PLAN DE IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA UNIDAD ADMINISTRATIVA PARQUES NACIONALES NATURALES DE COLOMBIA, SEGÚN NORMA ISO 27001:2013

EDUIN GONZALEZ TABARES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
MEDELLIN
2018

PLAN DE IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA UNIDAD ADMINISTRATIVA PARQUES NACIONALES NATURALES DE COLOMBIA, SEGÚN NORMA ISO 27001:2013

ING. EDUIN GONZALEZ TABARES

Trabajo de grado para optar el título de:
Especialista en Seguridad Informática

Director del Proyecto:
Esp. DANIEL FELIPE PALOMO LUNA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
MEDELLIN
2018

Nota de Aceptación:

Aprobado por el comité de grado en cumplimiento de los requisitos exigidos por la Universidad Nacional Abierta y a Distancia UNAD Colombia Para optar por el título de Especialista en Seguridad Informática

---

Presidente del Jurado

Jurado

Jurado

Medellín, 01 de noviembre de 2018

DEDICATORIA

A toda mi familia,
A mi madre: María del socorro Tabares,
Mis hermanas Daysi, Sulma Danny
A mi esposa Laura
Mi hijo: Samuel González Rúa
A mis sobrinas
Y a mí fallecido padre: Gildardo González
Porque todos han tomado parte
y han contribuido en el desarrollo de este proyecto
no solo de grado sino de vida.

AGRADECIMIENTOS

Este proyecto de grado lo quiero dedicar:

En primer lugar, dedicarle a Dios por las múltiples bendiciones otorgadas en mi vida y darme la posibilidad de alcanzar metas y superarme cada día más, a mi madre por el apoyo incondicional igual a mis hermanas e hijo por el aliento constante cuando se me pasaba por la mente desertar.

Gracias a la UNAD cuerpo docente, asesores, directores de grado por su respaldo, apoyo, guía y orientación en el trascurso del desarrollo de la especialización

Gracias Dios a ti te dedico este inmenso éxito.

EDUIN GILDARDO GONZALEZ TABARES

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

pág.

INTRODUCCION

La entidad desea tener una propuesta que permita identificar, disminuir y mitigar los riesgos a los que se encuentra expuesta actualmente, desea contar con un Sistema de Gestión de Seguridad de la Información (SGSI) que permita proteger la confidencialidad, integridad y disponibilidad de sus datos. Esta propuesta será de gran importancia para la entidad, teniendo en cuenta que no ha definido políticas que tengan que ver con seguridad informática, otro aspecto inexistente es la asignación de responsabilidades en materia de seguridad el uso inadecuado de los recursos tecnológicos falta de control en navegación y uso inadecuado del correo electrónico.

La entidad no posee ningún método o control que le permita gestionar la seguridad de la información e identificar vulnerabilidades, riesgos y ataques a los que puede ser sometida, no existe documentación que evidencia procedimientos proactivos o de SGSI que puedan ayudar a solventar estas deficiencias poniendo en riesgo los activos de la organización.

La certificación de la entidad en la norma ISO 27001:2013 con un ente certificador no entra dentro de los objetivos prioritarios del plan de implantación del SGSI, pero es deseable el mayor cumplimiento posible de dicha norma, así como el cumplimiento del estándar de buenas prácticas ISO27002:2013 incluido en la norma.

1. PLANTEAMIENTO DEL PROBLEMA.

La entidad PARQUES NACIONALES NATURALES DE COLOMBIA, ha sido consciente de la necesidad de gestionar correctamente sus activos en materia de seguridad, y ya en 2017 se sentaron las bases de un proyecto para implantar su Sistema de gestión de la Seguridad de la Información, en adelante SGSI. Actualmente, la entidad ha querido dar aval al desarrollo e implantación de su SGSI, para conseguir su certificación.

La obtención de la ISO27001 es clave para que PARQUES NACIONALES NATURALES DE COLOMBIA, pueda ofrecer Integridad, confiabilidad y disponibilidad, buena conocedora de las necesidades actuales y futuras
La obtención de la certificación evidenciará el compromiso de PARQUES NACIONALES NATURALES DE COLOMBIA con la seguridad de los organismos contratantes, siendo un punto diferencial en comparación a las otras entidades del estado.

1.1 TRABAJOS PREVIOS.

El área de Redes y Sistemas de la Unidad Administrativa Especial denominada Parques Nacionales Naturales de Colombia no cuenta con un Sistema de Gestión de Seguridad de la Información (SGSI), que permita mantener la seguridad de la información y la de los activos de la institución en materia de *Hardware* , *Software* y equipo de comunicaciones, que admita asegurar la confidencialidad, integridad y disponibilidad de los datos; y las responsabilidades que debe asumir cada uno de los empleados de la organización. Actualmente el área de Redes y Sistemas no tiene documentación que le proporcione información sobre los procesos que se realizan por el personal del área, no existen manuales técnicos para el manejo de los sistemas de información, ni las políticas necesarias para el aseguramiento de la información.

Parques Nacionales Naturales de Colombia cuenta con varios procedimientos en los cuales se procesa información de gran importancia para la institución, permitiendo así; que trámites y servicios se realicen de manera más rápida en tiempo y formar, estos procesos están enfocados a la premisas del Modelo Estándar de Control Interno MECI 2014 (Decreto 943 de 2014), Norma Técnica de Calidad de la Gestión Pública NTC GP 1000:2009, Modelo Integrado de Planeación y Gestión MIPG (Decreto 2482 de 2012) para brindar un servicio y producto de calidad.

2. DEFINICIÓN DEL PROBLEMA.

¿Cuenta la entidad PARQUES NACIONALES NATURALES DE COLOMBIA, con un Modelo que le permita implementar un Sistema de Gestión de Seguridad de la información (SGSI) y/o protocolos de Seguridad que contribuyan al departamento de informática o área de sistemas a realizar una mejor gestión y control de los riesgos informáticos identificados por la entidad?

2.1 ANTECEDENTES DEL PROBLEMA.

Actualmente la entidad PARQUES NACIONALES NATURALES DE COLOMBIA. no posee ningún método o control que le permita gestionar la seguridad de la información e identificar vulnerabilidades, riesgos y ataques a los que puede ser sometida, no existe documentación que evidencia procedimientos proactivos o de SGSI que puedan ayudar a solventar estas deficiencias poniendo en riesgo los activos de la organización.

2.2 DESCRIPCION DEL PROBLEMA.

La entidad PARQUES NACIONALES NATURALES DE COLOMBIA desea tener una propuesta que permita identificar, disminuir y mitigar los riesgos al que se encuentra expuesta actualmente, Desea contar con un modelo de Gestión de Seguridad de la Información (SGSI) permitiendo proteger la confidencialidad, integridad y disponibilidad de la información. Esta propuesta será de gran importancia para la entidad, teniendo en cuenta que no ha definido políticas que tengan que ver con seguridad informática, otro aspecto inexistente es la asignación de responsabilidades en materia de seguridad, no se cuenta con procedimientos en materia de seguridad física y desastres de origen natural que afecten los activos de la entidad, entre los problemas más graves se encuentra el uso inadecuado de los recursos tecnológicos, falta de control en navegación por la internet y uso inadecuado del correo electrónico.

3. JUSTIFICACION.

La información es uno de los activos más valiosos de Parques Nacionales Naturales de Colombia y por lo tanto poder garantizar su integridad, confidencialidad, disponibilidad, autenticidad y trazabilidad es vital para conseguir los objetivos de negocio.

Continuamente las empresas están expuestas a riesgos, no sólo externos sino también internos, que ponen en peligro la integridad de la información y en consecuencia la viabilidad de los negocios.
Para poder trabajar en un entorno seguro, Parques Nacionales Naturales de Colombia ha decidido implementar un Sistema de Gestión de Seguridad de la información, a fin de preservar los dominios de la información que se acaban de citar, mediante una gestión efectiva de los riesgos. Esta decisión ha contado con el apoyo de la dirección, coordinación y la participación de toda la organización.

Definir los objetivos, necesidades y estructura de la entidad, definir el alcance de la implantación del SGSI. Esta implantación se llevará a cabo siguiendo un modelo PDCA, por sus siglas en inglés, *plan-do-check-act*, esto es, planificar-hacer-verificar-actuar, basado en un ciclo de mejora constante: una vez analizados los resultados de la primera aplicación, se vuelve a empezar.

La implantación de un SGSI basado en la norma UNE ISO / IEC27001 es un método de bajo costo que se encuentra al alcance de las grandes y pequeñas organizaciones y que les permitirá reducir los riesgos gracias al establecimiento y seguimiento de controles sobre estos y el ahorro de costos derivados de la racionalización de recursos ya que se eliminan inversiones ineficientes derivadas de desestimar o sobrestimar algunos riesgos. En paralelo la obtención opcional del certificado ISO / IEC27001 contribuye a mejorar la competitividad en el mercado diferenciando a la empresa y mejorando su imagen y confianza ante sus clientes, proveedores y socios.

4. OBJETIVOS.

4.1 OBJETIVO GENERAL.

Planear la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) para la Unidad Administrativa Parques Nacionales Naturales de Colombia, según la norma ISO 27001:2013, para poder reducir los riesgos, amenazas y vulnerabilidades que pueden afectar a los activos del área.

4.2 OBJETIVOS ESPECÍFICOS.

- Localizar los puntos más vulnerables dentro del área.
- Identificar las amenazas y los riesgos de que ocurran éstas.
- Seleccionar los controles de la norma ISO 27001 para la reducción de riesgos y amenazas en el área.
- Identificar el estado actual de los activos informáticos que serán objeto de protección por el SGSI
- Describir los fundamentos de un SGSI y Diseñar un SGSI acorde a las necesidades de la entidad
- Elaborar una guía básica con políticas y procedimientos, en base a las normas internacionales.

5. MARCO REFERENCIAL

La entidad necesita mejorar sus procesos para aplicar y cumplir la conceptualización SGSI y proponer una solución que permitirá reducir problemas y facilitar el desempeño de las actividades propias de cada dependencia dentro de la entidad.

5.1 MARCO TEORICO

La información y los procesos que la utilizan hacen parte de los activos más importantes de una organización. Definir, lograr, mantener y mejorar la seguridad de la información es esencial para mantener una ventaja competitiva que permita alcanzar el éxito y lograr continuidad en un mercado globalizado.

Para una organización competitiva es necesario implantar un sistema para la gestión de la seguridad de la información, que permita tener unos objetivos claros de seguridad y una evaluación de los riesgos posibles a los que esté expuesta su información, asegurando así la continuidad del negocio, minimizando el riesgo comercial y maximizando el retorno de las inversiones y las oportunidades comerciales.

La *International Organization for Standardization e International Electrotechnical Commission* ISO/IEC son los encargados de los estándares que proporcionan un marco de la gestión de la seguridad de la información utilizable para cualquier tipo de organización, privada o pública, pequeña o grande.

La norma ISO 17799 es un código de buenas prácticas para la Gestión de la Seguridad de la Información, esta norma surge como evolución histórica de la norma británica BS 7799 y actualmente existen varias adaptaciones de esta que convergerán en un futuro próximo a las normas de la serie ISO 27000.

La ISO 17799 introduce un cambio importante en los sistemas de gestión de la seguridad de la información ya que los aborda desde un punto de vista de continuidad de negocio y de mejora continua. Esta norma hereda muchos conceptos de la serie de normas ISO 9000 y subraya la seguridad entendida como proceso.

ISO/IEC 27000 es un conjunto de estándares desarrollados -o en fase de desarrollo- por ISO y IEC que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña; Los rangos de numeración reservados por ISO van de 27000 a 27019 y de 27030 a 27044.

La entidad necesita afinar sus procesos para aplicar y cumplir la conceptualización SGSI y proponer una solución que permitirá reducir problemas y facilitar el desempeño de las actividades propias de cada dependencia dentro de la entidad.

La evolución de las tecnologías de la información ha permitido automatizar y optimizar la gran mayoría de procesos y actividades que se llevan a cabo dentro de una entidad, convirtiéndose en uno de los activos más importantes.

Para implementar y gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27001, se utiliza el ciclo continuo PDCA, tradicional en los sistemas de gestión de la calidad.

- Plan (planificar): establecer el SGSI, se definen políticas y alcances.
- Do (hacer): implementar y utilizar el SGSI.
- Check (verificar): monitorizar, revisar y auditar el SGSI.
- Act (actuar): mantener y mejorar el SGSI tomando acciones correctivas y preventivas.

Mediante un Plan Director de Seguridad se definen y priorizan un conjunto de proyectos en materia de seguridad de la información, dirigiéndose a reducir los riesgos a los que está expuesta una entidad hasta unos niveles aceptables, partiendo de un análisis inicial.

5.2 MARCO CONCEPTUAL.

Se reseñan algunas definiciones significativas relacionadas al plan de implementación del sistema de gestión de seguridad de la información para la UNIDAD ADMINISTRATIVA PARQUES NACIONALES NATURALES DE COLOMBIA, según norma ISO 27001:2013.

5.2.1 **Dominios de control de las normas:** Cada una de las áreas o dominios de control de las normas establece una serie de pautas que serán seleccionadas dependiendo de los resultados obtenidos en el análisis de riesgos, además, existen controles obligatorios para toda organización, como es el de las políticas de seguridad cuyo número dependerá más de la organización que del estándar, el cual no establece este nivel de detalle.

5.2.1.1 **Políticas de seguridad:** El estándar define que se deben constituir las políticas de seguridad donde se documenten los procedimientos internos de la organización, reflejando las expectativas en materia de seguridad, las cuales deben servir de soporte para el comité de seguridad que revisa y actualiza dichos procedimientos.

5.2.1.2 **Estructura organizativa para la seguridad:** El estándar define que se deben constituir las políticas de seguridad donde se documenten los procedimientos internos de la organización, reflejando las expectativas en materia de seguridad, las cuales deben servir de soporte para el comité de seguridad que revisa y actualiza dichos procedimientos.

5.2.1.3 **Clasificación y control de activos:** se debe elaborar un inventario de activos relacionados con los recursos de información, para asegurar un nivel de protección adecuado a estos con base en ciertos criterios de clasificación y etiquetado de información, es decir, los activos serán etiquetados de acuerdo con su nivel de confidencialidad. Los recursos más importantes se describen a continuación:

- Computadoras (PCs, portátiles, servidores, mini e impresoras).
- Equipos de comunicaciones (*módem, switch, router, PBX, fax,* etc.)
- Archivos y bases de datos (con independencia de los medios de comunicación: el disco duro, *CD-ROM*, cinta, etc.)
- Aplicaciones (*Software*)
- Documentos (contratos, procedimientos, planes, registros, etc.).1

5.2.1.4 **Seguridad en el personal:** La seguridad del personal no se orienta desde la óptica de protección civil, sino para proporcionar controles a las acciones del personal que opera con los activos de información. El objetivo contempla establecer un plan que permita informar a los empleados sobre como operar con los activos de información en materia de seguridad y confidencialidad. Cada persona debe ser consciente de implementar los procesos adecuados y saber que está sujeto a sanciones (incluso legales) en caso de incumplimiento.

[1] SENA – Presentación ppt Estándares seguridad de la información. consultado el 20 de diciembre 2016 en: https://senaintro.blackboard.com/bbcswebdav/institution/semillas/217219_1_VIRTUAL/OAAPs/OAAP1/aa1/oa_estandarseguridad/index.html

5.2.1.5 **Seguridad física y del entorno:** Este dominio trata sobre la incorporación de medidas de protección a los equipos y *Software*, así como los controles en el manejo y transferencia de información y el acceso a las diferentes áreas, son puntos de vital importancia para evitar pérdidas o daños tanto físicos como lógicos en la información.

El perímetro de seguridad de un local debe ser protegido contra accesos no autorizados y contar con sistemas de protección ante riesgos o desastres naturales tales como fuego, inundaciones, sismos, etc. Esta debe ser una de las primeras acciones en ser implementada.

5.2.1.6 **Gestión de comunicaciones y operaciones:** Se debe asegurar la operación de la infraestructura tecnológica y de controles de seguridad para evitar la pérdida, modificación o uso indebido de la información que se intercambia dentro y desde la organización.

Para esto se integran los procedimientos de operación de la infraestructura tecnológica y de controles de seguridad documentados, documentando los procesos que van desde el control de cambios en la configuración de los equipos, manejo de incidentes, administración de aceptación de sistemas, hasta el control de código malicioso.

5.2.1.7 **Control de accesos:** Establecer mecanismos que permitan monitorear y controlar el acceso a los activos de información, para esto se deben definir procedimientos para la gestión de usuarios, identificación de responsabilidades o perfiles de seguridad y el control de acceso a las aplicaciones.

5.2.1.8 **Desarrollo y mantenimiento de sistemas:** Se deben incorporar controles de seguridad en todas las etapas del procesamiento de sistemas dentro de la organización, a partir de la gestión de las operaciones que se establezcan para garantizar la seguridad de acuerdo con las mejores prácticas definidas en las normas.

Se deben disponer de procedimientos que garanticen la calidad y seguridad de los sistemas desarrollados para tareas específicas de la organización.

5.2.1.9 **Gestión de continuidad del negocio:** Para garantizar la disponibilidad del servicio se deben contemplar planes de contingencia y recuperación ante desastres, donde se detallen los procedimientos a seguir para contrarrestar interrupciones en las actividades de la organización, así como los procesos más importantes, los cuales deberán ser revisados de manera constante para determinar las limitaciones de los mismos.

5.2.1.10 **Cumplimiento o conformidad de la legislación:** Se debe verificar que el cumplimiento de la norma concuerda con otros requisitos jurídicos. La organización debe establecer los requerimientos de seguridad que deben todas las partes involucradas en los procesos y estos se encontrarán formalizados en los contratos o convenios.

5.2.2 **Normas ISO 27000:** El estándar ISO 27000 apunta a exigir niveles concretos y adecuados de seguridad informática, niveles necesarios para las entidades que compiten a través del comercio electrónico y que por lo tanto tienen que exponer sus infraestructuras de información.[2]

Al aplicar en una entidad o institución un estándar como ISO 27000 el trabajo sobre la norma debe ser continuo, pues ISO año tras año publica nuevas modificaciones con el fin de asegurar una correcta gestión de la información de las organizaciones. Modificaciones orientadas a cubrir todas las posibles brechas de seguridad informática, que puedan llevar a cualquier tipo de riesgo la información de una organización.

La certificación ISO 27000 será una obligación de cualquier organización que desee exigir niveles concretos y adecuados de seguridad informática.

Algunas normas que están en fase de desarrollo son las ISO/IEC 27010, ISO/IEC 27013, ISO/IEC 27014, ISO/IEC 27015, ISO/IEC TR 27016, ISO/IEC 27017, ISO/IEC 27032, ISO/IEC 27033, ISO/IEC 27034, ISO/IEC 27036, ISO/IEC 27037, ISO/IEC 27038, ISO/IEC 27039, ISO/IEC 27040.

5.2.2.1 **ISO/IEC 27000:** Publicada 1 de junio de 2009.- Norma general de toda la serie 27000, una introducción a los SGSI, una breve descripción del ciclo PDCA.

[2] SENA – Presentación ppt Estándares seguridad de la información. consultado el 20 de diciembre 2016 en: https://senaintro.blackboard.com/bbcswebdav/institution/semillas/217219_1_VIRTUAL/OAAPs/OAAP1/aa1/oa_estandarseguridad/index.html

5.2.2.2 **ISO/IEC 27001:** Publicada el 15 de octubre de 2005.- Contiene requisitos de los SGSI, es el origen de la norma BS 7799-2:2002 (que ya quedó anulada), es la única norma de la serie 27000 que es certificable.

5.2.2.3 **ISO/IEC 27002:** Publicada el 1 de Julio de 2007.- Nuevo nombre de la ISO 17799:2005. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información.

5.2.2.4 **ISO/IEC 27003:** Publicada el 1 de febrero de 2010.- Se centra en el diseño, implementación, procesos, aprobación y planes en marcha para la dirección de un SGSI. Origen ANEXO B de la norma BS7799-2.

5.2.2.5 **ISO/IEC 27004:** Publicada el 15 de diciembre de 2009.- Determina la eficacia de un SGSI mediante el desarrollo de técnicas, controles y grupos implementados según ISO/IEC 27001.

5.2.2.6 **ISO/IEC 27005:** Publicado el 15 de junio de 2008 segunda edición 1 de junio 2011.- Proporcionado para la gestión de riesgo en la seguridad de la información, ayuda a la aplicación de la seguridad basada en el enfoque de gestión de riesgos.[3]

5.2.3 **Seguridad:** Una organización debe identificar sus requerimientos de seguridad, existen tres fuentes generales para fomentar la seguridad de la información.

5.2.3.1 **Requerimientos de seguridad:** A continuación, se presenta una breve relación de los principales requerimientos a considerar en cuento a seguridad

- Evaluar los Riesgos: Se toman de los objetivos y estrategias de la organización, se evalúan la vulnerabilidad y la probabilidad de ocurrencia.
- Requerimientos Legales: Satisfacer a sus socios comerciales, proveedores y contratistas.
- Principios Comerciales: Procesa la información de la organización para sostener sus operaciones.

[3] DIPLOMATURA INTERNACIONAL MANAGER SEGURIDAD DE LA INFORMACION consultado el 20 de enero 2017 http://www.infosecurityvip.com/newsletter/papers/ISEC%20EDUCATION%20CENTER%202016%20TRACK%20INFOSEC%20MANAGEMENT.PDF

5.2.3.2 **Principios de seguridad:** Se aseguran los tres pilares

- Confidencialidad: Asegurar que únicamente personal autorizado tenga acceso a la información.
- Integridad: Garantizar que la información no será alterada, eliminada o destruida por entidades no autorizadas
- Disponibilidad: Asegurar que los usuarios autorizados tendrán acceso a la información cuando la requieran.

5.2.3.3 **Modelo de capacidad de madurez (CMM):** es un modelo de evaluación de los procesos de una organización Los modelos más reconocidos son los pertenecientes a la familia CMM/CMMI (*Capability Maturity Model y CMM Integration*) [4] del *Software Engineering Institute (SEI) de EE.UU*.; si bien están orientados al desarrollo, mantenimiento y adquisición de productos y servicios de *Software*, su estructura de niveles de capacidad y madurez, y su mecanismo para determinar dichos niveles han sido replicados por muchos otros modelos en otros ámbitos. En la definición del SEI un modelo de madurez y capacidad que contiene los elementos esenciales de procesos efectivos para una o más disciplinas y describe un camino de mejoramiento evolutivo desde procesos caóticos hasta procesos maduros con calidad y efectividad mejorada. [5]

5.3 MARCO LEGAL.

5.3.1 **Decreto 2578 de 2012:** Por el cual se reglamenta el sistema nacional de archivos, se establece la red nacional de archivos, se deroga el decreto 2124 de 2004, y se dictan otras disposiciones relativas a la administración de los archivos del Estado. [6]

[4] Modelo de Capacidad y Madurez Disponible en: https://web.stanford.edu/~gvaldesu/articles/MScThesisSummary-eGovMM-gvaldes.pdf.
[5] Software Engineering Institute: CMMI for Development, Version 1.2. EE.UU. (2006). Disponible en: https://resources.sei.cmu.edu/asset_files/TechnicalReport/2010_005_001_15287.pdf
[6] COLOMBIA. MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACIÓN. DECRETO 2578 de 2012**.** Disponible en: http://www.mintic.gov.co/portal/604/articles-3526_documento.pdf.13. 2012.

5.3.2 **Decreto número - 2573 de 2014:** Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones. [7]

5.3.3 **Ley 527 de 1999 comercio electrónico:** Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales. [8]

5.3.4 **Ley 599 de 2000:** Por la cual se expide el Código Penal. Se crea el bien jurídico de los derechos de autor e incorpora algunas conductas relacionadas indirectamente con los delitos informáticos como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas, y manifiesta que el acceso abusivo a un sistema informático protegido con medida de seguridad o contra la voluntad de quien tiene derecho a excluirlo, incurre en multa. [9]

5.3.5 **Ley 1150 de 2007:** Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos. [10]

5.3.6 **Ley 1273 de 2009:** Por medio de la cual se modifica el Código Penal, se crea un nuevo bien tutelado denominado “de la protección de la información y los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. [11]

5.3.7 **Ley 1341 de 2009:** Estableció el marco general del sector de las Tecnologías de la Información y las Comunicaciones, incorporando principios, conceptos y competencias sobre su organización y desarrollo e igualmente señaló que las Tecnologías de la Información y las Comunicaciones deben servir al interés general y, por tanto, es deber del Estado promover su acceso eficiente y en igualdad de oportunidades a todos los habitantes del territorio nacional. [12]

---

[7] COLOMBIA. MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACIÓN. DECRETO 2573 DE 2014. Disponible en: https://www.mintic.gov.co/portal/604/articles-14673_docu

[8] COLOMBIA. MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACIÓN. Ley 527 de 1999 Comercio Electrónico Disponible en: https://solosam.files.wordpress.com/2011/07/ley-de-comercio-electrc3b3nico-en-colombia2.p

[9] COLOMBIA. CONGRESO REPUBLICA DE COLOMBIA. Ley 599 DE 2000. Disponible en internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000_pr008.html

[10] COLOMBIA. MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACIÓN. Ley 1150 DE 2007. Disponible en internet: https://www.mintic.gov.co/portal/604/articles-3656_documento.pdf

[11] COLOMBIA. CONGRESO REPUBLICA DE COLOMBIA. ley 1273 de 2009. Disponible en internet: http://www.sic.gov.co/sites/default/files/normatividad/Ley_1273_2009.pdf

[12]COLOMBIA. MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACIÓN. Ley 1341 de 2009. Disponible en: http://www.mintic.gov.co/portal/604/articles-15319_docu

5.4 MARCO CONTEXTUAL.

Para realizar el Plan Director de Seguridad de ’ PARQUES NACIONALES NATURALES DE COLOMBIA ’ a continuación se definirá una primera fase para determinar sus objetivos estratégicos, alcance, obligaciones y buenas prácticas de seguridad.

Así pues, en esta primera fase se presentará inicialmente la empresa, sus objetivos y la situación actual de la misma en materia de seguridad, considerando todo tipo de aspectos: técnicos, organizativos, regulatorios y normativos. Cabe citar que, para la elaboración del presente Plan Director, se cuenta con el apoyo de la Dirección de PARQUES NACIONALES NATURALES DE COLOMBIA consiguiendo que el proyecto esté alineado en todo momento con la filosofía y la estrategia de la entidad.

5.4.1 **Antecedentes de la entidad:** El sistema de parques nacionales naturales de Colombia se define como el conjunto de áreas con valores excepcionales para el patrimonio natural nacional que, en beneficio de los habitantes de la nación y debido a sus características naturales, culturales o históricas, se reserva y declara comprendida en cualquiera de las categorías que adelante se enumeran. (CRN art. 327)

Colombia tiene un «Sistema Nacional de Áreas Protegidas» (SINAP) que tiene como elemento más destacado a nivel nacional el «Sistema de Parques Nacionales Naturales» (SPNN), que cuenta con 56 parques naturales, con una extensión de unas 12.602.320,7 hectáreas (126.023,21 Kilómetros cuadrados) y que suponen más de un 11,04% del territorio continental colombiano.

La República de Colombia ha organizado un complejo «Sistema Nacional de Áreas Protegidas» (SINAP) constituido por el conjunto de áreas naturales protegidas —sean de carácter público, privado o comunitario, y en los distintos ámbitos de gestión pública nacional, regional y local—, por los actores sociales —agentes y administraciones— y por las estrategias e instrumentos de gestión que los articulan. Su finalidad es contribuir como un todo al cumplimiento de los objetivos de conservación que el país persigue.

Las áreas que conforman el SINAP se organizan en cuatro grandes grupos:

- Áreas protegidas de orden nacional. El principal es el «Sistema de Parques Nacionales», aunque existen otros relacionados con los bosques, la fauna y la ecología.
- Áreas protegidas de orden regional. Hay ya 10 SIDAP creados y hay varias más

en proyecto. Simultáneamente, hay un nivel de coordinación regional que promueve la aparición de varios SIRAPs, entre ellos, Caribe, Eje Cafetero, y Macizo.

- Áreas protegidas de orden local. Existen 20 reservas municipales y más de 100 aparecen en el listado de reservas por constituir.
- Áreas protegidas privadas. Integran la «Red de Reservas naturales de la sociedad civil» (RNSC), constituida por más de 160 áreas privadas.13
- El sistema de Parques Nacionales de Colombia El Sistema de Parques Nacionales se define como el conjunto de áreas con valores excepcionales para el patrimonio nacional que, en beneficio de los habitantes de la nación y debido a sus características naturales, culturales o históricas, se reserva y declara comprendida en cualquiera de las categorías que adelante se enumeran. (CRN art. 327). Tiene como finalidades:
- Conservar valores sobresalientes de fauna, flora y paisajes o reliquias históricas, culturales o arqueológicas, para darles un régimen especial de manejo fundado en una planeación integral con principios ecológicos, para que permanezcan sin deterioro.
- Perpetuar en estado natural muestras de comunidades bióticas, regiones fisiográficas, unidades biogeográficas, recursos genéticos y especies silvestres amenazadas de extinción, para: 1) Proveer puntos de referencia ambientales para investigaciones científicas, estudios generales y educación ambiental: 2) Mantener la diversidad biológica; 3) Asegurar la estabilidad ecológica
- Proteger ejemplares de fenómenos naturales, culturales, históricos y otros de interés internacional, para contribuir a la preservación del patrimonio común de la humanidad. (CRN art. 328) Se organiza del siguiente modo:

Parques Nacionales Naturales (PNN): áreas en la que su extensión permite El Autorregulación ecológica, cuyos ecosistemas no han sido alterados sustancialmente por la explotación u ocupación humana y donde las especies vegetales y animales, complejos geomorfológicos y manifestaciones históricas o culturales tienen valor científico, educativo, estético y recreativo nacional. Actualmente son 42.

Santuarios de Fauna y flora (SFF): áreas dedicadas a preservar comunidades vegetales o de animales silvestres, útiles para conservar recursos genéticos de la flora o fauna nacional. Actualmente son 10

Reserva Natural (RNN): área en condiciones primitivas de flora, fauna e individuos del reino inorgánico. Se destina a la conservación, investigación y estudio de sus riquezas naturales. Actualmente son 2.

[13] PARQUES NACIONALES NATURALES DE COLOMBIA consultado el 10 de noviembre 2016 en: http://www.parquesnacionales.gov.co/portal/es/sistema-nacional-de-areas-protegidas-sinap/

5.4.2 **Misión**: Administrar las áreas del Sistema de Parques Nacionales Naturales y coordinar el Sistema Nacional de Áreas Protegidas, en el marco del ordenamiento ambiental del territorio, con el propósito de conservar in situ la diversidad biológica y ecosistémica representativa del país, proveer y mantener bienes y servicios ambientales, proteger el patrimonio cultural y el hábitat natural donde se desarrollan las culturas tradicionales como parte del Patrimonio Nacional y aportar al Desarrollo Humano Sostenible; bajo los principios de transparencia, solidaridad, equidad, participación y respeto a la diversidad cultural.

5.4.3 **Visión**: Ser una entidad pública posicionada en el ámbito nacional, con reconocimiento internacional y legitimidad social, con capacidad técnica, esquema organizacional efectivo, incidencia política y solidez financiera; que ejerce como autoridad ambiental en las áreas del Sistema de Parques Nacionales Naturales, lidera procesos de conservación, administración y coordinación de áreas protegidas, contribuyendo al ordenamiento ambiental del país.[14]

5.4.4 **Política de calidad:** "Nuestro compromiso es la mejora continua de los procesos para la conservación, promoción y protección del patrimonio natural y cultural de las Áreas del Sistema de Parques Nacionales Naturales y para la coordinación del Sistema Nacional de Áreas Protegidas, con el propósito de conservar in situ la diversidad biológica del país para el cumplimiento de la misión institucional".

5.4.5 **Objetivos de calidad:** Mejorar continuamente los procesos para la conservación, promoción y protección del patrimonio natural y cultural de las Áreas del Sistema de Parques Nacionales Naturales y para la coordinación del Sistema Nacional de Áreas Protegidas.

Responder a las necesidades y requerimientos para el cumplimiento de la misión institucional de acuerdo con las características definidas para los productos o servicios que presta la UAESPNN (Unidad Administrativa Especial denominada Parques Nacionales Naturales de Colombia).

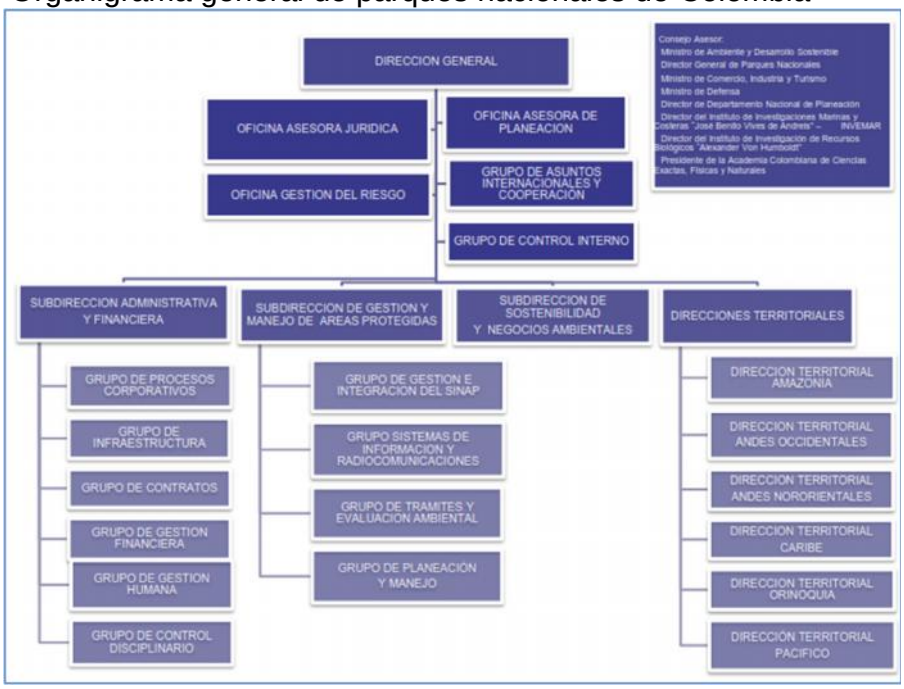
[14] PARQUES NACIONALES NATURALES DE COLOMBIA consultado el 18 de diciembre 2016 en: http://www.parquesnacionales.gov.co/portal/es/organizacion/mision-vision/

Desarrollar estrategias oportunas de comunicación e interacción con la ciudadanía y las partes involucradas para la conservación, promoción y protección del patrimonio natural y cultural.[15]

5.4.6 **Descripción del área donde se realizó la estadía:** El área de Redes y Sistemas de información denominada GSIR en la Unidad Administrativa Especial denominada Parques Nacionales Naturales de Colombia se encarga de brindar soporte en infraestructura tecnología, aplicaciones y servidores, proporcionando conectividad, acceso a los sistemas de información, mantenimiento del equipo de cómputo y de los sistemas de información; para las direcciones territoriales y Áreas Protegidas adscritas con el fin de garantizar que sus funcionarios y contratistas pueden realizar las actividades concernientes a la misión de la entidad en la **Figura 1.** Se puede ver el organigrama general de parques nacionales de Colombia a groso modo con sus direcciones territoriales y sus distintas subdirecciones.

Descripción:

Figura 1. Organigrama general de parques nacionales de Colombia



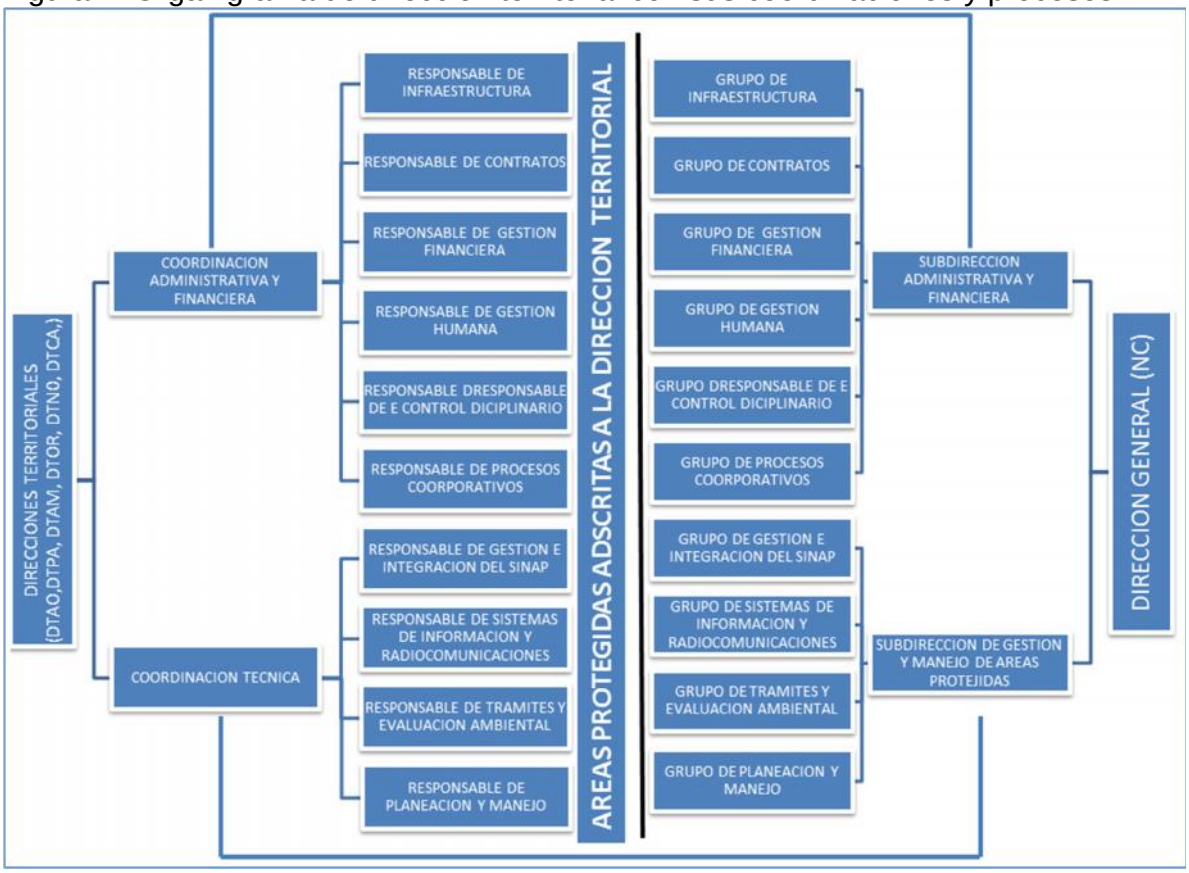
Fuente: Intranet - Parques Nacionales De Colombia[16]

[15] PARQUES NACIONALES NATURALES DE COLOMBIA consultado el 20 de diciembre 2016 en: http://www.parquesnacionales.gov.co/portal/es/planeacion-gestion-y-control/eficiencia-administrativa/gestion-de-la-calidad/

[16] INTRANET - PARQUES NACIONALES NATURALES DE COLOMBIA consultado el 12 de diciembre 2016 en: INSITU/portal

En la siguiente **Figura 2.** se muestra el organigrama de cada dirección territorial con sus coordinaciones y procesos, apuntando a la gestión de las áreas protegidas y a su vez acobijadas desde dirección general con las subdirecciones administrativas y de gestión:

Figura 2. Organigrama de dirección territorial con sus coordinaciones y procesos



Fuente: Intranet - Parques Nacionales De Colombia[17]

Instalaciones:

La entidad tiene su sede central en Bogotá D.C, cuenta con diferentes delegaciones de nivel territorial en todo Colombia subdividiéndose en 6 territoriales (**Región Amazonía, Región Andes Nororientales, Región Andes Occidentales Región Caribe, Región Orinoquía, Región Pacífico**), pudiendo considerarse que la mayoría de sus usuarios internos y externos son remotos.

[17] INTRANET - PARQUES NACIONALES NATURALES DE COLOMBIA consultado el 12 de diciembre 2016 en: INSITU/portal

Direcciones Territoriales

Mediante la Resolución 0155 del 26 de agosto de 2010, Parques Nacionales reorganiza sus Direcciones Territoriales y modifica la adscripción de las áreas del Sistema, de acuerdo con lo dispuesto en el documento CONPES 3680 de julio de 2010, que en su capítulo IV hace énfasis en las Acciones Estratégicas para el cumplimiento de los objetivos y estructura del Sistema Nacional de Áreas Protegidas.

Estructura que debe ser coordinada por la Unidad de Parques Nacionales Naturales de Colombia, a nivel nacional generando espacios regionales y reconociendo espacios locales. Para garantizar lo anterior, la Dirección General creó 6 subsistemas regionales como unidades de planificación y de articulación obedeciendo a criterios biofísicos, económicos, sociales, y culturales de acuerdo con los límites municipales, distribuidas de la siguiente manera:

Dirección Territorial Caribe - DTCA
Dirección Territorial Pacífico - DTPA
Dirección Territorial Andes Occidentales - DTAO
Dirección Territorial Andes Nororientales - DTAN
Dirección Territorial Amazonia - DTAM
Dirección Territorial Orinoquia – DTOR

Personal:

En la siguiente tabla se enlista el número de persones que constituyen los diferentes departamentos:

Tabla 1. Relación de personal

Ubicación	Descripción	Personas
Nivel Central	•DIRECCION GENERAL (NIVEL CENTRAL)	59
Dirección Territorial Amazonía	•DIRECTOR TERRITORIAL	91
Dirección Territorial Andes Nororientales	•DIRECTOR TERRITORIAL	75
Dirección Territorial Andes Occidentales	•DIRECTOR TERRITORIAL	116
Dirección Territorial Caribe	•DIRECTOR TERRITORIAL	100
Dirección Territorial Orinoquía	•DIRECTOR TERRITORIAL	61
Dirección Territorial Pacífico	•DIRECTOR TERRITORIAL	79
GRAN TOTAL		**581**

Fuente: El Autor

Como se observa en la **Tabla 1. Relación de personal.** el área técnica y misional es la más amplia, el equipo técnico-misional formado por jefes de áreas, operarios y profesionales dentro de las áreas protegidas son los encargados de hacer realidad la misión y visión de la entidad, los administrativos son los que llevan consigo la responsabilidad administrativa la cadena presupuestal y legal como son coordinación administrativa y financiera, responsable de infraestructura, contratos, gestión financiera, gestión humana, control disciplinario , procesos corporativos y los analistas e ingenieros de sistemas que se encargan del desarrollo y sostenibilidad de los sistemas de información.

