguientes pasos:

    - Clasificación por categorías: Para determinar la importancia de la información y el impacto que se puede dar en caso de afectaciones graves.
    - Selección de controles: Con base en la categorización de la data se deben escoger salvaguardas técnicas, operativas y de proceso para establecer una línea base de controles.

[14] NIST Special Publication 800-37, Guide for Applying the Risk Management Framework. Recuperado de: https://www.nist.gov/system/files/documents/2018/03/28/vickie_nist_risk_management_framework_overview-hpc.pdf

- Implementación de controles: Este paso consiste en la redacción de políticas y procedimientos y en la ejecución de las mejores prácticas de ingeniería en los diferentes activos.
- Evaluación: Para Determinar la eficacia de los controles de seguridad a través de la implementación de indicadores.
- Autorización: Se debe asignar un rol a una persona o grupo de personas que se encarguen de establecer si los riesgos detectados se pueden tolerar.
- Monitorear: Implementando una revisión permanente para detectar posibles cambios y para establecer oportunidades de mejora.

c. Asignación de responsables y presupuestos: Una vez que se establezcan las opciones de tratamiento se deben asignar recursos técnicos, administrativos, financieros y logísticos con los que se pueda garantizar el cumplimiento de los planes y la mejora continua de la gestión de seguridad. De igual manera, cada opción de tratamiento escogida debe ser encargada a una persona, área o entidad que lidere las actividades y que haga seguimiento a la mejora a través de indicadores de gestión.

   Para hacer el seguimiento se propone el uso del formato relacionado en la Tabla 7:

Tabla 7 Formato para seguimiento de Riesgos

ID Riesgo	Calificación Riesgo	Opción de tratamiento escogida	Responsable Interno	Presupuesto asignado	Indicador de Gestión			
					Q1	Q2	Q3	Q4

Fuente: Elaboración propia

d. Elección de las opciones de tratamiento del riesgo: basándose en el apetito al riesgo de la entidad se puede escoger:

- Aceptar: Tolerar el riesgo en la organización ya que no afecta los procesos ni la seguridad
- Reducir: Manejar el riesgo a través de la implementación de controles.
- Transferir: Ceder el riesgo a un tercero para compartir los métodos de control.
- Eliminar: Retirar de la organización procesos, sistemas de información o data que puedan causar incidentes de seguridad.
- Dispersar: Dividir la actividad que causa riesgo en diferentes subactividades para no tener concentración de responsabilidades.

De acuerdo con el análisis de riesgos realizado en el desarrollo del objetivo 1 se proponen las siguientes opciones de tratamiento para los riesgos detectados:

Tabla 8 Tratamiento del Riesgo sugerido

ID Riesgo	Descripción Riesgo	Calificación Riesgo	Opción de Tratamiento	Justificación
R1	Sistemas de información mal configurados por falta de conocimiento de los implementadores	12	Reducir	Ejecutar tunning de las aplicaciones
R2	Usuarios finales sin una adecuada sensibilización en temas de seguridad de la información y ciberseguridad	16	Transferir	Encargar a un tercero de capacitar a los usuarios
R3	Afectaciones a los sistemas de información y a la data causados por funcionarios y voluntarios de la Asociación que tengan motivaciones personales en contra de la organización.	5	Reducir	Firmar acuerdos de confidencialidad con funcionarios y sensibilizar a los voluntarios
R4	Acceso físico no autorizado a las oficinas por fallas en los controles de acceso.	10	Transferir	Contratar una empresa de vigilancia que realice monitoreo
R5	Acceso lógico no autorizado a los sistemas de información por fallas en los controles de acceso.	5	Transferir	Encargar a un tercero (contratado o voluntario) del monitoreo de los sistemas de información
R6	Equipos de cómputo propios con firmas de antivirus desactualizadas	8	Reducir	Revisar periódicamente las actualizaciones
R7	Equipos de cómputo en modelo BYOD con firmas de antivirus desactualizadas o sin un software de antivirus.	12	Transferir	Revisar periódicamente las actualizaciones por parte del usuario
R8	Afectaciones en el servicio de energía eléctrica que provoquen daños en hardware y pérdida de información.	12	Aceptar	La organización puede tolerar tiempos sin el servicio
R9	Equipos de cómputo que han superado su vida útil y siguen en uso poniendo en peligro la integridad de la información	12	Eliminar	Dar de baja equipos sin soporte
R10	Daño físico de discos duros extraíbles y memorias USB generando pérdida de información	10	Eliminar	Compartir información exclusivamente por el servicio de OneDrive de Microsoft ®

R11	Uso no autorizado de dispositivos removibles en los que se pueda extraer información sensible.	15	Eliminar	Compartir información exclusivamente por el servicio de OneDrive de Microsoft ®
R12	Falta de rutinas de mantenimiento de software y hardware que ocasionen daños irreparables	10	Reducir	Crear cronograma de mantenimiento anual
R13	Permitir que en las aplicaciones se utilicen usuarios administradores por default (ej, root, admin, administrador)	5	Reducir	Crear usuarios con perfil administrativo, pero no super usuario
R14	Software no actualizado a sus últimas versiones que puede generar vulnerabilidades a toda la red.	15	Reducir	Revisar periódicamente las actualizaciones de software disponibles
R15	Instalación no autorizada de software en equipos corporativos.	20	Eliminar	Permitir las actualizaciones únicamente a administradores autorizados
R16	Software no licenciado o crackeado que puede generar inconvenientes legales a la Asociación.	8	Eliminar	Creación de línea base de software autorizado y eliminación de apps detectadas
R17	Dispositivos de red con altos niveles de desgaste que disminuyan el performance de la red.	2	Aceptar	Convivir con el riesgo mientras se suben servicios de red a nube
R18	Acceso a sitios web desde los que se pueda descargar malware.	20	Reducir	Implementar control de navegación web
R19	Acceso a sitios web que generen alto tráfico generando afectaciones al rendimiento de la red.	15	Reducir	Implementar control de navegación web
R20	Canales de comunicación sin redundancia lo que puede generar afectaciones a la disponibilidad de los servicios.	15	Aceptar	La organización puede tolerar tiempos sin el servicio
R21	Bases de datos inadecuadamente protegidas generando posibilidad de robo o pérdida de información sensible.	10	Reducir	Realizar revisión permanente de permisos y seguridad de las bases de datos
R22	Datos de niñas, niños y adolescentes protegidos de manera inadecuada, ocasionando faltas a la Ley 1581 de 2012.	5	Reducir	Realizar revisión permanente de permisos y seguridad de las bases de datos
R23	Respaldos de información mal ejecutados o ausencia de los mismos.	10	Eliminar	Archivar datos exclusivamente En el servicio de OneDrive de Microsoft ®
R24	Repositorios de datos protegidos inadecuadamente	5	Eliminar	Archivar datos exclusivamente En el servicio de OneDrive de Microsoft ®

Fuente: Elaboración propia

DESARROLLO DE OBJETIVO 3 – PRESENTACIÓN DEL ESTADO DE LA SEGURIDAD DE LA ENTIDAD

La socialización del estado de la seguridad es un documento de alto nivel que será presentado al Consejo Scout Nacional como máximo organismo de la entidad y se compone de los siguientes ítems:

Importancia de la Seguridad Digital para la Asociación

La esencia de las actividades de la Asociación Scouts de Colombia se centra en la vida al aire libre y en el desarrollo de habilidades blandas para los niños y jóvenes de 6 a 21 años; esto no sería posible sin el respaldo administrativo de la Oficina Nacional y su equipo de colaboradores y voluntarios. En el desarrollo de esas actividades operativas se hace necesaria la mejora de capacidades corporativas orientadas hacia la seguridad digital; los esfuerzos que en materia de transformación digital se realicen se pueden ver disminuidos si los nuevos sistemas de información no son configurados y protegidos adecuadamente.

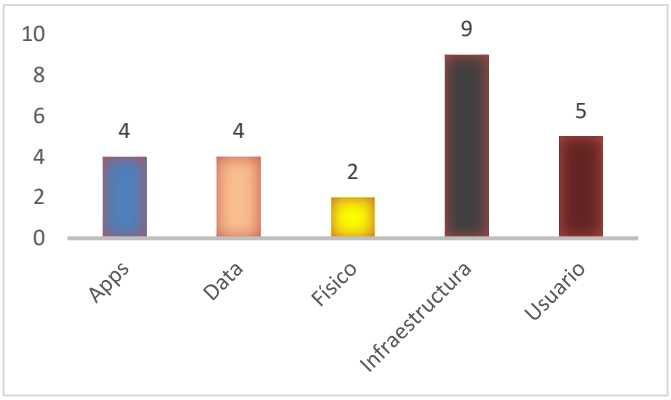
Establecer una postura de seguridad digital corporativa con unos requisitos mínimos para el funcionamiento de la arquitectura de T.I empresarial se convierte en un ejercicio de responsabilidad corporativa y se debe integrar al ADN de la Asociación pues hay exposición permanente al riesgo de robo de información, situación que puede acarrear efectos secundarios como perdida de la imagen corporativa y detrimento al patrimonio.

Adicionalmente, alinear la Asociación Scouts de Colombia hacia procesos de calidad y mejora continua como los que se derivan de la gestión de la seguridad digital, puede despertar la atención de nuevos patrocinadores desde la empresa privada que por sus políticas internas sólo pueden realizar donaciones a entidades eficientes y con visión de control.