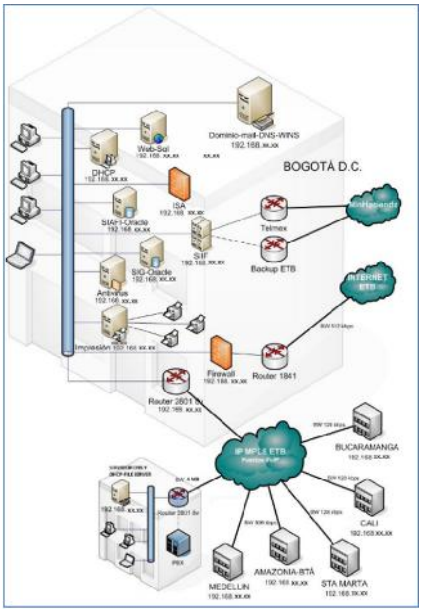
En el momento de la contratación del personal se piden profesionales universitarios ingenieros y / o titulados superiores especialistas en los temas específicos, se pide que se aporte el título y tarjeta profesional, se verifican referencias laborales y de estudios. En el momento de la contratación y / o en la firma del compromiso de contratación se firma una cláusula de confidencialidad.

Anualmente todos los empleados deben leer la política de seguridad y realizar un curso y test sobre seguridad de los sistemas en el lugar de trabajo.

Arquitectura/infraestructura

La siguiente **Figura 3**. muestra un diagrama de alto nivel de la arquitectura e infraestructura de la entidad censurando el detalle del direccionamiento y puertos.

Figura 3. Diagrama de alto nivel



Fuente: El Autor

La gestión de los recursos se lleva a cabo bajo un dominio de *Microsoft Windows* en su versión 2008. En la actualidad los equipos clientes se encuentran ejecutando diferentes versiones de sistemas operativos. Se tienen 580 *Windows* 7, 1 *Windows* 8. LICENCIADOS.

El servidor principal, bajo *Windows* 2008 Y 6 espejos en *Windows* 2008, sí posee una licencia valida junto con 300 licencias CAL para acceso Terminal *Server*. Dichas licencias son usadas por los usuarios para conectarse al programa SIIF. Este servidor principal alberga todos los datos de la entidad incluyendo bases de datos de programas, También proporciona servicio de compartición de ficheros (carpetas compartidas departamentales), colas de impresión de las impresoras en red y perfiles de usuario.

También existen otros servidores como PNSVRDTCA, PNSVRDTPA, PNSVRDTAO, PNSVRDTAN, PNSVRDTAM, PNSVRDTOR y adicionalmente en la dirección territorial se cuenta con un segundo servidor, ejecutando *Windows Server* 2008 licenciado, el cual es el encargado de realizar la copia de seguridad nocturna de todos los datos que genera la DTAO (PNSVRDTAO01), las demás territoriales el procedimiento de *Backus* se realiza en su único servidor, luego estos datos se resguardan a su vez en un file *server* alojado en nivel central. TODOS los enlaces son dedicados en fibra entre sedes.

EQUIPO INFORMATIVO

- Dirección Territorial Caribe - DTCA
- Dirección Territorial Pacífico - DTPA
- Dirección Territorial Andes Occidentales - DTAO
- Dirección Territorial Andes Nororientales - DTAN
- Dirección Territorial Amazonia - DTAM
- Dirección Territorial Orinoquia – DTOR

Con respecto con **Tabla 2. Equipamiento** se enlista el equipamiento informático, periféricos y los medios con los que cuenta la entidad propios y en outsourcing:

Tabla 3. Equipamiento

Grupo	Ubicación	Descripción	Cantidad
EQUIPOS	**NIVEL CENTRAL**	PC USUARIO WIN 7	59
IMPRESION	**NIVEL CENTRAL**	IMPRESORAS	6
RED	**NIVEL CENTRAL**	*SWITCH*	5
RED	**NIVEL CENTRAL**	*ROUTER*	5

Tabla 2. (Continuación)

Grupo	Ubicación	Descripción	Cantidad
SERVIDORES	**NIVEL CENTRAL**	SERVIDOR 1	1
SERVIDORES	**NIVEL CENTRAL**	SERVIDOR 2	2
SERVIDORES	**NIVEL CENTRAL**	SERVIDOR 3	5
SERVIDORES	**NIVEL CENTRAL**	SERVIDOR 4	6
SOFTWARE	**NIVEL CENTRAL**	OFFICE 2013	59
SOFTWARE	**NIVEL CENTRAL**	ANTIVIRUS	59
SOFTWARE	**NIVEL CENTRAL**	*WINDOWS* 7	59
SOFTWARE	**NIVEL CENTRAL**	*WINDOWS* 2008	4
SOFTWARE	**NIVEL CENTRAL**	*TERMINAL SERVER CALC*	59
EQUIPOS	**DTPA**	PC USUARIO WIN 7	79
IMPRESION	**DTPA**	IMPRESORAS	9
RED	**DTPA**	*SWITCH*	1
RED	**DTPA**	*ROUTER*	1
SERVIDORES	**DTPA**	*SERVIDOR DNS Y DHCP*	1
SOFTWARE	**DTPA**	OFFICE 2013	79
SOFTWARE	**DTPA**	ANTIVIRUS	79
SOFTWARE	**DTPA**	*WINDOWS* 7	79
SOFTWARE	**DTPA**	*WINDOWS* 2008	1
SOFTWARE	**DTPA**	*TERMINAL SERVER CALC*	79
EQUIPOS	**DTOR**	PC USUARIO WIN 7	61
IMPRESION	**DTOR**	IMPRESORAS	7
RED	**DTOR**	*SWITCH*	1
RED	**DTOR**	*ROUTER*	1
SERVIDORES	**DTOR**	*SERVIDOR DNS Y DHCP*	1
SOFTWARE	**DTOR**	OFFICE 2013	61
SOFTWARE	**DTOR**	ANTIVIRUS	61
SOFTWARE	**DTOR**	*WINDOWS* 7	61
SOFTWARE	**DTOR**	*WINDOWS* 2008	1
SOFTWARE	**DTOR**	TERMINAL *SERVER* CALC	61
EQUIPOS	**DTCA**	PC USUARIO WIN 7	100
IMPRESION	**DTCA**	IMPRESORAS	12
RED	**DTCA**	SWITCH	1
RED	**DTCA**	*ROUTER*	1
SERVIDORES	**DTCA**	SERVIDOR DNS Y DHCP	1
SOFTWARE	**DTCA**	OFFICE 2013	100
SOFTWARE	**DTCA**	ANTIVIRUS	100

Tabla 2. (Continuación)

Grupo	Ubicación	Descripción	Cantidad
SOFTWARE	**DTCA**	*WINDOWS* 7	100
SOFTWARE	**DTCA**	*WINDOWS* 2008	1
SOFTWARE	**DTCA**	TERMINAL *SERVER* CALC	100
EQUIPOS	**DTAO**	PC USUARIO WIN 7	116
IMPRESION	**DTAO**	IMPRESORAS	13
RED	**DTAO**	SWITCH	1
RED	**DTAO**	*ROUTER*	1
SERVIDORES	**DTAO**	SERVIDOR DNS Y DHCP	1
SERVIDORES	**DTAO**	SERVIDOR FILE *SERVER*	1
SOFTWARE	**DTAO**	OFFICE 2013	116
SOFTWARE	**DTAO**	ANTIVIRUS	116
SOFTWARE	**DTAO**	*WINDOWS* 7	116
SOFTWARE	**DTAO**	*WINDOWS* 2008	2
SOFTWARE	**DTAO**	TERMINAL *SERVER* CALC	116
EQUIPOS	**DTAN**	PC USUARIO WIN 7	75
IMPRESION	**DTAN**	IMPRESORAS	9
RED	**DTAN**	SWITCH	1
RED	**DTAN**	*ROUTER*	1
SERVIDORES	**DTAN**	SERVIDOR DNS Y DHCP	1
SOFTWARE	**DTAN**	OFFICE 2013	75
SOFTWARE	**DTAN**	ANTIVIRUS	75
SOFTWARE	**DTAN**	*WINDOWS* 7	75
SOFTWARE	**DTAN**	*WINDOWS* 2008	1
SOFTWARE	**DTAN**	TERMINAL *SERVER* CALC	75
EQUIPOS	**DTAM**	PC USUARIO WIN 7	91
IMPRESION	**DTAM**	IMPRESORAS	11
RED	**DTAM**	SWITCH	1
RED	**DTAM**	*ROUTER*	1
SERVIDORES	**DTAM**	SERVIDOR DNS Y DHCP	1
SOFTWARE	**DTAM**	OFFICE 2013	91
SOFTWARE	**DTAM**	ANTIVIRUS	91
SOFTWARE	**DTAM**	*WINDOWS* 7	91
SOFTWARE	**DTAM**	*WINDOWS* 2008	1
SOFTWARE	**DTAM**	TERMINAL *SERVER* CALC	91

Fuente: El Autor

5.4.7 **Funcionalidades y servicios:** En la **Tabla 3. funcionalidades y servicios** se enlistan las funcionalidades o servicios con las que Parques Nacionales Naturales De Colombia cuenta:

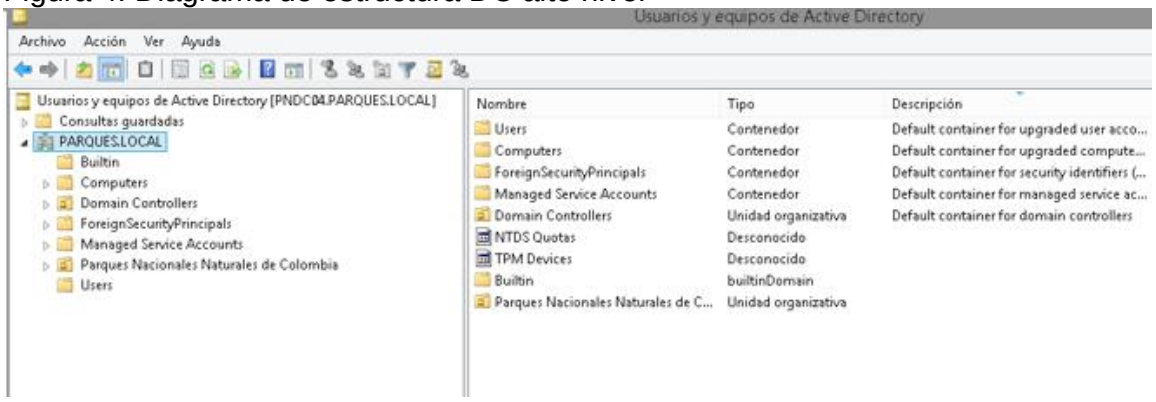
Tabla 4. Tabla de funcionalidades y servicios

Subgrupo	**Ubicación descripción**	**Descripción**
Interno	Todas las sedes	Correo electrónico
Interno	Todas las sedes	Navegación web
Interno	Todas las sedes	Sistema gestión proyectos
Interno	Todas las sedes	Copias de seguridad
Interno	Todas las sedes	BBDD clientes
Interno	Todas las sedes	BBDD contratos y licitaciones
Interno	Todas las sedes	Ofimática
Web	Acceso público	Página web corporativa

Fuente: El Autor

La siguiente **Figura 4**. muestra un diagrama de estructura DC de la entidad censurando el detalle.

Figura 4. Diagrama de estructura DC alto nivel



Fuente: El Autor

6. METODOLOGÍA DE DESARROLLO DEL PROYECTO.

La propuesta de investigación es de tipo **APLICADA**.

Como tipo de investigación aplicada se analizó la situación inicial de la entidad, se aplicaron las técnicas necesarias para recolectar y analizar datos con el fin de describir, generar e implementar normas y/o procedimientos acordes con las necesidades de la Entidad. Se hizo una comparación entre procedimientos y políticas existentes, para realizar un análisis diferencial de las medidas y normas en relación con la seguridad de la información que tenía la organización, mediante la metodología *Magerit v.3*. tomando como referencia la norma ISO / IEC27001: 2013 y el código de buenas prácticas detallado en la ISO / IEC27002: 2013, contemplando los controles y objetivos de los dominios.

Por consiguiente, el plan de implementación de la ISO / IEC 27001: 2013 es un aspecto clave en cualquier organización que quiera alinear sus procedimientos con esta norma. Para conseguir el objetivo final del proyecto con éxito, se ha tomado como fundamento el modelo PDCA, enmarcados dentro de las etapas Planear, Hacer, Verificar y Actuar.

ETAPAS CICLO PDCA

Planear

- Definir el alcance del SGSI
- Definir la política de seguridad
- Metodología para la evaluación de riesgos
- Inventario de Activos
- Identificar amenazas y vulnerabilidades
- Identificar el impacto
- Análisis y evaluación de riesgos
- Selección de Controles y SOA

Hacer

- Definir el plan de tratamiento de riesgos
- Implementar el plan de tratamiento de riesgos
- Implementar los controles
- Formar y concientizar
- Aplicar el SGSI

Verificar

- Revisar el SGSI
- Medir la eficacia de los controles
- Revisar los riesgos residuales
- Realizar auditorías internas del SGSI
- Registrar eventos y acciones

Actuar

- Implementar mejoras al SGSI
- Aplicar acciones correctivas
- Aplicar acciones preventivas
- Comprobar la eficacia de las acciones

Para favorable desarrollo del plan de implementación de la ISO / IEC 27001: 2013 dentro de la estructura interna de la entidad y sin salirnos del marco de la metodología PDCA del ciclo de mejora continua, se ha re-estructurado en seis fases.

- **FASE I:** Situación actual: Contextualización, objetivos y análisis diferencial.
- **FASE II:** Sistema de Gestión Documental.
- **FASE III:** Análisis de riesgos.
- **FASE IV:** Propuesta de Proyectos
- **FASE V:** Auditoría de Cumplimiento de la ISO IEC 27002: 2013
- **FASE VI:** Presentación de resultados y entrega de informes

En primer lugar, se ha realizado una descripción de los objetivos, alcance y expectativas a cumplir, partiendo de un análisis de la situación inicial a nivel de seguridad de la información.

El análisis de riesgos se ha hecho siguiendo la metodología ***Magerit*** **v.3**, y ha consistido en identificar los riesgos de seguridad en la entidad, determinando su magnitud e identificando las áreas que necesitan implantar salvaguardias.

A partir de la información derivada del análisis de riesgos, se han definido un conjunto de iniciativas y proyectos necesarios para conseguir el nivel de seguridad que PARQUES NACIONALES NATURALES DE COLOMBIA necesita. Las mejoras producidas por la ejecución del proyecto se han orientado a reducir el riesgo inicial de la Organización y a evolucionar el cumplimiento **ISO** hasta el nivel adecuado.

En tanto que todo Sistema de Gestión de Seguridad de la Información se apoya en un cuerpo documental para el cumplimiento normativo, se han desarrollado los principales documentos del SGSI de PARQUES NACIONALES NATURALES DE COLOMBIA: política de seguridad, procedimiento de auditorías internas, gestión de indicadores, procedimiento de revisión por dirección, gestión de roles y responsabilidades, comité de seguridad, Declaración de Aplicabilidad (SoA por las siglas en inglés de *Statement of Applicability*) y análisis de riesgos.

Finalmente, una vez ejecutados los diferentes proyectos, mediante una auditoría de cumplimiento se ha evaluado la madurez de la seguridad, en cuanto a los diferentes **dominios y controles de la ISO / IEC 27002: 2013**.

6.1 ENFOQUE Y MÉTODO A SEGUIR.

Para el análisis de riesgos Sistema de Información, se realizó una clasificación de activos según (metodología) ***MAGERIT*v.3**, se identificó todos los activos y sus riesgos. catalogándolos y valorándolos según su naturaleza en los siguientes grupos: servicios, datos / información que se convierten en el núcleo del sistema, aplicaciones SW, equipos informáticos, personal, redes para el movimiento de la información, soportes físicos de almacenamiento de la información, equipamiento auxiliar e instalaciones. Las técnicas, métodos y procedimientos utilizados para recopilar información consistieron en entrevistas, cuestionarios, observaciones, inventarios y muestreos; estos fueron verbales, escritas y mixtas aplicado al personal de los diferentes departamentos incluidos dentro del alcance del SGSI.

A nivel normativo, se ha tomado como norma de referencia **ISO / IEC27001: 2013** y el código de buenas prácticas detallado en la **ISO / IEC27002: 2013**. Esta versión 2013 de la ISO, contempla 114 controles distribuidos en los 35 objetivos de los 14 dominios siguientes:

- Política de seguridad
- Aspectos organizativos de la seguridad de la información.
- Seguridad de los Recursos Humanos.
- Gestión de activos.
- Control de Accesos.
- Criptografía.
- Seguridad Física y Ambiental.
- Seguridad de las operaciones.
- Seguridad de las comunicaciones.
- Adquisición de sistemas, desarrollo y mantenimiento
- Relaciones con los proveedores.
- Gestión de incidencias.
- Gestión de la Continuidad de Negocio.
- Cumplimiento [18]

FASE I: Situación actual: Contextualización, objetivos y análisis diferencial.

Una vez elegida la entidad objeto de estudio, se ha realizado una descripción de esta a nivel general, sobre su actividad, organización, distribución territorial, etc. A continuación, se han definido los objetivos y el alcance del plan director de seguridad. Seguidamente se ha llevado a cabo un análisis diferencial de las

[18] El portal de ISO 27001 en Español consultado el 10 de diciembre 2016 en: http://www.iso27000.es/iso27000.html

medidas de seguridad y normativa en relación con la seguridad de la información que tenía la organización, tomando como referencia las buenas prácticas definidas en la ISO 27002: 2013.

FASE II: Sistema de Gestión Documental.

En esta fase se han creado algunos de los documentos que lo constituyen. Los documentos elegidos son:

- Política de Seguridad.
- Procedimiento de Auditorías Internas.
- Gestión de Indicadores.
- Procedimiento de Revisión por Dirección.
- Gestión de Roles y Responsabilidades.
- Comité De Seguridad Del SGSI
- Declaración de Aplicabilidad (SOA).
- Metodología de Análisis de Riesgos. [19]

FASE III: Análisis de riesgos.

El análisis de riesgos es un proceso que consiste en identificar los riesgos de seguridad en la entidad, determinando su magnitud e identificando las áreas que necesitan implantar salvaguardias. Así pues, esta fase ha comenzado con una primera etapa de evaluación de activos, amenazas e impacto.

FASE IV: Propuesta de Proyectos

En base al análisis de riesgos de la fase anterior, en esta fase se proponen un conjunto de proyectos que ayudarán a la mitigación del riesgo inicial de la organización, evolucionando en el cumplimiento de la ISO hasta a nivel adecuado.

FASE V: Auditoría de Cumplimiento de la ISO IEC 27002: 2013

Una vez implementados los proyectos de la fase IV, se ha llevado a cabo una auditoría de cumplimiento para evaluar hasta qué punto la entidad cumple con las buenas prácticas en materia de seguridad.

FASE VI: Presentación de resultados y entrega de informes

Una vez alcanzadas las fases anteriores, se puede comenzar con la implementación del SGSI.[20]

[19] El portal de ISO consultado el 10 de diciembre 2016 en: www.iso27000.es/sgsi.htm
[20] Portal de ISO consultado el 10 de diciembre 2016 en: http://www.iso27000.es/download/doc_sgsi_all.pdf

7. FASE I SITUACIÓN ACTUAL: CONTEXTUALIZACIÓN, OBJETIVOS Y ANÁLISIS DIFERENCIAL

7.1 CONTEXTUALIZACIÓN Y OBJETIVOS

La evolución de las tecnologías de la información ha permitido automatizar y optimizar la gran mayoría de procesos y actividades que se llevan a cabo dentro de una entidad, convirtiéndose así pues en uno de los activos más importantes de la misma.

Mediante un Plan Director de Seguridad o “PDS” por sus siglas, se definen y priorizan un conjunto de proyectos en materia de seguridad de la información, dirigiéndose a reducir los riesgos a los que está expuesta una entidad hasta unos niveles aceptables, partiendo de un análisis inicial.

Para realizar el Plan Director de Seguridad de ’ PARQUES NACIONALES NATURALES DE COLOMBIA ’ a continuación se definirá una primera fase para determinar sus objetivos estratégicos, alcance, obligaciones y buenas prácticas de seguridad.

Así pues, en esta primera fase se presentará inicialmente la entidad, sus objetivos y la situación actual de la misma en materia de seguridad, considerando todo tipo de aspectos: técnicos, organizativos, regulatorios y normativos.

7.2 OBJETIVOS Y ALCANCE DEL PLAN DIRECTOR DE SEGURIDAD (PDS)

Una vez identificado uno de los activos más críticos de PARQUES NACIONALES NATURALES DE COLOMBIA, se puede definir como alcance del presente PDS: los enseres y equipos relacionados con el Sistema de Gestión de Proyectos, personal, aplicaciones necesarias y todo tipo de riesgos específicos relacionados con este Sistema principal.

Tal y como se ha comentado, la entidad ha tratado de implementar desde el año 2015 su SGSI y en la actualidad ha considerado oportuna la mejora en materia de seguridad para la obtención de la certificación ISO 27001. La obtención de esta certificación aumentará la confianza de los clientes, al tiempo que validará que el conjunto de medidas de seguridad a nivel de información y de los sistemas informáticos de la entidad.

Los objetivos del presente plan director son los siguientes:

- Inculcar una “cultura de la seguridad” entre todos los empleados de la entidad.
- Conseguir que la seguridad sea parte importante en todos los procesos y aspectos de la entidad.
- Asegurar la correcta configuración de todo sistema Informático, incluyendo la protección e integridad de los mismos, así como de los datos que estos sistemas contienen.
- Asegurar un control de acceso controlado a la información de la entidad, evitando filtraciones, robos o fugas.
- Asegurar el cumplimiento de las leyes aplicables en materia de privacidad y confidencialidad.
- Definición de roles y responsabilidades en materia de seguridad, incluyendo responsabilidades contractuales del personal colaborador externo.
- Control e inventariado de activos críticos de la entidad.
- Identificación y análisis de los riesgos y amenazas a los que están expuestos los activos. Definición de las oportunas acciones correctivas que permitan obtener un riesgo controlado y asumido por la entidad.
- Asegurar la continuidad del negocio y un sistema robusto y probado de copias de seguridad.

Así pues, el objetivo más importante del presente Plan Director de Seguridad es identificar posibles riesgos para proteger uno de los activos de mayor peso e importancia para PARQUES NACIONALES NATURALES DE COLOMBIA como es la información y la memoria institucional.

7.3 ANÁLISIS DIFERENCIAL DE LA SITUACIÓN INICIAL RESPECTO A LA NORMA ISO/IEC 27001:2013.

A continuación, se ha realizado un análisis diferencial de las medidas de seguridad y la normativa que tiene PARQUES NACIONALES NATURALES DE COLOMBIA, respecto a la norma ISO/IEC 27001:2013

Como resultados recopilados, se ha evaluado el nivel de madurez porcentual de los diferentes controles, consiguiendo una visión del estado de seguridad en conjunto, Para llevar a cabo este análisis se ha utilizado el Modelo de Capacidad de Madurez (CMM), cuya escala se define en la **Tabla 5. Tabla de valoración de nivel de madurez (CMM)**
:

Tabla 6. Tabla de valoración de nivel de madurez (CMM)

Valor	Efectividad	Significado	Descripción
L0	0%	Inexistente	Carencia completa de cualquier proceso conocido.
L1	10%	Inicial / Ad-hoc	Procedimientos inexistentes o localizados en áreas concretas. El éxito de las tareas se debe a esfuerzos personales.
L2	50%	Reproducible, pero intuitivo	Existe un método de trabajo basado en la experiencia, aunque sin comunicación formal. Dependencia del conocimiento individual
L3	90%	Proceso definido	La organización en su conjunto participa en el proceso. Los procesos están implantados, documentados y comunicados.
L4	95%	Gestionado y medible	Se puede seguir la evolución de los procesos mediante indicadores numéricos y estadísticos. Hay herramientas para mejorar la calidad y la eficiencia
L5	100%	Optimizado	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos
L6	N/A	No aplica	

Fuente: Investigación

La entidad nunca se basó en ninguna norma, ha trabajado el tema del SGSI de forma empírica por tal motivo carece de cualquier plan director previo. Por este motivo, como era previsible, el resultado de esta comparativa muestra que el grado de cumplimiento con la norma UNE-ISO/IEC 27001 es casi inexistente. Por dominio de requerimientos, se puede observar en la **Tabla 7.** las cifras de cumplimiento.

Tabla 8. Porcentaje de conformidad con respecto a la norma ISO27001 por requerimientos

	Dominio	% de conformidad	# NC mayores	# NC menores	# NC OK
4	**Contexto de la organización**	5%	5	0	0
5	**Liderazgo**	1%	14	0	0
6	**Planificación**	0%	31	0	0
7	**Soporte**	0%	26	0	0
8	**Funcionamiento**	0%	3	0	0
9	**Evaluación de Rendimiento**	0%	23	0	0
10	**Proceso de mejora**	0%	11	0	0

Fuente: El Autor[21]

[21] TALLER MODELO DE GESTION consultado el 18 de ENERO 2017 en: http://master2000.net/recursos/menu/195/1028/mper_arch_27838_TALLER%20MODELO%20GESTI%C3%93N%20IE.pptx

En la **Tabla 6.** Se observa el modelo de capacidad de madurez, el recuento de los controles de la norma agrupados por nivel.

Tabla 9. Numero de requerimientos de la norma 27001, agrupados en base a CMM (Modelo de Capacidad de Madurez)

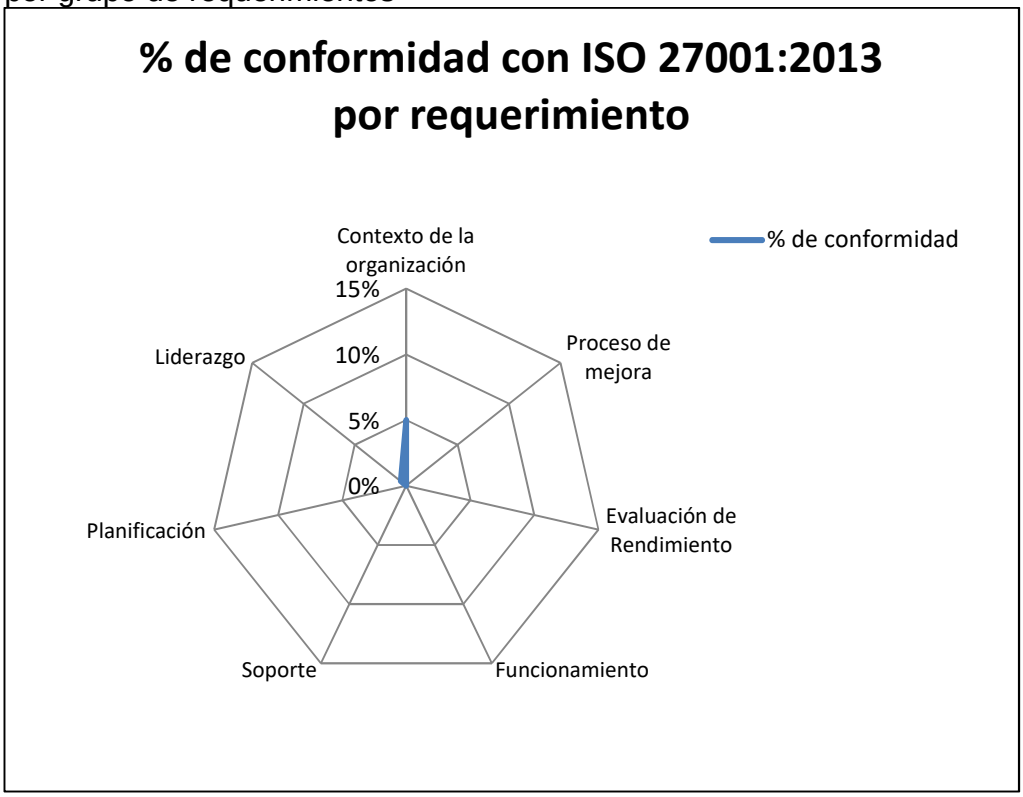
Valor	Efectividad	Significado	Descripción	Número
L0	0%	Inexistente	Carencia completa de cualquier proceso conocido.	111
L1	10%	Inicial / Ad-hoc	Procedimientos inexistentes o localizados en áreas concretas. El éxito de las tareas se debe a esfuerzos personales.	2
L2	50%	Reproducible, pero intuitivo	Existe un método de trabajo basado en la experiencia, aunque sin comunicación formal. Dependencia del conocimiento individual	0
L3	90%	Proceso definido	La organización en su conjunto participa en el proceso. Los procesos están implantados, documentados y comunicados.	0
L4	95%	Gestionado y medible	Se puede seguir la evolución de los procesos mediante indicadores numéricos y estadísticos. Hay herramientas para mejorar la calidad y la eficiencia	0
L5	100%	Optimizado	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos	0
L6	N/A	No aplica		0

Fuente: Investigación[22]

En la siguiente **Figura 5.** de radar se muestra gráficamente el nivel de conformidad con los requerimientos de la norma ISO27001:2013.

[22] HERRAMIENTA PILAR ESQUEMA NACIONAL DE SEGURIDAD consultado el 18 de ENERO 2017 en: http://www.rediris.es/difusion/eventos/foros-seguridad/fs2010/pres/CCN-Pilar-ENS-fs2010-2010.04.pdf

Figura 5. Porcentaje de conformidad con respecto a la norma la norma ISO27001 por grupo de requerimientos [23]



Fuente: El Autor

El detalle de los requerimientos analizados se encuentra en el archivo llamado CMM-ISO27001-2013 Inicial.
Ver Anexos F1
ANEXO A. FASE 1 - CMM-ISO27001-2013 INICIAL

7.4 ANÁLISIS DIFERENCIAL DE LA SITUACIÓN INICIAL RESPECTO A LA NORMA ISO/IEC 27002:2013.

Se ha realizado un análisis para determinar las áreas de mejora que habría que abordar, para ello se ha realizado una comparación tomando como referencia los controles recomendados en la norma ISO 27002:2013. Este análisis nos permitirá establecer un punto de partida que será tomado como referencia a la hora de

[23] NORMAS ISO27001 CAMBIOS 2005 A 2013 consultado el 20 de ENERO 2017 en: https://es.slideshare.net/JaimeAndrsBelloVieda/iso-27001-cambios-2005-a-2013

comparar y evaluar los logros y avances que se materializarán en la consecución del plan director.

Las valoraciones de los resultados plasmados en la **Tabla 7.** que se muestran para cada uno de los dominios se han obtenido realizando un promedio de la efectividad de todos los controles que conforman cada uno de los dominios. Como muestran las cifras que se detallan a continuación, el grado de conformidad con los controles definidos en la ISO 27002 es también muy bajo (un promedio de un 1%).

Por dominios, las cifras de cumplimiento son las siguientes:

Tabla 10. Porcentaje de conformidad con respecto a la norma ISO 27002 por dominio

	Dominio	% de conformidad	# NC MAYOR (L0,L1)	# NC MENOR (L2,L3)	# NC OK (L4,L5)
A.5	**POLÍTICAS DE SEGURIDAD**	5%	2	0	0
A.6	**ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION.**	0%	7	0	0
A.7	**SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.**	3%	6	0	0
A.8	**GESTIÓN DE ACTIVOS.**	0%	10	0	0
A.9	**CONTROL DE ACCESOS.**	3%	14	0	0
A.10	**CIFRADO.**	0%	2	0	0
A.11	**SEGURIDAD FÍSICA Y AMBIENTAL.**	1%	15	0	0
A.12	**SEGURIDAD EN LA OPERATIVA.**	5%	13	1	0
A.13	**SEGURIDAD EN LAS TELECOMUNICACIONES.**	0%	7	0	0
A.14	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.**	0%	13	0	0
A.15	**RELACIONES CON SUMINISTRADORES.**	0%	5	0	0
A.16	**GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.**	0%	7	0	0
A.17	**ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.**	3%	4	0	0
A.18	**CUMPLIMIENTO.**	1%	8	0	0

Fuente: El Autor

En la **Tabla 8.** Se visualiza el recuento total de controles de la norma ISO27002 ajustados al modelo de la entidad en base a CMM

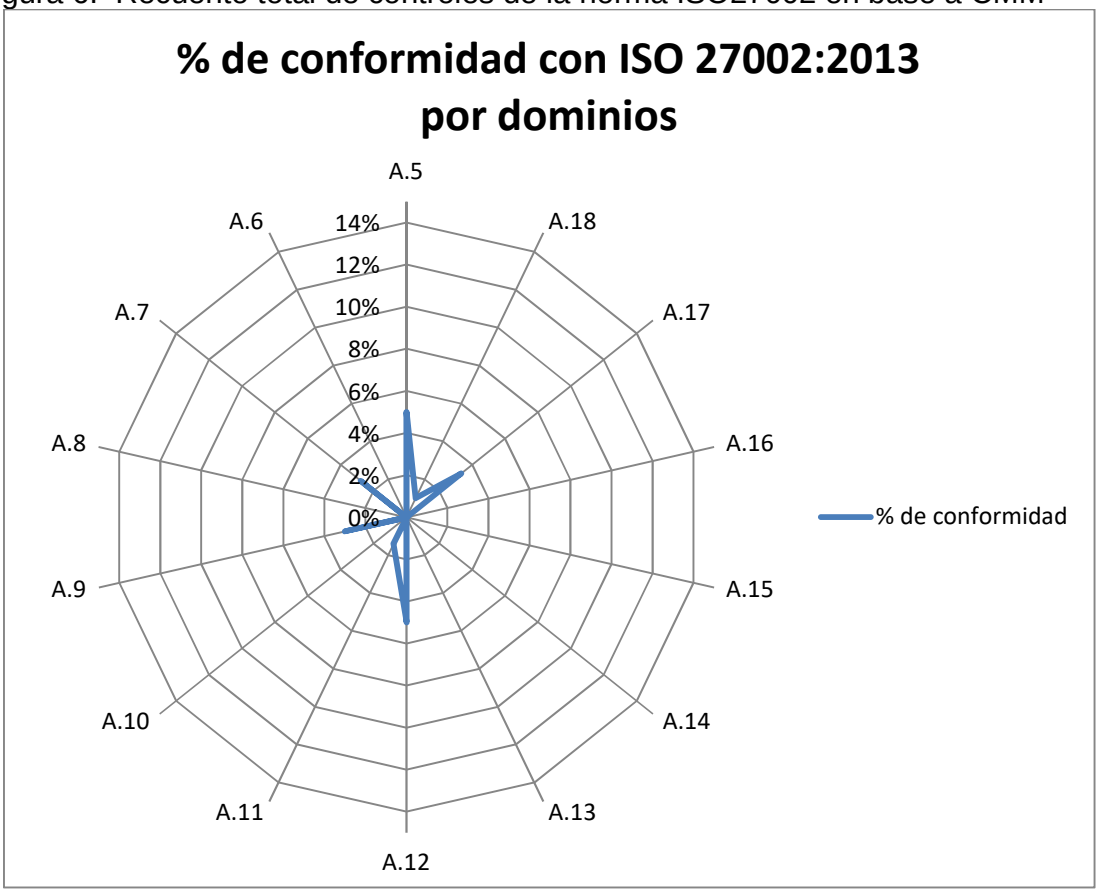
Tabla 11. Recuento total de controles de la norma ISO27002 en base a CMM

Valor	Efectividad	Significado	Descripción	Número
L0	0%	Inexistente	Carencia completa de cualquier proceso conocido.	84
L1	10%	Inicial / Ad-hoc	Procedimientos inexistentes o localizados en áreas concretas. El éxito de las tareas se debe a esfuerzos personales.	15
L2	50%	Reproducible, pero intuitivo	Existe un método de trabajo basado en la experiencia, aunque sin comunicación formal. Dependencia del conocimiento individual	1
L3	90%	Proceso definido	La organización en su conjunto participa en el proceso. Los procesos están implantados, documentados y comunicados.	0
L4	95%	Gestionado y medible	Se puede seguir la evolución de los procesos mediante indicadores numéricos y estadísticos. Hay herramientas para mejorar la calidad y la eficiencia	0
L5	100%	Optimizado	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos	0
L6	N/A	No aplica		14

Fuente: El Autor

En la siguiente **Figura 6.** de figura de radar, se muestra gráficamente el nivel de cumplimiento por dominios:

Figura 6. Recuento total de controles de la norma ISO27002 en base a CMM[24]



Fuente: El Autor

El detalle de los controles analizados se encuentra en el anexo B

.

Ver Anexos F1

ANEXO B. FASE 1 - CMM-ISO27002-2013 INICIAL

[24] PORTAL ISO consultado el 18 de ENERO 2017 en: http://www.iso27000.es/iso27002.html

8. FASE II SISTEMA DE GESTIÓN DOCUMENTAL.

8.1 INTRODUCCION.

El Sistema de Gestión de Seguridad de la Información de PARQUES NACIONALES NATURALES DE COLOMBIA se apoya en un cuerpo documental para el cumplimiento normativo que puede ser consultado en la CARPETA - ANEXO F2 del presente proyecto. A continuación, se listan los documentos que pueden ser consultados en el ANEXO citado, determinando los objetivos de los mismos:

- Política de Seguridad.
- Procedimiento de Auditorías Internas.
- Gestión de Indicadores.
- Procedimiento de Revisión por Dirección.
- Gestión de Roles y Responsabilidades.
- Comité De Seguridad Del SGSI
- Declaración de Aplicabilidad (SOA).
- Metodología de Análisis de Riesgos. [25]

- **SGSI-01 Política de Seguridad.** PARQUES NACIONALES NATURALES DE COLOMBIA ha desarrollado su política de seguridad de la información que afecta a la confidencialidad, integridad y disponibilidad de la información tratada por PARQUES NACIONALES NATURALES DE COLOMBIA a todos los niveles de sensibilidad y confidencialidad, en base a las leyes y normativas vigentes, la ISO 27001: 2013 y las buenas prácticas de la ISO 27002: 2013. Esta política cubre todos los aspectos administrativos y de control que se deben cumplir para todo el personal interno de la entidad y terceras partes, para conseguir un nivel correcto de protección de las características de la seguridad y la calidad de la información relacionada.
  Ver Anexos F2
  ANEXO C. FASE 2 - SGSI-01 POLÍTICA DE SEGURIDAD

- **SGSI-02 Procedimiento de Auditorías Internas.** El objetivo de este documento es establecer el procedimiento a seguir para la planificación y realización de las auditorías internas del SGSI de la entidad, describiendo las pautas para realizar un examen sistemático de éste que permita su correcta aplicación y eficacia, identificando las anomalías y posibles mejoras o correcciones.
  Ver Anexos F2
  ANEXO D. FASE 2 - SGSI-02 PROCEDIMIENTO DE AUDITORÍAS INTERNAS

[25] El portal de ISO consultado el 10 de diciembre 2016 en: www.iso27000.es/sgsi.htm

- **SGSI-03 Gestión de Indicadores.** En este documento se definen los indicadores para medir la eficacia de los controles de seguridad implementados, así como la sistemática para hacer las medidas.
  Ver Anexos F2
  ANEXO E. FASE 2 - SGSI-03 GESTIÓN DE INDICADORES

- **SGSI-04 Procedimiento de Revisión por Dirección.** En este procedimiento se describe la metodología de revisión del SGSI, a fin de promover su continua adecuación.
  Ver Anexos F2
  ANEXO F. FASE 2 - SGSI-04 PROCEDIMIENTO DE REVISIÓN POR DIRECCIÓN

- **SGSI-05 Gestión de Roles y Responsabilidades.** En este procedimiento se definen y documentan los roles y responsabilidades del personal del SGSI, atendiendo a Política de Seguridad de la Información de PARQUES NACIONALES NATURALES DE COLOMBIA.
  Ver Anexos F2
  ANEXO G. FASE 2 - SGSI-05 GESTIÓN DE ROLES Y RESPONSABILIDADES

- **SGSI-05B Comité de Seguridad del SGSI**. En este procedimiento se define la composición, las principales funciones y la organización del Comité de Seguridad del SGSI, como órgano principal para el tratar aspectos estratégicos de la gestión de la seguridad de la información de manera coordinada y eficaz.
  Ver Anexos F2
  ANEXO H. FASE 2 - SGSI-05B COMITÉ DE SEGURIDAD DEL SGSI

- **SGSI-06 Declaración de Aplicabilidad.** El objetivo de la declaración de aplicabilidad es especificar los controles de seguridad de acuerdo con la normativa que aplica PARQUES NACIONALES NATURALES DE COLOMBIA.
  Ver Anexos F2
  ANEXO I. FASE 2 - SGSI-06 DECLARACIÓN DE APLICABILIDAD

- **SGSI-07 Metodología del Análisis de Riesgos.** El análisis de riesgos persigue diferentes objetivos como describir los elementos que intervienen en la metodología y las relaciones entre ellos, establecer un método sencillo y preciso para obtener el nivel del riesgo soportado por cada activo y proceso, etc. Asimismo, define una metodología de evaluación de los riesgos apropiada para los procesos que intervienen en el SGSI, alineada con los objetivos de negocio y con los requisitos legales, regulatorios y reglamentarios.
  Ver Anexos F2
  ANEXO J. FASE 2 - SGSI-07 METODOLOGÍA DEL ANÁLISIS DE RIESGOS

9. FASE III ANÁLISIS DE RIESGOS.

9.1 INTRODUCCION.

El análisis de riesgos es uno de los elementos fundamentales dentro del proceso de implantación de un SGSI ya que en esta fase es donde se cuantifica la importancia de los activos para la seguridad de la organización.

De las diferentes metodologías existentes para llevar a cabo el análisis de riesgos, en el presente proyecto, se ha empleado la metodología *Magerit*.

Se valorarán los activos, se tipificarán permitiendo su identificación posterior mediante agrupaciones por tipo de activo. Ayudando a la identificación de amenazas potenciales y la elección de salvaguardas apropiadas para cada uno de los tipos en la **Tabla 9**. se enlista los activos considerados junto a las abreviaturas basadas en la metodología *MageritV3*.