Hallazgos del Análisis de Riesgos

Con base en el análisis GAP realizado y en las vulnerabilidades detectadas, se consideraron 24 riesgos relacionados con diferentes categorías de los servicios de T.I de la entidad como se pueden apreciar en la Figura 7 – Riesgos por Categoria:

Figura 7 Riesgos por Categoría

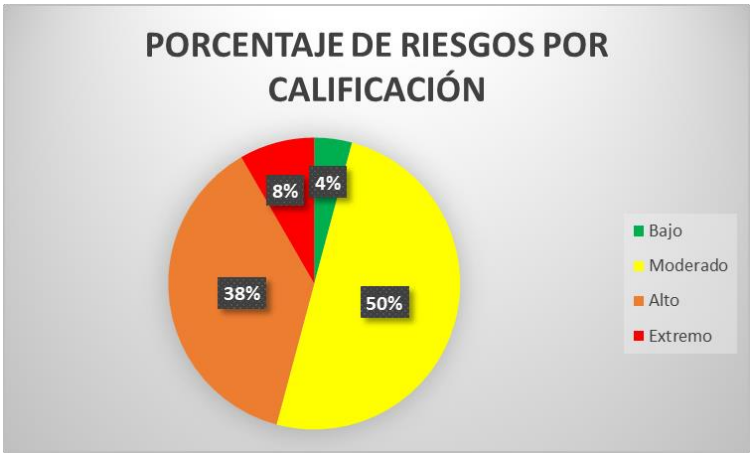


Fuente: Elaboración propia

La mayoría de los riesgos corresponden a temas relacionados con la infraestructura de T.I, se evidencia que la falta de procedimientos y supervisión en la materia inciden en la exposición; muchas organizaciones optan por tercerizar estas actividades para ceder el riesgo, pero la gran cantidad de voluntarios de la Asociación que son profesionales en temas de T.I y que pudieran donar parte de su tiempo es una oportunidad de mejora que se ve en el camino, la motivación para obtener esas manos de apoyo se puede dar a través de la socialización de los resultados del análisis de riesgos realizado para el presente estudio.

La calificación de los 24 riesgos por mapa de calor está distribuida porcentualmente como se puede apreciar en la Figura 8 Riesgos por Calificación

Figura 8 Riesgos por Calificación



Fuente: Elaboración propia

El 46% de los riesgos de seguridad de la información para la Asociación Scouts de Colombia están en niveles no tolerables, por lo que se hace inmediata la intervención. Al realizar un análisis sobre la calificación del impacto de los riesgos

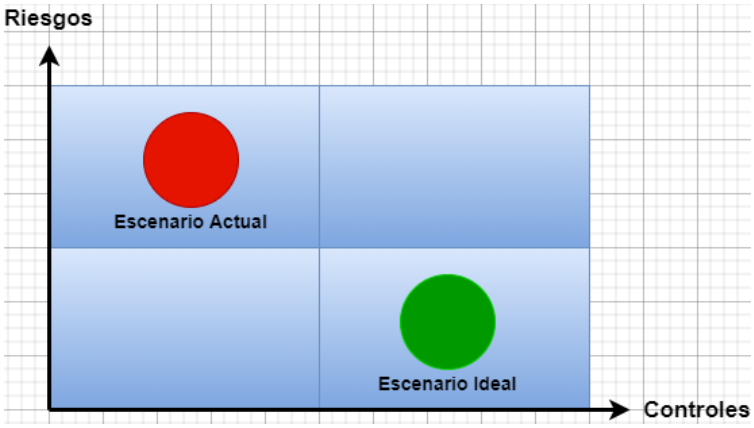
analizados, se puede establecer que frente a la materialización y sin controles el impacto sería elevado pues 21 de los 24 riesgos están en los niveles mayor y catastrófico.

Estado de la Seguridad

El análisis de riesgos efectuado para los servicios de T.I de la Asociación Scouts de Colombia evidencia que el estado de la seguridad se encuentra en un nivel bajo con elevadas oportunidades de mejora debido a la falta de controles, de políticas y a la cantidad de amenazas del entorno.

En la Figura 9 - Escenarios se muestra el estado actual y donde se pretende llegar con la implementación de las mejoras:

Figura 9 Escenarios



Fuente: Elaboración propia

Mantener el Escenario Actual puede traer implicaciones a nivel de todos los procesos de la Asociación, repercutir en gastos económicos no presupuestados y dar al traste con las iniciativas de transformación digital patrocinadas desde el Consejo Scout Nacional.

Oportunidades de mejora

Después del análisis e investigación realizados al interior de la entidad se han detectado las siguientes oportunidades de mejora:

a. Los sistemas de información corporativos como SISCOUT y Talento 360 cuentan con niveles de seguridad básicos, la administración debe dedicar esfuerzos especiales para fortalecer este aspecto.
b. No existe una política de seguridad de la información establecida para la entidad, su redacción y puesta en marcha puede cimentar la estrategia de protección hacia el futuro.

c. La gestión de riesgos en materia de seguridad de la información y ciberseguridad debe ser incluida en los planes corporativos.
d. No es evidente el compromiso del Consejo Scout Nacional como máximo órgano rector de la entidad con la seguridad digital.
e. Los equipos de cómputo propios y en modalidad BYOD que sean usados por los colaboradores y voluntarios para el tratamiento de información corporativa requieren un proceso de revisión permanente que garantice unos mínimos de protección.
f. La data corporativa reposa en diferentes ubicaciones, se deben preferir los sitios seguros y con respaldo permanente.
g. Las comunicaciones a través de correo electrónico en el nivel corporativo no se realizan exclusivamente a través del dominio @scout.org.co aspecto que pone en riesgo la confidencialidad de los datos.
h. No se han surtido procesos de análisis de vulnerabilidades y/o ethical hacking a los activos de información corporativos, por lo que se desconoce qué tan vulnerables pueden ser.
i. Al no generar restricciones en la navegación web se corre el riesgo de contagio por accesos indebidos a contenido inseguro.
j. No se mide la reputación de la Asociación en las redes sociales

Plan Director de Seguridad (PDS)

Este plan consiste en definir y dar prioridad a una serie de proyectos con los cuales se minimicen los riesgos de seguridad de la información y ciberseguridad; estos planes deben responder a las necesidades de la Asociación y estar en línea con los proyectos estratégicos de la Dirección Nacional de Desarrollo Institucional.

El PDS para la Asociación Scouts de Colombia se debe implementar con las siguientes fases:

a. Análisis de Cumplimiento: Para establecer que los controles propuestos se ejecutan adecuadamente a través de la medición de la madurez de estos y para revisar en conjunto con los asesores jurídicos que las obligaciones en materia de protección de datos se cumplan acorde a la ley.
b. Definir objetivos de seguridad: Con el análisis de riesgos y los proyectos estratégicos como base se deben establecer las metas a cumplir en el corto, mediano y largo plazo; deben ser prioridad entre otros el dar cumplimiento a los principios de seguridad en todos los sistemas de información, asegurar que no haya fuga de datos en ninguna parte de la cadena de procesos corporativos y garantizar la continuidad del negocio.
c. Establecer proyectos de seguridad: Para poder garantizar umbrales de protección adecuados se deben priorizar los siguientes proyectos:

- Establecimiento de una política de seguridad de la información documentada y aprobada por el Consejo Scout Nacional.
- Sensibilización en materia de seguridad de la información y ciberseguridad para los colaboradores y voluntarios de la Asociación.
- Implementación de herramientas de prevención de perdida de datos (DLP)
- Establecer una metodología de etiquetado y clasificación de información corporativa.
- Mejorar las capacidades de la Asociación en materia de respaldo de información para la data ubicada tanto en Office 365 como en los diferentes sistemas de información.

d. Poner en marcha el plan con la aprobación y asignación de presupuesto por parte del Consejo Scout Nacional.

DESARROLLO DE OBJETIVO 4 – PROPUESTA DE CONTROLES

En seguridad de la información, un control o salvaguarda es una medida preventiva que toma una organización para aumentar los niveles de protección de los activos de información. Estos controles se pueden catalogar desde el proceso en preventivos, detectivos y correctivos y desde la ejecución en técnicos, administrativos y físicos.

Después del análisis de riesgos y teniendo en cuenta el marco de la metodología NIST y la naturaleza de la organización se sugiere la implementación de los siguientes controles en la Asociación Scouts de Colombia distribuidos para cada fase del NIST de la siguiente manera:

Fase de Identificación

Teniendo en cuenta que esta fase aborda procesos relacionados con la caracterización de la seguridad en una organización, se recomiendan los controles relacionados en la Tabla 9 – Controles Fase de Identificación:

Tabla 9 Controles Fase de Identificación

ID_Control	Categoría	Descripción del Control	Periodicidad
IDE-1	Gestión de activos	El software, hardware y sistemas de telecomunicaciones deben ser inventariados asignando responsable, criticidad y valor.	Anual
IDE-2	Gestión de activos	Los sistemas de información deben estar adecuadamente catalogados	Anual
IDE-3	Gestión de activos	Se deben establecer responsables para la gestión de la seguridad digital dentro de la Asociación.	Anual
IDE-4	Entorno empresarial	Garantizar que dentro de los planes estratégicos de la Asociación se incluyan acciones encaminadas en la mejora continua de la seguridad digital.	Anual
IDE-5	Gobernanza	Establecer y comunicar la Política de Seguridad a las partes interesadas.	Anual
IDE-6	Gobernanza	Revisar los requisitos legales y de compliance con respecto a temas de seguridad digital.	Anual
IDE-7	Evaluación de riesgos	identificar y documentar las vulnerabilidades detectadas en los activos de información.	Semestral
IDE-8	Evaluación de riesgos	Estar en contacto permanente con expertos en la materia para estar actualizados sobre las novedades.	Diario
IDE-9	Evaluación de riesgos	Identificar y documentar las amenazas del entorno e internas.	Anual
IDE-10	Evaluación de riesgos	Identificar y evaluar las probabilidades e impactos de las amenazas.	Anual
IDE-11	Evaluación de riesgos	Determinar el riesgo residual de seguridad digital.	Anual
IDE-12	Estrategia de gestión de riesgos	Garantizar tratamiento adecuado a los riesgos detectados y evaluados.	Anual