Tabla 12. Tipos de activo considerados junto con la abreviatura basada en *Magerit*[26]

TIPO	ABREVIATURA
Instalaciones	[L]
Hardware	[HW]
Software	[SW]
Datos/Información	[D]
Redes de comunicaciones	[COM]
Equipamiento Auxiliar	[AUX]
Personal	[P]
Soporte de información	[MEDIA]

Fuente: Investigación

- Parametrización

  Inicialmente, se han realizado un dimensionamiento, identificando y definiendo los parámetros siguientes:

[26] MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información consultado el 18 de ENERO 2017 en: https://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Documentacion/Metodologias-y-guias/Mageritv3/2012_Magerit_v3_libro2_catalogo-de-elementos_es_NIPO_630-12-171-8/2012_Magerit_v3_libro2_catalogo%20de%20elementos_es_NIPO_630-12-171-8.pdf

Se elabora **Tabla 10**. Con la valoración económica de los activos que se encuentren dentro del alcance del análisis basada en *Magerit*

Tabla 13. Valor de los activos basada en *Magerit*[27]

ABREVIATURA	VALORACIÓN	RANGO
MA	Muy alta	valor> $ 100.000
A	Alta	$ 20.000 < valor > $ 100.000
M	Media	$ 5.000 < valor > $ 20.000
B	Baja	$ 1.000 < valor > $ 5.000
MB	Muy baja	Valor < $ 1.000

Fuente: El Autor

- Análisis de activos

En los sistemas de información hay dos cosas esenciales: la información que gestionan y los servicios que prestan. por consiguiente, se valorará cada activo en las distintas dimensiones de seguridad, ponderando cuál de ellas resulta más crítica e importante para cada activo. Se evaluará en las 5 dimensiones de la seguridad que valora la tabla ACIDA.

[A] Autenticidad: Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. Contra la autenticidad de la información se puede tener manipulación del origen o el contenido de los datos. Contra la autenticidad de los usuarios de los servicios de acceso, se puede tener suplantación de identidad.

[C] Confidencialidad: Que la información llegue solamente a las personas autorizadas. Contra la confidencialidad o secreto pueden darse fugas y filtraciones de información, así como accesos no autorizados. La confidencialidad es una propiedad de difícil recuperación, pudiendo minar la confianza de los demás en la

[27] MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información consultado el 18 de ENERO 2017 en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

organización que no es diligente en el mantenimiento del secreto, y pudiendo suponer el incumplimiento de leyes y compromisos contractuales relativos a la custodia de los datos.

[I] Integridad: Mantenimiento de las características de completitud y corrección de los datos. Contra la integridad, la información puede aparecer manipulada, corrupta o incompleta. La integridad afecta directamente al correcto desempeño de las funciones de una Organización.

[D] Disponibilidad: Disposición de los servicios a ser usados cuando sea necesario. La carencia de disponibilidad supone una interrupción del servicio. La disponibilidad afecta directamente a la productividad de las organizaciones.

[A] Auditabilidad/Trazabilidad: Asegurar que en todo momento se podrá determinar quién hizo qué y en qué momento. La trazabilidad es esencial para analizar los incidentes, perseguir a los atacantes y aprender de la experiencia. La trazabilidad se materializa en la integridad de los registros de actividad.[28]

Para dimensionar la valoración de los activos, se calculan las consecuencias de los impactos, los criterios con los que se evaluara dichos impactos son en base a la metodología *Magerit* para medir y valorar los perjuicios Se elabora **Tabla 11**. Con la valoración de pérdida de los activos según impacto y criterio.

Tabla 14. Valoración pérdida del activo[29]

IMPACTO		**Criterio**	**VALOR**	
MA	Muy alto	Daño extremadamente grave	100%	10
A	Alto	Daño muy grave	75%	9
M	Medio	Daño grave	50%	6 - 8
B	Bajo	Daño importante	20%	3-5
MB	Muy bajo	Daño menor	5%	1- 2
NA	Despreciable	Irrelevante a efectos prácticos	0%	0

Fuente: El Autor

[28] Mintic - Guía para la Gestión y Clasificación de Activos de Información. consultado el 18 de ENERO 2017 en: https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

[29] MAGERIT V.3 : METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN CONSULTADO EL 18 DE ENERO 2017 EN: HTTPS://GOO.GL/GB5WBD

Se tuvo en cuenta la dependencia entre activos. Estos se encuentran jerarquizados donde los activos superiores dependen de los inferiores, como resultado, si se materializa una amenaza en un activo inferior, tendrá un impacto perjudicial en sus activos superiores. Esto se tuvo en cuenta a la hora de evaluar cada activo. Se consideraron las siguientes reglas.

- *Hardware* [HW] depende de equipo auxiliar [AUX], como aire acondicionado o corriente eléctrica.
- *Software* [SW] depende del *Hardware* [HW].
- Datos [D] depende del *Hardware* [HW] y *Software* [SW]
- Comunicaciones [COM] depende de *Hardware* [HW] e Instalaciones [L]
- Servicios [S] depende del *Hardware* [HW], *Software* [SW] y Comunicaciones [COM]
- Soportes de información [SI] dependen de instalaciones [L] y de equipo auxiliar [AUX]
- Auxiliares [AUX] depende de otros [AUX].
- Personal [P] no tiene dependencias.[30]

9.2 INVENTARIO Y VALORACION DE LOS ACTIVOS.

La entidad dispone de una sede principal en Bogotá y cinco subsedes. A pesar de desarrollar una tabla de activos para cada ubicación, la numeración de estos será correlativa independientemente de la sede a la que pertenezcan aplique o no aplique.

En las siguiente **Tabla 12. Inventario y valoración de los activos de la sede principal y direcciones territoriales,** se puede visualizar el resultado de la valoración de los activos.

[30] MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información consultado el 18 de ENERO 2017 en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Tabla 15. Inventario y valoración de los activos de la sede principal y direcciones territoriales

INVENTARIO Y VALORACION DE LOS ACTIVOS											
TIPO	**ÁMBITO**	**Activo**	**ID**	**UBICACIÓN**	**VALOR**	**DEPENDENCIAS**	**CRITICIDAD/DIMEN**				
							Autenticidad	**C**onfidencialidad	**I**ntegridad	**D**isponibilidad	**A**udibilidad
L	Instalaciones	Rack principal (CPD a efectos prácticos)	[L1]	NIVEL CENTRAL	MA	[AUX1][AUX2]	8	9	10	10	8
		Archivo	[L2]	NIVEL CENTRAL	A	-	8	9	9	7	6
		Rack secundario (CPD a efectos prácticos)	[L3]	TERRITORIALES	MA	[AUX1][AUX2]	8	9	10	10	8
AUX		Aire acondicionado en sala de asistentes donde se encuentra el Rack	[AUX1]	NIVEL CENTRAL	MB	[AUX4]-	0	0	0	8	0
		UPS Estabilizador para todo el rack.	[AUX2]	NIVEL CENTRAL	MB	[AUX4]	0	0	0	8	0
		Cableado LAN	[AUX3]	NIVEL CENTRAL	MB	-	0	0	0	10	0
		Cableado suministro eléctrico	[AUX4]	NIVEL CENTRAL	B	-	0	0	0	10	0
		Aire acondicionado en sala de asistentes	[AUX5]	TERRITORIALES	MB	[AUX8]-	0	0	0	8	0
		UPS Estabilizador para todo el rack.	[AUX6]	TERRITORIALES	MB	[AUX8]	0	0	0	8	0
		Cableado LAN	[AUX7]	TERRITORIALES	MB	-	0	0	0	10	0
		Cableado suministro eléctrico	[AUX8]	TERRITORIALES	B	-	0	0	0	10	0

Tabla 12. (Continuación)

INVENTARIO Y VALORACION DE LOS ACTIVOS

TIPO	ÁMBITO	Activo	ID	UBICACIÓN	VALOR	DEPENDENCIAS	CRITICIDAD/DIMEN				
							Autenticidad	**C**onfidencialidad	Integridad	**D**isponibilidad	**A**udibilidad
COM	Comuniciones	Router fibra NETLAN Telefónica, une las sedes y da conexión a Internet	[COM1]	NIVEL CENTRAL	MB	[AUX2]	7	8	9	10	6
		Router fibra RAVEC Telefónica, une las sedes y da conexión a Internet	[COM2]	TERRITORIALES	MB	[AUX6]	7	8	9	10	6
HW	Hardware	Centralita IP + switch propio	[HW1]	NIVEL CENTRAL	MB	[AUX4]	5	7	8	8	5
		Fax	[HW2]	NIVEL CENTRAL	MB	[AUX4]	5	7	6	7	5
		10 PC ofimática	[HW3]	NIVEL CENTRAL	MB	[AUX3] [AUX4]	4	6	6	7	5
		1 Servidor principal	[HW4]	NIVEL CENTRAL	M	[AUX3][AUX2][AUX1][AUX4]	9	9	10	10	8
		2 impresoras red	[HW5]	NIVEL CENTRAL	B	[AUX3] [AUX4]	3	4	5	5	4
		1 impresora local	[HW6]	NIVEL CENTRAL	MB	[AUX4]	3	4	5	3	4
		1 switch Gigabit LAN	[HW7]	NIVEL CENTRAL	MB	[AUX3] [AUX4]	4	3	3	10	4
		3 Escáner local USB	[HW8]	NIVEL CENTRAL	MB	[AUX4]	3	2	5	5	2
		Centralita IP + switch propio	[HW9]	TERRITORIALES	MB	[AUX8]	5	7	8	8	5
		Fax	[HW10]	TERRITORIALES	MB	[AUX8]	5	7	6	7	5
		5 PC ofimática	[HW11]	TERRITORIALES	MB	[AUX7] [AUX8]	4	6	6	7	5

Tabla 12. (Continuación)

INVENTARIO Y VALORACION DE LOS ACTIVOS

TIPO	ÁMBITO	Activo	ID	UBICACIÓN	VALOR	DEPENDENCIAS	CRITICIDAD/DIMEN				
							Autenticidad	**C**onfidencialidad	**I**ntegridad	**D**isponibilidad	**A**udibilidad
HW	Hardware	1 Servidor de respaldo (BACKUP remoto)	[HW12]	TERRITORIALES	M	[AUX5][AUX6][AUX7] [AUX8]	9	9	10	10	8
		2 impresoras red	[HW13]	TERRITORIALES	B	[AUX7] [AUX8]	3	4	5	5	4
		1 switch 100mbs LAN	[HW14]	TERRITORIALES	MB	[AUX7] [AUX8]	4	3	3	10	4
		3 Escáner local USB	[HW15]	TERRITORIALES	MB	[AUX8]	3	2	5	5	2
		1 laptop privado siendo utilizado dentro de FINALIN S.L.	[HW16]	TERRITORIALES	MB	[AUX7][AUX8]	5	8	8	8	3
MEDIA	Media	Disco duro externo USB para backup redundante local.	[MEDIA1]	NIVEL CENTRAL	MB	-	7	8	8	7	7
		Archivo pólizas en papel	[MEDIA2]	NIVEL CENTRAL	M	-	8	8	8	8	8
DATOS	Datos	Código fuente (webs + programa Decesos)	[DATOS1]	NIVEL CENTRAL	M		7	8	8	8	7
		Backup secundario en ext HD	[DATOS2]	NIVEL CENTRAL	A	[HW4]	8	9	10	9	8
		Datos SegurLif (cartera de pólizas generales)	[DATOS3]	NIVEL CENTRAL	MA	[HW4]	8	10	10	10	8

Tabla 12. (Continuación)

INVENTARIO Y VALORACION DE LOS ACTIVOS

TIPO	ÁMBITO	Activo	ID	UBICACIÓN	VALOR	DEPENDENCIAS	CRITICIDAD/DIMEN				
							Autenticidad	**C**onfidencialidad	Integridad	**D**isponibilidad	**A**udibilidad
DATOS	Datos	Datos contabilidad	[DATOS4]	NIVEL CENTRAL	A	[HW4]	8	9	9	9	8
		BBDD pólizas decesos	[DATOS5]	NIVEL CENTRAL	MA	[HW4]	8	10	10	10	8
		Imagen Corporativa	[DATOS6]	NIVEL CENTRAL	B	-	0	0	0	0	0
SW	Aplicaciones	10 LibreOffice 4	[SW1]	NIVEL CENTRAL	MB	[HW3]	5	4	5	5	3
		Office 2010	[SW2]	NIVEL CENTRAL	MB	[HW3]	5	3	4	5	3
		Antivirus	[SW3]	NIVEL CENTRAL	MB	[HW4]	5	3	8	7	5
		8 Windows 7	[SW4]	NIVEL CENTRAL	MB	[HW3]	8	4	6	7	4
		2 WinXP	[SW5]	NIVEL CENTRAL	MB	[HW3]	7	4	6	7	4
		SegurLif	[SW6]	NIVEL CENTRAL	B	[HW4]	8	8	8	9	7
		ContaSol	[SW7]	NIVEL CENTRAL	MB	[HW4]	8	8	8	7	5
		Access 97 Runtime	[SW8]	NIVEL CENTRAL	MB	[HW3]	5	5	5	6	4
		Windows 2003	[SW9]	NIVEL CENTRAL	MB	[HW4]	8	7	8	9	5
		Terminal server CALC	[SW10]	NIVEL CENTRAL	MB	[SW9]	8	6	8	8	5
		5 LibreOffice 4	[SW11]	TERRITORIALES	MB	[HW11]	5	4	5	5	3
		5 Windows 7	[SW12]	TERRITORIALES	MB	[HW11]	5	8	8	8	4
		1 Windows 8	[SW13]	TERRITORIALES	MB	[HW11]	5	8	8	8	5
		Windows 2012	[SW14]	TERRITORIALES	MB	[HW4]	8	8	10	9	7

Tabla 12. (Continuación)

INVENTARIO Y VALORACION DE LOS ACTIVOS											
		Activo	**ID**	**UBICACIÓN**	**VALOR**	**DEPENDENCIAS**	**CRITICIDAD/DIMEN**				
TIPO	**ÁMBITO**						**A**utenticidad	**C**onfidencialidad	**I**ntegridad	**D**isponibilidad	**A**udibilidad
S	Servicios	Servicios externos de terceros (web corporativa publica , Inet + Email)	[S1]	NIVEL CENTRAL	MB	[COM1]	8	8	10	10	5
		Sistemas internos (compartición ficheros, grupo whatsapp,mensajería interna)	[S2]	NIVEL CENTRAL	MB	[HW4]	7	7	8	7	5
P	Personal	2 Asistentes	[P01]	NIVEL CENTRAL	A	-	0	0	0	5	0
		4 responsables	[P02]	NIVEL CENTRAL	A	-	0	0	0	6	0
		6 Asistentes	[P03]	TERRITORIALES	A	-	0	0	0	5	0

Fuente: El Autor

ACLARACIONES

Por simplicidad todos los servicios ofrecidos por la entidad se han agrupado en internos y externos incluyendo si son tercerizados, adicional a esto se evaluaron nivel central y territoriales en un solo conjunto, teniendo en cuenta que son 5 territoriales se evaluara como una sola localidad.

9.3 ANALISIS DE AMENZAS.

Siendo consecuentes con la metodología *MAGERIT*, se consideran las siguientes posibles amenazas:[31]

[31] MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información consultado el 18 de ENERO 2017 en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

[N] Desastres naturales.
Sucesos que pueden ocurrir sin intervención de los seres humanos con causa directa indirecta.
[N.1] Fuego
[N.2] Daños por agua
[N.3] Desastres naturales

[I] De origen industrial. Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental deliberada.
Origen: Natural (accidental)
[I.1] Fuego
[I.2] Daños por agua
[I.3] Desastres industriales
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura humedad
[I.8] Falla de servicios de comunicaciones
[I.9] Interrupción de otros servicios y suministros esenciales
[I.10] Degradación de los soportes de almacenamiento de la información
[I.11] Emanaciones electromagnéticas

[E] Errores y fallos no intencionados.
Fallos no intencionales causados por las personas.
Origen: Humano (accidental)
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.3] Errores de monitorización
[E.4] Errores de configuración
[E.8] Difusión de *Software* (SW) dañino
[E.9] Errores de [re]-encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de la información
[E.19] Fugas de información
[E.20] Vulnerabilidades de los programas (SW)
[E.21] Errores de mantenimiento / actualización de programas (SW)
[E.23] Errores de mantenimiento / actualización de equipos (HW)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[E.28] Indisponibilidad del personal

[A] Ataques intencionados.
Fallos deliberados causados por las personas.

Origen: Humano (deliberado)
[A.3] Manipulación de los registros de actividad (log)
[A.4] Manipulación de la configuración
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.8] Difusión de *Software* dañino
[A.9] [Re-] encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no Autorizado
[A.12] Análisis de tráfico
[A.13] Repudio
[A.14] Interceptación de información (escucha)
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.22] Manipulación de programas
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
[A.27] Ocupación enemiga
[A.28] Indisponibilidad del personal
[A.29] Extorsión
[A.30] Ingeniería social[32]

Se plasma en la **Tabla 13**. La frecuencia de ocurrencia de amenazas y se ha decidido tomar un rango máximo de una vez al día y uno mínimo de una vez al año, para calcular la frecuencia de ocurrencia de cada amenaza expresada en valores numéricos:

Tabla 16. Frecuencia de ocurrencia de amenaza

ID	**Vulnerabilidad**	**Rango**	**Valor**
FE	Frecuencia Extrema	cada día	100
FA	Frecuencia Alta	Cada 30 días	10
FM	Frecuencia Media	Cada 3 meses	1
FB	Frecuencia Baja	Cada 6 meses	0.1
FMB	Frecuencia Muy Baja	Cada 12 meses	0.01

Fuente: El Autor

[32] MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información consultado el 18 de ENERO 2017 en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Se elabora **Tabla 14.** con la Amenazas propuestas por la metodología Magerit incluyendo su frecuencia e impacto en las dimensiones ACIDA

Tabla 17. Amenazas propuestas con frecuencia e impacto

ACTIVOS [HW] Equipamiento Servidor	**FRECUENCIA**	**Autenticidad**	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Audibilidad**
[HW4] Servidor principal	**FB**		100%	50%	100%	
[HW12] Servidor de respaldo (*BACKUP* remoto)	**FB**		100%	50%	100%	
LISTA DE AMENAZAS						
[N.1] Fuego	**FMB**				100%	
[N.2] Daños por agua	**FMB**				100%	
[N.*] Desastres naturales	**FMB**				100%	
[I.1] Fuego	**FMB**				100%	
[I.2] Daños por agua	**FMB**				100%	
[I.*] Desastres industriales	**FMB**				100%	
[I.3] Contaminación mecánica	**FMB**				100%	
[I.4] Contaminación electromagnética	**FMB**				100%	
[I.5] Avería de origen físico o lógico	**FMB**				100%	
[I.6] Corte del suministro eléctrico	**FB**				50%	
[I.7] Condiciones inadecuadas de temperatura o humedad	**FMB**				75%	
[I.11] Emanaciones electromagnéticas – no aplicable -						
[E.2] Errores del administrador	**FB**		50%	50%	50%	
[E.23] Errores de mantenimiento / actualización de equipos (*Hardware)*	**FMB**				100%	
[E.24] Caída del sistema por agotamiento de recursos	**FMB**				75%	
[E.25] Pérdida de equipos	**FMB**		100%		100%	
[A.6] Abuso de privilegios de acceso	**FMB**		100%	50%	50%	
[A.7] Uso no previsto	**FB**		100%	50%	100%	
[A.11] Acceso no autorizado	**FMB**		50%	50%		
[A.23] Manipulación de los equipos	**FMB**		50%		50%	
[A.24] Denegación de servicio	**FMB**				100%	
[A.25] Robo	**FMB**		100%		100%	
[A.26] Ataque destructivo	**FMB**				100%	
[HW1] [HW9] Central IP + switch propio	**FM**		100%	25%	100%	
[HW2] [HW10] Fax	**FM**		100%	25%	100%	
[HW3] [HW11] PC ofimática	**FM**		100%	25%	100%	
[HW5] [HW13] Impresoras red	**FM**		100%	25%	100%	
[HW6] 1 impresora local	**FM**		100%	25%	100%	
[HW7] 1 switch Gigabit LAN	**FM**		100%	25%	100%	
[HW 8] [HW15] Escáner local USB	**FM**		100%	25%	100%	
[HW14] 1 switch 100mbs LAN	**FM**		100%	25%	100%	
[HW16] Laptop privado siendo utilizado dentro de FINALIN S.L.	**FM**		100%	25%	100%	

Tabla 14. (Continuación)

ACTIVOS [HW] Equipamiento HW excluyendo Servidores	FRECUENCIA	Autenticidad	Confidencialidad	Integridad	Disponibilidad	Audibilidad
LISTA DE AMENAZAS						
[N.1] Fuego	**FMB**				100%	
[N.2] Daños por agua	**FMB**				100%	
[N.*] Desastres naturales	**FMB**				100%	
[I.1] Fuego	**FMB**				100%	
[I.2] Daños por agua	**FMB**				100%	
[I.*] Desastres industriales	**FMB**				100%	
[I.3] Contaminación mecánica	**FMB**				100%	
[I.4] Contaminación electromagnética	**FMB**				100%	
[I.5] Avería de origen físico o lógico	**FM**				100%	
[I.6] Corte del suministro eléctrico	**FB**				100%	
[I.7] Condiciones inadecuadas de temperatura o humedad	**FMB**				75%	
[I.11] Emanaciones electromagnéticas – no aplicable -						
[E.2] Errores del administrador	**FB**		30%	20%	50%	
[E.23] Errores de mantenimiento / actualización de equipos (*Hardware)*	**FB**				100%	
[E.24] Caída del sistema por agotamiento de recursos	**FB**				50%	
[E.25] Pérdida de equipos	**FMB**		100%		100%	
[A.6] Abuso de privilegios de acceso	**FMB**		100%	20%	50%	
[A.7] Uso no previsto	**FB**		100%	10%	100%	
[A.11] Acceso no autorizado	**FMB**		50%	25%		
[A.23] Manipulación de los equipos	**FMB**		30%		30%	
[A.24] Denegación de servicio	**FMB**				100%	
[A.25] Robo	**FMB**		100%		100%	
[A.26] Ataque destructivo	**FMB**				100%	
[SW3] Antivirus	**FA**	**100%**	100%	100%	100%	
[SW6] SegurLit	**FA**	**100%**	100%	100%	100%	
[SW7] ContabiSol	**FA**	**100%**	100%	100%	100%	
[SW9] *Windows* 2003	**FA**	**100%**	100%	100%	100%	
[SW10] Terminal *server* CALC	**FA**	**100%**	100%	100%	100%	
[SW14] *Windows* 2012	**FA**	**100%**	100%	100%	100%	
LISTA DE AMENAZAS						
[I.5] Avería de origen físico o lógico	**FMB**				70%	
[E.1] Errores de los usuarios	**FB**		10%	10%	10%	
[E.2] Errores del administrador	**FMB**		30%	30%	30%	
[E.8] Difusión de *Software* dañino	**FMB**		30%	30%	50%	
[E.9] Errores de [re-]encaminamiento	**FMB**		10%			
[E.10] Errores de secuencia	**FMB**			10%		
[E.15] Alteración accidental de la información	**FMB**			10%		
[E.18] Destrucción de información	**FMB**				50%	
[E.19] Fugas de información	**FMB**		20%			
[E.20] Vulnerabilidades de los programas (*Software*)	**FMB**		25%	25%	25%	

Tabla 14. (Continuación)

ACTIVOS [SW] *Software* Servidor	**FRECUENCIA**	**Autenticidad**	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Audibilidad**
[E.21] Errores de mantenimiento / actualización de programas (*Software*)	**FA**			30%	30%	
[A.5] Suplantación de la identidad del usuario	**FMB**	100%	50%	100%		
[A.6] Abuso de privilegios de acceso	**FMB**		40%	25%	25%	
[A.7] Uso no previsto	**FMB**		10%	10%	50%	
[A.8] Difusión de *Software* dañino	**FMB**		80%	80%	80%	
[A.9] [Re-]encaminamiento de mensajes	**FMB**		50%			
[A.10] Alteración de secuencia	**FMB**			25%		
[A.11] Acceso no autorizado	**FMB**		50%	25%		
[A.15] Modificación deliberada de la información	**FMB**			50%		
[A.18] Destrucción de información	**FMB**				20%	
[A.19] Divulgación de información	**FMB**		50%			
[A.22] Manipulación de programas	**FMB**		100%	100%	100%	
[SW1] [SW11] LibreOffice 4	**FA**	**100%**	100%	100%	100%	
[SW2] Office 2010	**FA**	**100%**	100%	100%	100%	
[SW4] [SW12] *Windows* 7	**FA**	**100%**	100%	100%	100%	
[SW5] WinXP	**FA**	**100%**	100%	100%	100%	
[SW8] Access 97 Runtime	**FA**	**100%**	100%	100%	100%	
[SW13] *Windows* 8	**FA**	**100%**	100%	100%	100%	
LISTA DE AMENAZAS						
[I.5] Avería de origen físico o lógico	**FM**				50%	
[E.1] Errores de los usuarios	**FB**		15%	15%	15%	
[E.2] Errores del administrador	**FB**		20%	20%	20%	
[E.8] Difusión de *Software* dañino	**FB**		10%	10%	20%	
[E.9] Errores de [re-]encaminamiento	**FMB**		10%			
[E.10] Errores de secuencia	**FMB**			10%		
[E.15] Alteración accidental de la información	**FMB**			20%		
[E.18] Destrucción de información	**FMB**				50%	
[E.19] Fugas de información	**FMB**		50%			
[E.20] Vulnerabilidades de los programas (*Software*)	**FB**		30%	30%	50%	
[E.21] Errores de mantenimiento / actualización de programas (*Software*)	**FA**			50%	50%	
[A.5] Suplantación de la identidad del usuario	**FMB**	**100%**	100%	100%		
[A.6] Abuso de privilegios de acceso	**FMB**		30%	30%	50%	
[A.7] Uso no previsto	**FB**		20%	20%	100%	
[A.8] Difusión de *Software* dañino	**FMB**		90%	90%	100%	
[A.9] [Re-]encaminamiento de mensajes	**FMB**		50%			
[A.10] Alteración de secuencia	**FMB**			50%		
[A.11] Acceso no autorizado	**FMB**		100%	100%		
[A.15] Modificación deliberada de la información	**FMB**			50%		
[A.18] Destrucción de información	**FMB**				50%	
[A.19] Divulgación de información	**FMB**		50%			
[A.22] Manipulación de programas	**FMB**		100%	100%	100%	

Tabla 14. (Continuación)

ACTIVOS [D] Datos / Información	FRECUENCIA	Autenticidad	Confidencialidad	Integridad	Disponibilidad	Audibilidad
[DATOS1]Código Fuente (webs + programa Decesos)	FA	100%	100%	75%	100%	
[DATOS2]*Backup* Secundario en ext HD	FA	100%	100%	75%	100%	
[DATOS3]Datos SegurLit(cartera de pólizas generales)	FA	100%	100%	75%	100%	
[DATOS4]Datos Contabilidad	FA	100%	100%	75%	100%	
[DATOS5]BBDD Pólizas Decesos	FA	100%	100%	75%	100%	
[DATOS6]Imagen Corporativa	FA	100%	100%	75%	100%	
LISTA DE AMENAZAS						
[E.1] Errores de los usuarios	**FA**		25%	25%	25%	
[E.2] Errores del administrador	**FMB**		30%	30%	30%	
[E.15] Alteración accidental de la información	**FB**			20%		
[E.18] Destrucción de información	**FB**			25%		
[E.19] Fugas de información	**FMB**			20%		
[A.5] Suplantación de la identidad del usuario	**FMB**	100%	50%	30%		
[A.6] Abuso de privilegios de acceso	**FMB**		100%	50%	100%	
[A.11] Acceso no autorizado	**FMB**		100%	50%		
[A.15] Modificación deliberada de la información	**FMB**			75%		
[A.18] Destrucción de información	**FMB**				100%	
[A.19] Divulgación de información	**FMB**		100%			
[AUX1] [AUX5]Aire acondicionado en sala de asistentes donde se encuentra el Rack	**FB**		100%	50%	100%	
[AUX2] [AUX6]UPS Estabilizador para todo el rack.	**FB**		100%	50%	100%	
[AUX3] [AUX7]Cableado LAN	**FB**		100%	50%	100%	
[AUX4] [AUX8]Cableado suministro eléctrico	**FB**		100%	50%	100%	
LISTA DE AMENAZAS						
[N.1] Fuego	**FMB**				100%	
[N.2] Daños por agua	**FMB**				100%	
[N.*] Desastres naturales	**FMB**				100%	
[I.1] Fuego	**FMB**				100%	
[I.2] Daños por agua	**FMB**				100%	
[I.*] Desastres industriales	**FMB**				100%	
[I.3] Contaminación mecánica	**FMB**				100%	
[I.4] Contaminación electromagnética	**FMB**				100%	
[I.5] Avería de origen físico o lógico	**FMB**				100%	
[I.6] Corte del suministro eléctrico	**FMB**				100%	
[I.7] Condiciones inadecuadas de temperatura o humedad	**FMB**				100%	
[I.9] Interrupción de otros servicios y suministros esenciales	**FB**				100%	
[I.11] Emanaciones electromagnéticas – NO APLICA -						
[E.23] Errores de mantenimiento / actualización de equipos (*Hardware)*	**FMB**				100%	
[E.25] Pérdida de equipos	**FMB**		5%		30%	

Tabla 14. (Continuación)

ACTIVOS [AUX] Equipamiento auxiliar	**FRECUENCIA**	**Autenticidad**	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Audibilidad**
[A.7] Uso no previsto	**FMB**		10%	10%	20%	
[A.11] Acceso no autorizado	**FMB**		50%	50%		
[A.23] Manipulación de los equipos	**FMB**		50%		100%	
[A.25] Robo	**FMB**		100%		100%	
[A.26] Ataque destructivo	**FMB**				100%	
[L1]Rack principal (CPD a efectos prácticos)	**FB**	100%	75%	100%		
[L2]Archivo	**FB**	100%	75%	100%		
[L3] Rack secundario (CPD a efectos prácticos)	**FB**	100%	75%	100%		
LISTA DE AMENAZAS						
[N.1] Fuego	FMB			100%		
[N.2] Daños por agua	FMB			100%		
[N.*] Desastres naturales	FMB			100%		
[I.1] Fuego	FMB			100%		
[I.2] Daños por agua	FMB			100%		
[I.*] Desastres industriales	FMB			100%		
[I.11] Emanaciones electromagnéticas NO APLICA						
[E.15] Alteración accidental de la información	FB		25%			
[E.18] Destrucción de información	FMB			50%		
[E.19] Fugas de información	FMB	15%				
[A.7] Uso no previsto	FMB	50%	50%	50%		
[A.11] Acceso no autorizado	FMB	50%	50%			
[A.15] Modificación deliberada de la información	FMB		75%			
[A.18] Destrucción de información	FMB			75%		
[A.19] Divulgación de información	FMB	80%				
[A.26] Ataque destructivo	FMB			100%		
[A.27] Ocupación enemiga	FMB	100%		100%		
[COM1] [COM2] *Router* fibra RAVEG Telefonica, une las sedes y da conexión a Internet	FB	100% 50%	40%	80%		
LISTA DE AMENAZAS						
[I.8] Fallo de servicios de comunicaciones	FMB			50%		
[E.2] Errores del administrador	FMB	25%	25%	25%		
[E.9] Errores de [re-]encaminamiento	FMB	10%				
[E.10] Errores de secuencia	FMB		10%			
[E.15] Alteración accidental de la información	FMB		20%			
[E.18] Destrucción de información	FMB			30%		
[E.19] Fugas de información	FMB	10%				
[E.24] Caída del sistema por agotamiento de recursos	FMB			50%		

Tabla 14. (Continuación)

ACTIVOS [COM] Redes de comunicaciones	FRECUENCIA	Autenticidad	Confidencialidad	Integridad	Disponibilidad	Audibilidad
[A.5] Suplantación de la identidad del usuario	FMB	100%	40%	25%		
[A.6] Abuso de privilegios de acceso	FMB		35%	10%	35%	
[A.7] Uso no previsto	FB		10%	10%	75%	
[A.9] [Re-]encaminamiento de mensajes	FMB		10%			
[A.10] Alteración de secuencia	FMB			10%		
[A.11] Acceso no autorizado	FMB		50%	30%		
[A.12] Análisis de tráfico	FMB		20%			
[A.14] Interceptación de información (escucha)	FMB		40%			
[A.15] Modificación deliberada de la información	FMB			40%		
[A.19] Divulgación de información	FMB		40%			
[A.24] Denegación de servicio	FMB				80%	
[P02] Responsables	**FB**		70%	50%	75%	
LISTA DE AMENAZAS						
[E.19] Fugas de información	**FMB**		70%			
[E.28] Indisponibilidad del personal	**FB**				20%	
[A.28] Indisponibilidad del personal	**FMB**				75%	
[A.29] Extorsión	**FMB**		50%	50%	50%	
[A.30] Ingeniería social (picaresca)	**FMB**		20%	20%	20%	
[P01] [P03] Asistentes	**FMB**		50%	10%	40%	
LISTA DE AMENAZAS						
[E.19] Fugas de información	**FMB**		50%			
[E.28] Indisponibilidad del personal	**FMB**				10%	
[A.28] Indisponibilidad del personal	**FMB**				40%	
[A.29] Extorsión	**FMB**		10%	10%	10%	
[A.30] Ingeniería social (picaresca)	**FMB**		10%	10%	10%	
[MEDIA1]Disco duro externo USB para *backup* redundante local.	**FMB**		100%	75%	100%	
LISTA DE AMENAZAS						
[N.1] Fuego	**FMB**				100%	
[N.2] Daños por agua	**FMB**				100%	
[N.*] Desastres naturales	**FMB**				100%	
[I.1] Fuego	**FMB**				100%	
[I.2] Daños por agua	**FMB**				100%	
[I.*] Desastres industriales	**FMB**				100%	
[I.3] Contaminación mecánica	**FMB**				100%	
[I.4] Contaminación electromagnética	**FMB**				100%	
[I.5] Avería de origen físico o lógico	**FMB**				100%	
[I.6] Corte del suministro eléctrico	**FMB**				100%	
[I.7] Condiciones inadecuadas de temperatura o humedad	**FMB**				50%	

Tabla 14. (Continuación)

ACTIVOS [Media] Soportes de información - ELECTRONICO	FRECUENCIA	Autenticidad	Confidencialidad	Integridad	Disponibilidad	Audibilidad
[I.10] Degradación de los soportes de almacenamiento de la información	**FMB**				50%	
[I.11] Emanaciones electromagnéticas – NO APLICA						
[E.1] Errores de los usuarios	**FMB**		10%	10%	10%	
[E.2] Errores del administrador	**FMB**		20%	20%	40%	
[E.15] Alteración accidental de la información	**FMB**			10%		
[E.18] Destrucción de información	**FMB**				10%	
[E.19] Fugas de información	**FMB**		50%			
[E.23] Errores de mantenimiento / actualización de equipos (*Hardware)*	**FMB**				50%	
[E.25] Pérdida de equipos	**FMB**		10%		100%	
[A.7] Uso no previsto	**FMB**		30%		50%	
[A.11] Acceso no autorizado	**FMB**		100%	50%		
[A.15] Modificación deliberada de la información	**FMB**			75%		
[A.18] Destrucción de información	**FMB**				75%	
[A.19] Divulgación de información	**FMB**		75%			
[A.23] Manipulación de los equipos	**FMB**		50%		50%	
[A.25] Robo	**FMB**		100%		100%	
[A.26] Ataque destructivo	**FMB**				100%	
[MEDIA2]Archivo pólizas en papel	**FMB**		75%	75%	100%	
LISTA DE AMENAZAS						
[N.1] Fuego	**FMB**				100%	
[N.2] Daños por agua	**FMB**				100%	
[N.*] Desastres naturales	**FMB**				100%	
[I.1] Fuego	**FMB**				100%	
[I.2] Daños por agua	**FMB**				100%	
[I.*] Desastres industriales	**FMB**				50%	
[I.3] Contaminación mecánica	**FMB**				10%	
[I.4] Contaminación electromagnética	**FMB**				0%	
[I.5] Avería de origen físico o lógico	**FMB**				0%	
[I.6] Corte del suministro eléctrico	**FMB**				0%	
[I.7] Condiciones inadecuadas de temperatura o humedad	**FMB**				50%	
[I.10] Degradación de los soportes de almacenamiento de la información	**FMB**				50%	
[I.11] Emanaciones electromagnéticas – NO APLICA	**-**	**-**	-	-	-	

Tabla 14. (Continuación)

ACTIVOS [Media] Soportes de información	FRECUENCIA	Autenticidad	Confidencialidad	Integridad	Disponibilidad	Audibilidad
[E.1] Errores de los usuarios	**FMB**		10%	20%	20%	
[E.2] Errores del administrador	**FMB**		10%	20%	20%	
[E.15] Alteración accidental de la información	**FMB**			30%		
[E.18] Destrucción de información	**FMB**				30%	
[E.19] Fugas de información	**FMB**		30%			
[E.23] Errores de mantenimiento / actualización de equipos (*Hardware*)	**-**	-	-	-	-	
[E.25] Pérdida de equipos	**FMB**		50%		100%	
[A.7] Uso no previsto	**-**		-	-	-	
[A.11] Acceso no autorizado	**FMB**		75%	75%	0%	
[A.15] Modificación deliberada de la información	**FMB**			15%		
[A.18] Destrucción de información	**FMB**				50%	
[A.19] Divulgación de información	**FMB**		50%			
[A.23] Manipulación de los equipos	**-**	-	-	-	-	
[A.25] Robo	**FMB**		75%		100%	
[A.26] Ataque destructivo	**FMB**				100%	
[S1]Servicios externos de terceros (web corporativa publica, unet + Email)	**FM**	**100%**	100%	50%	100%	100%
[S2]Sistemas internos (compartición ficheros, grupo WhatsApp, mensajería interna)	**FM**	**100%**	100%	50%	100%	100%
LISTA DE AMENAZAS						
[E.1] Errores de los usuarios	**FB**		25%	25%	10%	
[E.2] Errores del administrador	**FMB**		40%	40%	40%	
[E.9] Errores de [re-]encaminamiento	**FMB**		40%			
[E.10] Errores de secuencia	**FMB**			40%		
[E.15] Alteración accidental de la información	**FM**			50%		
[E.18] Destrucción de información	**FM**				50%	
[E.19] Fugas de información	**FB**		50%			
[E.24] Caída del sistema por agotamiento de recursos	**FMB**				100%	
[A.5] Suplantación de la identidad del usuario	**FMB**	**100%**	50%	20%		
[A.6] Abuso de privilegios de acceso	**FMB**		25%	25%	10%	
[A.7] Uso no previsto	**FMB**		10%	10%	30%	
[A.9] [Re-]encaminamiento de mensajes	**FMB**		20%			
[A.10] Alteración de secuencia	**FMB**			20%		
[A.11] Acceso no autorizado	**FMB**		50%	40%		
[A.13] Repudio	**FMB**					100%
[A.15] Modificación deliberada de la información	**FMB**			30%		
[A.18] Destrucción de información	**FMB**				100%	
[A.19] Divulgación de información	**FMB**		100%			
[A.24] Denegación de servicio	**FMB**				100%	

Fuente: Investigación

9.4 IMPACTO POTENCIAL.

Teniendo como resultado las tablas presentadas en los ítems anteriores, se puede determinar el impacto potencial que se puede estimar en la entidad en caso de que llegue a materializarse las amenazas consideradas en cada activo.

La definición del impacto que se puede producir en la entidad se resume sobre los activos esenciales, es decir donde se centra la información que se maneja y los servicios prestados.

El impacto potencial será calculado en cada una de las dimensiones del activo mediante la siguiente formula:

Impacto Potencial = Valor Activo X Porcentaje de Impacto

En la **Tabla 15**. se muestra la valoración del impacto potencial para los activos de PARQUES NACIONALES NATURALES DE COLOMBIA agrupados por tipo de activo.