IDE-13	Estrategia de gestión de riesgos	Establecer los niveles de tolerancia y apetito de riesgo digital de la Asociación.	Anual
IDE-14	Gestión del riesgo de la cadena de suministro	Identificar y comunicar a la alta dirección cuales riesgos de seguridad digital pueden impactar los procesos core de la Asociación.	Anual
IDE-15	Gestión del riesgo de la cadena de suministro	Garantizar que en los contratos con terceros prestadores de servicios de T.I se establezcan acuerdos de confidencialidad.	Anual
IDE-16	Gestión del riesgo de la cadena de suministro	Evaluar periódicamente los proveedores de servicios de T.I	Anual

Fuente: Elaboración propia

Fase de Protección

Teniendo en cuenta que esta fase aborda procesos relacionados con la puesta en marcha de líneas de defensa adecuadas a nivel corporativo, se recomiendan los controles relacionados en la Tabla 10 – Controles Fase de Protección:

Tabla 10 Controles Fase de Protección

ID_Control	Categoría	Descripción del Control	Periodicidad
PRO-1	Gestión de identidad	Se debe realizar gestión del acceso físico que se pueda tener a los activos de información	Anual
PRO-2	Gestión de identidad	Se deben entregar usuarios a los colaboradores y voluntarios con los mínimos privilegios	Permanente
PRO-3	Gestión de identidad	Garantizar que los accesos realizados de manera remota se realicen bajo condiciones óptimas de seguridad.	Anual
PRO-4	Gestión de identidad	Se deben eliminar las cuentas de usuario que ya no estén en uso por retiro del colaborador o voluntario.	Mensual
PRO-5	Concientización y capacitación	Todos los colaboradores y voluntarios que intervengan en procesos que incluyan manejo de información deben recibir capacitación sobre la política y buenas prácticas de seguridad digital.	Anual
PRO-6	Concientización y capacitación	El Consejo Scout Nacional debe estar al tanto de su responsabilidad frente a la seguridad digital.	Anual
PRO-7	Concientización y capacitación	Los responsables de la seguridad digital deben comprender su rol y capacitarse permanentemente en la materia.	Permanente
PRO-8	Seguridad de los datos	Se deben establecer medidas para la protección de los datos en transito	Semestral
PRO-9	Seguridad de los datos	Se deben establecer medidas para la protección de los datos en reposo	Semestral
PRO-10	Seguridad de los datos	Los datos deben ser respaldados periódicamente y se debe garantizar retención adecuada de la información de	Mensual

		acuerdo con las necesidades de la Asociación.	
PRO-11	Seguridad de los datos	Implementar medidas de protección de perdida de datos (DLP) en las diferentes plataformas de software	Anual
PRO-12	Seguridad de los datos	Realizar ejercicios con los que se garantice la integridad de la data en las diferentes bases de datos.	Semestral
PRO-13	Procesos y procedimientos de protección de la información	Crear y mantener configuraciones base (líneas base o hardening) de software y hardware	Anual
PRO-14	Procesos y procedimientos de protección de la información	Se deben realizar instalaciones e implementaciones sólo después de haber surtido un proceso de verificación (Gestión de cambios)	Trimestral
PRO-15	Procesos y procedimientos de protección de la información	El borrado y destrucción de información sólo se puede realizar con autorización de los dueños de los activos y se debe documentar.	Semestral
PRO-16	Procesos y procedimientos de protección de la información	Se debe aplicar un proceso de gestión de incidentes de seguridad digital.	Semestral
PRO-17	Procesos y procedimientos de protección de la información	Se debe aplicar un proceso de gestión de vulnerabilidades.	Semestral
PRO-18	Procesos y procedimientos de protección de la información	Los equipos de cómputo propios y en modelo BYOD deben estar protegidos con una solución de antivirus.	Semestral
PRO-19	Mantenimiento	Los mantenimientos preventivos y correctivos a los diferentes activos de información deben planearse y documentarse	Semestral
PRO-20	Mantenimiento	Si se realizan mantenimientos preventivos y correctivos de forma remota se deben realizar bajo condiciones óptimas de seguridad.	Semestral
PRO-21	Tecnología de protección	Los sistemas de información deben tener habilitadas las opciones de auditoria en caso de requerirse para la atención de incidentes de seguridad.	Anual
PRO-22	Tecnología de protección	Se debe restringir el uso de medios extraíbles, los autorizados deben estar documentados.	Trimestral
PRO-23	Tecnología de protección	La red interna debe protegerse física y lógicamente	Semestral

Fuente: Elaboración propia

Fase de Detección

Teniendo en cuenta que esta fase aborda procesos relacionados con el descubrimiento oportuno de amenazas y debilidades, se recomiendan los controles relacionados en la Tabla 11 – Controles Fase de Detección:

Tabla 11 Controles Fase de Detección

ID_Control	Categoría	Descripción del Control	Periodicidad
DET-1	Anomalías y Eventos	Se deben analizar los eventos relevantes de los sistemas de información y se determina su impacto.	Mensual
DET-2	Monitoreo Continuo	La red debe ser monitoreada para determinar disminuciones en el performance y posibles incidentes de seguridad	Mensual
DET-3	Monitoreo Continuo	Los accesos físicos y las instalaciones en general se deben monitorear para determinar novedades que puedan afectar la seguridad digital	Mensual
DET-4	Monitoreo Continuo	El acceso a Internet debe ser monitoreado para evitar el acceso a sitios que puedan tener malware o que sean fuente de robo de información	Mensual
DET-5	Monitoreo Continuo	Se deben realizar ejercicios de análisis de vulnerabilidades y ethical hacking a las plataformas	Anual

Fuente: Elaboración propia

Fase de Respuesta

Teniendo en cuenta que esta fase aborda procesos relacionados con la oportunidad de reacción ante incidentes, se recomiendan los controles relacionados en la Tabla 12 – Controles Fase de Respuesta:

Tabla 12 Controles Fase de Respuesta

ID_Control	Categoría	Descripción del Control	Periodicidad
RES-1	Planificación de la Respuesta	Se debe ejecutar un plan de respuesta a incidentes durante y después de la ocurrencia del mismo	Permanente
RES-2	Comunicaciones	Todos los colaboradores y voluntarios deben conocer sus roles frente a un incidente de seguridad	Permanente
RES-3	Comunicaciones	Los incidentes de seguridad digital se comunican a diferentes niveles de acuerdo a su relevancia	Permanente
RES-4	Análisis	Se realiza valoración del impacto de los incidentes de seguridad.	Permanente
RES-5	Análisis	Se realiza clasificación de los incidentes de seguridad según las categorías preestablecidas.	Permanente

RES-6	Análisis	Según la gravedad del incidente, se realiza análisis forense de los activos de información.	Permanente
RES-7	Mitigación	Al momento de presentarse un incidente se contiene y mitiga documentando cada paso y recolectando las evidencias	Permanente
RES-8	Mejora	Todo incidente de seguridad digital debe dejar lecciones aprendidas para la Asociación	Permanente

Fuente: Elaboración propia

Fase de Recuperación

Teniendo en cuenta que esta fase aborda procesos relacionados con la capacidad de resilencia, se recomiendan los controles relacionados en la Tabla 11 – Controles Fase de Detección:

Tabla 13 Controles Fase de Recuperación

ID_Control	Categoría	Descripción del Control	Periodicidad
REC-1	Planificación de la recuperación	Se debe ejecutar un plan de recuperación ante incidentes después de la ocurrencia del mismo	Permanente
REC-2	Mejoras	Los planes de recuperación deben incluir lecciones aprendidas	Permanente
REC-3	Mejoras	Después de un incidente se deben actualizar los mecanismos y estrategias de recuperación	Permanente
REC-4	Comunicaciones	Si el incidente afectó la imagen institucional se debe establecer un plan de comunicaciones para reparar los daños.	Permanente
REC-5	Comunicaciones	Las tareas de recuperación después de un incidente de seguridad digital se comunican a diferentes niveles de acuerdo a su relevancia	Permanente

Fuente: Elaboración propia

CONCLUSIONES

- El análisis de riesgos realizado para la Asociación Scouts de Colombia utilizando la metodología SP 800-30 del NIST permitió determinar una serie de debilidades que requieren atención urgente y compromiso de la alta dirección por el establecimiento de controles adecuados y definición de presupuesto para la materia; adicionalmente implementar esta revisión de manera periódica puede generar mayor visibilidad a las falencias acelerando el proceso de gestión del riesgo e impulsando un ambiente de cumplimiento normativo y regulatorio aceptable

- El tratamiento de riesgos debe iniciar cuanto antes para minimizar los efectos de la exposición a la que está expuesta la entidad; es importante empezar por los riesgos que se pueden reducir o eliminar en el corto plazo e inmediatamente continuar con los que se transferirán. Se deben asignar responsables para cada plan de acción a implementar que lideren la puesta en marcha de las actividades y que reporten resultados a la Alta Dirección

- Hace sentido la implementación del Plan Director de Seguridad para subir el nivel de confianza y preservar de esta manera los principios de la seguridad de la información; por la naturaleza de la entidad es importante poder establecer las pautas en las que los voluntarios realizarán su ejecución así como el apoyo requerido de los colaboradores directos, en su implementación el plan debe entregar los parámetros para futuras adquisiciones de software y servicios de T.I con un enfoque orientado a la seguridad digital.

- La propuesta de controles realizada busca mejorar el nivel de seguridad de la entidad, sólo la evaluación al menos anual de la eficacia de los controles y el seguimiento a los planes de mejora puede garantizar que el objetivo de hacer una entidad más segura con el paso de los años sea viable. Adicionalmente se puede implementar una figura de “autocontrol” en la que los dueños de los activos de información que no necesariamente sean técnicos puedan ejecutar medidas de revisión y monitoreo de activos.

RECOMENDACIONES

De acuerdo con el análisis realizado en cumplimiento de los objetivos del proyecto aplicado y entendiendo la naturaleza, funcionamiento y actividades de la Asociación Scouts de Colombia se sugiere tener en cuenta las siguientes recomendaciones presentadas con el objeto de mejorar los niveles de seguridad y mitigar los riesgos asociados al procesamiento y almacenamiento de información:

- Establecer una Política de Seguridad Digital: para darle un marco corporativo a la seguridad y mostrar que es un tema que se trata con preocupación desde el Consejo Nacional.
- Implementar análisis de riesgos de seguridad digital: Para tener una visual adecuada de los peligros a los que se exponen los activos de información corporativa.
- Sensibilizar a los usuarios finales: Para permear a toda la Asociación sobre los riesgos de seguridad digital y las mejores prácticas que desde su puesto de trabajo pueden realizar para mejorar la seguridad.
- Garantizar el uso del software antivirus: Para tener una primera línea de defensa contra ciberataques en los endpoint.
- Definir mecanismos de continuidad: Para poder continuar con el cumplimiento de las funciones administrativas y de programa frente a circunstancias adversas.
- Mejorar el proceso de uso de medios extraíbles: Para evitar la fuga no controlada de información y disminuir la posibilidad de ingreso de malware a la red corporativa.
- Evaluar los permisos de administración: Para entregar a cada usuario únicamente los accesos necesarios partiendo del principio del mínimo privilegio.
- Controlar el acceso a Internet: Para evitar el uso inadecuado de la herramienta que puede redundar en afectaciones al performance de la red, fuga de información e ingreso de malware a la red.
- Monitorear la reputación de la entidad en las redes sociales: Para disminuir el riesgo de ataques contra la marca y detener a tiempo los que se sucedan.
- Implementar un Plan Director de Seguridad que sea la guía para la mejora continua de los umbrales de protección de información.

BIBLIOGRAFÍA

- ABBSOH, Omar – BISELL Kelly. SECURING THE DIGITAL ECONOMY. {En línea} 2019. {Octubre 7 de 2020} Disponible en: https://www.accenture.com/_acnmedia/thought-leadership-assets/pdf/accenture-securing-the-digital-economy-reinventing-the-internet-for-trust.pdf

- AMBIT BST. ¿Para qué sirve un SGSI? Controles y fases. {En línea} 2021. {Octubre 22 de 2021} Disponible en: https://www.ambit-bst.com/blog/para-qu%C3%A9-sirve-un-sgsi-controles-y-fases

- ASOCIACIÓN SCOUTS DE COLOMBIA. Política Nacional de Desarrollo Institucional. {En línea} 2017. {Julio 21 de 2020} Disponible en: https://scout.org.co/wp-content/uploads/2019/11/Politica-Nacional-de-Desarrollo-Institucional-2017.pdf

- BUSTAMANTE TOLEDO, Pedro. Una metodología simplificada de gestión de riesgo en seguridad de información basada en ISO/IEC27005 y modelado de amenazas para una institución de educación superior. {En línea} 2020. {Marzo 6 de 2021} Disponible en https://www.mti.cl/wp-content/uploads/2020/01/Tesina_final-1.pdf

- CARALT, Emilia – CARRERAS Ignasi – SUREDA, María. La transformación digital en las ONG. Conceptos, soluciones y casos prácticos. {En línea} 2017. {Octubre 17 de 2020} Disponible en: https://www.pwc.es/es/fundacion/assets/transformacion-digital-en-las-ong-pwc-esade-iis.pdf

- CASTELLI, Christopher – GABRIEL, Barbara. Global State of Information Security Survey. {En línea} 2017. {Noviembre 1 de 2020} Disponible en: https://www.pwc.com/us/en/cybersecurity/assets/pwc-strengthening-digital-society-against-cyber-shocks.pdf

- CATALINA M. - Agente de Soporte de Microsoft. ¿Que es un Tenant?. {En línea} 2019. {Octubre 3 de 2020} Disponible en: https://trainingsupport.microsoft.com/es-es/msia/forum/all/qu%C3%A9-es-un-tenant/d1087068-a90e-44d3-b5ba-44955e34afd3

- CCIT – POLICIA NACIONAL DE COLOMBIA – CISCO. Informe de las tendencias del cibercrimen en Colombia 2019-2020. {En línea} 2020. {Abril 14

de 2021} Disponible en: https://www.ccit.org.co/wpcontent/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

- CISET. ¿Qué es el hardening de sistemas operativos?. {En línea} 2020. {Febrero 3 de 2021}. Disponible en: https://www.ciset.es/publicaciones/blog/746-hardening

- DEPARTAMENTO ADMINISTRATIVO PARA LA PROSPERIDAD SOCIAL. Plan de Tratamiento de Riesgos y Seguridad de la Información. {En línea} 2021. {Junio 2 de 2021}. Disponible en: http://centrodedocumentacion.prosperidadsocial.gov.co/2021/OAP/2-Planes-Estrategicos/Plan-Tratamiento-de-Riesgos-y-seguridad-de-la-informacion-2021.pdf

- ESET LATINOAMERICA. Security Report – Latinoamérica 2020. {En línea} 2021. {Junio 2 de 2021}.Disponible en: https://www.welivesecurity.com/wp-content/uploads/2020/08/ESET-Security-Report-LATAM_2020.pdf

- FEDERAL TRADE COMMISION. Ciberseguridad para pequeños negocios. {En línea} Sin fecha específica en documento. {Junio 2 de 2021}. Disponible en: https://www.ftc.gov/es/system/files/attachments/understanding-nistcybersecurity-framework/cybersecurity_sb_nist-cyber-framework-es.pdf

- INCIBE. Protección de la Información. {En línea} 2020. {Noviembre 22 de 2020}. Disponible en: https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_proteccion-de-la-informacion.pdf

- INCIBE. Plan Director de Seguridad. {En línea} Sin fecha específica en documento. {Julio 14 de 2021}. Disponible en: https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan-director-seguridad.pdf

- INSTITUTO NACIONAL DE ESTÁNDARES Y TECNOLOGÍA – Estados Unidos. Marco para la mejora de la seguridad cibernética en infraestructuras críticas. {En línea} 2018. {Agosto 16 de 2020}. Disponible en: https://www.nist.gov/system/files/documents/2018/12/10/frameworkesmellrev_20181102mn_clean.pdf

- INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Norma Técnica Colombiana ISO 31000. Gestión del riesgo. principios y directrices. Requisitos. 2013

- INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Norma técnica NTC-ISO/IEC Colombiana 27000 Tecnología de la Información. técnicas de seguridad. Sistemas de gestión de seguridad de la información (SGSI). Visión general y vocabulario. 2013

- INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. Information technology — Security techniques — Guidelin. {En línea} Sin fecha específica en documento. {Febrero 14 de 2021}. Disponible en: https://www.iso.org/standard/44375.html

- MINTIC COLOMBIA. Elaboración de la política general de seguridad y privacidad de la información. {En línea} 2016. {Agosto 18 de 2020}. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

- MUÑOZ, Carlos. Metodología de la Investigación. D.R. © Oxford University Press México, S.A. de C.V. {En línea} 2016. {Agosto 19 de 2020}. Disponible en: https://corladancash.com/wp-content/uploads/2019/08/56-Metodologia-de-la-investigacion-Carlos-I.-Munoz-Rocha.pdf

- NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Guide for Conducting Risk Assessments. {En línea} 2012. {Septiembre 1 de 2020}. Disponible en: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

- NEDETEL. Seguridad Informática. {En línea} Sin fecha específica en documento. {Agosto 19 de 2020}. Disponible en: https://www.nedetel.net/seguridad-informatica/

- OEA – AWS. Marco de Ciberseguridad NIST / Un abordaje integral de la Ciberseguridad. {En línea} 2019. {Agosto 30 de 2020}. Disponible en: https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-CiberseguridadESP.pdf

- OFICINA DE SEGURIDAD DEL INTERNAUTA. Wireshark. {En línea} Sin fecha específica en documento. {Agosto 19 de 2020}. Disponible en: https://www.osi.es/es/herramientas-gratuitas/wireshark

- PAGO SIMPLE. Seguridad de la Información. {En línea} Sin fecha específica en documento. {Febrero 3 de 2021}. Disponible en: https://pagosimple.com/seguridad-de-la-informacion/

- RIVEROS, Jorge. Manual de gestión para el área Administrativa y Financiera Asociación Scouts de Colombia. {En línea} 2014. {Noviembre 19 de 2020}. Disponible en : https://scout.org.co/wp-content/uploads/2019/11/Manual-Area-Administrativa-y-Financiera-V4-2015.pdf