Tabla 18. Impacto potencial

IMPACTO POTENCIAL																
		CRITICIDAD					% DE IMPACTO					IMPACTO POTENCIAL				
TIPO	ID	Autenticidad	Confidencialidad	Integridad	Disponibilidad	Audibilidad	Autenticidad	Confidencialidad	Integridad	Disponibilidad	Audibilidad	Autenticidad	Confidencialidad	Integridad	Disponibilidad	Audibilidad
L	[L1]	8	9	10	10	8	0	100%	75%	100%	0	0	9	7,5	10	0
	[L2]	8	9	9	7	6	0	100%	75%	100%	0	0	9	6,75	7	0
	[L3]	8	9	10	10	8	0	100%	75%	100%	0	0	9	7,5	10	0
AUX	[AUX1]	0	0	0	8	0	0	100%	50%	100%	0	0	0	0	8	0
	[AUX2]	0	0	0	8	0	0	100%	50%	100%	0	0	0	0	8	0
	[AUX3]	0	0	0	10	0	0	100%	50%	100%	0	0	0	0	10	0
	[AUX4]	0	0	0	10	0	0	100%	50%	100%	0	0	0	0	10	0
	[AUX5]	0	0	0	8	0	0	100%	50%	100%	0	0	0	0	8	0
	[AUX6]	0	0	0	8	0	0	100%	50%	100%	0	0	0	0	8	0
	[AUX7]	0	0	0	10	0	0	100%	50%	100%	0	0	0	0	10	0
	[AUX8]	0	0	0	10	0	0	100%	50%	100%	0	0	0	0	10	0
COM	[COM1]	7	8	9	10	6	100%	50%	40%	80%	0	7	4	3,6	8	0
	[COM2]	7	8	9	10	6	100%	50%	40%	80%	0	7	4	3,6	8	0

Tabla 15. (Continuación)

		IMPACTO POTENCIAL														
		CRITICIDAD					% DE IMPACTO					IMPACTO POTENCIAL				
TIPO	ID	Autenticidad	Confidencialidad	Integridad	Disponibilidad	Audibilidad	Autenticidad	Confidencialidad	Integridad	Disponibilidad	Audibilidad	Autenticidad	Confidencialidad	Integridad	Disponibilidad	Audibilidad
HW	[HW1]	5	7	8	8	5	0	100%	25%	100%	0	0	7	2	8	0
	[HW2]	5	7	6	7	5	0	100%	25%	100%	0	0	7	1,5	7	0
	[HW3]	4	6	6	7	5	0	100%	25%	100%	0	0	6	1,5	7	0
	[HW4]	9	9	10	10	8	0	100%	50%	100%	0	0	9	5	10	0
	[HW5]	3	4	5	5	4	0	100%	25%	100%	0	0	4	1,25	5	0
	[HW6]	3	4	5	3	4	0	100%	25%	100%	0	0	4	1,25	3	0
	[HW7]	4	3	3	10	4	0	100%	25%	100%	0	0	3	0,75	10	0
	[HW8]	3	2	5	5	2	0	100%	25%	100%	0	0	2	1,25	5	0
	[HW9]	5	7	8	8	5	0	100%	25%	100%	0	0	7	2	8	0
	[HW10]	5	7	6	7	5	0	100%	25%	100%	0	0	7	1,5	7	0
	[HW11]	4	6	6	7	5	0	100%	25%	100%	0	0	6	1,5	7	0
	[HW12]	9	9	10	10	8	0	100%	50%	100%	0	0	9	5	10	0
	[HW13]	3	4	5	5	4	0	100%	25%	100%	0	0	4	1,25	5	0
	[HW14]	4	3	3	10	4	0	100%	25%	100%	0	0	3	0,75	10	0
	[HW15]	3	2	5	5	2	0	100%	25%	100%	0	0	2	1,25	5	0
	[HW16]	5	8	8	8	3	0	100%	25%	100%	0	0	8	2	8	0
MEDIA	[MEDIA1]	7	8	8	7	7	0	100%	75%	100%	0	0	8	6	7	0
	[MEDIA2]	8	8	8	8	8	0	75%	75%	100%	0	0	6	6	8	0
DATOS	[DATOS1]	7	8	8	8	7	100%	100%	75%	100%	0	7	8	6	8	0
	[DATOS2]	8	9	10	9	8	100%	100%	75%	100%	0	8	9	7,5	9	0
	[DATOS3]	8	10	10	10	8	100%	100%	75%	100%	0	8	10	7,5	10	0
	[DATOS4]	8	9	9	9	8	100%	100%	75%	100%	0	8	9	6,75	9	0
	[DATOS5]	8	10	10	10	8	100%	100%	75%	100%	0	8	10	7,5	10	0
	[DATOS6]	0	0	0	0	0	100%	100%	75%	100%	0	0	0	0	0	0

Tabla 15. (Continuación)

IMPACTO POTENCIAL																
		CRITICIDAD					% DE IMPACTO					IMPACTO POTENCIAL				
TIPO	ID	Autenticidad	Confidencialidad	Integridad	Disponibilidad	Audibilidad	Autenticidad	Confidencialidad	Integridad	Disponibilidad	Audibilidad	Autenticidad	Confidencialidad	Integridad	Disponibilidad	Audibilidad
SW	[SW1]	5	4	5	5	3	100%	100%	100%	100%	0	5	4	5	5	0
	[SW2]	5	3	4	5	3	100%	100%	100%	100%	0	5	3	4	5	0
	[SW3]	5	3	8	7	5	100%	100%	100%	100%	0	5	3	8	7	0
	[SW4]	8	4	6	7	4	100%	100%	100%	100%	0	8	4	6	7	0
	[SW5]	7	4	6	7	4	100%	100%	100%	100%	0	7	4	6	7	0
	[SW6]	8	8	8	9	7	100%	100%	100%	100%	0	8	8	8	9	0
	[SW7]	8	8	8	7	5	100%	100%	100%	100%	0	8	8	8	7	0
	[SW8]	5	5	5	6	4	100%	100%	100%	100%	0	5	5	5	6	0
	[SW9]	8	7	8	9	5	100%	100%	100%	100%	0	8	7	8	9	0
	[SW10]	8	6	8	8	5	100%	100%	100%	100%	0	8	6	8	8	0
	[SW11]	5	4	5	5	3	100%	100%	100%	100%	0	5	4	5	5	0
	[SW12]	5	8	8	8	4	100%	100%	100%	100%	0	5	8	8	8	0
	[SW13]	5	8	8	8	5	100%	100%	100%	100%	0	5	8	8	8	0
	[SW14]	8	8	10	9	7	100%	100%	100%	100%	0	8	8	10	9	0
S	[S1]	8	8	10	10	5	100%	100%	50%	100%	100%	8	8	5	10	5
	[S2]	7	7	8	7	5	100%	100%	50%	100%	100%	7	7	4	7	5
P	[P01]	0	0	0	5	0	0	50%	10%	40%	0	0	0	0	2	0
	[P02]	0	0	0	6	0	0	70%	50%	75%	0	0	0	0	4,5	0
	[P03]	0	0	0	5	0	0	50%	10%	40%	0	0	0	0	2	0

Fuente: El Autor

9.5 RIESGO POTENCIAL.

Al determinar el impacto potencial, se debe determinar el riesgo que asume la entidad al no tener implementados controles de seguridad. En tal sentido, se tiene en cuenta también, que se debe estimar el riesgo por cada activo y en cada dimensión. Para *Magerit*, se denomina riesgo a la medida del daño probable sobre un sistema.

Este riesgo es calculado para cada activo en cada dimensión mediante la siguiente formula: **Riesgo = Frecuencia X Impacto Potencial**
En la **Tabla 16.** se muestra el riesgo potencial para los activos de PARQUES NACIONALES NATURALES DE COLOMBIA

Tabla 19. Riesgo potencial

RIESGO POTENCIAL													
				IMPACTO POTENCIAL					**RIESGO**				
TIPO	**ID**	**FRECUENCIA**		**A**utenticidad	**C**onfidencialidad	**I**ntegridad	**D**isponibilidad	**A**udibilidad	**A**utenticidad	**C**onfidencialidad	**I**ntegridad	**D**isponibilidad	**A**udibilidad
L	[L1]	(FB)	0,1	0	9	7,5	10	0	**0**	**0,9**	**0,75**	**1**	**0**
	[L2]	(FB)	0,1	0	9	6,75	7	0	**0**	**0,9**	**0,675**	**0,7**	**0**
	[L3]	(FB)	0,1	0	9	7,5	10	0	**0**	**0,9**	**0,75**	**1**	**0**
AUX	[AUX1]	(FB)	0,1	0	0	0	8	0	**0**	**0**	**0**	**0,8**	**0**
	[AUX2]	(FB)	0,1	0	0	0	8	0	**0**	**0**	**0**	**0,8**	**0**
	[AUX3]	(FB)	0,1	0	0	0	10	0	**0**	**0**	**0**	**1**	**0**
	[AUX4]	(FB)	0,1	0	0	0	10	0	**0**	**0**	**0**	**1**	**0**
	[AUX5]	(FB)	0,1	0	0	0	8	0	**0**	**0**	**0**	**0,8**	**0**
	[AUX6]	(FB)	0,1	0	0	0	8	0	**0**	**0**	**0**	**0,8**	**0**
	[AUX7]	(FB)	0,1	0	0	0	10	0	**0**	**0**	**0**	**1**	**0**
	[AUX8]	(FB)	0,1	0	0	0	10	0	**0**	**0**	**0**	**1**	**0**
COM	[COM1]	(FB)	0,1	7	4	3,6	8	0	**0,7**	**0,4**	**0,36**	**0,8**	**0**
	[COM2]	(FB)	0,1	7	4	3,6	8	0	**0,7**	**0,4**	**0,36**	**0,8**	**0**
	[HW1]	(FM)	1	0	7	2	8	0	0	**7**	**2**	**8**	**0**
	[HW2]	(FM)	1	0	7	1,5	7	0	0	**7**	**1,5**	**7**	**0**
	[HW3]	(FM)	1	0	6	1,5	7	0	0	**6**	**1,5**	**7**	**0**
	[HW4]	(FB)	0,1	0	9	5	10	0	0	**0,9**	**0,5**	**1**	**0**
	[HW5]	(FM)	1	0	4	1,25	5	0	0	**4**	**1,25**	**5**	**0**
	[HW6]	(FM)	1	0	4	1,25	3	0	0	**4**	**1,25**	**3**	**0**
	[HW7]	(FM)	1	0	3	0,75	10	0	0	**3**	**0,75**	**10**	**0**
	[HW8]	(FM)	1	0	2	1,25	5	0	0	**2**	**1,25**	**5**	**0**
	[HW9]	(FM)	1	0	7	2	8	0	0	**7**	**2**	**8**	**0**
	[HW10]	(FM)	1	0	7	1,5	7	0	0	**7**	**1,5**	**7**	**0**
	[HW11]	(FM)	1	0	6	1,5	7	0	0	**6**	**1,5**	**7**	**0**
	[HW12]	(FB)	0,1	0	9	5	10	0	0	**0,9**	**0,5**	**1**	**0**
	[HW13]	(FM)	1	0	4	1,25	5	0	0	**4**	**1,25**	**5**	**0**
	[HW14]	(FM)	1	0	3	0,75	10	0	0	**3**	**0,75**	**10**	**0**
	[HW15]	(FM)	1	0	2	1,25	5	0	0	**2**	**1,25**	**5**	**0**
	[HW16]	(FM)	1	0	8	2	8	0	0	**8**	**2**	**8**	**0**

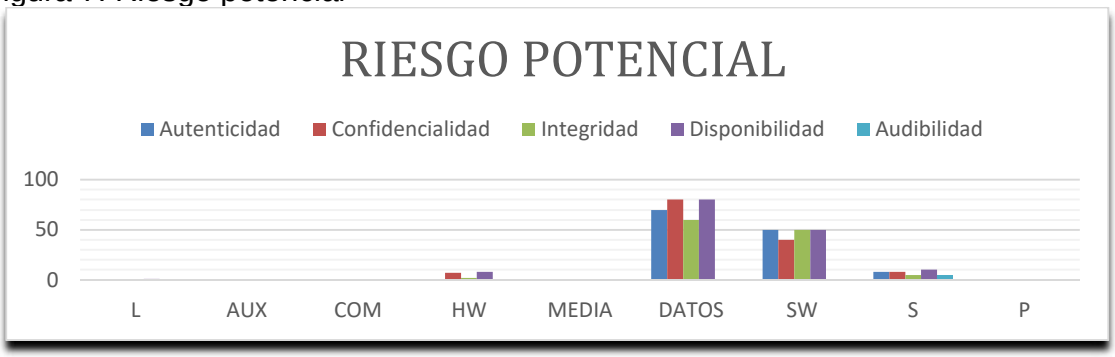
Tabla 16. (Continuación)

RIESGO POTENCIAL													
				IMPACTO POTENCIAL					**RIESGO**				
TIPO	**ID**	**FRECUENCIA**		**A**utenticidad	**C**onfidencialidad	**I**ntegridad	**D**isponibilidad	**A**udibilidad	**A**utenticidad	**C**onfidencialidad	**I**ntegridad	**D**isponibilidad	**A**udibilidad
MEDIA	[MEDIA1]	(FMB)	0,01	0	8	6	7	0	**0**	**0,08**	**0,06**	**0,07**	**0**
	[MEDIA2]	(FMB)	0,01	0	6	6	8	0	**0**	**0,06**	**0,06**	**0,08**	**0**
DATOS	[DATOS1]	(FA)	10	7	8	6	8	0	**70**	**80**	**60**	**80**	**0**
	[DATOS2]	(FA)	10	8	9	6,75	8	0	**80**	**90**	**67,5**	**80**	**0**
	[DATOS3]	(FA)	10	8	10	7,5	8	0	**80**	**100**	**75**	**80**	**0**
	[DATOS4]	(FA)	10	8	9	6,75	9	0	**80**	**90**	**67,5**	**90**	**0**
	[DATOS5]	(FA)	10	8	10	7,5	10	0	**80**	**100**	**75**	**100**	**0**
	[DATOS6]	(FA)	10	0	0	0	0	0	**0**	**0**	**0**	**0**	**0**
SW	[SW1]	(FA)	10	5	4	5	5	0	50	**40**	**50**	**50**	**0**
	[SW2]	(FA)	10	5	3	4	5	0	50	**30**	**40**	**50**	**0**
	[SW3]	(FA)	10	5	3	8	7	0	50	**30**	**80**	**70**	**0**
	[SW4]	(FA)	10	8	4	6	7	0	80	**40**	**60**	**70**	**0**
	[SW5]	(FA)	10	7	4	6	7	0	70	**40**	**60**	**70**	**0**
	[SW6]	(FA)	10	8	8	8	9	0	80	**80**	**80**	**90**	**0**
	[SW7]	(FA)	10	8	8	8	7	0	80	**80**	**80**	**70**	**0**
	[SW8]	(FA)	10	5	5	5	6	0	50	**50**	**50**	**60**	**0**
	[SW9]	(FA)	10	8	7	8	9	0	80	**70**	**80**	**90**	**0**
	[SW10]	(FA)	10	8	6	8	8	0	80	**60**	**80**	**80**	**0**
	[SW11]	(FA)	10	5	4	5	5	0	50	**40**	**50**	**50**	**0**
	[SW12]	(FA)	10	5	8	8	8	0	50	**80**	**80**	**80**	**0**
	[SW13]	(FA)	10	5	8	8	8	0	50	**80**	**80**	**80**	**0**
	[SW14]	(FA)	10	8	8	10	9	0	80	**80**	**100**	**90**	**0**
S	[S1]	(FM)	1	8	8	5	10	5	**8**	**8**	**5**	**10**	**5**
	[S2]	(FM)	1	7	7	4	7	5	**7**	**7**	**4**	**7**	**5**
P	[P01]	(FMB)	0,01	0	0	0	2	0	**0**	**0**	**0**	**0,02**	**0**
	[P02]	(FB)	0,1	0	0	0	4,5	0	**0**	**0**	**0**	**0,45**	**0**
	[P03]	(FMB)	0,01	0	0	0	2	0	**0**	**0**	**0**	**0,02**	**0**

Fuente: El Autor

En el gráfico de la Figura 7. se visualiza que tanto los activos [DATOS] como [SW] son los que poseen mayor riesgo medio, teniendo 4 dimensiones muy cerca o superando el valor límite de 60 establecido por la entidad. Sera en estos activos donde se debe concentrar los esfuerzos con el objetivo de mitigar este riesgo hasta niveles aceptables

Figura 7. Riesgo potencial



Fuente: El Autor

En [DATOS] se agrupan todos aquellos activos de tipo datos, incluyendo, por ejemplo, SIIF, NOMINA de PARQUES NACIONALES NATURALES DE COLOMBIA, copias de seguridad y código fuente de desarrollos, internos, aplicaciones Bases de Datos y web de la entidad. Siendo esta información fundamental para el correcto funcionamiento. Por tanto, debe ser protegida adecuadamente y los riesgos mitigados adecuadamente con las salvaguardas correspondientes.

En [SW] se agrupan aquellos activos de tipo *Software* como sistemas operativos de cliente y servidor, antivirus, MS Office, entre otros… Es *Software* utilizado por usuarios para el cumplimiento de la misión de la entidad y está expuesto a errores de los propios usuarios como a amenazas externas como virus, malware, etc. Su protección es de vital importancia.
Ver Anexos F3
ANEXO K. FASE 3 - CONSOLIDADO TABLAS

9.6 RIESGOS A TRATAR.

Como resultados de los análisis de riesgos es prioritario la definición de proyectos que protejan y reduzcan el riesgo potencial de los activos detectados como los más críticos, estos son [SW] y [DATOS].

10. FASE IV PROPUESTAS DE PROYECTOS.

10.1 INTRODUCCION.

Posterior a la FASE 3, donde se procedió a realizar un análisis completo de los riesgos de la entidad PARQUES NACIONALES NATURALES DE COLOMBIA., En la FASE 4 una vez identificados los activos más vulnerables, se mitigan los riesgos detectados más relevantes.

10.2 PROPUESTAS DE MEJORA.

A partir de la información recopilada hasta ahora, se ha definido un conjunto de iniciativas y proyectos necesarios para conseguir el nivel de seguridad que PARQUES NACIONALES NATURALES DE COLOMBIA necesita. El detalle de los proyectos se puede consultar en el CARPETA - ANEXO F4 del presente proyecto.

La mejora producida por la ejecución de los siguientes proyectos reducirá el riesgo actual a la Organización y evolucionará el cumplimiento ISO hasta el nivel adecuado.

Dado que el análisis que se ha llevado a cabo incluye diferentes ámbitos como RRHH, Dirección, Mantenimiento, etc. los proyectos e iniciativas también serán de diferente ámbito.

Los proyectos contemplan iniciativas dirigidas a mejorar la metodología de trabajo actual, a fin de que éstas cumplan con los controles establecidos por el marco normativo y regulatorio y garantizar e implementar controles técnicos y físicos detectados. Con la ejecución de estos proyectos también se persigue gestionar los riesgos por encima del umbral de riesgo aceptable.

La lista de proyectos propuestos se muestra a continuación, siendo todos ellos detallados en el archivo llamado **PROPUESTAS DE PROYECTOS**. El orden de ejecución de los mismos se ha establecido priorizando a la continuidad del servicio.
Ver Anexos F4
ANEXO L. FASE 4 - PROPUESTAS DE PROYECTOS

ID	PROYECTO
P01	ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD
P02	DOCUMENTAR UNA POLÍTICA DE USO DE MEDIOS TECNOLÓGICOS
P03	DOCUMENTAR LA POLÍTICA DE GESTIÓN DE ACCESO

P04 DOCUMENTAR UNA POLÍTICA DE INTERCAMBIO DE INFORMACIÓN
P05 DOCUMENTAR POLÍTICA DE ENCAMINAMIENTO
P06 DOCUMENTAR POLÍTICA DE ELIMINACIÓN SEGURA DE SOPORTES DE INFORMACIÓN
P07 POLÍTICA DE TRATAMIENTO DE LA INFORMACIÓN
P08 POLÍTICA DE FORMACIÓN EN MATERIA DE SEGURIDAD
P09 CRITERIOS DE SELECCIÓN DE PERSONAL
P10 SOPORTE Y SEGURIDAD DEL CABLEADO
P11 SISTEMATIZACIÓN DEL INVENTARIO DE ACTIVOS
P12 SISTEMATIZACIÓN DEL REGISTRO DE INTERCAMBIOS DE INFORMACIÓN
P13 SISTEMA DE ACCESO EL PC POR LECTURA TARJETA EMPLEADO + CONTRASEÑA
P14 SEGUIMIENTO Y MEDICIÓN LOS OBJETIVOS Y CONTROLES

10.3 PLANIFICACION TEMPORAL DE EJECUCIÓN.

En la **Tabla 17.** se visualiza la planificación a mediano, corto y largo plazo de la ejecución de los proyectos propuestos en el Plan Director de Seguridad, para la entidad PARQUES NACIONALES NATURALES DE COLOMBIA. La duración de cada proyecto se ha hecho teniendo en cuenta que la persona encargada de llevarlo a cabo es la responsable del área de informática y dará prioridad a los eventos e incidentes del día a día.

Tabla 20. Planificación de proyectos

NOMBRE DE LA TAREA	TIEMPO	FECHA INICIO	FECHA FINAL	DURACIÓN DÍAS
ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD	CORTO PLAZO	16/09/2017	21/09/2017	5
DOCUMENTAR UNA POLÍTICA DE USO DE MEDIOS TECNOLÓGICOS	CORTO PLAZO	22/09/2017	23/09/2017	1
DOCUMENTAR LA POLÍTICA DE GESTIÓN DE ACCESO	CORTO PLAZO	22/09/2017	28/09/2017	6
DOCUMENTAR UNA POLÍTICA DE INTERCAMBIO DE INFORMACIÓN	MEDIO PLAZO	27/09/2017	29/11/2017	63

Tabla 17 (Continuación)

NOMBRE DE LA TAREA	TIEMPO	FECHA INICIO	FECHA FINAL	DURACIÓN DÍAS
POLÍTICA DE TRATAMIENTO DE LA INFORMACIÓN	CORTO PLAZO	28/09/2017	05/10/2017	7
DOCUMENTAR POLÍTICA DE ENCAMINAMIENTO	MEDIO PLAZO	28/09/2017	04/11/2017	37
POLÍTICA DE FORMACIÓN EN MATERIA DE SEGURIDAD	CORTO PLAZO	04/10/2017	06/10/2017	2
DOCUMENTAR POLÍTICA DE ELIMINACIÓN SEGURA DE SOPORTES DE INFORMACIÓN	CORTO PLAZO	05/10/2017	09/10/2017	4
CRITERIOS DE SELECCIÓN DE PERSONAL	CORTO PLAZO	07/10/2017	10/10/2017	3
SOPORTE Y SEGURIDAD DEL CABLEADO	MEDIO PLAZO	09/10/2017	12/11/2017	34
SISTEMATIZACIÓN DEL INVENTARIO DE ACTIVOS	MEDIO PLAZO	11/10/2017	14/11/2017	34
SISTEMATIZACIÓN DEL REGISTRO DE INTERCAMBIOS DE INFORMACIÓN	MEDIO PLAZO	15/10/2017	17/11/2017	33
SISTEMA DE ACCESO EL PC POR LECTURA TARJETA EMPLEADO + CONTRASEÑA	MEDIO PLAZO	19/10/2017	20/11/2017	32
SEGUIMIENTO Y MEDICIÓN LOS OBJETIVOS Y CONTROLES	LARGO PLAZO	23/11/2017	23/04/2018	211

Fuente: El Autor

10.4 EVALUACIÓN DEL RIESGO TRAS LA IMPLANTACIÓN DE LOS PROYECTOS.

Con la ejecución de los proyectos presentados se provoca una positiva evolución en la disminución del riesgo de la entidad como se puede ver la **Tabla 18.** La evolución del riesgo y el impacto tras la ejecución de los proyectos es significativa tanto en el impacto potencial como en el riesgo potencial.

Tabla 21. Evolución del riesgo y el impacto tras la ejecución de los proyectos

RIESGO POTENCIAL													
				IMPACTO POTENCIAL					**RIESGO**				
TIPO	**ID**	**FRECUENCIA**		**A**utenticidad	**C**onfidencialidad	**I**ntegridad	**D**isponibilidad	**A**udibilidad	**A**utenticidad	**C**onfidencialidad	**I**ntegridad	**D**isponibilidad	**A**udibilidad
L	[L1]	(FB)	0,1	0	9	7,5	10	0	**0**	**0,9**	**0,75**	**1**	**0**
	[L2]	(FB)	0,1	0	9	6,75	7	0	**0**	**0,9**	**0,675**	**0,7**	**0**
	[L3]	(FB)	0,1	0	9	7,5	10	0	**0**	**0,9**	**0,75**	**1**	**0**
AUX	[AUX1]	(FB)	0,1	0	0	0	8	0	**0**	**0**	**0**	**0,8**	**0**
	[AUX2]	(FB)	0,1	0	0	0	8	0	**0**	**0**	**0**	**0,8**	**0**
	[AUX3]	(FB)	0,1	0	0	0	10	0	**0**	**0**	**0**	**1**	**0**
	[AUX4]	(FB)	0,1	0	0	0	10	0	**0**	**0**	**0**	**1**	**0**
	[AUX5]	(FB)	0,1	0	0	0	8	0	**0**	**0**	**0**	**0,8**	**0**
	[AUX6]	(FB)	0,1	0	0	0	8	0	**0**	**0**	**0**	**0,8**	**0**
	[AUX7]	(FB)	0,1	0	0	0	10	0	**0**	**0**	**0**	**1**	**0**
	[AUX8]	(FB)	0,1	0	0	0	10	0	**0**	**0**	**0**	**1**	**0**
COM	[COM1]	(FB)	0,1	7	4	3,6	8	0	**0,7**	**0,4**	**0,36**	**0,8**	**0**

Tabla 18. (Continuación)

RIESGO POTENCIAL													
				IMPACTO POTENCIAL					**RIESGO**				
TIPO	**ID**	**FRECUENCIA**		**A**utenticidad	**C**onfidencialidad	**I**ntegridad	**D**isponibilidad	**A**udibilidad	**A**utenticidad	**C**onfidencialidad	**I**ntegridad	**D**isponibilidad	**A**udibilidad
HW	[COM2]	(FB)	0,1	7	4	3,6	8	0	**0,7**	**0,4**	**0,36**	**0,8**	**0**
	[HW1]	(FM)	1	0	7	2	8	0	**0**	**7**	**2**	**8**	**0**
	[HW2]	(FM)	1	0	7	1,5	7	0	**0**	**7**	**1,5**	**7**	**0**
	[HW3]	(FM)	1	0	6	1,5	7	0	**0**	**6**	**1,5**	**7**	**0**
	[HW4]	(FB)	0,1	0	9	5	10	0	**0**	**0,9**	**0,5**	**1**	**0**
	[HW5]	(FM)	1	0	4	1,25	5	0	**0**	**4**	**1,25**	**5**	**0**
	[HW6]	(FM)	1	0	4	1,25	3	0	**0**	**4**	**1,25**	**3**	**0**
	[HW7]	(FM)	1	0	3	0,75	10	0	**0**	**3**	**0,75**	**10**	**0**
	[HW8]	(FM)	1	0	2	1,25	5	0	**0**	**2**	**1,25**	**5**	**0**
	[HW9]	(FM)	1	0	7	2	8	0	**0**	**7**	**2**	**8**	**0**
	[HW10]	(FM)	1	0	7	1,5	7	0	**0**	**7**	**1,5**	**7**	**0**
	[HW11]	(FM)	1	0	6	1,5	7	0	**0**	**6**	**1,5**	**7**	**0**
	[HW12]	(FB)	0,1	0	9	5	10	0	**0**	**0,9**	**0,5**	**1**	**0**
	[HW13]	(FM)	1	0	4	1,25	5	0	**0**	**4**	**1,25**	**5**	**0**
	[HW14]	(FM)	1	0	3	0,75	10	0	**0**	**3**	**0,75**	**10**	**0**
	[HW15]	(FM)	1	0	2	1,25	5	0	**0**	**2**	**1,25**	**5**	**0**
	[HW16]	(FM)	1	0	8	2	8	0	**0**	**8**	**2**	**8**	**0**
MEDIA	[MEDIA1]	(FMB)	0,01	0	8	6	7	0	**0**	**0,08**	**0,06**	**0,07**	**0**
	[MEDIA2]	(FMB)	0,01	0	6	6	8	0	**0**	**0,06**	**0,06**	**0,08**	**0**
DATOS	[DATOS1]	(FA)	10	7	8	6	8	0	**70**	**80**	**60**	**80**	**0**
	[DATOS2]	(FA)	10	8	9	6,75	8	0	**80**	**90**	**67,5**	**80**	**0**
	[DATOS3]	(FA)	10	8	10	7,5	8	0	**80**	**100**	**75**	**80**	**0**
	[DATOS4]	(FA)	10	8	9	6,75	9	0	**80**	**90**	**67,5**	**90**	**0**
	[DATOS5]	(FA)	10	8	10	7,5	10	0	**80**	**100**	**75**	**100**	**0**
	[DATOS6]	(FA)	10	0	0	0	0	0	**0**	**0**	**0**	**0**	**0**

Tabla 18. (Continuación)

RIESGO POTENCIAL													
				IMPACTO POTENCIAL					**RIESGO**				
TIPO	**ID**	**FRECUENCIA**		**A**utenticidad	**C**onfidencialidad	**I**ntegridad	**D**isponibilidad	**A**udibilidad	**A**utenticidad	**C**onfidencialidad	**I**ntegridad	**D**isponibilidad	**A**udibilidad
SW	[SW1]	(FA)	10	5	4	5	5	0	**50**	**40**	**50**	**50**	**0**
	[SW2]	(FA)	10	5	3	4	5	0	**50**	**30**	**40**	**50**	**0**
	[SW3]	(FA)	10	5	3	8	7	0	**50**	**30**	**80**	**70**	**0**
	[SW4]	(FA)	10	8	4	6	7	0	**80**	**40**	**60**	**70**	**0**
	[SW5]	(FA)	10	7	4	6	7	0	**70**	**40**	**60**	**70**	**0**
	[SW6]	(FA)	10	8	8	8	9	0	**80**	**80**	**80**	**90**	**0**
	[SW7]	(FA)	10	8	8	8	7	0	**80**	**80**	**80**	**70**	**0**
	[SW8]	(FA)	10	5	5	5	6	0	**50**	**50**	**50**	**60**	**0**
	[SW9]	(FA)	10	8	7	8	9	0	**80**	**70**	**80**	**90**	**0**
	[SW10]	(FA)	10	8	6	8	8	0	**80**	**60**	**80**	**80**	**0**
	[SW11]	(FA)	10	5	4	5	5	0	**50**	**40**	**50**	**50**	**0**
	[SW12]	(FA)	10	5	8	8	8	0	**50**	**80**	**80**	**80**	**0**
	[SW13]	(FA)	10	5	8	8	8	0	**50**	**80**	**80**	**80**	**0**
	[SW14]	(FA)	10	8	8	10	9	0	**80**	**80**	**100**	**90**	**0**
S	[S1]	(FM)	1	8	8	5	10	5	**8**	**8**	**5**	**10**	**5**
	[S2]	(FM)	1	7	7	4	7	5	**7**	**7**	**4**	**7**	**5**
P	[P01]	(FMB)	0,01	0	0	0	2	0	**0**	**0**	**0**	**0,02**	**0**
	[P02]	(FB)	0,1	0	0	0	4,5	0	**0**	**0**	**0**	**0,45**	**0**
	[P03]	(FMB)	0,01	0	0	0	2	0	**0**	**0**	**0**	**0,02**	**0**

Fuente: El Autor

Los proyectos presentados repercuten muy favorablemente tanto en la reducción de la frecuencia de aparición de las distintas amenazas, como en el porcentaje de impacto sobre los activos.

En la **Figura 8.** se muestra el resultado, evolución del riesgo y el impacto tras la ejecución de los proyectos, se visualiza en azul los indicadores de riesgo que antes estaban por encima del umbral permitido (>60). Éstos corresponden principalmente

a activos de tipo [SW] y [DATOS]. Tras la ejecución de los proyectos, todos los valores se sitúan por debajo de 1, representando un riesgo muy bajo, similar al del resto de los activos de la entidad.

Figura 8. Evolución del riesgo y el impacto tras la ejecución de los proyectos

Fuente: El Autor

10.5 NIVEL DE CUMPLIMIENTOS DE LA NORMA ISO/IEC 27002:2013.

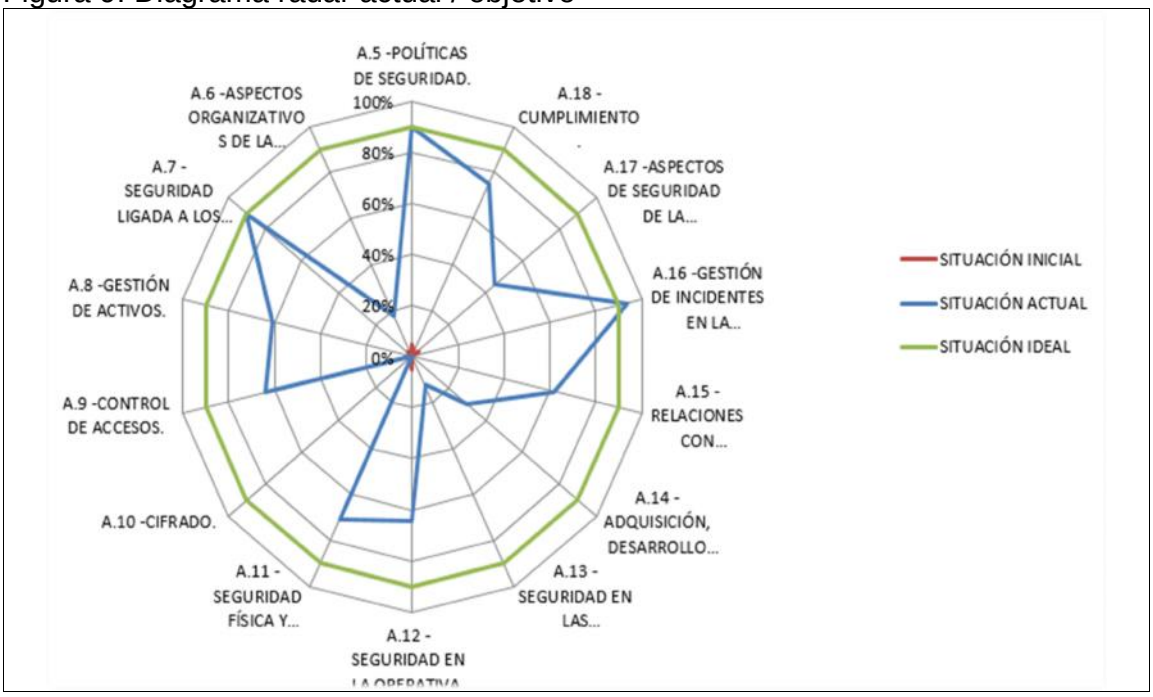
Se han definido 14 proyectos a realizar en un plazo de 06 meses. El objetivo principal es mitigar el nivel de riesgo de los activos, desarrollando proyectos focalizados en los puntos vulnerables con riesgos más altos como son datos [DATOS] y *Software* [SW] el nivel de riesgo potencial está por encima del umbral aceptado por la entidad. Aunque esta reducción del riesgo es importante, también se tiene como objetivo la evolución positiva del nivel de cumplimiento de los diferentes dominios de la norma ISO 27002:2013.

A futuro la finalidad es lograr la certificación, cumpliendo los diferentes dominios que aplican para la entidad bajo la norma ISO 27002:2013, en el siguiente grafico se visualiza la evolución en cuanto al cumplimiento de la norma una vez aplicados y desarrollados los proyectos. Es importante resaltar que el presente plan director no tiene como objetivo principal la certificación, esto se debe a que no se tiene presupuesto disponible en la presente vigencia 2018, el objetivo principal es realizar un análisis profundo de la entidad en materia de seguridad de la información y establecer unas bases bajo la norma ISO 27002:2013 que asegurasen que el riesgo encontrado es identificado y mitigado adecuadamente. [33]

[33] PORTAL ISO - ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES consultado el 19 de ENERO 2017 en: http://www.iso27000.es/download/ControlesISO27002-2013.pdf

Seguidamente se presenta en la **Figura 9.** el diagrama RADAR con la SITUACIÓN INICIAL con respecto al SITUACIÓN ACTUAL resultante a la ejecución de los proyectos planteados apuntando a conseguir una SITUACIÓN IDEAL

Figura 9. Diagrama radar actual / objetivo



Fuente: El Autor

11. FASE V AUDITORIA DEL CUMPLIMIENTO.

11.1 INTRODUCCION.

Una vez implementados los proyectos propuestos en el punto anterior y con el objetivo de evaluar la madurez de la seguridad, se analiza en este apartado el cumplimiento de la ISO / IEC 27001: 2013 que incluye los controles de la ISO / IEC 27002: 2013, de acuerdo con las fases previas de definición del SGSI de PARQUES NACIONALES NATURALES DE COLOMBIA.

11.2 OBJETIVO.

El objetivo de la auditoria es determinar el grado de cumplimiento del SGSI de PARQUES NACIONALES NATURALES DE COLOMBIA a la fecha de ejecución de la auditoría respecto a la norma ISO / IEC27001: 2013 y evaluar su eficacia para conseguir los objetivos inicialmente especificados.

Cabe destacar que la auditoria se realiza partiendo del supuesto que todos los proyectos presentados en la Fase 4 han sido ejecutados y cumplidos con éxito. Esta fase se desarrollará en el espacio de tiempo entre la finalización de los proyectos y la fecha propuesta para realizar la auditoria oficial, que daría a PARQUES NACIONALES NATURALES DE COLOMBIA la certificación oficial ISO 27001.

11.3 PLAN DE AUDITORIA.

En la **Tabla 19.** Se referencia el resumen del plan de auditoria de cumplimiento.

Tabla 19. Resumen plan de auditoria de cumplimiento

AUDITORIA DE CUMPLIMIENTO	
Razón Social	PARQUES NACIONALES NATURALES DE COLOMBIA
Fecha de la auditoria	06 de marzo 2017 – 01 mayo 2018
Lugar de la auditoria	NIVEL CENTRAL
Tipo de auditoria	Interna De Cumplimiento ISO 27002:2013
Normas y Referencias legales	ISO 27001 y ISO27002

Fuente: El Autor

11.4 ALCANCE.

Se han auditado todas las áreas de PARQUES NACIONALES NATURALES DE COLOMBIA que están relacionadas con el alcance del SGSI (sistemas y personas involucradas con los sistemas informáticos, la información almacenada en estos, los sistemas en red y la documentación en papel que gestiona entidad)

11.5 EVOLUCION DEL ANALISIS DIFERENCIAL.

Aunque el informe de auditoría resultante se presenta en el archivo Auditoria De Cumplimiento en el presente proyecto, se consolidan los resultados de alto nivel de esta en:

Ver Anexos F5
ANEXO M. FASE 5 - AUDITORIA DE CUMPLIMIENTO

Para una mejor comprensión, en la siguiente **Tabla 20.** se muestra, a modo de resumen, las valoraciones obtenidas de todos los dominios agrupando todos sus controles. Se realiza la comparación del estado inicial "Fase 1" con el estado una vez finalizada la auditoria "Fase 5" (estado alcanzado una vez finalizados los proyectos presentados en Fase 4).

Tabla 20. Resumen comparativo de valoraciones CMM de los dominios en las fases 1 y 5

Dominio Bajo La Norma ISO 27002:2013	% de conformidad INICIAL	% de conformidad POS-AUDITORIA
A.5 POLÍTICAS DE SEGURIDAD.	5%	90%
A.6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION.	0%	18%
A.7 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	3%	90%
A.8 GESTIÓN DE ACTIVOS.	0%	61%
A.9 CONTROL DE ACCESOS.	3%	64%
A.10 CIFRADO.	0%	0%
A.11 SEGURIDAD FÍSICA Y AMBIENTAL.	1%	71%
A.12 SEGURIDAD EN LA OPERATIVA.	5%	64%
A.13 SEGURIDAD EN LAS TELECOMUNICACIONES.	0%	13%

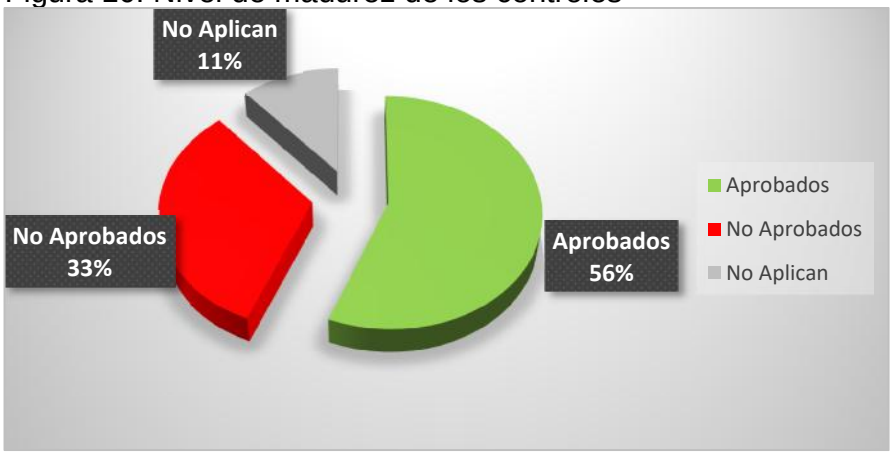
Table 20 (Continuación)

Dominio Bajo La Norma ISO 27002:2013	% de conformidad INICIAL	% de conformidad POS-AUDITORIA
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.	0%	30%
A.15 RELACIONES CON SUMINISTRADORES.	0%	62%
A.16 GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	0%	93%
A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.	3%	45%
A.18 CUMPLIMIENTO.	2%	75%

Fuente: El Autor

Se puede apreciar en la **Figura 10.** el Nivel de madurez de los controles, el porcentaje de controles que alcanzan cada uno de los niveles considerados en CMM. Se observa en la gráfica que solamente el 56% de los controles alcanzan un nivel de madurez considerado aceptable (CMM >= L3). Es importante que en los próximos planes directores se preste atención a ese 33% de controles, que se encuentran en niveles demasiado bajos (L0, L1 y L2).

Figura 10. Nivel de madurez de los controles



Fuente: El Autor

Para una mejor comprensión, en la siguiente **Tabla 21.** se muestra, a modo de resumen el nivel de madurez de los controles alcanzados una vez finalizados los proyectos presentados en Fase IV

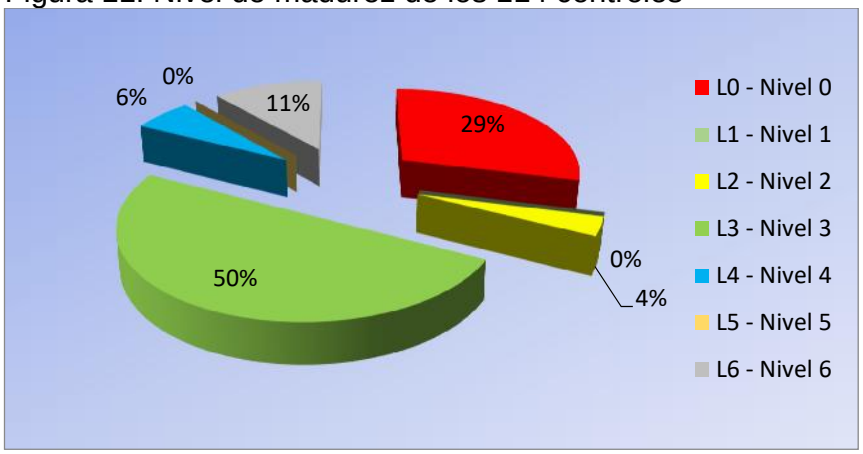
Tabla 21. Nivel de madurez de los controles

Valor	Efectividad	Significado	Descripción	Número
L0	0%	Inexistente	Carencia completa de cualquier proceso conocido.	33
L1	10%	Inicial / Ad-hoc	Procedimientos inexistentes o localizados en áreas concretas. El éxito de las tareas se debe a esfuerzos personales.	0
L2	50%	Reproducible, pero intuitivo	Existe un método de trabajo basado en la experiencia, aunque sin comunicación formal. Dependencia del conocimiento individual	4
L3	90%	Proceso definido	La organización en su conjunto participa en el proceso. Los procesos están implantados, documentados y comunicados.	57
L4	95%	Gestionado y medible	Se puede seguir la evolución de los procesos mediante indicadores numéricos y estadísticos. Hay herramientas para mejorar la calidad y la eficiencia	7
L5	100%	Optimizado	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos	0
L6	N/A	No aplica		13

Fuente: El Autor

Se puede apreciar en la **Figura 11.** el Nivel de madurez de los 114 controles, el porcentaje de controles que alcanzan cada uno de los niveles considerados en CMM. Se observa en la gráfica

Figura 11. Nivel de madurez de los 114 controles



Fuente: El Autor

Atendiendo al Modelo de Madurez de la Capacidad (COM) se extraen las siguientes conclusiones:

En la **Tabla 22**. Se enlista el resumen del nivel de madurez de los controles

- Se ha detectado un total de 37 no conformidades menores
- Se ha detectado un total de 64 aprobados
- Como se observa el 80% de los controles se encuentran en valores iguales o superiores al 90%, es decir que sus procesos asociados están definidos e implementados.
- Un 50% de los procesos / controles son reproducibles ya que diferentes personas con la misma tarea han sido capaces de reproducirlos.

Tabla 22. Resumen nivel de madurez de los controles

Valor	**Número**
Aprobados	64
No Aprobados	37
No Aplican	13

Fuente: El Autor

Ver Anexos F5
ANEXO N. FASE 5 - NIVEL DE MADUREZ DE LOS CONTROLES - CMM_ISO_27002_2013

11.6 FICHAS DE NO CONFORMIDADES (NC).

cómo se puede ver la **Tabla 23.** Se en lista una ficha comparativa de las No Conformidades con relación a la Fase 1 y la Fase 5, en esta se encuentran todas las fichas de las no conformidades (NC) detectadas a lo largo de la auditoria. A continuación, se muestran los resultados resumidos de estas fichas.