- ROJAS, Marcelo. Tipos de Investigación científica: Una simplificación de la complicada incoherente nomenclatura y clasificación. REDVET. Revista Electrónica de Veterinaria, vol. 16, núm. 1, 2015, pp. 1-14Veterinaria Organización Málaga, España. {En línea} 2015 {Septiembre 1 de 2020}. Disponible en: https://www.redalyc.org/pdf/636/63638739004.pdf

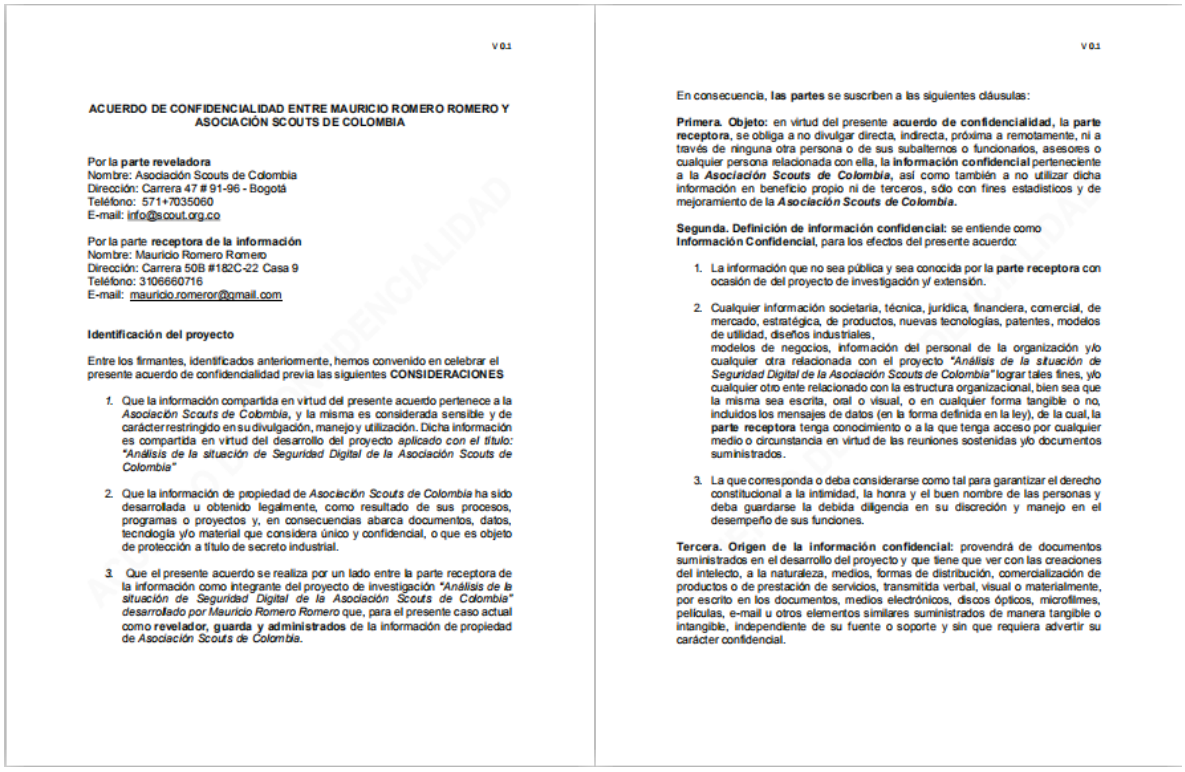
- SOFISTIC CYBERSECURITY. La breve historia de la ciberseguridad. {En línea} 2019 {Septiembre 13 de 2020}. Disponible en: https://www.sofistic.com/blog-ciberseguridad/la-breve-historia-de-la-ciberseguridad/

- VARELA, Alfredo. (2018). Estado de la Seguridad Digital en las pymes de Latinoamérica. {En línea} 2018 {Novtiembre 11 de 2020}. Disponible en: https://ticsyformacion.com/2018/08/19/estado-de-la-seguridad-digital-en-las-pymes-de-latinoamerica-infografia-ciberseguridad/

- WORLD SCOUT BUREAU INC. Pauta de Política de Gestión de Riesgos - Movimiento Scout Seguro. {En línea} 2017 {Agosto 21 de 2020}. Disponible en: https://www.scout.org/sites/default/files/library_files/Pauta%20Politica%20de%20gestion%20de%20riesgos%20final%20%28marzoLDM%29.pdf

ANEXOS

ANEXO A ACUERDO DE CONFIDENCIALIDAD ENTRE LAS PARTES



V 0.1

ACUERDO DE CONFIDENCIALIDAD ENTRE MAURICIO ROMERO ROMERO Y ASOCIACIÓN SCOUTS DE COLOMBIA

Por la **parte reveladora**
Nombre: Asociación Scouts de Colombia
Dirección: Carrera 47 # 91-96 - Bogotá
Teléfono: 571+7035060
E-mail: info@scout.org.co

Por la parte **receptora de la información**
Nombre: Mauricio Romero Romero
Dirección: Carrera 50B #182C-22 Casa 9
Teléfono: 3106660716
E-mail: mauricio.romeror@gmail.com

Identificación del proyecto

Entre los firmantes, identificados anteriormente, hemos convenido en celebrar el presente acuerdo de confidencialidad previa las siguientes **CONSIDERACIONES**

1. Que la información compartida en virtud del presente acuerdo pertenece a la *Asociación Scouts de Colombia*, y la misma es considerada sensible y de carácter restringido en su divulgación, manejo y utilización. Dicha información es compartida en virtud del desarrollo del proyecto *aplicado con el título: "Análisis de la situación de Seguridad Digital de la Asociación Scouts de Colombia"*

2. Que la información de propiedad de *Asociación Scouts de Colombia* ha sido desarrollada u obtenido legalmente, como resultado de sus procesos, programas o proyectos y, en consecuencias abarca documentos, datos, tecnología y/o material que considera único y confidencial, o que es objeto de protección a título de secreto industrial.

3. Que el presente acuerdo se realiza por un lado entre la parte receptora de la información como integrante del proyecto de investigación *"Análisis de la situación de Seguridad Digital de la Asociación Scouts de Colombia" desarrollado por Mauricio Romero Romero* que, para el presente caso actual como **revelador, guarda y administrados** de la información de propiedad de *Asociación Scouts de Colombia*.

V 0.1

En consecuencia, **las partes** se suscriben a las siguientes cláusulas:

Primera. Objeto: en virtud del presente **acuerdo de confidencialidad**, la **parte receptora**, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, asesores o cualquier persona relacionada con ella, la **información confidencial** perteneciente a la ***Asociación Scouts de Colombia***, así como también a no utilizar dicha información en beneficio propio ni de terceros, sólo con fines estadísticos y de mejoramiento de la ***Asociación Scouts de Colombia***.

Segunda. Definición de información confidencial: se entiende como **Información Confidencial**, para los efectos del presente acuerdo:

1. La información que no sea pública y sea conocida por la **parte receptora** con ocasión de del proyecto de investigación y/ extensión.

2. Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales,
modelos de negocios, información del personal de la organización y/o cualquier otra relacionada con el proyecto *"Análisis de la situación de Seguridad Digital de la Asociación Scouts de Colombia"* lograr tales fines, y/o cualquier otro ente relacionado con la estructura organizacional, bien sea que la misma sea escrita, oral o visual, o en cualquier forma tangible o no, incluidos los mensajes de datos (en la forma definida en la ley), de la cual, la **parte receptora** tenga conocimiento o a la que tenga acceso por cualquier medio o circunstancia en virtud de las reuniones sostenidas y/o documentos suministrados.

3. La que corresponda o deba considerarse como tal para garantizar el derecho constitucional a la intimidad, la honra y el buen nombre de las personas y deba guardarse la debida diligencia en su discreción y manejo en el desempeño de sus funciones.

Tercera. Origen de la información confidencial: provendrá de documentos suministrados en el desarrollo del proyecto y que tiene que ver con las creaciones del intelecto, a la naturaleza, medios, formas de distribución, comercialización de productos o de prestación de servicios, transmitida verbal, visual o materialmente, por escrito en los documentos, medios electrónicos, discos ópticos, microfilmes, películas, e-mail u otros elementos similares suministrados de manera tangible o intangible, independiente de su fuente o soporte y sin que requiera advertir su carácter confidencial.

Cuarta. Obligaciones de la parte receptora: Se considerará como **parte receptora** de la **información confidencial** a la persona que recibe la información, o que tenga acceso a ella. La parte receptora se obliga a:

De ser necesario o conveniente según la necesidad del titular de la información, se adicionarán las obligaciones que se consideren pertinentes:

1. Mantener la **información confidencial** segura, usarla solamente para los propósitos relacionados con él, en caso de ser solicitada, devolverla toda (incluyendo copias de esta) en el momento en que ya no requiera hacer uso de la misma o cuando termine la relación, caso en el cual, deberá entregar dicha información antes de la terminación de la vinculación.
2. Proteger la **información confidencial**, sea verbal, escrita, visual, tangible, intangible o que por cualquier otro medio reciba, siendo legítima poseedora de la misma *Asociación Scouts de Colombia*, restringiendo su uso exclusivamente a las personas que tengan absoluta necesidad de conocerla.
3. Abstenerse de publicar la **información confidencial** que conozca, reciba o intercambie con ocasión de las reuniones sostenidas.
4. Usar la **información confidencial** que se le entregue, únicamente para los efectos señalados al momento de la entrega de dicha información.
5. Mantener la **información confidencial** en reserva hasta tanto adquiera el carácter de pública.
6. Responder por el mal uso que le den sus representantes a la **información confidencial.**
7. Guardar la reserva de la **información confidencial** como mínimo, con el mismo cuidado con la que protege la **información confidencial.**
8. La **parte receptora** se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la **información confidencial** sin el previo consentimiento por escrito por parte de la ***Asociación Scouts de Colombia.***
9. La **parte receptora** se compromete a establecer que los datos a utilizar son: *Información de los sistemas de información utilizados por la Asociación en el desarrollo de sus actividades misionales, reportes de redes sociales, datos de proyectos que involucren aspectos tecnológicos y toda la información que la Asociación considere necesaria para hacer los seguimientos del caso.*

10. La información capturada por la **parte receptora** se observará como *cifras para estudio estadístico, comparativo, información cualitativa*, no existirá ningún tipo de ganancia económica, es netamente educativo.
11. La identidad de todo el personal de la ***Asociación Scouts de Colombia*** no será revelada, dado que no se capturará sus nombres completos ni algún otro tipo de información que revele su identidad física o digital.
12. Las pruebas realizadas por la **parte receptora** nunca pondrán en peligro los activos tecnológicos de ***Asociación Scouts de Colombia,*** ni violentará la ley de delitos informáticos colombiana 1273 de 2009 estando en el margen de las buenas prácticas y los procesos legales pertinentes.
13. El estudiante *Mauricio Romero Romero* se compromete a difuminar, bloquear y ocultar toda información que revele la identidad de la empresa *Asociación Scouts de Colombia* para salvaguardar la confidencialidad e identidad de la empresa en el documento final del proyecto el cual será publicado en el respositorio institucional y de acceso público.
14. El título del proyecto no podrá contener el nombre de la empresa u organización con la que se firma el presente acuerdo de confidencialidad, este nombre deberá ser reemplazado.

Parágrafo: Cualquier divulgación autorizada de la **información confidencial** a terceras personas estará sujeta a las mismas obligaciones de confidencialidad derivadas del presente **Acuerdo** y la **parte receptora** deberá informar estas restricciones incluyendo la identificación de la información cono confidencial.

Quinta. Obligaciones de la parte reveladora: Son obligaciones de la parte reveladora:

1. Mantener la reserva de la **información confidencial** hasta tanto adquiera el carácter de pública.
2. Documentar toda la **información confidencial** que transmita de manera escrita, oral o visual, mediante documentos, medios electrónicos, discos ópticos, microfilmes, películas, e-mails u otros elementos similares o en cualquier forma tangible o no, incluidos los mensajes de datos, como registro de la misma para la determinación de sus alcance, e indicar específicamente y de manera clara e inequívoca el carácter confidencia de la información suministrada de la **parte receptora.**

Sexta. Exclusiones a la confidencialidad: La **parte receptora** queda relevada o eximida de la obligación de confidencialidad, únicamente en los siguientes casos:

1. Cuando la **información confidencial** haya sido o sea de dominio público. Si la información se hace de dominio público durante el plazo del presente acuerdo, por un hecho ajeno a la **parte receptora,** esta conservará su deber de reserva sobre la información que no haya sido afectada.
2. Cuando la **información confidencial** deba ser revelada por sentencia en firme de un tribunal o autoridades competentes en desarrollo de sus funciones que ordenen el levantamiento de la reserva y soliciten el suministro de esta información. No obstante, en este caso la parte reveladora será la encargada de dar cumplimiento a la orden, restringiendo la divulgación a la información estrictamente necesaria, y en el evento de que la confidencialidad se mantenga, no eximirá a la parte receptora del deber de reserva.
3. Cuando la **parte receptora pruebe** que la **información confidencial** ha sido obtenida por otras fuentes.
4. Cuando la **información confidencial** ya la tenía en su poder la parte receptora antes de la entrega de la información reservada.

Séptima. Responsabilidad: la parte que contravenga el acuerdo será responsable ante la otra parte o ante los terceros de buena fe sobre los cuales se demuestre que se han visto afectados por la inobservancia del presente **acuerdo,** por los perjuicios morales y económicos que estos puedan sufrir como resultado del incumplimiento de las obligaciones aquí contenidas.

Octava. Solución de controversias: Las partes (*Mauricio Romero Romero – Asociación Scouts de Colombia*) se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente **acuerdo.** En caso de no llegar a una solución directa para la controversia planteada, someterán la cuestión controvertida a las leyes colombianas y a la jurisdicción competente en el momento de presentarse la diferencia. La Universidad Nacional Abierta y a Distancia como institución educativa no se hace responsable del no cumplimiento de las cláusulas del presente acuerdo de confidencialidad por parte de *Mauricio Romero Romero*

Novena. Legislación aplicable: Este **acuerdo** se regirá por las leyes de la República de Colombia y se interpretará de acuerdo con las mismas.

Décima. Aceptación del Acuerdo: Las partes han leído y estudiado de manera detenida los términos y el contenido del presente **Acuerdo** y por tanto manifiestan estar conformes y aceptan todas las condiciones.

Firman en Bogotá D.C., a los 15 días del mes de Octubre de 2020

Como Parte Receptora:

Mauricio Romero Romero.
Estudiante UNAD.
C.C. No. 79971195 de Bogotá

Por la parte reveladora:

Representante Legal
Asociación Scouts de Colombia
C.C. No.508.213 de Medellín

ANEXO B RESPUESTAS CUESTIONARIO GAP

Función	Categoría	Descripción categoría	Subcategoría	Descripción Subcategoría	Respuesta/comentario	Valoración % cumplimiento
1. IDENTIFICAR (ID)	1. Gestión de activos (ID.AM)	Los datos, el personal, los dispositivos, los sistemas y las instalaciones que permiten a la organización alcanzar los objetivos empresariales se identifican y se administran de forma coherente con su importancia relativa para los objetivos organizativos y la estrategia de riesgos de la organización.	ID.AM-1	Los dispositivos y sistemas físicos dentro de la organización están inventariados.	Se tiene inventario desde la parte contable de los equipos propios y del software adquirido	50%
1. IDENTIFICAR (ID)	1. Gestión de activos (ID.AM)	Los datos, el personal, los dispositivos, los sistemas y las instalaciones que permiten a la organización alcanzar los objetivos empresariales se identifican y se administran de forma coherente con su importancia relativa para los objetivos organizativos y la estrategia de riesgos de la organización.	ID.AM-2	Las plataformas de software y las aplicaciones dentro de la organización están inventariadas.	Sólo desde el punto de vista contable	50%
1. IDENTIFICAR (ID)	1. Gestión de activos (ID.AM)	Los datos, el personal, los dispositivos, los sistemas y las instalaciones que permiten a la organización alcanzar los objetivos empresariales se identifican y se administran de forma coherente con su importancia relativa para los objetivos organizativos y la estrategia de riesgos de la organización.	ID.AM-3	La comunicación organizacional y los flujos de datos están mapeados.	Hay encargados y procesos para las comunicaciones , pero no todos los flujos de datos han sido mapeados	60%
1. IDENTIFICAR (ID)	1. Gestión de activos (ID.AM)	Los datos, el personal, los dispositivos, los sistemas y las instalaciones que permiten a la organización alcanzar los objetivos empresariales se identifican y se administran de forma coherente con su importancia relativa para los objetivos organizativos y la estrategia de riesgos de la organización.	ID.AM-4	Los sistemas de información externos están catalogados.	No	0%
1. IDENTIFICAR (ID)	1. Gestión de activos (ID.AM)	Los datos, el personal, los dispositivos, los sistemas y las instalaciones que permiten a la organización alcanzar los objetivos empresariales se identifican y se administran de forma coherente con su importancia relativa para los objetivos organizativos y la estrategia de riesgos de la organización.	ID.AM-5	Los recursos (por ejemplo, hardware, dispositivos, datos, tiempo, personal y software) se priorizan en función de su clasificación, criticidad y valor comercial.	La valoración se realiza sólo desde el punto de vista contable	50%
1. IDENTIFICAR (ID)	1. Gestión de activos (ID.AM)	Los datos, el personal, los dispositivos, los sistemas y las instalaciones que permiten a la organización alcanzar los objetivos empresariales se identifican y se administran de forma coherente con su importancia relativa para los objetivos organizativos y la estrategia de riesgos de la organización.	ID.AM-6	Los roles y las responsabilidades de la seguridad cibernética para toda la fuerza de trabajo y terceros interesados (por ejemplo, proveedores, clientes, socios) están establecidas.	No	0%
1. IDENTIFICAR (ID)	2. Entorno empresarial (ID.BE)	Se entienden y se priorizan la misión, los objetivos, las partes interesadas y las actividades de la organización; esta información se utiliza para informar los roles, responsabilidades y decisiones de gestión de los riesgos de seguridad cibernética.	ID.BE-1	Se identifica y se comunica la función de la organización en la cadena de suministro.	Si, las funciones de la Asociación son conocidas por la sociedad civil	70%
1. IDENTIFICAR (ID)	2. Entorno empresarial (ID.BE)	Se entienden y se priorizan la misión, los objetivos, las partes interesadas y las actividades de la organización; esta información se utiliza para informar los roles, responsabilidades y decisiones de gestión de los riesgos de seguridad cibernética.	ID.BE-2	Se identifica y se comunica el lugar de la organización en la infraestructura crítica y su sector industrial.	Si, se comparte información con otras Organizaciones Juveniles	70%