Tabla 23. Tabla de no conformidades - auditoria de cumplimiento

CONTROL	TITULO	VALOR FASE 1	VALOR FASE 5
A.5	**POLÍTICAS DE SEGURIDAD**	5%	90%
A.5.1	**Directrices de la Dirección en seguridad de la información**	5%	90%
A.5.1.1	Conjunto de políticas para la seguridad de la información	10% (L1)	90% (L3)
A.5.1.2	Revisión de las políticas para la seguridad de la información	0% (L0)	90% (L3)
A.6	**ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INF.**	0%	20%
A.6.1	**Organización interna**	0	40%
A.6.1.1	Asignación de responsabilidades para la segur. de la información.	0% (L0)	90% (L3)
A.6.1.2	Segregación de tareas.	0% (L0)	90% (L3)
A.6.1.3	Contacto con las autoridades	0% (L0)	0% (L0)
A.6.1.4	Contacto con grupos de interés especial	0% (L0)	0% (L0)
A.6.1.5	Seguridad de la información en la gestión de proyectos	0% (L0)	0% (L0)
A.6.2	**Dispositivos para movilidad y teletrabajo.**	0	0
A.6.2.1	Política de uso de dispositivos para movilidad.	0% (L0)	0% (L0)
A.6.2.2	Teletrabajo.	No aplica(L6)	No aplica(L6)
A.7	**SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.**	2.78%	90%
A.7.1	**Organización interna**	10%	90%
A.7.1.1	Investigación de antecedentes.	10% (L1)	90% (L3)
A.7.1.2	Términos y condiciones de contratación.	0% (L0)	90% (L3)
A.7.2	**Durante la contratación.**	3.3%	90%
A.7.2.1	Responsabilidades de gestión.	10%(L1)	90% (L3)
A.7.2.2	Concienciación, educación y capacitación en seguridad de la información	0%(L0)	90% (L3)
A.7.2.3	Proceso disciplinario.	0%(L0)	90% (L3)

Tabla 23 (Continuación)

CONTROL	TITULO	VALOR FASE 1	VALOR FASE 5
A.7.3	**Cese o cambio de puesto de trabajo.**	0%	90%
A.7.3.1	Cese o cambio de puesto de trabajo.	0%(L0)	90% (L3)
A.8	**GESTIÓN DE ACTIVOS.**	0	60%
A.8.1	**Responsabilidad sobre los activos.**	0	50%
A.8.1.1	Inventario de activos.	0% (L0)	95% (L4)
A.8.1.2	Propiedad de los activos.	0% (L0)	0% (L0)
A.8.1.3	Uso aceptable de los activos.	0% (L0)	0% (L0)
A.8.1.4	Devolución de activos.	0% (L0)	90% (L3)
A.8.2	**Clasificación de la información.**	0	90%
A.8.2.1	Directrices de clasificación.	0% (L0)	90% (L3)
A.8.2.2	Etiquetado y manipulado de la información.	0% (L0)	90% (L3)
A.8.2.3	Manipulación de activos.	0% (L0)	90% (L3)
A.8.3	**Manejo de los soportes de almacenamiento.**	0	50%
A.8.3.1	Gestión de soportes extraíbles.	0% (L0)	0% (L0)
A.8.3.2	Eliminación de soportes.	0% (L0)	90% (L3)
A.8.3.3	Soportes físicos en tránsito	No aplica(L6)	No aplica(L6)
A.9	**CONTROL DE ACCESOS.**	3%	63.75%
A.9.1	Requisitos de negocio para el control de accesos.	5%	90%
A.9.1.1	Política de control de accesos.	0% (L0)	90% (L3)
A.9.1.2	Control de acceso a las redes y servicios asociados.	10% (L1)	90% (L3)
A.9.2	**Gestión de acceso de usuario.**	5%	75%
A.9.2.1	Gestión de altas/bajas en el registro de usuarios.	0% (L0)	90% (L3)
A.9.2.2	Gestión de los derechos de acceso asignados a usuarios.	10% (L1)	90% (L3)
A.9.2.3	Gestión de los derechos de acceso con privilegios especiales.	10% (L1)	90% (L3)
A.9.2.4	Gestión de información confidencial de autenticación de usuarios.	0% (L0)	0% (L0)
A.9.2.5	Revisión de los derechos de acceso de los usuarios.	0% (L0)	90% (L3)
A.9.2.6	Retirada o adaptación de los derechos de acceso	10% (L1)	90% (L3)
A.9.3	**Responsabilidades del usuario.**	0%	0%
A.9.3.1	Uso de información confidencial para la autenticación.	0% (L0)	0% (L0)
A.9.4	**Control de acceso a sistemas y aplicaciones.**	2%	90%
A.9.4.1	Restricción del acceso a la información.	0% (L0)	90% (L3)
A.9.4.2	Procedimientos seguros de inicio de sesión.	0% (L0)	90% (L3)
A.9.4.3	Gestión de contraseñas de usuario.	0% (L0)	90% (L3)
A.9.4.4	Uso de herramientas de administración de sistemas.	10% (L1)	90% (L3)
A.9.4.5	Control de acceso al código fuente de los programas.	0% (L0)	90% (L3)
A.10	CIFRADO.	0%	0%
A.10.1	Controles criptográficos.	0%	0%
A.10.1.1	Política de uso de los controles criptográficos.	No aplica(L6)	No aplica(L6)
A.10.1.2	Gestión de claves.	No aplica(L6)	No aplica(L6)

Tabla 23. (Continuación)

CONTROL	TITULO	VALOR FASE 1	VALOR FASE 5
A.11	**SEGURIDAD FÍSICA Y AMBIENTAL.**	1.4%	70.6%
A.11.1	**Áreas seguras.**	0%	68%
A.11.1.1	Perímetro de seguridad física.	0% (L0)	90% (L3)
A.11.1.2	Controles físicos de entrada.	0% (L0)	90% (L3)
A.11.1.3	Seguridad de oficinas, despachos y recursos.	0% (L0)	0% (L0)
A.11.1.4	Protección contra las amenazas externas y ambientales.	0% (L0)	90% (L3)
A.11.1.5	El trabajo en áreas seguras.	No aplica(L6)	No aplica(L6)
A.11.2	**Seguridad de los equipos.**	2.8%	73.75%
A.11.2.1	Emplazamiento y protección de equipos.	0% (L0)	90% (L3)
A.11.2.2	Instalaciones de suministro.	10% (L1)	90% (L3)
A.11.2.3	Seguridad del cableado.	No aplica(L6)	50% (L2)
A.11.2.4	Mantenimiento de los equipos.	10% (L1)	90% (L3)
A.11.2.5	Salida de activos fuera de las dependencias de la empresa.	0% (L0)	0% (L0)
A.11.2.6	Seguridad de los equipos y activos fuera de las instalaciones.	No aplica(L6)	No aplica(L6)
A.11.2.7	Reutilización o retirada segura de dispositivos de almacenamiento.	0% (L0)	90% (L3)
A.11.2.8	Equipo informático de usuario desatendido.	0% (L0)	90% (L3)
A.12.5	**Control del *Software* en explotación.**	0%	90%
A.12.5.1	Instalación del *Software* en sistemas en producción.	0% (L0)	90% (L3)
A.12.6	**Gestión de la vulnerabilidad técnica.**	5%	90%
A.12.6.1	Gestión de las vulnerabilidades técnicas.	0% (L0)	90% (L3)
A.12.6.2	Restricciones en la instalación de *Software*.	10% (L1)	90% (L3)
A.12.7	**Consideraciones de las auditorías de los sistemas de información.**	0%	0%
A.12.7.1	Controles de auditoría de los sistemas de información.	0% (L0)	0% (L0)
A.13	**SEGURIDAD EN LAS TELECOMUNICACIONES.**	0%	12.5%
A.13.1	**Gestión de la seguridad en las redes.**	0%	25%
A.13.1.1	Controles de red.	0% (L0)	50% (L2)
A.13.1.2	Mecanismos de seguridad asociados a servicios en red.	0% (L0)	0% (L0)
A.13.1.3	Segregación de redes.	No aplica(L6)	No aplica(L6)
A.13.2	**Intercambio de información con partes externas.**	0%	0%
A.13.2.1	Políticas y procedimientos de intercambio de información.	0% (L0)	0% (L0)
A.13.2.2	Acuerdos de intercambio.	No aplica(L6)	0%
A.13.2.3	Mensajería electrónica.	0% (L0)	0% (L0)
A.13.2.4	Acuerdos de confidencialidad y secreto.	0% (L0)	0% (L0)

Tabla 23. (Continuación)

CONTROL	TITULO	VALOR FASE 1	VALOR FASE 5
A.14	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.**	0%	30%
A.14.1	**Requisitos de seguridad de los sistemas de información.**	0%	90%
A.14.1.1	Análisis y especificación de los requisitos de seguridad.	0% (L0)	90% (L3)
A.14.1.2	Seguridad de las comunicaciones en servicios accesibles por redes públicas.	No aplica(L6)	No aplica(L6)
A.14.1.3	Protección de las transacciones por redes telemáticas.	0% (L0)	90% (L3)
A.14.2	**Seguridad en los procesos de desarrollo y soporte.**	0%	0%
A.14.2.1	Política de desarrollo seguro de *Software*.	0% (L0)	0% (L0)
A.14.2.2	Procedimientos de control de cambios en los sistemas.	0% (L0)	0% (L0)
A.14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	0% (L0)	0% (L0)
A.14.2.4	Restricciones a los cambios en los paquetes de *Software*.	0% (L0)	0% (L0)
A.14.2.5	Uso de principios de ingeniería en protección de sistemas.	0% (L0)	0% (L0)
A.14.2.6	Seguridad en entornos de desarrollo.	0% (L0)	0% (L0)
A.14.2.7	Externalización del desarrollo de *Software*.	No aplica(L6)	No aplica(L6)
A.14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas.	0% (L0)	0% (L0)
A.14.2.9	Pruebas de aceptación.	0% (L0)	0% (L0)
A.14.3	**Datos de prueba.**	0%	0%
A.14.3.1	Protección de los datos utilizados en pruebas.	0% (L0)	0% (L0)
A.15	**RELACIONES CON SUMINISTRADORES.**	0%	61.67%
A.15.1	**Seguridad de la información en las relaciones con suministradores.**	0%	33%
A.15.1.1	Política de seguridad de la información para suministradores.	0% (L0)	50% (L2)
A.15.1.2	Tratamiento del riesgo dentro de acuerdos de suministradores.	0% (L0)	50% (L2)
A.15.1.3	Cadena de suministro en tecnologías de la información y comunicaciones.	0% (L0)	0% (L0)
A.15.2	**Gestión de la prestación del servicio por suministradores.**	0%	90%
A.15.2.1	Supervisión y revisión de los servicios prestados por terceros.	0% (L0)	90% (L3)
A.15.2.2	Gestión de cambios en los servicios prestados por terceros.	0% (L0)	90% (L3)
A.16	**GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.**	0%	93%
A.16.1	**Gestión de incidentes de seguridad de la información y mejoras.**	0%	93%
A.16.1.1	Responsabilidades y procedimientos.	0% (L0)	90% (L3)
A.16.1.2	Notificación de los eventos de seguridad de la información.	0% (L0)	95% (L4)
A.16.1.3	Notificación de puntos débiles de la seguridad	0% (L0)	95% (L4)
A.16.1.4	Valoración de eventos de seguridad de la información y toma de decisiones.	0% (L0)	95% (L4)
A.16.1.5	Respuesta a los incidentes de seguridad.	0% (L0)	95% (L4)

Tabla 23. (Continuación)

CONTROL	TITULO	VALOR FASE 1	VALOR FASE 5
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información.	0% (L0)	95% (L4)
A.16.1.7	Recopilación de evidencias.	0% (L0)	95% (L4)
A.17	**ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**	3.33%	45%
A.17.1	**Continuidad de la seguridad de la información.**	7%	90%
A.17.1.1	Planificación de la continuidad de la seguridad de la información.	10% (L1)	90% (L3)
A.17.1.2	Implementación de la continuidad de la seguridad de la información.	10% (L1)	90% (L3)
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la Seguridad de la información.	0% (L0)	90% (L3)
A.17.2	**Redundancias.**	0%	0%
A.17.2.1	Disponibilidad de instalaciones para el procesamiento de la información.	0% (L0)	0% (L0)
A.18	**CUMPLIMIENTO.**	1.67%	75%
A.18.1	**Cumplimiento de los requisitos legales y contractuales.**	3%	90%
A.18.1.1	Identificación de la legislación aplicable.	10% (L1)	90% (L3)
A.18.1.2	Derechos de propiedad intelectual (DPI).	No aplica(L6)	No aplica(L6)
A.18.1.3	Protección de los registros de la organización.	0% (L0)	90% (L3)
A.18.1.4	Protección de datos y privacidad de la información personal.	0% (L0)	90% (L3)
A.18.1.5	Regulación de los controles criptográficos.	No aplica(L6)	No aplica(L6)
A.18.2	**Revisiones de la seguridad de la información.**	0%	60%
A.18.2.1	Revisión independiente de la seguridad de la información.	0% (L0)	0% (L0)
A.18.2.2	Comprobación del cumplimiento	0% (L0)	90% (L3)
A.18.2.3	Disponibilidad de instalaciones para el procesamiento de la información.	0% (L0)	90% (L3)

Fuente: Investigación

CONCLUSIONES.

En la actualidad el tema de seguridad de la información toma cada vez mayor importancia al interior de las organizaciones, y es creciente el número de organizaciones que necesitan asegurar sus sistemas, bien sea porque quieran certificarse para garantizar que sus sistemas sean seguros o porque de alguna forma han sufrido ataques y pretenden desarrollar una estrategia de seguridad basándose en las mejores prácticas de aseguramiento de la información expuestas en las normas internacionales.

El desarrollo e implementación del Sistema de Gestión de Seguridad de la Información (SGSI) para la Unidad Administrativa Parques Nacionales Naturales de Colombia, según la norma ISO 27001:2013, reduce los riesgos, amenazas y vulnerabilidades que pueden afectar a los activos del área, es una necesidad para todas las empresas que se preocupan por la gestión de la seguridad de la información o los riesgos relacionados con la TI.

En primer lugar, se localizaron los puntos más vulnerables dentro de la entidad, se Identificaron y analizaron las amenazas y los riesgos de que ocurran éstas, Se seleccionaron los controles de la norma ISO 27002 para la reducción de riesgos y amenazas en el área, se Identificaron los activos informáticos que son objeto de protección por el SGSI.

Las principales amenazas identificadas gracias a la ejecución del proyecto en la entidad fueron en su orden: Desastres naturales, desastres de origen industrial, ataques intencionados y errores o fallos no intencionados; de estas, son especialmente criticas aquellas que se relacionan con el accionar del usuario tanto de manera intencional como no intencional, es por esto por lo que se planteó la definición de proyectos específicos que se enfoquen en proteger y reducir el riesgo hacia los activos de tipo software y datos de la organización los cuales fueron catalogados como críticos.

Luego de comprender los procesos críticos de organización, se desarrolló el sistema de gestión documental y luego se elaboró su análisis de riesgo.

Gracias a la metodología empleada, se elabora una guía básica con políticas y procedimientos, en base a las normas internacionales y por último se diseña un SGSI acorde a las necesidades de la entidad

Gracias a esto y a una correcta aplicación de lo aquí expuesto, se cumple con el objetivo de mejorar el diagnóstico inicial del sistema de seguridad de la información, se definieron un conjunto de nuevos proyectos. y posterior a esto, se ha auditado el SGSI, verificando ISO / IEC27001: 2013 con resultados positivos para la entidad.

RECOMENDACIONES.

No perder la conexión alta gerencia y promotores SGSI

Aplicar los lineamientos estipulados en las políticas de seguridad informática, retroalimentaciones constantes y afinación de este si es necesario.

Referente a la madures de los controles, Cabe destacar que los dominios A6, A13 y A14 son los dominios donde se han detectado contrariedades mayores, que requieren un mayor trabajo para ser resueltos. Estos dominios recibirán proyectos específicos con mayor inversión, pues se trata de dominios que no han sido tenidos en cuenta dentro de la entidad desde hace mucho tiempo y se encuentran en niveles realmente bajos de cumplimiento (<=30%).

Realizar auditorías de forma constantes con auditores internos, posteriormente con auditores externos.

A partir del ciclo PDCA (Plan, Do, Check, Act-), en lo posible promover la mejora continua de los procesos, actualizando procesos y herramientas de acuerdo con las necesidades de la entidad. Este ciclo aplicarlo cuantas veces sea necesario con el fin de entender los problemas que surjan, cómo deben ser solucionados, sus causas raíz y consecuencias. Promover los cambios necesarios para alcanzar los resultados con más eficiencia.

Definir acuerdos de administración de las plataformas en conjunto con la Gerencias de control accesos, Telecomunicaciones y Seguridad de TI, donde realmente exista una adecuada segregación de funciones para los accesos a las aplicaciones servidores y equipos activos.

Capacitar a los empleados de acuerdo con su rol sobre cada una de las políticas de seguridad definidas.

BIBLIOGRAFÍA.

AGUSTÍN, N.; RUIZ, J. (1 de octubre del 2005). El portal de iso 27001 en español. Recuperado el 31 de marzo del 2012, de <http://iso27000.es/>

BLOG ESPECIALIZADO EN SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN. evaluación de los riesgos e implementación de las medidas de protección [en línea]. Disponible en: <http://www.pmg-ssi.com/2015/04/iso-27001-evaluacion-riesgos-implementacion- medidas-proteccion/>

ICONTEC. norma técnica NTC-ISO/IEC colombiana 27001. [en línea]. Disponible en: <http://www.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/nor

INCIBE. Conceptos básicos sobre seguridad de la información. Incibe [en línea]. Disponible en: <https://www.incibe.es/extfrontinteco/img/file/intecocert/sgsi/index.html>

Implantación de un SGSI en la entidad incibe [en línea]. Disponible en: <https://www.incibe.es/extfrontinteco/img/file/intecocert/sgsi/img/guia_apoyo_sgsi.pdf>

La seguridad y su justificación desde el punto de vista del negocio. Plan director [en línea]. Disponible en: <https://www.incibe.es/entidads/que_te_interesa/plan_director_de_seguridad/>

INTECO. Curso de sistemas de gestión de la seguridad de la información según la norma une iso iec 27001 [en línea]. Disponible en: <https://formacion-online.inteco.es/curso/index.php>

Sistema de gestión de seguridad de la información en una organización [en línea]. Disponible en: <http://cert.inteco.es/extfrontinteco/img/file/intecocert/sgsi/> ma.%20ntc-iso-iec%2027001.pdf> [citado en 10 de octubre de 2015]

PORTAL DE ISO 27001 EN ESPAÑOL. El anexo de iso 27001 en español [en línea]. Disponible en: <http://iso27002.wiki.zoho.com/>

Programa avanzado de estudio: seguridad en sistemas de información versión junio 2010 is&bca, sobre la iso 27001 [en línea]. Disponible en: kkmk<http://www.iso27001standard.com/es/iso-27001/blog>

PORTAL EDITORIAL BORRMART. Implementación de un sistema de gestión de seguridad de la información [en línea]. Disponible en: http://www.borrmart.es/eventos/pjisgsi.pdf

PORTAL SENA. Estándares para la seguridad de la información [en línea]. Disponible en: <https://senaintro.blackboard.com/bbcswebdav/1/oa_estandarseguridad/oc.pdf>

PORTAL UNIVERSIDAD TECNOLÓGICA DE LA HUASTECA HIDALGUENSE. Filosofía de la entidad [en línea]. Disponible en: <http://www.uthh.edu.mx/?op=tm90awnpyxnfdxq9na==>

SEGU-INFO . Políticas de seguridad de la información [en línea]. Disponible en: <http://www.segu-info.com.ar/politicas/polseginf.htm>

Certificación ISO-27001 [en línea]. Disponible en: <http://www.segu-info.com.ar/foro/?q=certificacion>

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. Gerencia de innovación y desarrollo tecnológico [en línea]. Disponible en: <http://datateca.unad.edu.co/contenidos/233004/47797859-iso-27002-espanol.pdf>

UNIVERSITAT OBERTA DE CATALUNYA [en línea]. Disponible en: <http://openaccess.uoc.edu/webapps/o2/bitstream/10609/>

ANEXOS.

ANEXOS AL DOCUMENTO PRINCIPAL

ANEXO A. FASE 1 - CMM-ISO27001-2013 INICIAL

Evaluación de Madurez respecto a los requerimientos definidos en la ISO 27001:2013

Dominio	% de conformidad	# NC mayores	# NC menores	# NC OK
4 Contexto de la organización	5%	5	0	0
5 Liderazgo	1%	14	0	0
6 Planificación	0%	31	0	0
7 Soporte	0%	26	0	0
8 Funcionamiento	0%	3	0	0
9 Evaluación de Rendimiento	0%	23	0	0
10 Proceso de mejora	0%	11	0	0

Valor	Número
Aprobados	0
No Aprobados	113
No Aplican	0

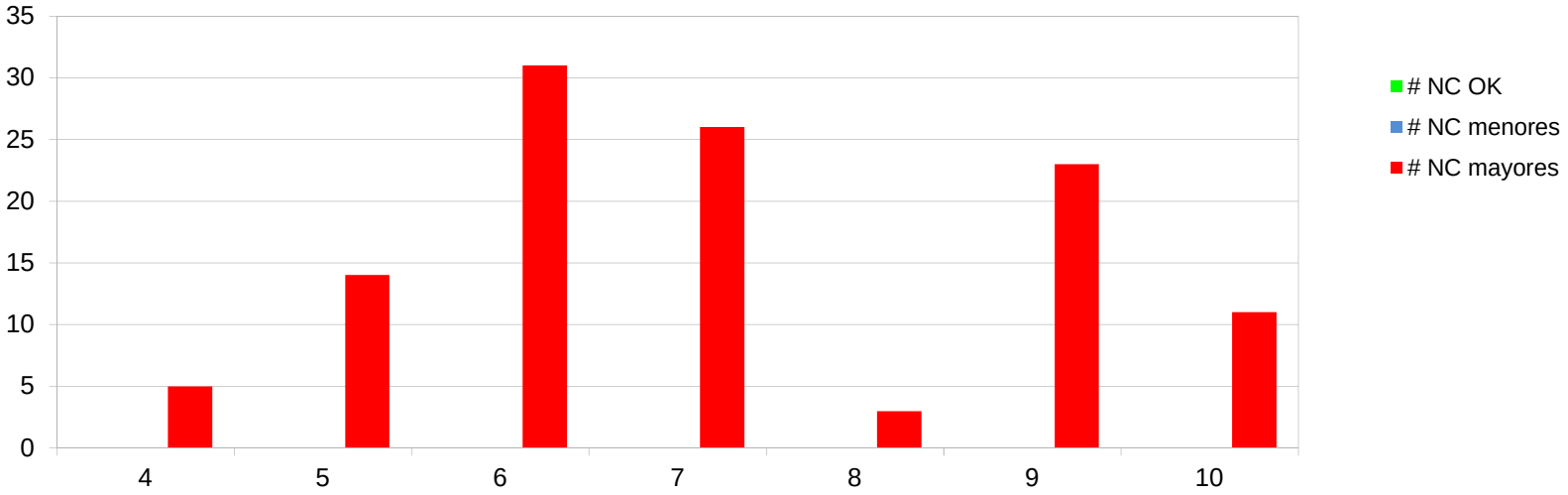

35
30
25
20
15
10
5
0
4
5
6
7
8
9
10
NC OK
NC menores
NC mayores

Tabla de Valores

Valor	Efectividad	Significado	Descripción	Número
L0	0%	Inexistente	Carencia completa de cualquier proceso conocido.	111
L1	10%	Inicial / Ad-hoc	Procedimientos inexistentes o localizados en áreas concretas. El éxito de las tareas se debe a esfuerzos personales.	2
L2	50%	Reproducible, pero intuitivo	Existe un método de trabajo basado en la experiencia, aunque sin comunicación formal. Dependencia del conocimiento individual	0
L3	90%	Proceso definido	La organización en su conjunto participa en el proceso. Los procesos están implantados, documentados y comunicados.	0
L4	95%	Gestionado y medible	Se puede seguir la evolución de los procesos mediante indicadores numéricos y estadísticos. Hay herramientas para mejorar la calidad y la eficiencia	0
L5	100%	Optimizado	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos	0
L6	N/A	No aplica		0

Control de ISO /IEC 27001:2013	Requerimientos	Valoración	Observaciones				
4	**Contexto de la organización**			0,05		**L0**	4
4,1	**Comprender la organización y su contexto**			**0,05**		**L1**	1
4,2	Comprender las necesidades y expectativas de las partes interesadas	L1		0,1		**L2**	0
4.2 (a)	las partes interesadas que son relevantes para el sistema de gestión de seguridad de la información	L0		0		**L3**	0
4.2 (b)	los requisitos de estas partes interesadas pertinentes a la seguridad de la información.	L0				**L4**	0
4,3	Determinación del alcance del sistema de gestión de seguridad de la información	L0				**L5**	0
4,4	Información de sistema de gestión de la seguridad	L0				**L6**	0
						NC Mayores	5
						NC Menores	0
						Observaciones	0

Control de ISO /IEC 27001:2013	Requerimientos	Valoración	Observaciones				
5	**Liderazgo**			0,005263158		**L0**	13
5,1	**Liderazgo y compromiso**			**0,00526316**		**L1**	1
5.1 (a)	garantizar la política de seguridad de la información y de los objetivos de seguridad de la información se establecen y son compatibles con la dirección estratégica de la organización;	L0		0		**L2**	0
5.1 (b)	garantizar la integración de los requisitos del sistema de gestión de seguridad de la información en	L0		0		**L3**	0
5.1 (c)	velar por que los recursos necesarios para el sistema de gestión de seguridad de la información est	L1		0,1		**L4**	0
5.1 (d)	comunicar la importancia de una gestión eficaz de seguridad de la información y de ajustarse a los	L0		0		**L5**	0
5.1 (e)	garantizar que el sistema de gestión de seguridad de la información alcanza su resultado previsto	L0		0		**L6**	0
5.1 (f)	la dirección y el apoyo a las personas a contribuir a la eficacia de la seguridad de la información sis	L0		0			
5.1 (g)	la promoción de la mejora continua;	L0		0			
5.1 (h)	el apoyo a otras funciones de gestión pertinentes para demostrar su liderazgo, ya que se aplica a s	L0		0		**NC Mayores**	14
5,2	La alta dirección debe establecer una política de seguridad de la información que:	L0		0		**NC Menores**	0
5.2 (a)	es apropiada para el propósito de la organización;	L0		0		**Observaciones**	0
5.2 (b)	incluye los objetivos de seguridad de la información (véase 6.2) o proporciona el marco para estable	L0		0			
5.2 (c)	incluye un compromiso de cumplir con los requisitos aplicables relacionados con la seguridad de la	L0		0			
5.2 (d)	incluye un compromiso de mejora continua del sistema de gestión de seguridad de la información	L0		0			
5.2 (e)	La política de seguridad de la información deberá estará disponible como información documentada.	L0		0			
5.2 (f)	La política de seguridad de la información deberá ser comunicada dentro de la organización;	L0		0			
5.2 (g)	La política de seguridad de la información deberá estar disponible para las partes interesadas, segú	L0		0			
5,3	Funciones de organización, responsabilidades y autoridades	L0		0			
5.3 (a)	garantizar que el sistema de gestión de seguridad de la información se ajusta a los requisitos de la	L0		0			
5.3 (b)	informar sobre el desempeño del sistema de gestión de seguridad de la información a la alta direcci	L0		0			

Control de ISO /IEC 27001:2013	Requerimientos	Valoración	Observaciones				
6	**Planificación**			0		**L0**	31
6,1	**Acciones para hacer frente a los riesgos y oportunidades**			**0**		**L1**	0
6.1.1	Generalidades					**L2**	0
6.1.1(a)	garantizar que el sistema de gestión de seguridad de la información puede alcanzar su resultado pr	L0		0		**L3**	0
6.1.1 (b)	prevenir o reducir los efectos no deseados; y	L0		0		**L4**	0
6.1.1 (c)	lograr la mejora continua.	L0		0		**L5**	0
6.1.1 (d)	La organización debe planificar las acciones para hacer frente a estos riesgos y oportunidades	L0		0		**L6**	0
6.1.1 (e1)	La organización debe planificar como integrar y poner en práctica las acciones en su sistema de ge	L0		0			
6.1.1 (e2)	La organización debe planificar como evaluar la eficacia de estas acciones.	L0		0			
6.1.2	Evaluación de riesgos de seguridad					**NC Mayores**	31
6.1.2 (a1)	establece y mantiene los criterios de riesgo de seguridad de información que incluyen los criterios d	L0		0		**NC Menores**	0
6.1.2 (a2)	establece y mantiene los criterios de riesgo de seguridad de información que incluyen los criterios p	L0		0		**Observaciones**	0
6.1.2 (b)	se asegura de que las evaluaciones de riesgos de seguridad de información repetidos producen con	L0		0			
6.1.2 (c1)	aplicar el proceso de evaluación de riesgos de seguridad de información para identificar los riesgos	L0		0			
6.1.2 (c2)	identificar a los propietarios de riesgo	L0		0			
6.1.2 (d1)	evaluar las posibles consecuencias que se derivarían si los riesgos identificados en 6.1.2 (c1) fueron	L0		0			
6.1.2 (d2)	evaluar la probabilidad realista de la ocurrencia de los riesgos identificados en 6.1.2 (c1)	L0		0			
6.1.2 (d3)	determinar los niveles de riesgo;	L0		0			
6.1.2 (e1)	comparar los resultados de análisis de riesgos con los criterios de riesgo establecidos en 6.1.2 a);	L0		0			
6.1.2 (e2)	dar prioridad a los riesgos analizados para el tratamiento del riesgo.	L0		0			
6.1.3	Información de tratamiento de riesgos de seguridad						
6.1.3 (a)	seleccionar las opciones de tratamiento de riesgos de seguridad de información adecuados y tenier	L0		0			
6.1.3 (b)	determinar todos los controles que sean necesarios para implementar el tratamiento de los riesgos	L0		0			
6.1.3 (c)	comparar los controles determinados en 6.1.3 b) anterior con los del Anexo A y comprobar que no e	L0		0			
6.1.3 (d)	producir una Declaración de aplicabilidad que contiene los controles necesarios (véase 6.1.3 b) yc))	L0		0			
6.1.3 (e)	formular un plan de información sobre el tratamiento de riesgos de seguridad; y	L0		0			
6.1.3 (f)	obtener la aprobación del plan de tratamiento de riesgos de seguridad de la información y la aceptac	L0		0			
6,2	Objetivos de seguridad de la Información y la planificación para alcanzarlos						
6.2 (a)	ser coherente con la política de seguridad de la información;	L0		0			
6.2 (b)	ser medibles (si es posible);	L0		0			
6.2 (c)	tener en cuenta los requisitos de seguridad de la información es aplicable, y los resultados de la ev	L0		0			
6.2 (d)	ser comunicada; y	L0		0			
6.2 (e)	se actualizará según corresponda.	L0		0			
6.2 (f)	lo que será hecho	L0		0			
6.2 (g)	qué recursos serán necesarios;	L0		0			
6.2 (h)	que será responsable;	L0		0			
6.2 (i)	cuando se completará; y	L0		0			
6.2 (j)	cómo se evaluarán los resultados.						

Control de ISO /IEC 27001:2013	Requerimientos	Valoración	Observaciones				
7	Soporte			0		L0	26
7,1	Recursos			0		L1	0
7,2	Competencia					L2	0
7.2 (a)	determinar la competencia necesaria de la persona (s) que hace el trabajo bajo su control que afect	L0		0		L3	0
7.2 (b)	asegurarse de que estas personas son competentes sobre la base de una educación adecuada, ca	L0				L4	0
7.2 (c)	en su caso, tomar acciones para adquirir la competencia necesaria, y evaluar la eficacia de las acc	L0				L5	0
7.2 (d)	retener la información documentada apropiada como evidencia de la competencia.	L0				L6	0
7,3	Conciencia						
7.3 (a)	la política de seguridad de la información;	L0					
7.3 (b)	su contribución a la eficacia del sistema de gestión de seguridad de la información, incluyendo los b	L0				NC Mayores	26
7.3 (c)	las consecuencias de que no se ajusten a los requisitos del sistema de gestión de seguridad de la	L0				NC Menores	0
7,4	Comunicación					Observaciones	0
7.4 (a)	en el qué comunicar;	L0					
7.4 (b)	cuando para comunicarse;	L0					
7.4 (c)	con quien comunicarse;	L0					
7.4 (d)	quien comunicará;	L0					
7.4 (e)	Los procesos mediante los cuales se efectúa la comunicación.	L0					
7,5	Información documentada						
7.5.1	General	L0					
7.5.1 (a)	La información requerida por esta Norma Internacional documentado; y	L0					
7.5.1 (b)	información documentada determinada por la organización como necesaria para la efectividad del si	L0					
7.5.2	Creación y actualización	L0					
7.5.2 (a)	identificación y descripción (por ejemplo, un título, fecha, autor, o el número de referencia);	L0					
7.5.2 (b)	formato (por ejemplo, el idioma, la versión de software, gráficos) y medios de comunicación (por eje	L0					
7.5.2 (c)	La revisión y aprobación de idoneidad y adecuación.	L0					
7.5.3	Control de la información documentada	L0					
7.5.3 (a)	asegurar está disponible y adecuado para su uso, donde y cuando sea necesario; y	L0					
7.5.3 (b)	asegurar que está protegido de manera adecuada (por ejemplo, de la pérdida de confidencialidad, u	L0					
7.5.3 (c)	asegurar la distribución, acceso, recuperación y uso	L0					
7.5.3 (d)	asegurar almacenamiento y conservación, incluyendo la preservación de la legibilidad	L0					
7.5.3 (e)	asegurar el control de cambios (por ejemplo, control de versiones);	L0					
7.5.3 (f)	asegurar la retención y disposición.	L0					

Control de ISO /IEC 27001:2013	Requerimientos	Valoración	Observaciones				
8	Funcionamiento			0		L0	3
8,1	Planificación y control operacional			0		L1	0
8,2	Evaluación del riesgo de seguridad	L0		0		L2	0
8,3	Información de tratamiento de riesgos de seguridad	L0		0		L3	0
		L0				L4	0
						L5	0
						L6	0
						NC Mayores	3
						NC Menores	0
						Observaciones	0

Control de ISO /IEC 27001:2013	Requerimientos	Valoración	Observaciones				
9	Evaluación de Rendimiento			0		L0	23
9,1	Monitoreo, medición, análisis y evaluación			0		L1	0
9.1 (a)	lo que necesita ser monitoreado y medido, incluidos los procesos y controles de seguridad de la inf	L0		0		L2	0
9.1 (b)	Determinar los métodos de vigilancia, medición, análisis y evaluación, en su caso, para garantizar r	L0		0		L3	0
9.1 (c)	Determinar cuando se llevarán a cabo el seguimiento y medición	L0				L4	0
9.1 (d)	Determinar que hará un seguimiento y medir	L0				L5	0
9.1 (e)	Determinar cuando se analizan y evalúan los resultados del seguimiento y medición	L0				L6	0
9.1 (f)	Determinar que deberá analizar y evaluar los resultados	L0					
9,2	La auditoría interna						
9.2 (a1)	cumple requisitos propios de la organización de su sistema de gestión de seguridad de la informaci	L0				NC Mayores	23
9.2 (a2)	Cumple los requisitos de esta norma internacional;	L0				NC Menores	0
9.2 (b)	se ha implementado y se mantiene de manera eficaz.	L0				Observaciones	0
9.2 (c)	planificar, establecer, implementar y mantener un programa (s) de auditoría, incluyendo la frecuenci	L0					
9.2 (d)	definir los criterios de auditoría y el alcance de cada auditoría;	L0					
9.2 (e)	seleccionar auditores y realizar auditorías que garanticen la objetividad y la imparcialidad del proces	L0					
9.2 (f)	asegurarse de que los resultados de las auditorías se reportan a la gestión pertinente; y	L0					
9.2 (g)	conservar la información documentada como prueba del programa (s) de auditoría y los resultados d	L0					
9,3	Revisión de la Gestión						
9.3 (a)	el estado de las acciones de las revisiones por la dirección previas;	L0					
9.3 (b)	los cambios en los problemas externos e internos que son relevantes para la gestión de seguridad d	L0					
9.3 (c1)	la retroalimentación sobre el desempeño de seguridad de la información, incluyendo las tendencias	L0					
9.3 (c2)	la retroalimentación sobre el desempeño de seguridad de la información, incluyendo las tendencias	L0					
9.3 (c3)	la retroalimentación sobre el desempeño de seguridad de la información, incluyendo las tendencias	L0					
9.3 (c4)	la retroalimentación sobre el desempeño de seguridad de la información, incluyendo las tendencias	L0					
9.3 (d)	la retroalimentación de las partes interesadas;	L0					
9.3 (e)	los resultados de la evaluación del riesgo y el estado del plan de tratamiento de riesgos; y	L0					
9.3 (f)	oportunidades de mejora continua.	L0					

Control de ISO /IEC 27001:2013	Requerimientos	Valoración	Observaciones				
10	**Proceso de mejora**			0		**L0**	11
10,1	No conformidad y acciones correctivas			**0**		**L1**	0
10.1 (a1)	reaccionan a la no conformidad, y según sea el caso tomar medidas para controlar y corregirlo	L0		0		**L2**	0
10.1 (a2)	reaccionan a la no conformidad, y según sea el caso hacer frente a las consecuencias;	L0		0		**L3**	0
10.1 (b1)	evaluar la necesidad de adoptar medidas para eliminar las causas de no conformidad, con el fin de	L0				**L4**	0
10.1 (b2)	evaluar la necesidad de adoptar medidas para eliminar las causas de no conformidad, con el fin de	L0				**L5**	0
10.1 (b3)	evaluar la necesidad de adoptar medidas para eliminar las causas de no conformidad, con el fin de	L0				**L6**	0
10.1 (c)	implementar cualquier acción necesaria;	L0					
10.1 (d)	revisar la eficacia de las medidas correctivas adoptadas; y	L0					
10.1 (e)	realizar cambios en el sistema de gestión de seguridad de la información, si es necesario.	L0				**NC Mayores**	11
10.1 (f)	la naturaleza de las no conformidades y de cualquier acción tomada posteriormente, y	L0				**NC Menores**	0
10.1 (g)	los resultados de cualquier acción correctiva.	L0				**Observaciones**	0
10,2	Mejora continua	L0					

ANEXO A. FASE 1 - CMM-ISO27001-2013 INICIAL

ANEXO B. FASE 1 - CMM-ISO27002-2013 INICIAL

Evaluación de Madurez respecto a los controles definidos en la ISO 27002:2013

	Dominio	% de conformidad	# NC baja efectividad	# NC alta efectividad	# NC OK
A.5	POLÍTICAS DE SEGURIDAD	5%	2	0	0
A.6	ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION.	0%	6	0	0
A.7	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	3%	6	0	0
A.8	GESTIÓN DE ACTIVOS.	0%	9	0	0
A.9	CONTROL DE ACCESOS.	3%	14	0	0
A.10	CIFRADO.	0%	0	0	0
A.11	SEGURIDAD FÍSICA Y AMBIENTAL.	1%	11	0	0
A.12	SEGURIDAD EN LA OPERATIVA.	5%	13	1	0
A.13	SEGURIDAD EN LAS TELECOMUNICACIONES.	0%	5	0	0
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	0%	11	0	0
A.15	RELACIONES CON SUMINISTRADORES.	0%	5	0	0
A.16	GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	0%	7	0	0
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.	3%	4	0	0
A.18	CUMPLIMIENTO.	2%	6	0	0