1. IDENTIFICAR (ID)	2. Entorno empresarial (ID.BE)	Se entienden y se priorizan la misión, los objetivos, las partes interesadas y las actividades de la organización; esta información se utiliza para informar los roles, responsabilidades y decisiones de gestión de los riesgos de seguridad cibernética.	ID.BE-3	Se establecen y se comunican las prioridades para la misión, los objetivos y las actividades de la organización.	Si, hay responsables de las comunicaciones corporativas pero no se incluyen temas de ciberseguridad	70%
1. IDENTIFICAR (ID)	2. Entorno empresarial (ID.BE)	Se entienden y se priorizan la misión, los objetivos, las partes interesadas y las actividades de la organización; esta información se utiliza para informar los roles, responsabilidades y decisiones de gestión de los riesgos de seguridad cibernética.	ID.BE-4	Se establecen las dependencias y funciones fundamentales para la entrega de servicios críticos.	No hay un area dedicada a Tecnología, sólo colaboradores ocasionales	60%
1. IDENTIFICAR (ID)	2. Entorno empresarial (ID.BE)	Se entienden y se priorizan la misión, los objetivos, las partes interesadas y las actividades de la organización; esta información se utiliza para informar los roles, responsabilidades y decisiones de gestión de los riesgos de seguridad cibernética.	ID.BE-5	Los requisitos de resiliencia para respaldar la entrega de servicios críticos se establecen para todos los estados operativos (p. ej. bajo coacción o ataque, durante la recuperación y operaciones normales).	No, aún no se diseñan planes de continuidad de la operación administrativa	20%
1. IDENTIFICAR (ID)	3. Gobernanza (ID.GV)	Las políticas, los procedimientos y los procesos para administrar y monitorear los requisitos regulatorios, legales, de riesgo, ambientales y operativos de la organización se comprenden y se informan a la gestión del riesgo de seguridad cibernética.	ID.GV-1	Se establece y se comunica la política de seguridad cibernética organizacional.	No existe una política de seguridad cibernética	0%
1. IDENTIFICAR (ID)	3. Gobernanza (ID.GV)	Las políticas, los procedimientos y los procesos para administrar y monitorear los requisitos regulatorios, legales, de riesgo, ambientales y operativos de la organización se comprenden y se informan a la gestión del riesgo de seguridad cibernética.	ID.GV-2	Los roles y las responsabilidades de seguridad cibernética están coordinados y alineados con roles internos y socios externos.	No hay un area dedicada a manejar temas de ciberseguridad, sólo colaboradores ocasionales	60%
1. IDENTIFICAR (ID)	3. Gobernanza (ID.GV)	Las políticas, los procedimientos y los procesos para administrar y monitorear los requisitos regulatorios, legales, de riesgo, ambientales y operativos de la organización se comprenden y se informan a la gestión del riesgo de seguridad cibernética.	ID.GV-3	Se comprenden y se gestionan los requisitos legales y regulatorios con respecto a la seguridad cibernética, incluidas las obligaciones de privacidad y libertades civiles.	Si, hay accciones frente a Ley 1581 de 2012	80%
1. IDENTIFICAR (ID)	3. Gobernanza (ID.GV)	Las políticas, los procedimientos y los procesos para administrar y monitorear los requisitos regulatorios, legales, de riesgo, ambientales y operativos de la organización se comprenden y se informan a la gestión del riesgo de seguridad cibernética.	ID.GV-4	Los procesos de gobernanza y gestión de riesgos abordan los riesgos de seguridad cibernética.	No, la gestión de riesgos no incluye temas de ciberseguridad	0%
1. IDENTIFICAR (ID)	4. Evaluación de riesgos (ID.RA)	La organización comprende el riesgo de seguridad cibernética para las operaciones de la organización (incluida la misión, las funciones, la imagen o la reputación), los activos de la organización y las personas.	ID.RA-1	Se identifican y se documentan las vulnerabilidades de los activos.	No	0%

1. IDENTIFICAR (ID)	4. Evaluación de riesgos (ID.RA)	La organización comprende el riesgo de seguridad cibernética para las operaciones de la organización (incluida la misión, las funciones, la imagen o la reputación), los activos de la organización y las personas.	ID.RA-2	La inteligencia de amenazas cibernéticas se recibe de foros y fuentes de intercambio de información.	No hay procesos al respecto, los terceros críticos se encargan de su producto	40%
1. IDENTIFICAR (ID)	4. Evaluación de riesgos (ID.RA)	La organización comprende el riesgo de seguridad cibernética para las operaciones de la organización (incluida la misión, las funciones, la imagen o la reputación), los activos de la organización y las personas.	ID.RA-3	Se identifican y se documentan las amenazas, tanto internas como externas.	No	0%
1. IDENTIFICAR (ID)	4. Evaluación de riesgos (ID.RA)	La organización comprende el riesgo de seguridad cibernética para las operaciones de la organización (incluida la misión, las funciones, la imagen o la reputación), los activos de la organización y las personas.	ID.RA-4	Se identifican los impactos y las probabilidades del negocio.	Desde los procesos administrativos y financieros se realizan estos análisis no desde lo tecnológivo	60%
1. IDENTIFICAR (ID)	4. Evaluación de riesgos (ID.RA)	La organización comprende el riesgo de seguridad cibernética para las operaciones de la organización (incluida la misión, las funciones, la imagen o la reputación), los activos de la organización y las personas.	ID.RA-5	Se utilizan las amenazas, las vulnerabilidades, las probabilidades y los impactos para determinar el riesgo.	Desde los procesos administrativos y financieros se realizan estos análisis no desde lo tecnológivo	60%
1. IDENTIFICAR (ID)	4. Evaluación de riesgos (ID.RA)	La organización comprende el riesgo de seguridad cibernética para las operaciones de la organización (incluida la misión, las funciones, la imagen o la reputación), los activos de la organización y las personas.	ID.RA-6	Se identifican y priorizan las respuestas al riesgo.	Desde los procesos administrativos y financieros se realizan estos análisis no desde lo tecnológivo	60%
1. IDENTIFICAR (ID)	5. Estrategia de gestión de riesgos (ID.RM)	Se establecen las prioridades, restricciones, tolerancias de riesgo y suposiciones de la organización y se usan para respaldar las decisiones de riesgos operacionales.	ID.RM-1	Los actores de la organización establecen, gestionan y acuerdan los procesos de gestión de riesgos.	Sólo para temas administrativos y financieros	60%
1. IDENTIFICAR (ID)	5. Estrategia de gestión de riesgos (ID.RM)	Se establecen las prioridades, restricciones, tolerancias de riesgo y suposiciones de la organización y se usan para respaldar las decisiones de riesgos operacionales.	ID.RM-2	La tolerancia al riesgo organizacional se determina y se expresa claramente.	Sólo para temas administrativos y financieros	60%
1. IDENTIFICAR (ID)	5. Estrategia de gestión de riesgos (ID.RM)	Se establecen las prioridades, restricciones, tolerancias de riesgo y suposiciones de la organización y se usan para respaldar las decisiones de riesgos operacionales.	ID.RM-3	La determinación de la tolerancia del riesgo de la organización se basa en parte en su rol en la infraestructura crítica y el análisis del riesgo específico del sector.	Sólo para temas administrativos y financieros	60%

1. IDENTIFICAR (ID)	6. Gestión del riesgo de la cadena de suministro (ID.SC)	Las prioridades, limitaciones, tolerancias de riesgo y suposiciones de la organización se establecen y se utilizan para respaldar las decisiones de riesgo asociadas con la gestión del riesgo de la cadena de suministro. La organización ha establecido e implementado los procesos para identificar, evaluar y gestionar los riesgos de la cadena de suministro.	ID.SC-1	Los actores de la organización identifican, establecen, evalúan, gestionan y acuerdan los procesos de gestión del riesgo de la cadena de suministro cibernética.	No, la gestión de riesgos no incluye temas de ciberseguridad	20%
1. IDENTIFICAR (ID)	6. Gestión del riesgo de la cadena de suministro (ID.SC)	Las prioridades, limitaciones, tolerancias de riesgo y suposiciones de la organización se establecen y se utilizan para respaldar las decisiones de riesgo asociadas con la gestión del riesgo de la cadena de suministro. La organización ha establecido e implementado los procesos para identificar, evaluar y gestionar los riesgos de la cadena de suministro.	ID.SC-2	Los proveedores y socios externos de los sistemas de información, componentes y servicios se identifican, se priorizan y se evalúan mediante un proceso de evaluación de riesgos de la cadena de suministro cibernético.	Se surten procesos de escogencia de proveedores con un procedimiento preestablecido	70%
1. IDENTIFICAR (ID)	6. Gestión del riesgo de la cadena de suministro (ID.SC)	Las prioridades, limitaciones, tolerancias de riesgo y suposiciones de la organización se establecen y se utilizan para respaldar las decisiones de riesgo asociadas con la gestión del riesgo de la cadena de suministro. La organización ha establecido e implementado los procesos para identificar, evaluar y gestionar los riesgos de la cadena de suministro.	ID.SC-3	Los contratos con proveedores y socios externos se utilizan para implementar medidas apropiadas diseñadas para cumplir con los objetivos del programa de seguridad cibernética de una organización y el plan de gestión de riesgos de la cadena de suministro cibernético.	Se incluyen clausulas de manejo de información sensible y acuerdos de confidencialidad	80%
1. IDENTIFICAR (ID)	6. Gestión del riesgo de la cadena de suministro (ID.SC)	Las prioridades, limitaciones, tolerancias de riesgo y suposiciones de la organización se establecen y se utilizan para respaldar las decisiones de riesgo asociadas con la gestión del riesgo de la cadena de suministro. La organización ha establecido e implementado los procesos para identificar, evaluar y gestionar los riesgos de la cadena de suministro.	ID.SC-4	Los proveedores y los socios externos se evalúan de forma rutinaria mediante auditorías, resultados de pruebas u otras formas de evaluación para confirmar que cumplen con sus obligaciones contractuales.	Revisión anual de proveedores desde lo financiero	50%
1. IDENTIFICAR (ID)	6. Gestión del riesgo de la cadena de suministro (ID.SC)	Las prioridades, limitaciones, tolerancias de riesgo y suposiciones de la organización se establecen y se utilizan para respaldar las decisiones de riesgo asociadas con la gestión del riesgo de la cadena de suministro. La organización ha establecido e implementado los procesos para identificar, evaluar y gestionar los riesgos de la cadena de suministro.	ID.SC-5	Las pruebas y la planificación de respuesta y recuperación se llevan a cabo con proveedores.	No, sólo se realizasn revisiones generales	20%

RESUMEN ANALÍTICO ESPECIALIZADO – RAE	
Fecha de Realización:	20/Nov/2021
Programa:	Especialización en Seguridad Informática
Línea de Investigación:	Gestión de Sistemas
Título:	ANÁLISIS DEL ESTADO DE LA SEGURIDAD DIGITAL DE LA ASOCIACIÓN SCOUTS DE COLOMBIA A TRAVÉS DEL USO DEL MARCO DE CIBERSEGURIDAD DEL NIST
Autor(es):	Romero Romero Javier Mauricio
Palabras Claves:	Ciberseguridad, NIST, Política de Seguridad, Controles de Seguridad, Riesgo Tecnológico
Descripción:	Las Organizaciones sin ánimo de lucro por la naturaleza propia de su misión tienen las TIC como instrumentos de apoyo pero la gran mayoría no ha podido fomentar iniciativas de seguridad por falta de presupuesto o de expertos en la materia e incluso porque aún no lo han visto como una necesidad; sin embargo los ciberdelincuentes están al acecho y no se detienen a la hora de atacar y su blanco puede ser cualquier tipo de organización, es más se han acercado a estas empresas del tercer sector de la economía pues manejan información bastante llamativa para sus malas intenciones. Este es el caso de la Asociación Scouts de Colombia, una entidad que presenta una necesidad en temas de protección de seguridad digital a causa del proyecto de modernización tecnológica que se inició recientemente; para determinar las mejoras requeridas se realizará un análisis de la situación actual y se propondrán acciones de mejora que permitan aumentar los niveles de seguridad corporativa. Para el desarrollo del proyecto aplicado que busca proteger los activos de información de la Asociación, se utilizará el marco del NIST; aplicando las 5 fases de este, realizando un análisis de riesgos de las diferentes plataformas e implementando los controles y procedimientos que surjan como parte del plan de tratamiento.

Fuentes bibliográficas destacadas:

- CARALT, Emilia – CARRERAS Ignasi – SUREDA, María. La transformación digital en las ONG. Conceptos, soluciones y casos prácticos. {En línea} 2017. {Octubre 17 de 2020} Disponible en: https://www.pwc.es/es/fundacion/assets/transformacion-digital-en-las-ong-pwc-esade-iis.pdf - Este documento es vital para el proyecto de grado pues da un marco sobre la realidad en temas de T.I de las organizaciones similares a que se está estudiando.

- INSTITUTO NACIONAL DE ESTÁNDARES Y TECNOLOGÍA – Estados Unidos. Marco para la mejora de la seguridad cibernética en infraestructuras críticas. {En línea} 2018. {Agosto 16 de 2020}. Disponible en: https://www.nist.gov/system/files/documents/2018/12/10/frameworkesmellrev_20181102mn_clean.pdf - Esta bibliografía se destaca por entregar todo el marco escogido para el análisis de riesgos e implementación de fases de trabajo para el diseño de los controles necesarios.

- INCIBE. Plan Director de Seguridad. {En línea} Sin fecha específica en documento. {Julio 14 de 2021}. Disponible en: https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan-director-seguridad.pdf - El documento del Plan Director es una guía en la que se sustenta una de las propuestas de mejora presentadas a la entidad analizada.

- MUÑOZ, Carlos. Metodología de la Investigación. D.R. © Oxford University Press México, S.A. de C.V. {En línea} 2016. {Agosto 19 de 2020}. Disponible en: https://corladancash.com/wp-content/uploads/2019/08/56-Metodologia-de-la-investigacion-Carlos-I.-Munoz-Rocha.pdf - La revisión de este texto permitió elaborar el marco metodológico del proyecto y darle el sustento teórico y académico necesario.

- WORLD SCOUT BUREAU INC. Pauta de Política de Gestión de Riesgos - Movimiento Scout Seguro. {En línea} 2017 {Agosto 21 de 2020}. Disponible en: https://www.scout.org/sites/default/files/library_files/Pauta%20Politica%20de%20gestion%20de%20riesgos%20final%20%28marzoLDM%29.pdf - Se utilizó este documento como base para conocer cómo funciona el tema de la gestión de Riesgos en el movimiento Scout en sus instancias superiores a nivel mundial y como estas mejores prácticas se pueden bajar a la oficina en Colombia.

Contenido del documento:	INTRODUCCIÓN 1. DEFINICIÓN DEL PROBLEMA o ANTECEDENTES DEL PROBLEMA o FORMULACIÓN DEL PROBLEMA 2. JUSTIFICACIÓN 3. OBJETIVOS o OBJETIVO GENERAL o OBJETIVOS ESPECÍFICOS 4. MARCO REFERENCIAL o MARCO TEÓRICO o MARCO CONCEPTUAL o MARCO TECNOLÓGICO o MARCO LEGAL o MARCO CONTEXTUAL 5. DISEÑO METODOLÓGICO 6. DESARROLLO DE LOS OBJETIVOS o DESARROLLO DE OBJETIVO 1 – ANÁLISIS DE RIESGOS o DESARROLLO DE OBJETIVO 2 – PLAN DE TRATAMIENTO DE RIESGOS o DESARROLLO DE OBJETIVO 3 – PRESENTACIÓN DEL ESTADO DE LA SEGURIDAD DE LA ENTIDAD o DESARROLLO DE OBJETIVO 4 – PROPUESTA DE CONTROLES CONCLUSIONES RECOMENDACIONES BIBLIOGRAFÍA ANEXOS
Diseño Metodológico:	Para el caso del estudio se busca indagar la situación actual de la seguridad de la entidad a través de la aplicación de las fases y actividades descritas por el marco de trabajo del NIST que se relacionan a continuación: 1. Identificación. 2. Protección. 3. Detección. 4. Respuesta. 5. Recuperación. Para la fase de Identificación fue necesario realizar una evaluación inicial del estado de la seguridad en la Asociación Scouts de Colombia a través de la aplicación de un cuestionario que mide el GAP frente a lo sugerido por el marco del NIST.

	Las fases de Protección, Detección, Respuesta y Recuperación se abordaron a través de la aplicación de la metodología de riesgos escogida y de los controles a implementar para cada fase que se derivan del análisis de riesgos realizado
Conceptos adquiridos:	En el desarrollo del presente proyecto se aprendió sobre el manejo de las TICS y la seguridad digital en las organizaciones del tercer sector de la economía; igualmente se adquirieron conocimientos en el desarrollo del marco de ciberseguridad del NIST como alternativa a los tradicionales ISO27001 y COBIT.
Conclusiones:	- El análisis de riesgos realizado para la Asociación Scouts de Colombia utilizando la metodología SP 800-30 del NIST permitió determinar una serie de debilidades que requieren atención urgente y compromiso de la alta dirección por el establecimiento de controles adecuados y definición de presupuesto para la materia; adicionalmente implementar esta revisión de manera periódica puede generar mayor visibilidad a las falencias acelerando el proceso de gestión del riesgo e impulsando un ambiente de cumplimiento normativo y regulatorio aceptable. - El tratamiento de riesgos debe iniciar cuanto antes para minimizar los efectos de la exposición a la que está expuesta la entidad; es importante empezar por los riesgos que se pueden reducir o eliminar en el corto plazo e inmediatamente continuar con los que se transferirán. Se deben asignar responsables para cada plan de acción a implementar que lideren la puesta en marcha de las actividades y que reporten resultados a la Alta Dirección. - Hace sentido la implementación del Plan Director de Seguridad para subir el nivel de confianza y preservar de esta manera los principios de la seguridad de la información; por la naturaleza de la entidad es importante poder establecer las pautas en las que los voluntarios realizarán su ejecución así como el apoyo requerido de los colaboradores directos, en su implementación el plan debe entregar los

	parámetros para futuras adquisiciones de software y servicios de T.I con un enfoque orientado a la seguridad digital. - La propuesta de controles realizada busca mejorar el nivel de seguridad de la entidad, sólo la evaluación al menos anual de la eficacia de los controles y el seguimiento a los planes de mejora puede garantizar que el objetivo de hacer una entidad más segura con el paso de los años sea viable. Adicionalmente se puede implementar una figura de “autocontrol” en la que los dueños de los activos de información que no necesariamente sean técnicos puedan ejecutar medidas de revisión y monitoreo de activos.