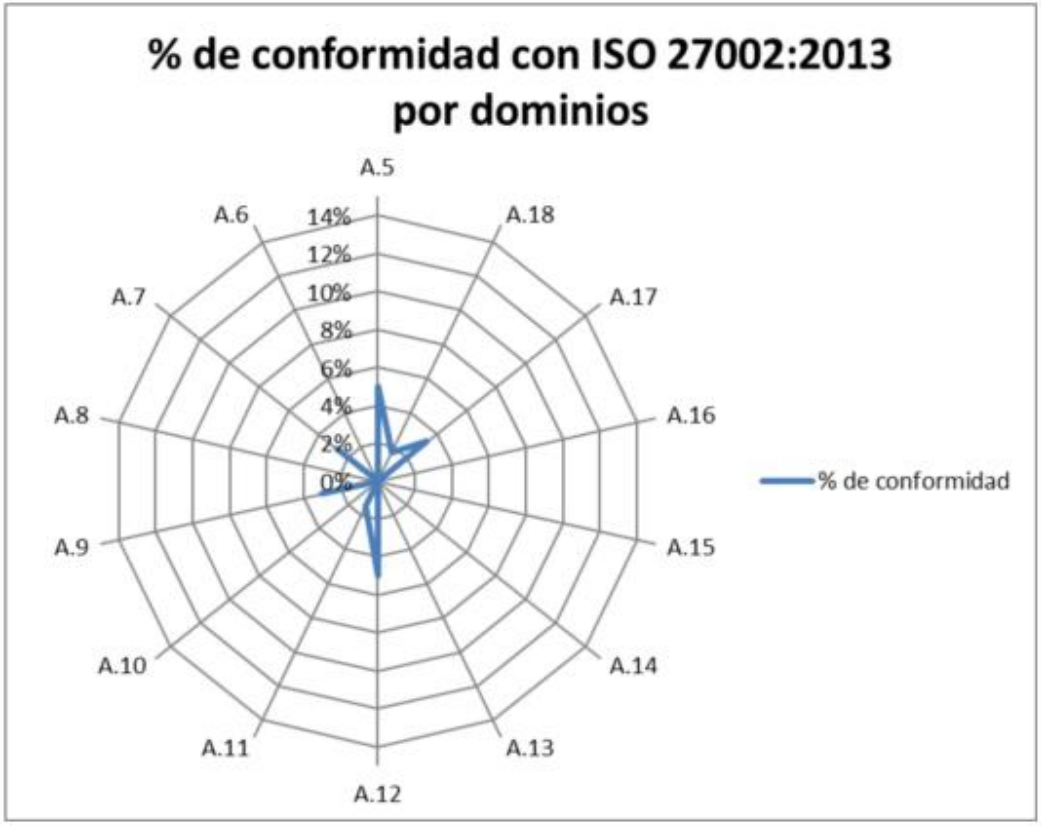
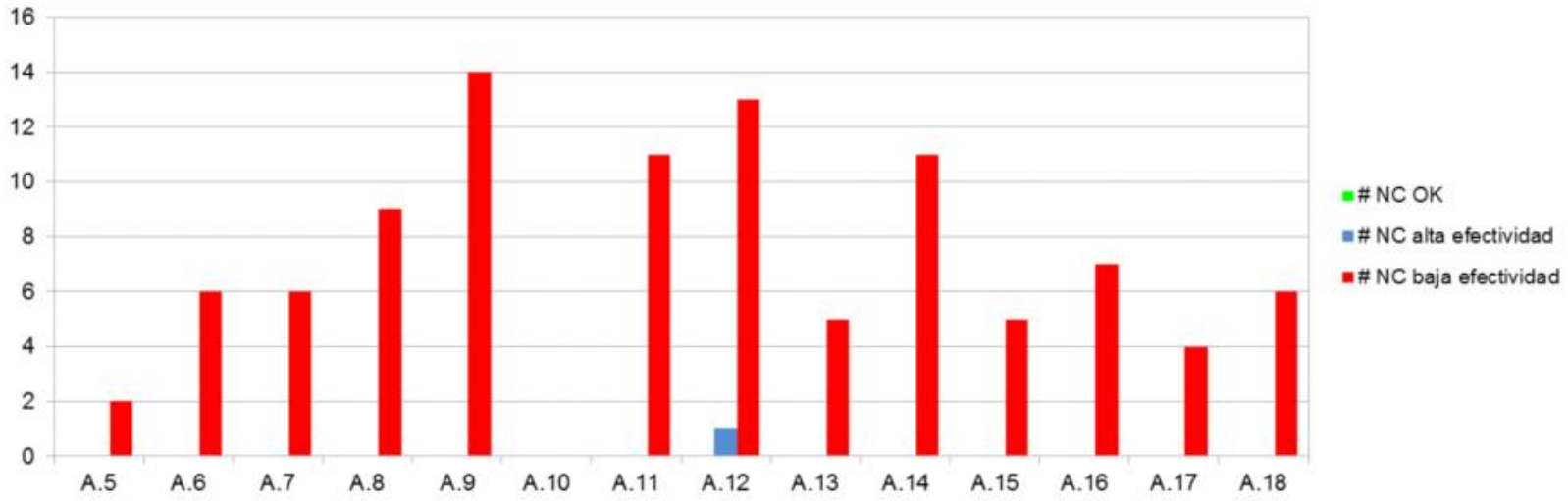
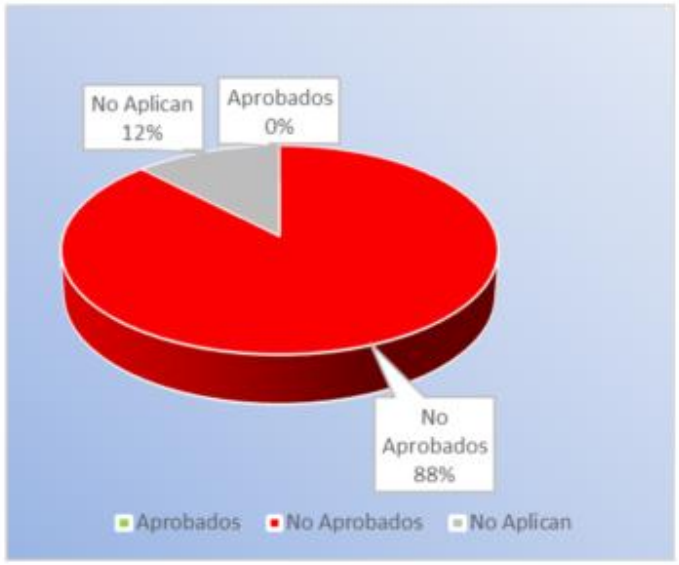

% de conformidad con ISO 27002:2013 por dominios
A.5
A.18
A.17
A.16
A.15
A.14
A.13
A.12
A.11
A.10
A.9
A.8
A.7
A.6
14%
12%
10%
8%
6%
4%
2%
0%
% de conformidad

Tabla de Valores

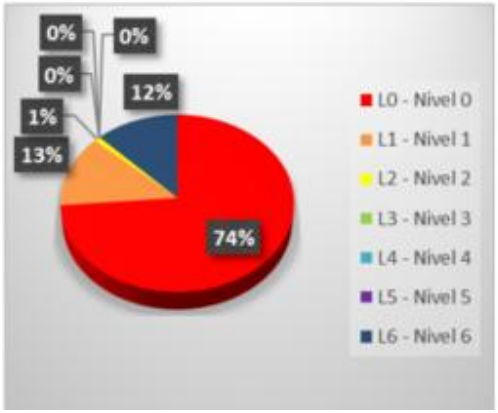
Valor	Efectividad	Significado	Descripción	Número
L0	0%	Inexistente	Carencia completa de cualquier proceso conocido.	84
L1	10%	Inicial / Ad-hoc	Procedimientos inexistentes o localizados en áreas concretas. El éxito de las tareas se debe a esfuerzos personales.	15
L2	50%	Reproducible, pero intuitivo	Existe un método de trabajo basado en la experiencia, aunque sin comunicación formal. Dependencia del conocimiento individual	1
L3	90%	Proceso definido	La organización en su conjunto participa en el proceso. Los procesos están implantados, documentados y comunicados.	0
L4	95%	Gestionado y medible	Se puede seguir la evolución de los procesos mediante indicadores numéricos y estadísticos. Hay herramientas para mejorar la calidad y la eficiencia	0
L5	100%	Optimizado	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos	0
L6	N/A	No aplica		14


16
14
12
10
8
6
4
2
0
A.5
A.6
A.7
A.8
A.9
A.10
A.11
A.12
A.13
A.14
A.15
A.16
A.17
A.18
NC OK
NC alta efectividad
NC baja efectividad

Valor	Número
Aprobados	0
No Aprobados	100
No Aplican	14



L0 - Nivel 0	84
L1 - Nivel 1	15
L2 - Nivel 2	1
L3 - Nivel 3	0
L4 - Nivel 4	0
L5 - Nivel 5	0
L6 - Nivel 6	14



Control de ISO /IEC 27002:2013	Controles y objetivos de control	Valoración	Anotaciones				
A.5	**POLÍTICAS DE SEGURIDAD**			0,05		**L0**	1
A.5.1	**Directrices de la Dirección en seguridad de la información**			**0,05**		**L1**	1
A.5.1.1	Conjunto de políticas para la seguridad de la información	L1		0,1		**L2**	0
A.5.1.2	Revisión de las políticas para la seguridad de la información	L0		0		**L3**	0
						L4	0
						L5	0
						L6	0
						NC Mayores	2
						NC Menores	0
						Observaciones	0

Control de ISO /IEC 27002:2013	Controles y objetivos de control	Valoración	Anotaciones				
A.6	**ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INF.**			0,0		**L0**	6
A.6.1	**Organización interna**			**0,0**		**L1**	0
A.6.1.1	Asignación de responsabilidades para la segur. de la información.	L0		0		**L2**	0
A.6.1.2	Segregación de tareas.	L0		0		**L3**	0
A.6.1.3	Contacto con las autoridades	L0		0		**L4**	0
A.6.1.4	Contacto con grupos de interés especial	L0		0		**L5**	0
A.6.1.5	Seguridad de la información en la gestión de proyectos	L0		0		**L6**	1
A.6.2	**Dispositivos para movilidad y teletrabajo.**			**0,0**			
A.6.2.1	Política de uso de dispositivos para movilidad.	L0		0			
A.6.2.2	Teletrabajo.	L6		N/A			
						NC Mayores	6
						NC Menores	0
						Observaciones	0

Control de ISO /IEC 27002:2013	Controles y objetivos de control	Valoración	Anotaciones				
A.7	**SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.**			0,0278		**L0**	4
A.7.1	**Organización interna**			**0,1**		**L1**	2
A.7.1.1	Investigación de antecedentes.	L1		0,1		**L2**	0
A.7.1.2	Términos y condiciones de contratación.	L0		0		**L3**	0
A.7.2	**Durante la contratación.**			**0,0333**		**L4**	0
A.7.2.1	Responsabilidades de gestión.	L1		0,1		**L5**	0
A.7.2.2	Concienciación, educación y capacitación en segur. de la informac.	L0		0		**L6**	0
A.7.2.3	Proceso disciplinario.	L0		0			
A.7.3	**Cese o cambio de puesto de trabajo.**			**0,0**			
A.7.3.1	Cese o cambio de puesto de trabajo.	L0		0			
						NC Mayores	6
						NC Menores	0
						Observaciones	0

Control de ISO /IEC 27002:2013	Controles y objetivos de control	Valoración	Anotaciones				
A.8	**GESTIÓN DE ACTIVOS.**			0,0000		**L0**	9
A.8.1	**Responsabilidad sobre los activos.**			**0,0**		**L1**	0
A.8.1.1	Inventario de activos.	L0		0		**L2**	0
A.8.1.2	Propiedad de los activos.	L0				**L3**	0
A.8.1.3	Uso aceptable de los activos.	L0				**L4**	0
A.8.1.4	Devolución de activos.	L0		0		**L5**	0
A.8.2	**Clasificación de la información.**			**0,0**		**L6**	1
A.8.2.1	Directrices de clasificación.	L0		0			
A.8.2.2	Etiquetado y manipulado de la información.	L0		0			
A.8.2.3	Manipulación de activos.	L0		0			
A.8.3	**Manejo de los soportes de almacenamiento.**			**0,0**			
A.8.3.1	Gestión de soportes extraíbles.	L0		0			
A.8.3.2	Eliminación de soportes.	L0		0			
A.8.3.3	Soportes físicos en tránsito	L6		N/A			
						NC Mayores	9
						NC Menores	0
						Observaciones	0

Control de ISO /IEC 27002:2013	Controles y objetivos de control	Valoración	Anotaciones				
A.9	**CONTROL DE ACCESOS.**			0,0300		**L0**	9
A.9.1	**Requisitos de negocio para el control de accesos.**			**0,05**		**L1**	5
A.9.1.1	Política de control de accesos.	L0		0		**L2**	0
A.9.1.2	Control de acceso a las redes y servicios asociados.	L1		0,1		**L3**	0
A.9.2	**Gestión de acceso de usuario.**			**0,05**		**L4**	0
A.9.2.1	Gestión de altas/bajas en el registro de usuarios.	L0		0		**L5**	0
A.9.2.2	Gestión de los derechos de acceso asignados a usuarios.	L1		0,1		**L6**	0
A.9.2.3	Gestión de los derechos de acceso con privilegios especiales.	L1		0,1			
A.9.2.4	Gestión de información confidencial de autenticación de usuarios.	L0		0			
A.9.2.5	Revisión de los derechos de acceso de los usuarios.	L0		0			
A.9.2.6	Retirada o adaptación de los derechos de acceso	L1		0,1			
A.9.3	**Responsabilidades del usuario.**			**0,0**			
A.9.3.1	Uso de información confidencial para la autenticación.	L0		0			
A.9.4	**Control de acceso a sistemas y aplicaciones.**			**0,02**			
A.9.4.1	Restricción del acceso a la información.	L0		0			
A.9.4.2	Procedimientos seguros de inicio de sesión.	L0		0			
A.9.4.3	Gestión de contraseñas de usuario.	L0		0			
A.9.4.4	Uso de herramientas de administración de sistemas.	L1		0,1			
A.9.4.5	Control de acceso al código fuente de los programas.	L0		0			
						NC Mayores	14
						NC Menores	0
						Observaciones	0

Control de ISO /IEC 27002:2013	Controles y objetivos de control	Valoración	Anotaciones				
A.10	**CIFRADO.**			0,0000		**L0**	0
A.10.1	**Controles criptográficos.**			**0,0**		**L1**	0
A.10.1.1	Política de uso de los controles criptográficos.	L6		N/A		**L2**	0
A.10.1.2	Gestión de claves.	L6		N/A		**L3**	0
						L4	0
						L5	0
						L6	2
						NC Mayores	0
						NC Menores	0
						Observaciones	0

Control de ISO /IEC 27002:2013	Controles y objetivos de control	Valoración	Anotaciones				
A.11	SEGURIDAD FÍSICA Y AMBIENTAL.			0,0143		L0	9
A.11.1	Áreas seguras.			0,0		L1	2
A.11.1.1	Perímetro de seguridad física.	L0		0		L2	0
A.11.1.2	Controles físicos de entrada.	L0		0		L3	0
A.11.1.3	Seguridad de oficinas, despachos y recursos.	L0		0		L4	0
A.11.1.4	Protección contra las amenazas externas y ambientales.	L0		0		L5	0
A.11.1.5	El trabajo en áreas seguras.	L6		N/A		L6	4
A.11.1.6	Áreas de acceso público, carga y descarga.	L6		N/A			
A.11.2	Seguridad de los equipos.			0,02857			
A.11.2.1	Emplazamiento y protección de equipos.	L0		0			
A.11.2.2	Instalaciones de suministro.	L1		0,1			
A.11.2.3	Seguridad del cableado.	L6		N/A			
A.11.2.4	Mantenimiento de los equipos.	L1		0,1			
A.11.2.5	Salida de activos fuera de las dependencias de la empresa.	L0		0			
A.11.2.6	Seguridad de los equipos y activos fuera de las instalaciones.	L6		N/A			
A.11.2.7	Reutilización o retirada segura de dispositivos de almacenamiento.	L0		0			
A.11.2.8	Equipo informático de usuario desatendido.	L0		0			
A.11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla.	L0		0			
						NC Mayores	11
						NC Menores	0
						Observaciones	0

Control de ISO /IEC 27002:2013	Controles y objetivos de control	Valoración	Anotaciones				
A.12	**SEGURIDAD EN LA OPERATIVA.**			0,0500		**L0**	11
A.12.1	**Responsabilidades y procedimientos de operación.**			**0,0**		**L1**	2
A.12.1.1	Documentación de procedimientos de operación.	L0		0		**L2**	1
A.12.1.2	Gestión de cambios.	L0		0		**L3**	0
A.12.1.3	Gestión de capacidades.	L0		0		**L4**	0
A.12.1.4	Separación de entornos de desarrollo, prueba y producción.	L0		0		**L5**	0
A.12.2	**Protección contra código malicioso.**			**0,10000**		**L6**	0
A.12.2.1	Controles contra el código malicioso.	L1		0,1			
A.12.3	**Copias de seguridad.**			**0,50000**			
A.12.3.1	Copias de seguridad de la información.	L2		0,5			
A.12.4	**Registro de actividad y supervisión.**			**0,00000**			
A.12.4.1	Registro y gestión de eventos de actividad.	L0		0			
A.12.4.2	Protección de los registros de información.	L0		0			
A.12.4.3	Registros de actividad del administrador y operador del sistema.	L0		0			
A.12.4.4	Sincronización de relojes.	L0		0			
A.12.5	**Control del software en explotación.**			**0,00000**			
A.12.5.1	Instalación del software en sistemas en producción.	L0		0			
A.12.6	**Gestión de la vulnerabilidad técnica.**			**0,05000**			
A.12.6.1	Gestión de las vulnerabilidades técnicas.	L0		0			
A.12.6.2	Restricciones en la instalación de software.	L1		0,1			
A.12.7	**Consideraciones de las auditorías de los sistemas de información.**			**0,00000**			
A.12.7.1	Controles de auditoría de los sistemas de información.	L0		0			
						NC Mayores	13
						NC Menores	1
						Observaciones	0

Control de ISO /IEC 27002:2013	Controles y objetivos de control	Valoración	Anotaciones				
A.13	**SEGURIDAD EN LAS TELECOMUNICACIONES.**			0,0000		**L0**	5
A.13.1	**Gestión de la seguridad en las redes.**			**0,0**		**L1**	0
A.13.1.1	Controles de red.	L0		0		**L2**	0
A.13.1.2	Mecanismos de seguridad asociados a servicios en red.	L0		0		**L3**	0
A.13.1.3	Segregación de redes.	L6		N/A		**L4**	0
A.13.2	**Intercambio de información con partes externas.**			**0,00000**		**L5**	0
A.13.2.1	Políticas y procedimientos de intercambio de información.	L0		0		**L6**	2
A.13.2.2	Acuerdos de intercambio.	L6		N/A			
A.13.2.3	Mensajería electrónica.	L0		0			
A.13.2.4	Acuerdos de confidencialidad y secreto.	L0		0			
					NC Mayores		5
					NC Menores		0
					Observaciones		0

Control de ISO /IEC 27002:2013	Controles y objetivos de control	Valoración	Anotaciones				
A.15	**RELACIONES CON SUMINISTRADORES.**			0,0000		**L0**	5
A.15.1	**Seguridad de la información en las relaciones con suministradores.**			**0,0**		**L1**	0
A.15.1.1	Política de seguridad de la información para suministradores.	L0		0		**L2**	0
A.15.1.2	Tratamiento del riesgo dentro de acuerdos de suministradores.	L0		0		**L3**	0
A.15.1.3	Cadena de suministro en tecnologías de la información y comunicaciones.	L0		0		**L4**	0
A.15.2	**Gestión de la prestación del servicio por suministradores.**			**0,00000**		**L5**	0
A.15.2.1	Supervisión y revisión de los servicios prestados por terceros.	L0		0			
A.15.2.2	Gestión de cambios en los servicios prestados por terceros.	L0		0			
					NC Mayores		5
					NC Menores		0
					Observaciones		0

Control de ISO /IEC 27002:2013	Controles y objetivos de control	Valoración	Anotaciones				
A.16	**GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.**			0,0000		**L0**	7
A.16.1	**Gestión de incidentes de seguridad de la información y mejoras.**			**0,0**		**L1**	0
A.16.1.1	Responsabilidades y procedimientos.	L0		0		**L2**	0
A.16.1.2	Notificación de los eventos de seguridad de la información.	L0		0		**L3**	0
A.16.1.3	Notificación de puntos débiles de la seguridad	L0		0		**L4**	0
A.16.1.4	Valoración de eventos de seguridad de la información y toma de decisiones.	L0		0		**L5**	0
A.16.1.5	Respuesta a los incidentes de seguridad.	L0		0		**L6**	0
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información.	L0		0			
A.16.1.7	Recopilación de evidencias.	L0		0			
					NC Mayores		7
					NC Menores		0
					Observaciones		0

Control de ISO /IEC 27002:2013	Controles y objetivos de control	Valoración	Anotaciones				
A.17	**ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.**			0,0333		**L0**	2
A.17.1	**Continuidad de la seguridad de la información.**			**0,07**		**L1**	2
A.17.1.1	Planificación de la continuidad de la seguridad de la información.	L1		0,1		**L2**	0
A.17.1.2	Implantación de la continuidad de la seguridad de la información.	L1		0,1		**L3**	0
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la Seguridad de la información.	L0		0		**L4**	0
A.17.2	**Redundancias.**			**0,00000**		**L5**	0
A.17.2.1	Disponibilidad de instalaciones para el procesamiento de la información.	L0		0		**L6**	0
					NC Mayores		4
					NC Menores		0
					Observaciones		0

Control de ISO /IEC 27002:2013	Controles y objetivos de control	Valoración	Anotaciones				
A.18	**CUMPLIMIENTO.**			0,0167		**L0**	5
A.18.1	**Cumplimiento de los requisitos legales y contractuales.**			**0,03**		**L1**	1
A.18.1.1	Identificación de la legislación aplicable.	L1		0,1		**L2**	0
A.18.1.2	Derechos de propiedad intelectual (DPI).	L6		N/A		**L3**	0
A.18.1.3	Protección de los registros de la organización.	L0		0		**L4**	0
A.18.1.4	Protección de datos y privacidad de la información personal.	L0		0		**L5**	0
A.18.1.5	Regulación de los controles criptográficos.	L6		N/A		**L6**	2
A.18.2	**Revisiones de la seguridad de la información.**			**0,00000**			
A.18.2.1	Revisión independiente de la seguridad de la información.	L0		0			
A.18.2.2	Comprobación del cumplimiento	L0		0			
A.18.2.3	Disponibilidad de instalaciones para el procesamiento de la información.	L0		0			
						NC Mayores	6
						NC Menores	0
						Observaciones	0

ANEXO B. FASE 1 - CMM-ISO27002-2013 INICIAL

ANEXO C. FASE 2 - SGSI-01 POLÍTICA DE SEGURIDAD

	SGSI – 01	Código: SGSI_01
	POLÍTICA DE SEGURIDAD	Versión: 1
		Vigente desde: 01/01/2016

HOJA DE CONTROL

TÍTULO	POLÍTICA DE SEGURIDAD		
CÓDIGO	SGSI – 01		
AUTOR	Equipo de innovación y seguridad de la información		
CLASIFICACIÓN	Uso interno	**TIPO DOCUMENTO**	
VERSIÓN	1.0	**FECHA VERSIÓN**	01/12/2015
REVISADO POR:	Resp. sistemas / TI	**FECHA REVISIÓN**	15/12/2015
APROBADO POR:	Comité seguridad	**FECHA**	31/12/2015

ÍNDICE

1. INTRODUCCIÓN

PARQUES NACIONALES NATURALES DE COLOMBIA y su Director General y Directores Territoriales identifican la información como un activo indispensable en la conducción y consecución de los objetivos definidos por la estrategia de la entidad. Siendo conscientes de la importancia que tiene para la compañía la seguridad de la información para conseguir un nivel óptimo de competitividad en el mercado, ha sido necesario el establecimiento de un marco de referencia que garantice que la información este protegida de una forma correcta independientemente de la forma como ésta sea gestionada, procesada o almacenada.

2. OBJETIVOS

En esta línea, PARQUES NACIONALES NATURALES DE COLOMBIA ha desarrollado la presente política de seguridad de la información que afecta a la confidencialidad, integridad y disponibilidad de la información tratada por PARQUES NACIONALES NATURALES DE COLOMBIA a todos los niveles de sensibilidad y confidencialidad, en base a las leyes y normativas vigentes, como son la ISO 27001: 2013 y las buenas prácticas de la ISO 27002: 2013.

Esta política cubre todos los aspectos administrativos y de control que se deben cumplir para todo el personal interno de la entidad y terceras partes, para conseguir un nivel correcto de protección de las características de la seguridad y la calidad de la información relacionada. Y en tanto que la seguridad de la información es una prioridad para PARQUES NACIONALES NATURALES DE COLOMBIA, es responsabilidad de todos velar por su cumplimiento.

3. PRINCIPIOS DE LA ORGANIZACIÓN

PARQUES NACIONALES NATURALES DE COLOMBIA, consciente de las necesidades actuales, implementa un modelo de gestión de seguridad de la información como herramienta que permita identificar y minimizar los riesgos actuales a los que se expone la información, ayudar a la reducción de costos operativos y financieros, estableciendo al mismo tiempo una cultura de seguridad y garantizando el cumplimiento de los requisitos legales, contractuales, regulatorios y de negocio vigentes.

Como evidencia de su compromiso, la dirección de PARQUES NACIONALES NATURALES DE COLOMBIA aprueba esta Política de Seguridad de la Información apoyando el diseño y la implantación de políticas eficientes que garanticen la seguridad de la información de la entidad, facilitando su divulgación a todos los miembros de la misma y velando por su cumplimiento.

Así pues, todo trabajador de PARQUES NACIONALES NATURALES DE COLOMBIA, independientemente de sus labores deben cumplir con la política y normativa para la seguridad de la información descrita en este documento.

En tanto que la seguridad de la información es cosa de todos, todas las posibles violaciones de la normativa y / o alteraciones que puedan suponer un riesgo para la información deberán ser comunicadas al departamento de seguridad de la información, ya sean propias o de terceros.

4. SISTEMAS INVOLUCRADOS

La normativa de seguridad de PARQUES NACIONALES NATURALES DE COLOMBIA afecta a todos los sistemas informáticos, la información almacenada en estos, los sistemas en red y la documentación en papel que gestiona la entidad.
El uso de los sistemas informáticos (PCs, portátiles, impresoras) y las redes de PARQUES NACIONALES NATURALES DE COLOMBIA se restringe al ámbito profesional, no permitiendo su

uso con fines personales. Asimismo, queda totalmente prohibido el uso de las direcciones de correo de la entidad, con fines personales.

Atendiendo a que los equipos informáticos se ponen a uso y disposición los empleados únicamente para uso profesional, PARQUES NACIONALES NATURALES DE COLOMBIA se reserva el derecho a inspeccionar- en cualquier momento, con el fin de garantizar el cumplimiento de la normativa y las leyes aplicables. Las inspecciones las llevará a cabo el departamento de seguridad.

5. RESPONSABILIDADES

PARQUES NACIONALES NATURALES DE COLOMBIA cuenta con un Comité de seguridad de la información dirigido por el responsable de sistemas de cada territorial que es a la vez responsable de coordinar las acciones orientadas a garantizar la seguridad de la información en todas sus formas (digital y papel) y durante todo su ciclo de vida (creación, mantenimiento, distribución, almacenamiento y destrucción).

Aparte de su responsabilidad, el comité toma decisiones consensuada en materia de seguridad de la información, cuenta con los siguientes miembros: el director general, el director de RRHH, director técnico y director financiero, siendo el director de RRHH, el responsable de comunicar a los trabajadores las posibles sanciones derivadas del incumplimiento de la política de seguridad.

6. GESTIÓN DE LA INFORMACIÓN Y USO DE LOS SISTEMAS INFORMÁTICOS

La información de PARQUES NACIONALES NATURALES DE COLOMBIA debe protegerse desde su creación según la su confidencialidad, empleando medidas de seguridad independientes de su formato (Digital o papel), medio de transmisión y sistema de procesamiento. La entidad dispone de copias de seguridad de la información, correctamente almacenados, y de mecanismos de copia automática de cada uno de los equipos de usuario.

Toda la información sensible de la entidad debe ser etiquetada como confidencial, en todos sus formatos (digital y papel) y durante todo su ciclo de vida. El resto de información puede etiquetarse como de uso interno o como información pública. Toda la información no pública se protegerá contra su difusión a terceros. en caso de divulgación accidental debe comunicarse al departamento de seguridad de la información.

La información en papel, confidencial, debe estar correctamente archivada. La entidad lleva a cabo iniciativas para mantener los puestos de trabajos limpios, sin documentación.
Asimismo, las impresoras funcionan con código de impresión.

El acceso a la información va ligada al rol y perfil de cada usuario, permitiendo el acceso sólo a aquella información necesaria para desarrollar su actividad.

Los administradores del departamento de sistemas se encargan de asignar un usuario y contraseña a cada uno de los usuarios y dotarlos de ciertos privilegios de acceso en función de su rol. Existe un registro de actividad que recoge los accesos de los usuarios a la información.

Cada miembro de la entidad es responsable de su cuenta de usuario y de velar por el correcto uso del mismo. Así pues, en ningún caso los usuarios pueden revelar sus contraseñas a otros usuarios ni almacenarlas en ningún fichero en papel ni digital.

El usuario debe elegir contraseñas seguras y difíciles de averiguar, evitando el uso de datos de carácter personal / profesional en estas y de palabras de diccionario. Todas las contraseñas deberán

tener 8 caracteres, al menos una mayúscula y un dígito. Estas solicitaran cambio cada 30 días por políticas de cuentas y contraseñas del directorio activo.

Cuando el sistema detecta inactividad durante un cierto período, activa un protector de pantalla con contraseña. Así mismo se recomienda a los usuarios que lo activen en el momento en que se levantan de su puesto de trabajo.

A nivel de propiedad intelectual, todos los desarrollos, programas, documentos o patentes, elaborados como resultado de la relación contractual son propiedad de PARQUES NACIONALES NATURALES DE COLOMBIA

7. GESTIÓN DE ACCESOS REMOTOS

En cuanto a los accesos remotos, aquellos trabajadores que requieran acceso remoto se podrán conectar con el servidor de proyectos únicamente vía VPN, previa aprobación del jefe de proyecto correspondiente.

Cuando sea necesario el teletrabajo, el jefe inmediato deberá autorizar la salida de los equipos de las instalaciones. Dentro de la oficina los equipos cuentan con sistemas de anclaje y seguridad físicos, y por política DC no permiten la extracción de información en disco duro ni USB.

Aparte de monitorizar el uso de los equipos informáticos, PARQUES NACIONALES NATURALES DE COLOMBIA controla el acceso a Internet a fin de evitar que los trabajadores accedan a webs que nada tienen que ver con su actividad laboral, evitando el uso excesivo de recursos y para garantizar que se cumplen las políticas establecidas.

Los trabajadores no pueden hablar en nombre de la empresa en ningún foro ni página web. Tampoco pueden almacenar información confidencial y / o interna a la nube, en repositorios como Drive y similares sino son los institucionales. Asimismo, está totalmente prohibido el envío de archivos por internet sin encriptación y codificación.

8. CONTROL DE INCIDENCIAS

Todos los equipos informáticos disponen de sistemas de detección de virus, para comprobar todos los archivos y software que provienen tanto de terceras personas como de otros grupos dentro de la compañía. Los sistemas de antivirus actúan antes de abrir el archivo y en ningún caso los usuarios pueden desactivarlos.

Cuando un usuario detecta un virus lo comunicará inmediatamente al departamento de seguridad que procederán a aislar el equipo de la red y en desinfectarlo. En ningún caso, el usuario debe intentar eliminar el virus por sí solo. Sólo podrán instalar nuevos programas los miembros del departamento de sistemas e informática. Para la restauración de los equipos infectados, todo el software debe ser copiado antes de su uso, almacenando las copias en un lugar seguro.

9. DIFUSIÓN

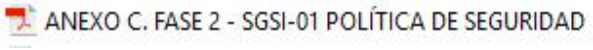
La Dirección del PARQUES NACIONALES NATURALES DE COLOMBIA velará por la difusión de la política de seguridad, garantizando que todas las personas de la entidad sean conocedoras.

10. REVISIÓN

Esta política será revisada periódicamente para garantizar la adecuación y eficacia.

11. POLÍTICA DE SANCIONES

PARQUES NACIONALES NATURALES DE COLOMBIA podrá emprender las medidas contra aquellas personas que incumplan la política y normativa de seguridad de la entidad, en tanto que dicho incumplimiento derive en un riesgo para el negocio o un incumplimiento de las normativas legales y acuerdos contractuales. El grado de las sanciones puede ir desde acciones correctivas hasta el despido, según la naturaleza, intencionalidad y alcance de los sucesos.



ANEXO D. FASE 2 - SGSI-02 PROCEDIMIENTO DE AUDITORÍAS INTERNAS

	SGSI – 01	Código: SGSI_02
	SGSI-02 PROCEDIMIENTO DE AUDITORÍAS INTERNAS	Versión: 1
		Vigente desde: 01/01/2016

HOJA DE CONTROL

TÍTULO	PROCEDIMIENTO DE AUDITORÍAS INTERNAS		
CÓDIGO	SGSI – 02		
AUTOR	Equipo de innovación y seguridad de la información		
CLASIFICACIÓN	Uso interno	**TIPO DOCUMENTO**	
VERSIÓN	1.0	**FECHA VERSIÓN**	01/12/2015
REVISADO POR:	Resp. sistemas / TI	**FECHA REVISIÓN**	15/12/2015
APROBADO POR:	Comité seguridad	**FECHA**	31/12/2015

ÍNDICE

12. INTRODUCCIÓN

En tanto que las auditorías internas del SGSI son un proceso necesario y obligatorio según la norma ISO / IEC27001: 2013, PARQUES NACIONALES NATURALES DE COLOMBIA se compromete a realizar las auditorías interna de su SGSI en intervalos planificados para verificar si está correctamente implantado y mantenido cubriendo todos los objetivos deseados, cumpliendo al mismo tiempo con los requerimientos de la norma internacional, la legislación y normativas vigentes, adicional a esto los requerimientos de seguridad de la información identificados.

13. OBJETIVOS

El objetivo del 'Procedimiento de auditorías internas' es establecer el procedimiento a seguir para la planificación y realización de las auditorías internas del SGSI de PARQUES NACIONALES NATURALES DE COLOMBIA, describiendo las pautas para realizar un examen sistemático de éste que permita su correcta aplicación y eficacia, identificando anomalías y posibles mejoras o correcciones.

14. ALCANCE

Este procedimiento es una herramienta de consulta y aplicación para aquellas áreas comprendidas dentro del alcance del SGSI de PARQUES NACIONALES NATURALES DE COLOMBIA.

15. AUDITORIA INTERNA DEL SGSI

El procedimiento comienza con la elaboración, aprobación y difusión del programa anual de auditorías del SGSI y finaliza con la revisión del estado de las acciones correctivas y / o preventivas detectadas. A su vez, este procedimiento es aplicable a todos los procesos incluidos dentro del alcance del SGSI, bajo la norma ISO / IEC 27001: 2013.

Elaboración del Plan de auditoría

El responsable del SGSI, elaborará el Programa Anual de Auditorías teniendo en cuenta la importancia y el estado de los procesos y las áreas a auditar, así como los resultados de las auditorías previas. El equipo auditor designado podrá estar formado por un mínimo de un auditor (según la complejidad de la auditoría) y podrán participar expertos técnicos y observadores (conocedores de la norma ISO / IEC 27001: 2013 e ISO / IEC 27002: 2013).

Las auditorías internas del SGSI serán programadas de tal manera que se efectúen en un ciclo completo de 1 año y serán aprobadas por la Dirección dentro del primer trimestre del periodo programado. Si se producen cambios en el programa, estos deberán ser aprobados por Dirección.

En el programa de auditorías se definirán:

Las actividades y / o las áreas a auditar (indicando las fechas de estas auditorías).

Los auditores que intervienen. Los auditores internos, serán independientes del área o proceso auditado, y en ningún caso se permitirá que auditen su propio trabajo. Estos estarán a disposición del Comité de seguridad cuando sean convocados. Si se considera oportuno, se podrá subcontratar a los auditores internos, siempre que estas terceras partes tengan las competencias pertinentes.

Los documentos a auditar.

- Preparación de la auditoría

El equipo auditor designado preparará la auditoría mediante la elaboración de un cuestionario de auditoría concreto según el área a auditar y un programa de entrevistas previstas con el personal involucrado.

Este cuestionario de entrevistas no se considera un registro del SGSI, por lo que podría ser eliminado una vez realizado el informe de auditoría pertinente.

PARQUES NACIONALES NATURALES DE COLOMBIA dispone de una plantilla donde se define una guía para la realización de la auditoría, teniendo en cuenta las necesidades documentales y de autoría 'in situ'.

- Realización de la auditoría

Las auditorías internas se realizarán según los plazos establecidos con el objetivo de determinar el grado en que el SGSI cumple con los requisitos de la norma ISO IEC 27001: 2013. Evaluando el cumplimiento de la documentación, objetivos y controles del SGSI, informes y registros generados del SGSI y cumplimiento de los requerimientos de seguridad de la información.

El proceso de auditoría interna comenzará con un muestreo de las fuentes de información obteniendo evidencias de auditoría que serán evaluados según los criterios de auditoría establecidos. Los resultados de esta serán revisados y finalmente se extraerán un conjunto de conclusiones de la auditoría.

El coordinador del departamento o responsable del proceso auditado deberá poner a disposición del equipo auditor los medios necesarios para la auditoría, facilitando el acceso a las instalaciones y documentos relevantes para la auditoría. Este deberá cooperar con los auditores en todo momento para garantizar el éxito de la auditoría, comprometiéndose a tomar las acciones correctivas necesarias sin retrasos injustificados para de eliminar las no conformidades detectadas durante la auditoría.

Las evidencias de auditoría que se encuentren serán clasificadas en No conformidades, observaciones y oportunidades de mejora del SGSI, para que posteriormente pueda revisar el Comité de Seguridad (ver anexo 05B).

- Elaboración del informe de auditoría

Los resultados de las auditorías servirán para llevar a cabo una evaluación de la eficacia del SGSI, permitiendo la identificación de oportunidades de mejora.

Como resultado de la auditoría, el equipo auditor realizará un informe que contendrá la siguiente la información

Número y fecha del informe

Número del control de la norma auditado o Departamento, alcance y personas auditadas o Resumen de los resultados

No conformidades detectadas.

- Distribución del informe

Una vez finalizada la auditoría, el informe con los resultados será enviado al responsable del SGSI, que deberá velar por su correcto archivo y etiquetado, evitando su pérdida o manipulación.

- Revisión del informe de auditoría

Una vez cerrada la auditoría, el Comité de seguridad analizará los puntos fuertes y débiles, las observaciones y oportunidades de mejora del SGSI señalados en el informe de auditoría, tomando las acciones y decisiones pertinentes y definiendo un responsable, el plazo de implementación y la verificación final de las acciones correctoras, en su caso.

- Plan de acción

El Comité de Seguridad propondrá y documentará las acciones correctivas derivadas de las No conformidades, elaborando las 'Solicitudes de acción' pertinentes donde se registrará el siguiente (ver anexo D):

La descripción de las No Conformidades reales o potenciales encuentros.

El análisis de las causas que originaron las No Conformidades reales y potenciales.

Las correcciones, acciones preventivas y / o correctivas implantadas, así como la revisión de la efectividad de estas.

- Implantación / verificación de las acciones correctivas.

El Comité de Seguridad verificará la implantación de las acciones correctivas.

Ítem 1. Descripción del procedimiento

Actividad		Responsable
Elaboración, aprobación y difusión del programa anual de Auditorías	Elabora el programa anual de auditoría del SGSI para un periodo determinado	Comité de seguridad
	Aprobación del programa anual de auditorías del SGSI	Comité de seguridad
Elaboración del plan de auditoría interna	Coordinación con los jefes de la áreas o procesos a auditar, las fechas y horas para la ejecución de las auditorías, para confirmar su disponibilidad	Comité de seguridad
	Selección del auditor interno que deberá cumplir con los requisitos especificados en el documento perfil del auditor.	Comité de seguridad
	Identificación del auditor líder por el proceso en auditar según su experiencia	Comité de seguridad
	Elaborar el plan de auditoría interna para el SGSI Según el formato que se muestra en el anexo.	Auditor líder
	Comunicar el plan de auditoría interna en el personal involucrado en los procesos a ser auditados.	Auditor líder

Preparación de la auditoría interna	Revisar la documentación correspondiente a los procesos a auditar, atendiendo a los resultados de las auditorías previas y relativas a la norma ISO 27001: 2013.	Auditor líder
Apertura	Reunión de apertura de la auditoría con el personal involucrado, según el plan de auditoría interna establecido, revisando y confirmando horarios, responsables y procesos a auditar, haciendo los cambios pertinentes en caso de ser necesario.	Auditor líder
Ejecución	Auditar los procesos y / o las áreas previstas, según la norma ISO 27001: 2013, recogiendo evidencias objetivas de las entrevistas, de la observación de las actividades y la revisión de los registros para verificar la implementación y efectividad del SGSI.	Equipo auditor
	Informar al área auditada de los resultados encontrados durante el proceso	Equipo auditor
Registro de no conformidades	Redactar las No Conformidades encontradas en el documento 'solicitud de acción' haciendo referencia al control de la norma que se está incumpliendo con el fin de entregar al Comité de seguridad.	Equipo auditor
Informe auditoría	Diligenciar el informe de auditoría	Auditor líder
	Presentar el informe al comité de seguridad, Adjuntando las solicitudes de acción en caso de encontrar no conformidades.	Auditor líder
Cierre	Reunión de cierre de acuerdo con el plan de auditoría interna, indicando los plazos para la resolución de las No conformidades pertinentes detectadas.	Auditor líder
	Gestionar el tratamiento de las No Conformidades según lo establecido en el procedimiento de acciones preventivas y correctivas	Comité de seguridad
	Evaluar cada auditor interno, después del proceso.	Comité de seguridad

Ilustración 1. Recapitulativo Procedimiento de auditoría

Ítem 2: Formato del plan de auditoría interna

PARQUES NACIONALES NATURALES DE COLOMBIA	PLAN DE AUDITORIA INTERNA

Número Auditoria		Norma Referencia		Fecha Elaboración	

Objetivo	
Alcance	

Auditor Líder		
Auditores Internos		
Expertos Técnicos		
Observadores		

Fecha	Hora	Proceso Auditado	Criterios de auditoría		Auditor	Auditado

Reunión de apertura				Reunión de cierre			
Fecha		Hora		Fecha		Hora	

Ítem 3: Formato del informe de auditoría

PARQUES NACIONALES NATURALES DE COLOMBIA	INFORME DE AUDITORÍA INTERNA

Datos de la auditoría interna	
Número Auditoría	
Norma de Referencia	
Período de la auditoría	
Lugar de la auditoría	
Equipo auditor	

Alcance de la auditoría interna

Objetivos de la auditoría interna
Determinar el grado de cumplimiento del SGSI de PARQUES NACIONALES NATURALES DE COLOMBIA respecto a la norma ISO / IEC27001: 2013.

Definiciones
No conformidad: incumplimiento de un requisito de la norma ISO / IEC27001: 2013, política o documentos del SGSI que pone en riesgo la efectividad del sistema de gestión y la calidad del servicio suministrado. **Observación:** falla aislada y esporádica en el contenido o la implementación de los documentos del SGSI o incumplimiento parcial de un requisito de la norma de referencia que no afecta al SGSI de manera crítica. **Oportunidad de mejora**: recomendación que de su implementación se deriva una mejora del SGSI.

Resultados de la auditoría
No conformidades:

Proceso	Descripción	Responsable	Auditor

Observaciones y oportunidades de mejora

Conclusiones

Ítem 4: Formato de solicitud de acción

PARQUES NACIONALES NATURALES DE COLOMBIA	SOLICITUD DE ACCIÓN

Num. Solicitud		Norma referencia	

Acciones Preventivas	Acciones Correctivas	Servicio No conforme

Descripció			
Informador			
Responsable		Fecha	
Análisis de las causas			
Responsable		Fecha	
Acciones a llevar a cabo			
Inmediata			
Preventiva/correctiva			
Núm	Actividad	Responsable	Tiempo
Responsable		Fecha	
Plazo de cierre			
Verificación			
Conforme		No	
Responsable		Fecha	

ANEXO D. FASE 2 - SGSI-02 PROCEDIMIENTO DE AUDITORÍAS INTERNAS

ANEXO E. FASE 2 - SGSI-03 GESTIÓN DE INDICADORES

	SGSI – 01	Código: SGSI_03
	SGSI-03 Gestión de Indicadores	Versión: 1
		Vigente desde: 01/01/2016

HOJA DE CONTROL

TÍTULO	GESTIÓN DE INDICADORES		
CÓDIGO	SGSI – 03		
AUTOR	Equipo de innovación y seguridad de la información		
CLASIFICACIÓN	Uso interno	**TIPO DOCUMENTO**	
VERSIÓN	1.0	**FECHA VERSIÓN**	01/12/2015
REVISADO POR:	Resp. sistemas / TI	**FECHA REVISIÓN**	15/12/2015
APROBADO POR:	Comité seguridad	**FECHA**	31/12/2015

ÍNDICE

16. INTRODUCCIÓN

PARQUES NACIONALES NATURALES DE COLOMBIA ha considerado oportuno definir una metodología para definir y gestionar los indicadores del SGSI que servirán para evaluar la eficiencia y efectividad de los objetivos y los controles de seguridad implantados.

17. OBJETIVOS

En el presente documento se definen los indicadores para medir la eficacia de los controles de seguridad implantados, así como la sistemática para hacer las medidas.

18. ALCANCE

Atendiendo al objetivo citado, el presente documento es aplicable al alcance del SGSI de PARQUES NACIONALES NATURALES DE COLOMBIA.

19. GESTIÓN DE INDICADORES

Seguidamente se define el procedimiento de gestión de los controles del SGSI de PARQUES NACIONALES NATURALES DE COLOMBIA.

a. Definición de indicadores

Para medir los objetivos y controles, PARQUES NACIONALES NATURALES DE COLOMBIA, utilizará aquellos indicadores que le permitan analizar la evolución o tendencia en su desarrollo.

Todos los objetivos y controles llevarán asociado un límite predefinido a partir del cual se consideren no conformes.

Asimismo, los indicadores utilizados para medir la eficacia de los objetivos y controles del SGSI se identificarán con los siguientes campos:

- Identificador del indicador
- Descripción del indicador
- Objetivo
- Periodicidad
- Responsable
- Criterio de medición
- Valor objetivo
- Valor mínimo
- Valor máximo
- Valor real

A raíz de las revisiones efectuadas sobre los controles, todos aquellos indicadores con valor real inferior al valor mínimo designado por el Comité de Seguridad generarán la apertura de un informe de No conformidad para evaluar las causas y realizar los cambios oportunos. Por otra parte, aquellos indicadores con valor real comprendido entre el valor mínimo y el valor objetivo designado generarán la apertura de un informe de No conformidad potencial para evaluar las causas y realizar los cambios oportunos para mejorar.

b. Cuadro de mandos

Para la medición y seguimiento de los objetivos y controles del SGSI implementará un cuadro de mandos que permita demostrar continuamente su evolución y mejora, en base a un listado de control de indicadores. este listado será identificado, documentado y actualizado por el responsable del SGSI, que deberá comunicar al Comité de Seguridad cualquier cambio significativo en el mismo.

c. Proceso de revisión

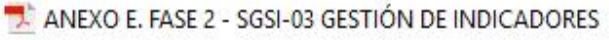
Las revisiones podrán ser periódicas o específicas.

En cuanto a las revisiones periódicas, éstas se llevarán a cabo una vez al año, y supondrán la revisión de los listados de controles, para actualizar posibles modificaciones en los parámetros característicos de los indicadores antes definidos.

Paralelamente, las revisiones específicas, se llevarán a cabo cuando se produzca algún suceso puntual que pueda afectar al listado de controles del SGSI, incluyendo la modificación del alcance del SGSI o bien, la ineficacia o ineficiencia de los existentes.

20. DOCUMENTACIÓN DE REFERENCIA

- ISO/IEC 27001:2013
- ISO/IEC 27002:2013



ANEXO F. FASE 2 - SGSI-04 PROCEDIMIENTO DE REVISIÓN POR DIRECCIÓN

	SGSI – 01	Código: SGSI_04
	SGSI-04 Procedimiento de Revisión por Dirección	Versión: 1
		Vigente desde: 01/01/2016

HOJA DE CONTROL

TÍTULO	PROCEDIMIENTO DE REVISIÓN POR DIRECCIÓN		
CÓDIGO	SGSI – 04		
AUTOR	Equipo de innovación y seguridad de la información		
CLASIFICACIÓN	Uso interno	**TIPO DOCUMENTO**	
VERSIÓN	1.0	**FECHA VERSIÓN**	01/12/2015
REVISADO POR:	Resp. sistemas / TI	**FECHA REVISIÓN**	15/12/2015
APROBADO POR:	Comité seguridad	**FECHA**	31/12/2015

ÍNDICE

21. INTRODUCCIÓN

PARQUES NACIONALES NATURALES DE COLOMBIA consideró oportuno definir el alcance que deben tener las revisiones del SGSI llevadas a cabo por el Comité de Gestión, a fin de mantener un ciclo de mejora continua, así como la adecuación y la eficacia del SGSI.

22. OBJETIVOS

En este procedimiento se describe la metodología de revisión del SGSI, a fin de promover su continua adecuación.

23. ALCANCE

Atendiendo al objetivo citado, el presente documento es aplicable al alcance del SGSI de PARQUES NACIONALES NATURALES DE COLOMBIA.

24. REVISIÓN DEL SGSI

Se diferencian dos tipos de revisiones del SGSI:

Revisiones periódicas

Anualmente se llevará a cabo una revisión global del SGSI de PARQUES NACIONALES NATURALES DE COLOMBIA, realizando las siguientes acciones de manera sistemática:

- Revisar y adecuar la Política de Seguridad, alcance y estrategia.
- Analizar los cambios organizativos, tecnológicos, regulatorios, etc. Con impacto directo sobre el SGSI.
- Revisar el cumplimiento de los objetivos.
- Plantear los objetivos de los siguientes períodos, así como las acciones que se consideren necesarias.
- Comprobar el grado de eficiencia y adecuación del SGSI, para garantizar su correcto funcionamiento.
- Revisar los resultados de las auditorías previas y los indicadores.
- Hacer seguimiento de los resultados de la última revisión global de los sistemas.
- Analizar el estado de las acciones correctivas, preventivas y de las no conformidades.
- Estudiar las oportunidades de mejora detectadas y los recursos necesarios para su implementación.
- Revisar el Análisis de Riesgos, la Declaración de aplicabilidad, de los resultados y tratamientos.
- Todas las revisiones efectuadas serán debidamente documentadas y cuentan con un acta a modo de registro para recoger evidencias de los temas tratados y los acuerdos establecidos.

Para llevar a cabo la revisión se podrá consultar la documentación necesaria, tales como:

- Los resultados de las auditorías y revisiones previas del SGSI.
- El seguimiento de las acciones derivadas de las revisiones previas.
- El estado de las acciones preventivas / correctivas del SGSI.
- Los resultados de las medidas de eficacia del SGSI.
- Las vulnerabilidades / amenazas no resueltas en la evaluación de riesgos previa.
- Los comentarios de las partes interesadas y recomendaciones de mejora.
- Cualquier cambio, ya fuera interno o externo, que pueda afectar al SGSI.

- Las técnicas, productos o procedimientos que podrían utilizarse para la mejora del comportamiento y eficacia del SGSI.

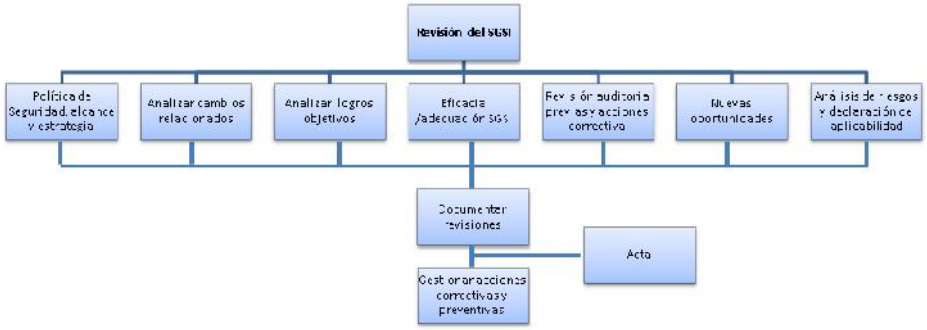
Los resultados de la revisión se recogerán en el acta pertinente, incluyendo:

- Mejora de la eficacia del SGSI.
- Actualización de la Evaluación de Riesgos, Declaración de aplicabilidad y propuesta de tratamiento de riesgos asociado.
- Modificación de los procedimientos y controles relativos a la Seguridad de la
- Información, en su caso, a fin de responder a sucesos internos / externos que puedan afectar al SGSI, incluyendo: requisitos de negocio, de Seguridad de la
- Información, procesos de negocio que afecten a los requisitos de negocios existentes, requisitos legales, obligaciones contractuales y niveles de riesgo.
- Necesidades de recursos.
- Mejora en el modo de medir la eficacia del SGSI.
- Una vez revisadas a nivel interno, las actas serán publicadas, considerando en este momento su aprobación.

Revisiones específicas

Las revisiones específicas tienen como objetivo conocer de qué manera afecta a un suceso en el estado global del SGSI y determinar los cambios, las modificaciones y las iniciativas necesarias. Estas revisiones se realizarán por petición de alguno de los miembros del Comité de Seguridad.

Flujograma del proceso de revisión del SGSI



25. DOCUMENTACIÓN DE REFERENCIA

- ISO/IEC 27001:2013
- ISO/IEC 27002:2013

ANEXO F. FASE 2 - SGSI-04 PROCEDIMIENTO DE REVISIÓN POR DIRECCION

ANEXO G. FASE 2 - SGSI-05 GESTIÓN DE ROLES Y RESPONSABILIDADES

	SGSI – 01	Código: SGSI_05
	SGSI-05	Versión: 1
	Gestión de Roles y Responsabilidades	Vigente desde: 01/01/2016

HOJA DE CONTROL

TÍTULO	GESTIÓN DE ROLES Y RESPONSABILIDADES		
CÓDIGO	SGSI – 05		
AUTOR	Equipo de innovación y seguridad de la información		
CLASIFICACIÓN	Uso interno	**TIPO DOCUMENTO**	
VERSIÓN	1.0	**FECHA VERSIÓN**	01/12/2015
REVISADO POR:	Resp. sistemas / TI	**FECHA REVISIÓN**	15/12/2015
APROBADO POR:	Comité seguridad	**FECHA**	31/12/2015

ÍNDICE

26. INTRODUCCIÓN

PARQUES NACIONALES NATURALES DE COLOMBIA ha considerado oportuno definir los perfiles de los puestos de trabajo que intervienen en SGSI incluyendo sus funciones y responsabilidades en materia de seguridad.

27. OBJETIVOS

En este procedimiento se definen y documentan los roles y responsabilidades del personal del SGSI, atendiendo a Política de Seguridad de la información de PARQUES NACIONALES NATURALES DE COLOMBIA

28. ALCANCE

Atendiendo al objetivo citado, el presente documento es aplicable dentro del alcance del SGSI de PARQUES NACIONALES NATURALES DE COLOMBIA

29. ROLES Y RESPONSABILIDADES

• Definición de Perfiles y comunicación de Roles

La definición de roles y responsabilidades del personal que trabaja con el SGSI de PARQUES NACIONALES NATURALES DE COLOMBIA se hace en base a:

- La Política de Seguridad.
- La protección de activos frente a accesos no autorizados, revelación, modificación o destrucción no autorizada.
- La ejecución de procesos o actividades particulares relacionadas con el SGSI.
- Garantizar que las responsabilidades se asignan al personal involucrado en el SGSI para las acciones necesarias.
- Informar sobre los acontecimientos que afecten el SGSI.

Los roles y responsabilidades relacionadas con el SGSI se comunicarán siempre por escrito al personal involucrado en el SGSI.

• Responsabilidades

La composición y asignación de responsabilidades del comité de seguridad se detallan en el documento 'Comité de Seguridad del SGSI'.

A continuación, se describen las responsabilidades asignadas a los responsables del SGSI:

Coordinar con el Comité de Seguridad del SGSI los objetivos, estrategias y políticas de seguridad.

- Implantar el SGSI.
- Realizar un Análisis de Riesgos y llevar a cabo la Gestión del Riesgo.
- Seleccionar los objetivos y controles a implantar.
- Preparar y actualizar la Declaración de Aplicabilidad.
- Registrar los incidentes de seguridad.
- Velar por la divulgación de las responsabilidades de los usuarios sobre el uso aceptable de los activos de información.
- Reportar al Comité de Seguridad los aspectos relacionados con la seguridad.
- Convocar las reuniones con el Comité de Seguridad, levantando acta de las mismas.

- Coordinar, dinamizar y asegurar la implantación de las acciones definidas en el Plan de acción.
- Gestionar las revisiones de seguridad.
- Comprobar la adecuación a la norma.

El SGSI dispone del documento 'Mapa de puestos de trabajo donde se indican de manera concreta las tareas asociadas a las diferentes responsabilidades indicadas.

Paralelamente las responsabilidades de las áreas de apoyo en materia del SGSI son liderar y supervisar la implantación los requerimientos derivados del SGSI en su área.

Finalmente, las responsabilidades asociadas a los perfiles técnicos involucrados en el SGSI son desarrollar e implementar en su área los requerimientos derivados del SGSI.

30. DOCUMENTACIÓN DE REFERENCIA

- ISO/IEC 27001:2013
- ISO/IEC 27002:2013

ANEXO H. FASE 2 - SGSI-05B COMITÉ DE SEGURIDAD DEL SGSI

	SGSI – 01	Código: SGSI_05B
	SGSI-05B	Versión: 1
	Comité de Seguridad del SGSI	Vigente desde: 01/01/2016

HOJA DE CONTROL

TÍTULO	Comité de Seguridad del SGSI		
CÓDIGO	SGSI – 05B		
AUTOR	Equipo de innovación y seguridad de la información		
CLASIFICACIÓN	Uso interno	**TIPO DOCUMENTO**	
VERSIÓN	1.0	**FECHA VERSIÓN**	01/12/2015
REVISADO POR:	Resp. sistemas / TI	**FECHA REVISIÓN**	15/12/2015
APROBADO POR:	Comité seguridad	**FECHA**	31/12/2015

ÍNDICE

31. INTRODUCCIÓN

PARQUES NACIONALES NATURALES DE COLOMBIA considera que la correcta definición y asignación de las responsabilidades y roles de gestión de la seguridad se convierte en la base necesaria para asegurar los procesos de la entidad, garantizando la integridad, disponibilidad y confidencialidad de los activos, cumpliendo con el marco legal vigente y respetando las directrices, normas y procedimientos establecidos.

32. OBJETIVOS

En este procedimiento se define la composición, las principales funciones y la organización del Comité de Seguridad del SGSI, como órgano principal para el tratar aspectos estratégicos de la gestión de la seguridad de la información de manera coordinada y eficaz.

33. ALCANCE

El personal que interviene en el Comité de Seguridad del SGSI y personal con responsabilidades dentro de los procesos comprendidos en el alcance del SGSI.

34. COMITÉ DE SEGURIDAD DEL SGSI

- Composición:

Atendiendo a la composición del Comité de Seguridad este estará formado por miembros permanentes, definidos en la Política de Seguridad, y miembros invitados que podrán participar en las reuniones del Comité con carácter temporal, con objeto de tratar aspectos relacionados con las áreas de su responsabilidad.

Los responsables permanentes, a excepción del director general, podrán delegar en otras personas de su confianza para que los representen en las reuniones del Comité.

- Objetivos

El objetivo principal del comité de seguridad es proporcionar evidencia clara, visible y demostrable del soporte y compromiso de la Dirección de PARQUES NACIONALES NATURALES DE COLOMBIA por el establecimiento, implantación, revisión y mejora continua del SGSI, promocionando a su vez la seguridad dentro de la entidad mediante una dirección, coordinación y un compromiso demostrado, proporcionando un apoyo visible a las iniciativas de seguridad e involucrando a las áreas relacionadas en tareas de seguridad.

- Funciones

Atendiendo a los objetivos citados, a continuación, se listan las funciones principales del Comité de Seguridad:

- Establecer, implantar, revisar y mejorar el SGSI mediante la aprobación y aceptación de las acciones y sus resultados, según las pautas definidas en el 'Procedimiento de Revisión del SGSI'.
- promocionar y velar por el cumplimiento de la Política de Seguridad de la Información, velando por su cumplimiento.
- Identificar los objetivos de Seguridad de la Información, asegurando su concordancia con los requisitos de PARQUES NACIONALES NATURALES DE COLOMBIA y su integración con los procesos críticos.

- Velar por la resolución de las no conformidades detectadas dentro del alcance del SGSI y proponer acciones correctivas,
- Suministrar los recursos internos y externos para garantizar el correcto funcionamiento del SGSI.

Concretamente, sus funciones específicas son:

- Definición, revisión y aprobación de los objetivos, estrategia y Política de Seguridad.
- Definición, revisión y aprobación del alcance del SGSI.
- Aprobación de la 'Declaración de aplicabilidad'.
- Revisión del el Análisis de Riesgos.
- Definición, revisión, aprobación y seguimiento del Plan de Gestión del Riesgo.
- Coordinación de la implantación de los controles de seguridad de la información.
- Aprobación de la asignación de funciones y responsabilidades específicas de seguridad de la información del SGSI.
- Coordinación y realización de las revisiones del SGSI.
- Definición de los indicadores de seguridad, así como el seguimiento de los resultados para la toma de decisiones oportunas.
- Revisión de la eficacia de la implantación de la Política de Seguridad, a través de la revisión de los indicadores definidos.
- Aprobación de la Normativa de Seguridad del SGSI.
- Aprobación del calendario de auditorías del SGSI.
- Coordinación de acciones para prevenir No Conformidades e incidencias.
- Aprobación del plan anual de formación atento a las necesidades detectadas.

- Reuniones

Para cumplir con sus funciones y responsabilidades, el comité de seguridad se reunirá (Ya sea física o virtualmente) cada 6 meses de manera sistemática para analizar posibles cambios relevantes en torno a los procesos comprendidos dentro del alcance del SGSI o sus procesos relacionados, así como por incidentes o nuevas iniciativas de seguridad.

Paralelamente, cualquier miembro del comité podrá solicitar alguna reunión extraordinaria si lo considera oportuno, como respuesta a incidentes, cambios organizativos o cualquier aspecto que pueda afectar al SGSI.

De forma anual, se realizará una revisión global del SGSI, atendiendo al procedimiento de revisión del SGSI.

35. DOCUMENTACIÓN DE REFERENCIA

- ISO/IEC 27001:2013
- ISO/IEC 27002:2013

ANEXO H. FASE 2 - SGSI-05B COMITÉ DE SEGURIDAD DEL SGSI

ANEXO I. FASE 2 - SGSI-06 DECLARACIÓN DE APLICABILIDAD

	SGSI – 01	Código: SGSI_06
	SGSI-06	Versión: 1
	Declaración de Aplicabilidad	Vigente desde: 01/01/2016

HOJA DE CONTROL

TÍTULO	Declaración de Aplicabilidad		
CÓDIGO	SGSI – 06		
AUTOR	Equipo de innovación y seguridad de la información		
CLASIFICACIÓN	Uso interno	**TIPO DOCUMENTO**	
VERSIÓN	1.0	**FECHA VERSIÓN**	01/12/2015
REVISADO POR:	Resp. sistemas / TI	**FECHA REVISIÓN**	15/12/2015
APROBADO POR:	Comité seguridad	**FECHA**	31/12/2015

ÍNDICE

36. INTRODUCCIÓN

La declaración de aplicabilidad incluye todos los controles de seguridad establecidos en PARQUES NACIONALES NATURALES DE COLOMBIA con el detalle de su aplicabilidad, estado y documentación relacionada.

37. OBJETIVOS

El objetivo de la declaración de aplicabilidad es especificar los controles de seguridad de acuerdo con la normativa que aplica PARQUES NACIONALES NATURALES DE COLOMBIA.

38. ALCANCE

Atendiendo al objetivo ciudad, el presente documento es aplicable dentro del alcance del SGSI de PARQUES NACIONALES NATURALES DE COLOMBIA.

39. DECLARACIÓN DE APLICABILIDAD

La siguiente tabla recoge la aplicabilidad de los controles, el estado y su documentación relacionada:

ITEM	CONTROL	APLICA	ESTADO	DOCUMENTACIÓN ASOCIADA
5	**POLÍTICA DE SEGURIDAD**			
5.1	**Política de seguridad de la información**			
5.1.1	Documento de política de seguridad de la información	SI	proceso definido	Política de seguridad de la información
5.1.2	Revisión de la política de seguridad de la información	SI	proceso definido	Política de seguridad de la información // Revisión del SGSI por el Comité de Seguridad // Comité de Seguridad
6	**ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN**			
6.1	**organización interna**			
6.1.1	Roles y responsabilidades de la seguridad de la información	SI	proceso definido	Política de seguridad
6.1.2	Segregación de tareas	SI	proceso definido	Política de procesos operativos
6.1.3	Contacto con las autoridades	SI	reproducible	buenas prácticas
6.1.4	Contacto con grupos de especial interés	SI	Incial / ad-hoc	procedimientos inexistentes

6.1.5	Seguridad de la información en la gestión de proyectos	SI	Incial / ad-hoc	procedimientos inexistentes
6.2	Dispositivos portátiles y teletrabajo			
6.2.1.	Política de uso de dispositivos en movilidad	SI	proceso definido	Política de teletrabajo
6.2.2	teletrabajo	SI	proceso definido	Política de teletrabajo
7	**SEGURIDAD DE LOS RECURSOS HUMANOS**			
7.1	**Antes de la contratación**			
7.1.1	Investigación de antecedentes	SI	Incial / ad-hoc	procedimientos inexistentes
7.1.2	Términos y condiciones de la contratación	SI	proceso definido	código ético
7.2	Durante la contratación			
7.2.1	Responsabilidades de dirección	SI	proceso definido	Roles y responsabilidades // código ético // Política de seguridad
7.2.2	Concienciación, formación y capacitación en seguridad	SI	Gestionado y medible	Política de seguridad
7.2.3	proceso disciplinario	SI	inexistente	Carencia de ningún proceso
7.3	Final contratación o cambio puesto trabajo			
7.3.1	Responsabilidad del cambio	SI	proceso definido	Política de seguridad
8	**GESTIÓN DE ACTIVOS**			
8.1	**Responsabilidad sobre los activos**			
8.1.1	Inventario de activos	SI	reproducible	buenas prácticas
8.1.2	Propiedad de los activos	SI	Incial / ad-hoc	procedimientos inexistentes
8.1.3	Uso aceptable de los activos	SI	proceso definido	Política de Seguridad
8.1.4	Devolución de activos	SI	proceso definido	Política de devolución de activos
8.2.	Clasificación de la información			
8.2.1	Directrices de la clasificación	SI	Incial / ad-hoc	procedimientos inexistentes
8.2.2	Etiquetado y manipulación de la información	SI	reproducible	buenas prácticas
8.3.2	Manipulación de activos	SI	reproducible	buenas prácticas
8.3.	Gestión de soportes de almacenamiento			
8.3.1	Gestión de soportes extraíbles	SI	proceso definido	Política de gestión de soportes
8.3.2	Eliminación de soportes	SI	proceso definido	Política de gestión de soportes
8.3.3	Soportes físicos en tránsito	SI	reproducible	buenas prácticas

9	**CONTROL DE ACCESO**			
9.1	**Requisitos de negocio para el control de acceso**			
9.1.1	Política de control de acceso	SI	reproducible	buenas prácticas
9.1.2	Control de acceso a redes y servicios asociados	SI	reproducible	buenas prácticas
9.2	Gestión de acceso del usuario			
9.2.1	Gestión de altas y bajas en los registros de usuario	SI	proceso definido	Política de usuarios y contraseñas
9.2.2	Gestión de los derechos de acceso asignados	SI	proceso definido	Política de usuarios y contraseñas
9.2.3	Gestión de los derechos de acceso con privilegios especiales	SI	reproducible	buenas prácticas
9.2.4	Gestión de la información confidencial de autenticación	SI	reproducible	buenas prácticas
9.2.5	Revisión de los derechos de acceso de los usuarios	SI	Incial / ad-hoc	procedimientos inexistentes
9.2.6	Retirada o adaptación de los derechos de acceso	SI	reproducible	buenas prácticas
9.3	Responsabilidades del usuario			
9.3.1	Uso de la información confidencial para la autenticación	SI	proceso definido	Política de uso de servicios
9.4	Control de acceso a los sistemas			
9.4.1	Restricción del acceso a la información	SI	proceso definido	Política de usuarios y contraseñas
9.4.2	Procedimientos seguros de inicio de sesión	SI	proceso definido	Política de usuarios y contraseñas
9.4.3	Gestión de contraseñas de usuario	SI	proceso definido	Política de usuarios y contraseñas
9.4.4	Uso de herramientas de administración de sistemas	SI	proceso definido	Política de procesos operativos
9.4.5	Control de acceso al código fuente de los programas	SI	proceso definido	Política de procesos operativos
10	**CIFRADO**			
10.1	**controles criptográficos**			
10.1.1	Política de uso de los controles criptográficos	SI	inexistente	Carencia de ningún proceso
10.1.2	Gestión de contraseñas	SI	inexistente	Carencia de ningún proceso
11	**SEGURIDAD FÍSICA Y DEL ENTORNO**			
11.1	**áreas seguras**			
11.1.1	Perímetro de seguridad	SI	Gestionado y medible	Política de seguridad física
11.1.2	Controles físicos de entrada	SI	Gestionado y medible	Política de seguridad física

11.1.3	Seguridad de las oficinas	SI	Gestionado y medible	Política de seguridad física
11.1.4	Protección contra amenazas externas y ambientales	SI	Gestionado y medible	Política de seguridad física
11.1.5	Trabajo en áreas seguras	NO		
11.1.6	Áreas de acceso al público y carga y descarga	NO		
11.2	Seguridad de los equipos			
11.2.1	Emplazamiento y seguridad de los equipos	SI	proceso definido	Política de instalaciones
11.2.2	Instalaciones de suministro	SI	proceso definido	Política de instalaciones
11.2.3	Seguridad del cableado	SI	reproducible	buenas prácticas
11.2.4	Mantenimiento de los equipos	SI	Gestionado y medible	
11.2.5	Salida de activos fuera de las instalaciones	SI	proceso definido	Política de Seguridad
11.2.6	Seguridad de los equipos fuera de las instalaciones	SI	Gestionado y medible	
11.2.7	Reutilización o retirada segura de los equipos	SI	proceso definido	Política de instalaciones
11.2.8	Equipo informático de usuario desatendido	SI	proceso definido	Política de usuarios y contraseñas
11.2.9	Política del puesto de trabajo y bloqueo de pantalla	SI	proceso definido	Política de usuarios y contraseñas
12	**SEGURIDAD EN LA OPERATIVA**			
12.1	**áreas seguras**			
12.1.1	Responsabilidad y procedimientos de operación	SI	proceso definido	Política de procesos operativos
12.1.2	Documentación de los procedimientos de operación	SI	proceso definido	Política de procesos operativos
12.1.3	Gestión de cambios	SI	proceso definido	Política de procesos operativos
12.1.4	Gestión de capacidades	SI	reproducible	buenas prácticas
12.1.5	Separación de entornos de desarrollo, pruebas y producción	SI	proceso definido	Política de procesos operativos
12.2	Protección contra código malicioso			
12.2.1	Controles contra código malicioso	SI	proceso definido	Política de antivirus
12.3	Copias de seguridad			
12.3.1	Copias de seguridad de la información	SI	Gestionado y medible	
12.4	Registro de actividad y supervisión			
12.4.1	Registro y gestión de eventos	SI	reproducible	buenas prácticas

12.4.2	Protección de los registros de información	SI	reproducible	buenas prácticas
12.4.3	Registros de actividad del administrador y operador del sistema	SI	reproducible	buenas prácticas
12.4.4	Sincronización de relojes	SI	proceso definido	Sincronización de relojes
12.5	Control del software de explotación			
12.5.1	Instalación de software a sistemas de producción	SI	reproducible	buenas prácticas
12.6	Gestión de la vulnerabilidad técnica			
12.6.1	Gestión de las vulnerabilidades técnicas	SI	proceso definido	Política de gestión de incidentes del SGSI
12.6.2	Restricciones en la instalación de software	SI	proceso definido	Restricciones cambios paquetes SW
12.7	Consideraciones de las auditorías de los sistemas de información			
12.7.1	Controles de auditoría de los sistemas de información	SI	reproducible	buenas prácticas
13	**SEGURIDAD EN LAS COMUNICACIONES**			
13.1	**Gestión de seguridad en las redes**			
13.1.1	Controles en la red	SI	proceso definido	Política de redes
13.1.2	Mecanismos de seguridad asociados a los servicios en red	SI	proceso definido	Política de redes
13.1.3	Segregación de redes	SI	inexistente	Carencia de ningún proceso
13.2	Intercambio de información con partes externas			
13.2.1	Políticas y procedimientos de intercambio de la información	SI	reproducible	buenas prácticas
13.2.2	Acuerdos de intercambio	SI	reproducible	buenas prácticas
13.2.3	mensajería electrónica	SI	reproducible	buenas prácticas
13.2.4	Acuerdos de confidencialidad y secreto	SI	reproducible	buenas prácticas
14	**ADQUISICIÓN, DESENVOLUPAMENTEMANTENIMENTDLOSSISTEM SE DE INFORMACION**			
14.1	**Requisitos de seguridad de los sistemas de información**			
14.1.1	Análisis y especificación de los requisitos de seguridad	SI	Incial / ad-hoc	procedimientos inexistentes
14.1.2	Seguridad de las comunicaciones en servicios accesibles para redes públicas	SI	reproducible	buenas prácticas
14.1.3	Protección de las transacciones por redes telemáticas	SI	reproducible	buenas prácticas
14.2	Seguridad en los procesos de desarrollo y apoyo			
14.2.1	Política de desarrollo seguro de software	SI	proceso definido	Política de procesos operativos
14.2.2	Procedimientos de control de cambios en los sistemas	SI	proceso definido	Política de procesos operativos

14.2.3	Revisión técnica de las aplicaciones después de efectuar cambios en el sistema operativo	SI	reproducible	buenas prácticas
14.2.4	Restricciones a los cambios en los paquetes de software	SI	reproducible	buenas prácticas
14.2.5	Uso de principios de ingeniería en protección de sistemas	SI	proceso definido	Política de procesos operativos
14.2.6	Seguridad en entornos de desarrollo	SI	proceso definido	Política de procesos operativos
14.2.7	Externalización del desarrollo software	no		
14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas	SI	proceso definido	Política de procesos operativos
14.2.9	Pruebas de aceptación	SI	proceso definido	Política de procesos operativos
14.3	Datos de prueba			
14.3.1	Protección de los datos de prueba	SI	proceso definido	Política de procesos operativos
15	**RELACIONES CON PROVEEDORES**			
15.1	**Seguridad de la información en las relaciones con proveedores**			
15.1.1	Política de seguridad de la información para proveedores	SI	reproducible	buenas prácticas
15.1.2	Tratamiento del riesgo dentro de los acuerdos de suministradores	SI	reproducible	buenas prácticas
15.1.3	Cadena de suministro en tecnologías de la información y las comunicaciones	SI	reproducible	buenas prácticas
15.2	Gestión de la prestación del servicio de los proveedores			
15.2.1	Supervisión y revisión de los servicios prestados por los terceros	SI	reproducible	buenas prácticas
15.2.2	Gestión de cambios en los servicios de terceros	SI	reproducible	buenas prácticas
16	**GESTIÓN DE INCIDENTES**			
16.1	**Gestión de incidentes de seguridad y mejoras**			
16.1.1	Responsabilidad y procedimientos	SI	Gestionado y medible	
16.1.2	Notificación de los eventos de seguridad de la información	SI	proceso definido	Política de gestión de incidentes del SGSI
16.1.3	Notificación de los puntos débiles de la seguridad	SI	proceso definido	Política de gestión de incidentes del SGSI
16.1.4	Valoración de los eventos de seguridad de la información y toma de decisiones	SI	proceso definido	Política de gestión de incidentes del SGSI
16.1.5	Respuesta a los incidentes de seguridad	SI	proceso definido	Política de gestión de incidentes del SGSI
16.1.6	Aprendizaje de los incidentes de seguridad de la información	SI	Gestionado y medible	
16.1.7	Recopilación de evidencias	SI	proceso definido	Política de gestión de incidentes del SGSI
17	**ASPECTOS DE LA SI EN LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO**			

17.1	**Continuidad de la seguridad de la información**			
17.1.1	Planificación de la continuidad de la seguridad de la información	SI	Incial / ad-hoc	procedimientos inexistentes
17.1.2	Implantación de la continuidad de la seguridad de la información	SI	Incial / ad-hoc	procedimientos inexistentes
17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	SI	inexistente	Carencia de ningún proceso
17.2	redundancias			
17.2.1	Actividades de control del riesgo	SI	Incial / ad-hoc	procedimientos inexistentes
18	**CUMPLIMIENTO**			
18.1	**Continuidad de la seguridad de la información**			
18.1.1	Identificación de la legislación aplicable	SI	reproducible	buenas prácticas
18.1.2	Derechos de la PI	SI	Incial / ad-hoc	procedimientos inexistentes
18.1.3	Protección de los registros de la organización	SI	reproducible	buenas prácticas
18.1.4	Protección de los datos y privacidad de la información personal	SI	inexistente	Carencia de ningún proceso
18.1.5	Regulación de los controles criptográficos	SI	inexistente	Carencia de ningún proceso
18.2	Revisiones de la seguridad de la información			
18.2.1	Revisión independiente de la seguridad de la información	SI	reproducible	buenas prácticas
18.2.2	Cumplimiento de las políticas y normas de seguridad	SI	proceso definido	Política de seguridad
18.2.3	Comprobación de cumplimiento	SI	proceso definido	Política de seguridad

40. DOCUMENTACIÓN DE REFERENCIA

- ISO/IEC 27001:2013
- ISO/IEC 27002:2013

ANEXO I. FASE 2 - SGSI-06 DECLARACIÓN DE APLICABILIDAD

ANEXO J. FASE 2 - SGSI-07 METODOLOGÍA DEL ANÁLISIS DE RIESGOS

	SGSI – 01	Código: SGSI_07
	SGSI-07	Versión: 1
	Metodología del Análisis de Riesgos	Vigente desde: 01/01/2016

HOJA DE CONTROL

TÍTULO	METODOLOGÍA DEL ANÁLISIS DE RIESGOS		
CÓDIGO	SGSI – 07		
AUTOR	Equipo de innovación y seguridad de la información		
CLASIFICACIÓN	Uso interno	**TIPO DOCUMENTO**	
VERSIÓN	1.0	**FECHA VERSIÓN**	01/12/2015
REVISADO POR:	Resp. sistemas / TI	**FECHA REVISIÓN**	15/12/2015
APROBADO POR:	Comité seguridad	**FECHA**	31/12/2015

ÍNDICE

41. INTRODUCCIÓN

El análisis de riesgos es el elemento base para establecer un SGSI, ya que, a partir de sus resultados, se tomarán las decisiones pertinentes para su gestión.

- Se entiende como riesgo la estimación del grado de exposición de un activo a que una amenaza se materialice sobre él, causando unos daños de terminados en la organización. En definitiva, el riesgo indica lo que podría pasar a los activos si no se protegen adecuadamente.

- Las amenazas son sucesos que pueden provocar un incidente produciendo daños materiales o inmateriales en los activos.

- Las vulnerabilidades son las debilidades de tienen los activos y que pueden ser aprovechadas por una amenaza.

42. OBJETIVOS

El análisis de riesgos persigue diferentes objetivos como describir los elementos que intervienen en la metodología y las relaciones entre ellos, establecer un método sencillo y preciso para obtener el nivel del riesgo soportado por cada activo y proceso, etc.

Así mismo definir una metodología de evaluación de los riesgos apropiada para los procesos que intervienen en el SGSI, alineada con los objetivos de negocio y con los requisitos legales, regulatorios y reglamentarios.

43. ALCANCE

Atendiendo al objetivo citado, el presente documento es aplicable al alcance del SGSI de PARQUES NACIONALES NATURALES DE COLOMBIA.

44. METODOLOGÍA DEL ANÁLISIS DE RIESGOS

El análisis de riesgos de PARQUES NACIONALES NATURALES DE COLOMBIA consiste en:

- Identificar los riesgos de seguridad.
- Determinar su magnitud.
- Identificar las áreas que requieren implantar salvaguardias.

Gracias a este análisis PARQUES NACIONALES NATURALES DE COLOMBIA podrá conocer el impacto económico de un fallo de seguridad y la probabilidad realista de que se produzca ésta.

Entre las premisas del análisis de riesgos se encuentra:

- Cubrir las necesidades de seguridad de la organización teniendo en cuenta los recursos económicos y humanos con los que ésta cuenta.
- Aportar objetividad los criterios que soportan la seguridad, ya que se centran en proteger los activos más críticos.
- Permite a la organización gestionar los riesgos por sí misma.
- Dar soporte a la toma de decisiones a partir de los riesgos propios.

El análisis de riesgos utiliza unos criterios claramente definidos que se pueden reproducir en ocasiones sucesivas para ir comparando el nivel de riesgo de la organización a medida que se va mejorando su SGSI.

El análisis de riesgos se realizará a partir del inventario de activos de la entidad. A continuación, identificarán las amenazas que podrían afectar. Realizando una valoración en función del impacto que la amenaza puede causar al activo en caso de que se materialice. Seguidamente se analizarán las vulnerabilidades de los activos identificados y se realizará una valoración de las mismas.

Una vez analizados los activos, las amenazas y las vulnerabilidades que pueden afectar a los activos, se llevará a cabo un análisis de las salvaguardias o medidas de seguridad ya implementadas en la organización.

Con todos estos datos se llevará a cabo un estudio del riesgo y del impacto de todas estas variables sobre los diferentes activos.

Como resultado PARQUES NACIONALES NATURALES DE COLOMBIA conocerá el nivel de riesgo al que se expone y podrá tomar las medidas pertinentes.

La metodología empleada será Magerit.

45. DOCUMENTACIÓN DE REFERENCIA

- ISO/IEC 27001:2013
- ISO/IEC 27002:2013

ANEXO J. FASE 2 - SGSI-07 METODOLOGÍA DEL ANÁLISIS DE RIESGOS

ANEXO K. FASE 3 - CONSOLIDADO TABLAS

Valoración Pérdida del activo

IMPACTO		Criterio	VALOR	
MA	Muy alto	Daño extremadamente grave	100%	10
A	Alto	Daño muy grave	75%	9
M	Medio	Daño grave	50%	6-8
B	Bajo	Daño importante	20%	3-5
MB	Muy bajo	Daño menor	5%	1-2
NA	Despreciable	Irrelevante a efectos prácticos	0%	0

Vulnerabilidad		Rango	Valor
FE	Frecuencia Extrema	cada día	100
FA	Frecuencia Alta	Cada 30 dias	10
FM	Frecuencia Media	Cada 3 meses	1
FB	Frecuencia Baja	Cada 6 meses	0.1
FMB	Frecuencia Muy Baja	Cada 12 meses	0.01

INVENTARIO Y VALORACION DE LOS ACTIVOS											
TIPO	**ÁMBITO**	**Activo**	**ID**	**UBICACIÓN**	**VALOR**	**DEPENDENCIAS**	**CRITICIDAD/DIMEN**				
							Autenticidad	**C**onfidencialidad	**I**ntegridad	**D**isponibilidad	**A**udibilidad
L	Instalaciones	Rack principal (CPD a efectos prácticos)	[L1]	NIVEL CENTRAL	MA	[AUX1][AUX2]	8	9	10	10	8
		Archivo	[L2]	NIVEL CENTRAL	A	-	8	9	9	7	6
		Rack secundario (CPD a efectos prácticos)	[L3]	TERRITORIALES	MA	[AUX1][AUX2]	8	9	10	10	8
AUX		Aire acondicionado en sala de asistentes donde se encuentra el Rack	[AUX1]	NIVEL CENTRAL	MB	[AUX4]-	0	0	0	8	0
		UPS Estabilizador para todo el rack.	[AUX2]	NIVEL CENTRAL	MB	[AUX4]	0	0	0	8	0
		Cableado LAN	[AUX3]	NIVEL CENTRAL	MB	-	0	0	0	10	0
		Cableado suministro eléctrico	[AUX4]	NIVEL CENTRAL	B	-	0	0	0	10	0
		Aire acondicionado en sala de asistentes	[AUX5]	TERRITORIALES	MB	[AUX8]-	0	0	0	8	0
		UPS Estabilizador para todo el rack.	[AUX6]	TERRITORIALES	MB	[AUX8]	0	0	0	8	0
		Cableado LAN	[AUX7]	TERRITORIALES	MB	-	0	0	0	10	0
		Cableado suministro eléctrico	[AUX8]	TERRITORIALES	B	-	0	0	0	10	0
COM	Comuniciones	Router fibra NETLAN Telefónica, une las sedes y da conexión a Internet	[COM1]	NIVEL CENTRAL	MB	[AUX2]	7	8	9	10	6
		Router fibra RAVEC Telefónica, une las sedes y da conexión a Internet	[COM2]	TERRITORIALES	MB	[AUX6]	7	8	9	10	6

HW	Hardware	Centralita IP + switch propio	[HW1]	NIVEL CENTRAL	MB	[AUX4]	5	7	8	8	5
		Fax	[HW2]	NIVEL CENTRAL	MB	[AUX4]	5	7	6	7	5
		10 PC ofimática	[HW3]	NIVEL CENTRAL	MB	[AUX3] [AUX4]	4	6	6	7	5
		1 Servidor principal	[HW4]	NIVEL CENTRAL	M	[AUX3][AUX2][AUX1][AUX4]	9	9	10	10	8
		2 impresoras red	[HW5]	NIVEL CENTRAL	B	[AUX3] [AUX4]	3	4	5	5	4
		1 impresora local	[HW6]	NIVEL CENTRAL	MB	[AUX4]	3	4	5	3	4
		1 switch Gigabit LAN	[HW7]	NIVEL CENTRAL	MB	[AUX3] [AUX4]	4	3	3	10	4
		3 Escáner local USB	[HW8]	NIVEL CENTRAL	MB	[AUX4]	3	2	5	5	2
		Centralita IP + switch propio	[HW9]	TERRITORIALES	MB	[AUX8]	5	7	8	8	5
		Fax	[HW10]	TERRITORIALES	MB	[AUX8]	5	7	6	7	5
		5 PC ofimática	[HW11]	TERRITORIALES	MB	[AUX7] [AUX8]	4	6	6	7	5
		1 Servidor de respaldo (BACKUP remoto)	[HW12]	TERRITORIALES	M	[AUX5][AUX6][AUX7] [AUX8]	9	9	10	10	8
		2 impresoras red	[HW13]	TERRITORIALES	B	[AUX7] [AUX8]	3	4	5	5	4
		1 switch 100mbs LAN	[HW14]	TERRITORIALES	MB	[AUX7] [AUX8]	4	3	3	10	4
		3 Escáner local USB	[HW15]	TERRITORIALES	MB	[AUX8]	3	2	5	5	2
		1 laptop privado siendo utilizado dentro de FINALIN S.L.	[HW16]	TERRITORIALES	MB	[AUX7][AUX8]	5	8	8	8	3
MEDIA	Media	Disco duro externo USB para backup redundante local.	[MEDIA1]	NIVEL CENTRAL	MB	-	7	8	8	7	7
		Archivo pólizas en papel	[MEDIA2]	NIVEL CENTRAL	M	-	8	8	8	8	8
DATOS	Datos	Código fuente (webs + programa Decesos)	[DATOS1]	NIVEL CENTRAL	M		7	8	8	8	7
		Backup secundario en ext HD	[DATOS2]	NIVEL CENTRAL	A	[HW4]	8	9	10	9	8
		Datos SegurLif (cartera de pólizas generales)	[DATOS3]	NIVEL CENTRAL	MA	[HW4]	8	10	10	10	8
		Datos contabilidad	[DATOS4]	NIVEL CENTRAL	A	[HW4]	8	9	9	9	8
		BBDD pólizas decesos	[DATOS5]	NIVEL CENTRAL	MA	[HW4]	8	10	10	10	8
		Imagen Corporativa	[DATOS6]	NIVEL CENTRAL	B	-	0	0	0	0	0

SW	Aplicaciones	10 LibreOffice 4	[SW1]	NIVEL CENTRAL	MB	[HW3]	5	4	5	5	3
		Office 2010	[SW2]	NIVEL CENTRAL	MB	[HW3]	5	3	4	5	3
		Antivirus	[SW3]	NIVEL CENTRAL	MB	[HW4]	5	3	8	7	5
		8 Windows 7	[SW4]	NIVEL CENTRAL	MB	[HW3]	8	4	6	7	4
		2 WinXP	[SW5]	NIVEL CENTRAL	MB	[HW3]	7	4	6	7	4
		SegurLif	[SW6]	NIVEL CENTRAL	B	[HW4]	8	8	8	9	7
		ContaSol	[SW7]	NIVEL CENTRAL	MB	[HW4]	8	8	8	7	5
		Access 97 Runtime	[SW8]	NIVEL CENTRAL	MB	[HW3]	5	5	5	6	4
		Windows 2003	[SW9]	NIVEL CENTRAL	MB	[HW4]	8	7	8	9	5
		Terminal server CALC	[SW10]	NIVEL CENTRAL	MB	[SW9]	8	6	8	8	5
		5 LibreOffice 4	[SW11]	TERRITORIALES	MB	[HW11]	5	4	5	5	3
		5 Windows 7	[SW12]	TERRITORIALES	MB	[HW11]	5	8	8	8	4
		1 Windows 8	[SW13]	TERRITORIALES	MB	[HW11]	5	8	8	8	5
		Windows 2012	[SW14]	TERRITORIALES	MB	[HW4]	8	8	10	9	7
S	Servicios	Servicios externos de terceros (web corporativa publica , Inet + Email)	[S1]	NIVEL CENTRAL	MB	[COM1]	8	8	10	10	5
		Sistemas internos (compartición ficheros, grupo whatsapp mensajería interna)	[S2]	NIVEL CENTRAL	MB	[HW4]	7	7	8	7	5
P	Personal	2 Asistentes	[P01]	NIVEL CENTRAL	A	-	0	0	0	5	0
		4 responsables	[P02]	NIVEL CENTRAL	A	-	0	0	0	6	0
		6 Asistentes	[P03]	TERRITORIALES	A	-	0	0	0	5	0

Impacto Potencial = Valor Activo X Porcentaje de Impacto

IMPACTO POTENCIAL																
		CRITICIDAD					% DE IMPACTO					IMPACTO POTENCIAL				
TIPO	ID	Autenticidad	Confidencialidad	Integridad	Disponibilidad	Audibilidad	Autenticidad	Confidencialidad	Integridad	Disponibilidad	Audibilidad	Autenticidad	Confidencialidad	Integridad	Disponibilidad	Audibilidad
L	[L1]	8	9	10	10	8	0	100%	75%	100%	0	0	9	7,5	10	0
	[L2]	8	9	9	7	6	0	100%	75%	100%	0	0	9	6,75	7	0
	[L3]	8	9	10	10	8	0	100%	75%	100%	0	0	9	7,5	10	0
AUX	[AUX1]	0	0	0	8	0	0	100%	50%	100%	0	0	0	0	8	0
	[AUX2]	0	0	0	8	0	0	100%	50%	100%	0	0	0	0	8	0
	[AUX3]	0	0	0	10	0	0	100%	50%	100%	0	0	0	0	10	0
	[AUX4]	0	0	0	10	0	0	100%	50%	100%	0	0	0	0	10	0
	[AUX5]	0	0	0	8	0	0	100%	50%	100%	0	0	0	0	8	0
	[AUX6]	0	0	0	8	0	0	100%	50%	100%	0	0	0	0	8	0
	[AUX7]	0	0	0	10	0	0	100%	50%	100%	0	0	0	0	10	0
	[AUX8]	0	0	0	10	0	0	100%	50%	100%	0	0	0	0	10	0
COM	[COM1]	7	8	9	10	6	100%	50%	40%	80%	0	7	4	3,6	8	0
	[COM2]	7	8	9	10	6	100%	50%	40%	80%	0	7	4	3,6	8	0

HW	[HW1]	5	7	8	8	5	0	100%	25%	100%	0	0	7	2	8	0
	[HW2]	5	7	6	7	5	0	100%	25%	100%	0	0	7	1,5	7	0
	[HW3]	4	6	6	7	5	0	100%	25%	100%	0	0	6	1,5	7	0
	[HW4]	9	9	10	10	8	0	100%	50%	100%	0	0	9	5	10	0
	[HW5]	3	4	5	5	4	0	100%	25%	100%	0	0	4	1,25	5	0
	[HW6]	3	4	5	3	4	0	100%	25%	100%	0	0	4	1,25	3	0
	[HW7]	4	3	3	10	4	0	100%	25%	100%	0	0	3	0,75	10	0
	[HW8]	3	2	5	5	2	0	100%	25%	100%	0	0	2	1,25	5	0
	[HW9]	5	7	8	8	5	0	100%	25%	100%	0	0	7	2	8	0
	[HW10]	5	7	6	7	5	0	100%	25%	100%	0	0	7	1,5	7	0
	[HW11]	4	6	6	7	5	0	100%	25%	100%	0	0	6	1,5	7	0
	[HW12]	9	9	10	10	8	0	100%	50%	100%	0	0	9	5	10	0
	[HW13]	3	4	5	5	4	0	100%	25%	100%	0	0	4	1,25	5	0
	[HW14]	4	3	3	10	4	0	100%	25%	100%	0	0	3	0,75	10	0
	[HW15]	3	2	5	5	2	0	100%	25%	100%	0	0	2	1,25	5	0
	[HW16]	5	8	8	8	3	0	100%	25%	100%	0	0	8	2	8	0
MEDIA	[MEDIA1]	7	8	8	7	7	0	100%	75%	100%	0	0	8	6	7	0
	[MEDIA2]	8	8	8	8	8	0	75%	75%	100%	0	0	6	6	8	0

DATOS	[DATOS1]	7	8	8	8	7	100%	100%	75%	100%	0	7	8	6	8	0
	[DATOS2]	8	9	10	9	8	100%	100%	75%	100%	0	8	9	7,5	9	0
	[DATOS3]	8	10	10	10	8	100%	100%	75%	100%	0	8	10	7,5	10	0
	[DATOS4]	8	9	9	9	8	100%	100%	75%	100%	0	8	9	6,75	9	0
	[DATOS5]	8	10	10	10	8	100%	100%	75%	100%	0	8	10	7,5	10	0
	[DATOS6]	0	0	0	0	0	100%	100%	75%	100%	0	0	0	0	0	0
SW	[SW1]	5	4	5	5	3	100%	100%	100%	100%	0	5	4	5	5	0
	[SW2]	5	3	4	5	3	100%	100%	100%	100%	0	5	3	4	5	0
	[SW3]	5	3	8	7	5	100%	100%	100%	100%	0	5	3	8	7	0
	[SW4]	8	4	6	7	4	100%	100%	100%	100%	0	8	4	6	7	0
	[SW5]	7	4	6	7	4	100%	100%	100%	100%	0	7	4	6	7	0
	[SW6]	8	8	8	9	7	100%	100%	100%	100%	0	8	8	8	9	0
	[SW7]	8	8	8	7	5	100%	100%	100%	100%	0	8	8	8	7	0
	[SW8]	5	5	5	6	4	100%	100%	100%	100%	0	5	5	5	6	0
	[SW9]	8	7	8	9	5	100%	100%	100%	100%	0	8	7	8	9	0
	[SW10]	8	6	8	8	5	100%	100%	100%	100%	0	8	6	8	8	0
	[SW11]	5	4	5	5	3	100%	100%	100%	100%	0	5	4	5	5	0
	[SW12]	5	8	8	8	4	100%	100%	100%	100%	0	5	8	8	8	0
	[SW13]	5	8	8	8	5	100%	100%	100%	100%	0	5	8	8	8	0
	[SW14]	8	8	10	9	7	100%	100%	100%	100%	0	8	8	10	9	0

S	[S1]	8	8	10	10	5	100%	100%	50%	100%	100%	8	8	5	10	5
	[S2]	7	7	8	7	5	100%	100%	50%	100%	100%	7	7	4	7	5
P	[P01]	0	0	0	5	0	0	50%	10%	40%	0	0	0	0	2	0
	[P02]	0	0	0	6	0	0	70%	50%	75%	0	0	0	0	4,5	0
	[P03]	0	0	0	5	0	0	50%	10%	40%	0	0	0	0	2	0

RIESGO POTENCIAL														
				IMPACTO POTENCIAL					RIESGO					
TIPO	ID	FRECUENCIA		Autenticidad	Confidencialidad	Integridad	Disponibilidad	Audibilidad	Autenticidad	Confidencialidad	Integridad	Disponibilidad	Audibilidad
L	[L1]	(FB)	0,1	0	9	7,5	10	0	**0**	**0,9**	**0,75**	**1**	**0**
	[L2]	(FB)	0,1	0	9	6,75	7	0	**0**	**0,9**	**0,675**	**0,7**	**0**
	[L3]	(FB)	0,1	0	9	7,5	10	0	**0**	**0,9**	**0,75**	**1**	**0**
AUX	[AUX1]	(FB)	0,1	0	0	0	8	0	**0**	**0**	**0**	**0,8**	**0**
	[AUX2]	(FB)	0,1	0	0	0	8	0	**0**	**0**	**0**	**0,8**	**0**
	[AUX3]	(FB)	0,1	0	0	0	10	0	**0**	**0**	**0**	**1**	**0**
	[AUX4]	(FB)	0,1	0	0	0	10	0	**0**	**0**	**0**	**1**	**0**
	[AUX5]	(FB)	0,1	0	0	0	8	0	**0**	**0**	**0**	**0,8**	**0**
	[AUX6]	(FB)	0,1	0	0	0	8	0	**0**	**0**	**0**	**0,8**	**0**
	[AUX7]	(FB)	0,1	0	0	0	10	0	**0**	**0**	**0**	**1**	**0**
	[AUX8]	(FB)	0,1	0	0	0	10	0	**0**	**0**	**0**	**1**	**0**
COM	[COM1]	(FB)	0,1	7	4	3,6	8	0	**0,7**	**0,4**	**0,36**	**0,8**	**0**
	[COM2]	(FB)	0,1	7	4	3,6	8	0	**0,7**	**0,4**	**0,36**	**0,8**	**0**

HW	[HW1]	(FM)	1	0	7	2	8	0	**0**	**7**	**2**	**8**	**0**
	[HW2]	(FM)	1	0	7	1,5	7	0	**0**	**7**	**1,5**	**7**	**0**
	[HW3]	(FM)	1	0	6	1,5	7	0	**0**	**6**	**1,5**	**7**	**0**
	[HW4]	(FB)	0,1	0	9	5	10	0	**0**	**0,9**	**0,5**	**1**	**0**
	[HW5]	(FM)	1	0	4	1,25	5	0	**0**	**4**	**1,25**	**5**	**0**
	[HW6]	(FM)	1	0	4	1,25	3	0	**0**	**4**	**1,25**	**3**	**0**
	[HW7]	(FM)	1	0	3	0,75	10	0	**0**	**3**	**0,75**	**10**	**0**
	[HW8]	(FM)	1	0	2	1,25	5	0	**0**	**2**	**1,25**	**5**	**0**
	[HW9]	(FM)	1	0	7	2	8	0	**0**	**7**	**2**	**8**	**0**
	[HW10]	(FM)	1	0	7	1,5	7	0	**0**	**7**	**1,5**	**7**	**0**
	[HW11]	(FM)	1	0	6	1,5	7	0	**0**	**6**	**1,5**	**7**	**0**
	[HW12]	(FB)	0,1	0	9	5	10	0	**0**	**0,9**	**0,5**	**1**	**0**
	[HW13]	(FM)	1	0	4	1,25	5	0	**0**	**4**	**1,25**	**5**	**0**
	[HW14]	(FM)	1	0	3	0,75	10	0	**0**	**3**	**0,75**	**10**	**0**
	[HW15]	(FM)	1	0	2	1,25	5	0	**0**	**2**	**1,25**	**5**	**0**
	[HW16]	(FM)	1	0	8	2	8	0	**0**	**8**	**2**	**8**	**0**
MEDIA	[MEDIA1]	(FMB)	0,01	0	8	6	7	0	**0**	**0,08**	**0,06**	**0,07**	**0**
	[MEDIA2]	(FMB)	0,01	0	6	6	8	0	**0**	**0,06**	**0,06**	**0,08**	**0**

DATOS	[DATOS1]	(FA)	10	7	8	6	8	0	70	80	60	80	0
	[DATOS2]	(FA)	10	8	9	6,75	8	0	80	90	67,5	80	0
	[DATOS3]	(FA)	10	8	10	7,5	8	0	80	100	75	80	0
	[DATOS4]	(FA)	10	8	9	6,75	9	0	80	90	67,5	90	0
	[DATOS5]	(FA)	10	8	10	7,5	10	0	80	100	75	100	0
	[DATOS6]	(FA)	10	0	0	0	0	0	0	0	0	0	0
SW	[SW1]	(FA)	10	5	4	5	5	0	50	40	50	50	0
	[SW2]	(FA)	10	5	3	4	5	0	50	30	40	50	0
	[SW3]	(FA)	10	5	3	8	7	0	50	30	80	70	0
	[SW4]	(FA)	10	8	4	6	7	0	80	40	60	70	0
	[SW5]	(FA)	10	7	4	6	7	0	70	40	60	70	0
	[SW6]	(FA)	10	8	8	8	9	0	80	80	80	90	0
	[SW7]	(FA)	10	8	8	8	7	0	80	80	80	70	0
	[SW8]	(FA)	10	5	5	5	6	0	50	50	50	60	0
	[SW9]	(FA)	10	8	7	8	9	0	80	70	80	90	0
	[SW10]	(FA)	10	8	6	8	8	0	80	60	80	80	0
	[SW11]	(FA)	10	5	4	5	5	0	50	40	50	50	0
	[SW12]	(FA)	10	5	8	8	8	0	50	80	80	80	0
	[SW13]	(FA)	10	5	8	8	8	0	50	80	80	80	0
	[SW14]	(FA)	10	8	8	10	9	0	80	80	100	90	0

S	[S1]	(FM)	1	8	8	5	10	5	**8**	**8**	**5**	**10**	**5**
	[S2]	(FM)	1	7	7	4	7	5	**7**	**7**	**4**	**7**	**5**
P	[P01]	(FMB)	0,01	0	0	0	2	0	**0**	**0**	**0**	**0,02**	**0**
	[P02]	(FB)	0,1	0	0	0	4,5	0	**0**	**0**	**0**	**0,45**	**0**
	[P03]	(FMB)	0,01	0	0	0	2	0	**0**	**0**	**0**	**0,02**	**0**

ANEXO K. FASE 3 - CONSOLIDADO TABLAS

ANEXO L. FASE 4 - PROPUESTAS DE PROYECTOS

ID	PROYECTO	DESCRIPCIÓN	BENEFICIOS	PRIORIDAD	TIEMPO	INDICADOR	COSTO ESTIMADO
P01	ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD.	UN MIEMBRO DEL DEPARTAMENTO DE INFORMÁTICA, INGENIERO INFORMÁTICO Y ESPECIALISTA EN SEGURIDAD DE LA INFORMACIÓN HARÁ SEGUIMIENTO DE LAS WEBS DE VULNERABILIDADES Y ATAQUES 0-DAY Y MANTENDRÁ EL CONTACTO CON EL COLCERT. LAS VULNERABILIDADES QUE PUEDAN AFECTAR A LOS TRABAJADORES / USUARIOS SERÁN COMUNICADAS A ESTOS POR EMAIL, PARA QUE ESTÉN ALERTA DE POSIBLES MAL FUNCIONAMIENTOS EN SUS EQUIPOS Y SISTEMAS.	EL CONOCIMIENTO DE VULNERABILIDADES A NIVELES DE SISTEMAS Y APLICATIVOS, PERMITIRÁ A LA ENTIDAD DETECTAR POSIBLES INFECCIONES DE SUS SISTEMAS, FUGAS DE INFORMACIÓN, QUE AFECTAN ENTRE OTROS A LOS SISTEMAS DE BACKUP, SERVIDOR, ETC. PUEDEN OCASIONAR LA PÉRDIDA DE INFORMACIÓN O LA NO DISPONIBILIDAD DE SERVICIO. * CUMPLIR CON LOS CONTROLES 6.1.6-6.1.7. * CONOCER VULNERABILIDADES EN LOS PROGRAMAS PARA ACTUAR EN CONSECUENCIA	MEDIA	CORTO PLAZO	ELABORACIÓN DE INFORMES SEMANALES. NOTIFICACIÓN DE VULNERABILIDADES MÁS RELEVANTES EL DIRECTOR DE SISTEMAS.	$ 210.000
P02	DOCUMENTAR UNA POLÍTICA DE USO DE MEDIOS TECNOLÓGICOS	EN LA POLÍTICA DE USO DE MEDIOS TECNOLÓGICOS SE DEFINIRÁN LOS SIGUIENTES ASPECTOS: * PROHIBICIONES DE USO, NORMAS DE SEGURIDAD A NIVEL DE ACCESO, CONFIGURACIÓN Y CUSTODIA DE LOS MEDIOS TECNOLÓGICOS, INSTALACIONES DE SOFTWARE, COMUNICACIONES, USO DEL CORREO ELECTRÓNICO Y EL ACCESO A INTERNET. NOTIFICACIÓN DEL DERECHO / OBLIGACIÓN DE PARQUES NACIONALES DE CUSTODIAR EL USO DE LOS EQUIPOS. EL OBJETIVO DEL MISMO ES DAR A CONOCER A LOS TRABAJADORES / USUARIOS LA IMPORTANCIA DEL CORRECTO USO DE LOS ACTIVOS DE LA INFORMACIÓN DE LA ENTIDAD.	* REDUCIR EL MAL USO DE LOS EQUIPOS Y ERRORES DE USUARIO RESULTADOS DE LA IGNORANCIA Y DESCONOCIMIENTO. * EVITAR INFECCIONES DE SW MALICIOSO MEDIANTE EL USO INDEBIDO DEL CORREO ELECTRÓNICO E INTERNET, LA DEGRADACIÓN DEL SERVICIO DE CORREO ELECTRÓNICO Y LA SATURACIÓN DE LOS BUZONES DE CORREO.	ALTA	CORTO PLAZO	CONFIRMACIÓN POR PARTE DE CADA TRABAJADOR DE HABER REVISADO EL DOCUMENTO UNA VEZ AL AÑO.	$ 35.000

P03	DOCUMENTAR LA POLÍTICA DE GESTIÓN DE ACCESO	SE DOCUMENTARÁ UN PROCEDIMIENTO DONDE SE DEFINA EL ACCESO DE LOS DIFERENTES PERFILES A LA INFORMACIÓN. ESTE ACCESO SE HARÁ EN FUNCIÓN DE SU NECESIDAD DE SABER. PARA CONTROLAR EL ACCESO A LOS ACTIVOS DE INFORMACIÓN SE ESTABLECERÁN LAS SIGUIENTES DIRECTRICES: * ESTABLECER REQUISITOS DE ACCESO INDIVIDUALES PARA CADA APLICACIÓN. * VERIFICACIÓN DE LA CONSISTENCIA ENTRE EL CONTROL DE ACCESO Y LA CLASIFICACIÓN DE LA INFORMACIÓN DE LOS DIFERENTES SISTEMAS Y REDES. * GESTIÓN DE LOS DERECHOS DE ACCESO A TODOS LOS ENTORNOS. * REVISIÓN PERIÓDICA DE LOS CONTROLES DE AUTORIZACIÓN DE ACCESO. * ELIMINACIÓN DE LOS DERECHOS DE ACCESO CUANDO SEA NECESARIO.	* EVITAR / REDUCIR EL ABUSO DE PRIVILEGIOS Y ACCESOS NO AUTORIZADOS	ALTA	CORTO PLAZO	REGISTROS DE SEGUIMIENTO LOS CONTROLES DE ACCESO.	$ 105.000
P04	DOCUMENTAR UNA POLÍTICA DE INTERCAMBIO DE INFORMACIÓN	EN LA POLÍTICA DE INTERCAMBIO DE INFORMACIÓN SE DEFINIRÁ COMO TODO INTERCAMBIO QUE SE REALICE, A NIVEL INTERNO Y EXTERNO, DEBE GARANTIZAR LA CONFIDENCIALIDAD Y LA INTEGRIDAD DE LA TRANSMISIÓN. A TAL EFECTO LOS RESPONSABLES DEL SGSI Y SUS USUARIOS DEBERÁN USAR: * TÉCNICAS CRIPTOGRÁFICAS PARA PROTEGER LA CONFIDENCIALIDAD, INTEGRIDAD Y AUTENTICIDAD DE LA INFORMACIÓN. * GARANTIZAR EL USO ACEPTABLE DE LOS RECURSOS DE COMUNICACIÓN POR PARTE DE LOS USUARIOS, TANTO A NIVEL INTERNO COMO EXTERNO, DEFINIDOS EN EL PROCEDIMIENTO USO ACEPTABLE DE ACTIVOS '. * UTILIZAR UN SW ANTIVIRUS ACTUALIZADO QUE EVITE LA APARICIÓN DE CÓDIGOS MALICIOSOS DURANTE LOS INTERCAMBIOS DE INFORMACIÓN.	* EVITAR / REDUCIR FUGAS DE INFORMACIÓN, INFECCIONES DE SW MALICIOSO, PÉRDIDA DE INFORMACIÓN. ASÍ COMO SE PODRÁN REDUCIR ERRORES DE USUARIO POR DESCONOCIMIENTO DEL CORRECTO PROCESO DE INTERCAMBIO. * DETECTAR ACCESOS NO AUTORIZADOS	ALTA	MEDIO PLAZO	REGISTRO DE TODOS LOS INTERCAMBIOS FÍSICOS QUE SE LLEVEN EN CUENTA Y REGISTRO DE COMUNICACIONES ELECTRÓNICAS.	$ 105.000

P05	DOCUMENTAR POLÍTICA DE ENCAMINAMIENTO	SIEMPRE QUE SE AÑADA UNA NUEVA RED A LOS SISTEMAS Y SERVICIOS, EL RESPONSABLE DEL SGSI, DEBERÁ IDENTIFICAR LAS NECESIDADES DE CONEXIÓN CON OTROS SISTEMAS O REDES, ASÍ COMO LAS CARACTERÍSTICAS QUE PERMITAN DETERMINAR EL PERÍMETRO DE SEGURIDAD PERTINENTE. EL DIRECCIONAMIENTO DE LA RED SE LLEVARÁ A CABO DESPUÉS DE UN ANÁLISIS DE ESTAS CARACTERÍSTICAS Y REQUISITOS, A TRAVÉS DE LAS MEDIDAS DE CONTROL DE TRÁFICO DE RED ESTABLECIDAS POR EL CORTAFUEGOS. EN CASO DE QUE SEA NECESARIO, SE PODRÁN ABRIR REGLAS AL CORTAFUEGOS QUE PERMITAN LA CORRECTA INTERCONEXIÓN DE LA NUEVA RED CON OTROS SISTEMAS CON LOS QUE SEA NECESARIA LA COMUNICACIÓN.	* EVITAR / REDUCIR ERRORES ENCAMINAMIENTO, USO NO PREVISTO DERIVADO DE ERRORES DE COMUNICACIONES, ETC.	ALTA	MEDIO PLAZO	DOCUMENTO ACTUALIZADO CON LOS CAMBIOS SOBRE LA RED Y LOS SISTEMAS.	$ 35.000
P06	DOCUMENTAR POLÍTICA DE ELIMINACIÓN SEGURA DE SOPORTES DE INFORMACIÓN	A TRAVÉS DE ESTA POLÍTICA SE DEFINIRÁ EL PROCEDIMIENTO DE GESTIÓN DE SOPORTES Y ELIMINACIÓN DEL CONTENIDO DE SOPORTES EXTRAÍBLES, LLEVANDO UN CONTROL / REGISTRO DE LA ENTRADA / SALIDA DE ESTOS SOPORTES HACIENDO USO DEL FORMULARIO PERTINENTE. ASIMISMO, LA ENTIDAD ACTUALIZARÁ LOS EQUIPOS Y SOPORTES OBSOLETOS PERIÓDICAMENTE Y SOLICITARÁ CERTIFICADOS DE DESTRUCCIÓN DE SOPORTES QUE VERIFIQUEN LA ELIMINACIÓN DE ESTOS.	* EVITAR / REDUCIR EL USO NO PREVISTO DE SOPORTES FÍSICOS Y GARANTIZAR SU CORRECTA ELIMINACIÓN	ALTA	CORTO PLAZO	INVENTARIO / REGISTRO DE GESTIÓN DE SOPORTES DE INFORMACIÓN	$ 105.000
P07	POLÍTICA DE TRATAMIENTO DE LA INFORMACIÓN	APARTE DE CLASIFICAR LA INFORMACIÓN, QUE YA LO HACE PARQUES NACIONALES, SE CONSIDERA IMPORTANTE DEFINIR UN PROCEDIMIENTO RELATIVO AL TRATAMIENTO DE LA INFORMACIÓN PARA EVITAR QUE LA INFORMACIÓN SEA UTILIZADA PARA FINES NO AUTORIZADAS. A TAL EFECTO, SE ESTABLECERÁN LAS SIGUIENTES DIRECTRICES: * MANIPULAR Y ETIQUETAR LOS SOPORTES TAL Y COMO INDICA SU NIVEL DE CLASIFICACIÓN * RESTRINGIR EL ACCESO A PERSONAL AUTORIZADO * ASEGURAR QUE LA ENTRADA DE DATOS ESTÁ COMPLETA Y QUE TAMBIÉN LO ESTÁ SU PROCESADO Y VALIDACIÓN	* EVITAR / REDUCIR ERRORES EN LA INFORMACIÓN * REDUCIR ACCESOS NO AUTORIZADOS	ALTA	CORTO PLAZO	CORRECTA CLASIFICACIÓN DOCUMENTAL Y REGISTRO DE MANIPULACIÓN	$ 35.000

		* DISTRIBUIR LOS DATOS AL MENOR NÚMERO DE DESTINATARIOS POSIBLE * ALMACENAR LOS SOPORTES DE ACUERDO CON LAS ESPECIFICACIONES DEL FABRICANTE.					
P08	POLÍTICA DE FORMACIÓN EN MATERIA DE SEGURIDAD	SE DOCUMENTARÁ UN PROCEDIMIENTO PARA GARANTIZAR QUE TODO EL PERSONAL DE PARQUES NACIONALES NATURALES DE COLOMBIA ESTÁ FORMADO EN MATERIA DE SEGURIDAD. LOS RESPONSABLES DEL SGSI EN COLABORACIÓN CON RRHH DEFINIRÁN LOS PLANES DE FORMACIÓN ADECUADOS, TENÍAN EN CUENTA: * CAMBIOS EN SISTEMAS Y SERVICIOS * CAMBIOS DE PUESTO DE TRABAJO * ACCIONES CORRECTIVAS / PREVENTIVAS	* GARANTIZAR QUE EL PERSONAL ES INFORMADO DE SUS FUNCIONES Y RESPONSABILIDADES * IDENTIFICAR LAS NECESIDADES DE FORMACIÓN DE LOS EMPLEADOS * GARANTIZAR LOS NIVELES DE FORMACIÓN, CONCIENCIACIÓN, SENSIBILIZACIÓN Y EXPERIENCIA NECESARIOS PARA LLEVAR A CABO SUS FUNCIONES * DOCUMENTAR Y MANTENER LOS REGISTROS RELATIVOS A LA FORMACIÓN RECIBIDA POR CADA UNO DE LOS TRABAJADORES. * REDUCIR INCIDENTES POR INGENIERÍA SOCIAL	ALTA	CORTO PLAZO	REGISTROS RELATIVOS A FORMACIÓN RECIBIDA	$ 35.000
P09	CRITERIOS DE SELECCIÓN DE PERSONAL	SE DOCUMENTARÁ UN PROCEDIMIENTO CON EL OBJETIVO DE DEFINIR LOS CRITERIOS A APLICAR EN EL PROCESO DE SELECCIÓN DE PERSONAL. DURANTE EL PROCESO DE SELECCIÓN RELATIVO A LAS INCORPORACIONES DE NUEVOS CANDIDATOS, DESDE RRHH SE COMPROBARÁN Y VERIFICARÁN LAS REFERENCIAS DEL CANDIDATO.	* GARANTIZAR LA SEGURIDAD A NIVEL DE RRHH Y CONTRACCIÓN DE PERSONAL.	MEDIA	CORTO PLAZO	REGISTRO DE ENTREVISTAS, DATOS CURRICULARES, ETC.	$ 35.000
P10	SOPORTE Y SEGURIDAD DEL CABLEADO	SE PROTEGERÁ EL CABLEADO DE ENERGÍA Y TELECOMUNICACIONES QUE DA APOYO A LOS ACTIVOS DEL SGSI CONTRA INTERFERENCIAS, INTRUSIONES Y DAÑOS, APLICANDO LAS SIGUIENTES MEDIDAS: * LA RED DE CABLEADO SE PROTEGERÁ MEDIANTE LA INSTALACIÓN EN EL TECHO DEL CABLEADO CORRESPONDIENTE A LA DETECCIÓN DE INCENDIOS, ILUMINACIÓN Y SEGURIDAD, LA INSTALACIÓN POR TIERRA DEL CABLEADO CORRESPONDIENTE A LA TENSIÓN ELÉCTRICA Y LAS COMUNICACIONES. LOS	* EVITAR LA MANIPULACIÓN DE CABLES Y AVERÍAS.	ALTA	MEDIO PLAZO	CERTIFICADO DE CORRECTA INSTALACIÓN	$ 210.000

		CABLES SE DESPLEGARÁN A TRAVÉS DE CONDUCTOS PROTECTORES Y SE GUIARÁN HASTA LAS TOMAS DE CORRIENTE DE MANERA ADECUADA, EVITANDO DEJAR CABLES AL AIRE. * TODOS LOS CABLES IRÁN CORRECTAMENTE ETIQUETADOS, PARA DIFERENCIAR LOS CORRESPONDIENTES AL SUMINISTRO DE VOZ, DATOS Y ELECTRICIDAD.					
P11	SISTEMATIZACIÓN DE EL INVENTARIO DE ACTIVOS	EL EQUIPO DE INNOVACIÓN DESARROLLARÁ UNA HERRAMIENTA INFORMÁTICA PARA EL REGISTRO INTERNO DE ACTIVOS.	EVITAR LA PÉRDIDA DE EQUIPOS, DOCUMENTOS Y EN CONSECUENCIA POSIBLES FUGAS DOCUMENTALES.	MEDIA	MEDIO PLAZO	SISTEMA DE ALERTAS QUE INDICA ANOMALÍAS O NO DEVOLUCIÓN DE ACTIVOS.	$ 175.000
P12	SISTEMATIZACIÓN DEL REGISTRO DE INTERCAMBIOS DE INFORMACIÓN	EL EQUIPO DE INNOVACIÓN DESARROLLARÁ UNA HERRAMIENTA INFORMÁTICA PARA CONTROLE EL INTERCAMBIO DE INFORMACIÓN, PERMITIENDO LA MONITORIZACIÓN DE LOS EQUIPOS Y LA GENERACIÓN DE ALERTAS EN CASO DE DETECTAR ENVÍOS SOSPECHOSOS.	EVITAR FUGAS DE INFORMACIÓN Y DETECCIÓN DE ENVÍOS SOSPECHOSOS.	MEDIA	MEDIO PLAZO	ALERTAS DE ENVÍOS / COPIA MASIVA DE DOCUMENTOS	$ 175.000
P13	SISTEMA DE ACCESO AL PC PARA LECTURA TARJETA EMPLEADO + CONTRASEÑA	EL ACCESO A LOS ORDENADORES SE HARÁ MEDIANTE LA TARJETA DE TRABAJADOR Y UNA CONTRASEÑA. LOS PCS YA ESTABAN PREPARADOS PARA ELLO, SIMPLEMENTE SE HA IMPLEMENTADO UN SOFTWARE INTERNO DE COMUNICACIONES. TODOS LOS ACCESOS Y CAMBIOS EN EL SISTEMA DE GESTIÓN DE PROYECTOS SERÁN TRAZABLES CON EL NÚMERO DE TRABAJADOR.	IDENTIFICAR LOS RESPONSABLES DE: * DESTRUCCIONES DE INFORMACIÓN * ALTERACIÓN DE INFORMACIÓN EVITAR / REDUCIR LA SUPLANTACIÓN DE IDENTIDADES	MEDIA	MEDIO PLAZO	REGISTRO DE EQUIPOS CON SW DE LECTURA DE TARJETA INTEGRADO	$ 105.000
P14	SEGUIMIENTO Y MEDICIÓN DE LOS OBJETIVOS Y CONTROLES	PARA LLEVAR A CABO LA MEDICIÓN Y SEGUIMIENTO DE LOS OBJETIVOS Y CONTROLES DEL SGSI, EL EQUIPO DE INNOVACIÓN IMPLEMENTARÁ UN CUADRO DE MANDO PARA PERMITIRÁ DEMOSTRAR EL AVANCE Y MEJORAS OBTENIDAS. LOS INDICADORES PARA MEDIR LOS OBJETIVOS Y CONTROLES SERÁN AQUELLOS QUE PERMITAN ANALIZAR LA EVOLUCIÓN O TENDENCIA EN EL DESARROLLO DE ESTOS. LOS INDICADORES CONTARÁN CON UNA DESCRIPCIÓN, CRITERIO DE MEDICIÓN, VALOR MÍNIMO / MÁXIMO / REAL, RESPONSABLES, OBJETIVO,	TENER CONOCIMIENTO ACTUALIZADO DEL ESTADO DEL SGSI	MEDIA	LARGO PLAZO	CUADRO DE MANDOS	$ 175.000

		PERIODICIDAD. TAMBIÉN SE DISTINGUIRÁ ENTRAS INDICADORES DE GESTIÓN O DE CONTROL. LAS REVISIONES DE LOS INDICADORES SE HARÁN DE MANERA PERIÓDICA (AL MENOS UNA VEZ AL AÑO) O ESPECÍFICA EN RESPUESTA A CUALQUIER CIRCUNSTANCIA QUE PUEDA AFECTAR AL SGSI.					

COSTO X DIA:

PERSONAL TÉCNICO: $35.000
PERSONAL TECNOLÓGICO: $105.000
PERSONAL PROFESIONAL: $175.000
PERSONAL ESPECIALIZADO: $210.000

ANEXO L. FASE 4 - PROPUESTAS DE PROYECTOS

ANEXO M. FASE 5 - AUDITORIA DE CUMPLIMIENTO

Datos de la auditoría interna	
Número Auditoria	AUDIT - 12/2015
Norma de Referencia	ISO/IEC 27001:2013
Período de la auditoría	La auditoría interna se llevó a cabo los días 06 y 01 de mayo 2018
Lugar de la auditoría	La auditoría del SGSI se realizó en las oficinas centrales de PARQUES NACIONALES NATURALES DE COLOMBIA en
Equipo auditor	Auditor Eduin González Tabares
Personal auditado	**El personal de PARQUES NACIONALES NATURALES DE COLOMBIA que ha sido auditado se lista continuación:** **• Director general** **• Director técnico** **• Director comercial** **• Director financiero** **• Director RRHH** **• Auxiliar de selección** **• Responsable de sistemas** **• Administrativo** **• Comercial** **• Técnico de sistemas informáticos** **• Técnico de innovación** **• Ingeniero Analista y programador producto** **• Ingeniero de soporte a producto**

Alcance de la auditoría interna
Se han auditado todas las áreas de PARQUES NACIONALES NATURALES DE COLOMBIA que están relacionadas con el alcance del SGSI (sistemas y personas involucradas con los sistemas informáticos, la información almacenada en estos, los sistemas en red y la documentación en papel que gestiona entidad)
Objetivos de la auditoría interna
Determinar el grado de cumplimiento del SGSI de PARQUES NACIONALES NATURALES DE COLOMBIA a la fecha de ejecución de la auditoría respecto a la norma ISO / IEC27001: 2013 y evaluar su eficacia para conseguir los objetivos inicialmente especificados.
Definiciones

No conformidad: incumplimiento de un requisito de la norma ISO / IEC27001: 2013, política o documentos del SGSI que pone en riesgo la efectividad del sistema de gestión y la calidad del servicio suministrado.

Observación: falla aislada y esporádica en el contenido o la implementación de los documentos del SGSI o incumplimiento parcial de un requisito de la norma de referencia que no afecta al SGSI de manera crítica.

Seguidamente se recogen los elementos identificados durante la auditoría, señalando las No Conformidades detectadas y Observaciones establecidas.

Resultados de la auditoría			
ID	elemento	tipo	comentario
SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN			
A.5. Política de seguridad			
	Nada que destacar		
A.6.Seguretat de la información			
A.6.1 Organización interna			
	Nada que destacar		
A.6.2 Dispositivos portátiles y teletrabajo			
1	_Roles y respondes. de la seguridad de la información - Segregación de tareas Controles 6.2.1 y 6.2.2	OBS-1	Aunque existe una política de seguridad en el ámbito de los dispositivos portátiles / teletrabajo no existen informes periódicos sobre el estado de seguridad de estos dispositivos.
A.7.Seguretat de los recursos humanos			
A.7.1 Antes de la contratación			
	Nada que destacar		
A.7.2 Durante la contratación			
2	_ Responsabilidades de dirección control 7.2.1	NC-1	La dirección debe pedir a terceras partes y contratistas aplicar la seguridad en concordancia con las políticas y procedimientos definidos. Se incluirá este punto en la política de seguridad.
A.7.3 Final contratación o cambio puesto trabajo			
	Nada que destacar		
A.8. Gestión de activos			
A.8.1 Responsabilidad sobre los activos			
3	_ Propiedad de los activos control 8.1.2	NC-2	Aunque existe una política de gestión de activos e inventario no se ha hecho una asignación de éstos a personas físicas

A.8.2. Clasificación de la información			
4	_ Etiquetado y manipulación de la información Control 8.2.2	OBS-2	Se han detectado algunas erratas en el etiquetado de la documentación
A.8.2. Gestión de soportes de almacenamiento			
	Nada que destacar		
A.9. Control de acceso			
A.9.1. Requisitos de negocio para el control de acceso			
	Nada que destacar		
A.9.2. Gestión de acceso del usuario			
5	_ Revisión de los derechos de acceso de los usuarios control 9.2.5	NC-3	En tanto que no se han definido los propietarios de los activos, la revisión de los derechos de acceso se hace de manera aleatoria por personal de sistemas, pero no se ha procedimentado su aprobación.
A.9.3. Responsabilidades del usuario			
	Nada que destacar		
A.9.4. Control de acceso a los sistemas			
	Nada que destacar		
A.10. encriptación			
A.10.1 Controles criptográficos			
6	_ Política de uso de los controles criptográficos _ Gestión de contraseñas Control 10.1.1 y 10.1.2	NC-4	No existe una política específica de uso de controles criptográficos
A.11. Seguridad física y del entorno			
A.11.1 Áreas seguras			
7	_Emplazamiento y seguridad de los equipos Control 11.2.1	OBS-3	Algunos portátiles no tenían conectado el cableado antirrobo
A.11.2 Seguridad de los equipos			
8	_Equipo Informático de usuario desatendido control 11.2.8	OBS-4	Aunque los sistemas activan un bloqueo automático de pantalla a los 30s de detectar inactividad, algunos usuarios no bloquean la pantalla al dejar el puesto de trabajo de manera esporádica. Se ha de aumentar su concienciación.
A.12. Seguridad en la operativa			
A.12.1 Áreas seguras			
9	_Gestión De capacidades control 12.1.4	NC-5	No existe un procedimiento para monitorizar y ajustar el uso de recursos con el fin de adelantarse a necesidades futuras

A.12.2 Protección contra código malicioso			
	Nada que destacar		
A.12.3 Copias de seguridad			
	Nada que destacar		
A.12.4 Registro de actividad y supervisión			
10	_Registro Y gestión de eventos _Protección De los registros de información _Registros De actividad del administrador y operador del sistema Controles: 12.4.1_12.4.2_12.4.3	NC-6	Se documentará e implementar un procedimiento para la gestión de registros de actividad aplicable a los diferentes departamentos
11	_Sincronización De relojes	OBS-5	Aunque está implementado aconseja que se formalice su implementación, realizando las medidas de efectividad oportunas
A.12.5 Control del software de explotación			
12	_Instalación de software a sistemas de producción Controles: 12.5.1	NC-7	Aunque existe un registro de instalaciones correctas y fallidas de Software a los sistemas se documentará un procedimiento para controlar la instalación de éste.
A.12.6 Gestión de la vulnerabilidad técnica			
	Nada que destacar		
A.12.7 Consideraciones de las auditorías de los sistemas de información			
	Nada que destacar		
A.13. Seguridad en las comunicaciones			
A.13.1 Gestión de seguridad en las redes			
13	_Segregación De redes control 13.1.3	OBS-6	El registro de incidentes debería hacerse atendiendo a la segregación de redes implementada
A.13.2 Intercambio de información con partes externas			
14	_Acuerdos De confidencialidad y secreto control 13.2.4	NC-8	Aunque se establecen acuerdos de confidencialidad a nivel contractual con las terceras partes, no se lleva a cabo una revisión procedimentada ni periódica
A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información			
	Nada que destacar		
A.15 Relaciones con proveedores			
A.15.1 Seguridad de la información en las relaciones con proveedores			
15	_Política de seguridad de la información para proveedores control 15.1.1	NC-9	No están documentado correctamente los requisitos de seguridad de la información requeridos por los activos

16	_Tratamiento Del riesgo dentro de los acuerdos de suministradores control 15.1.2	NC-10	Aunque existen medidas genéricas, no existe un registro de proveedores donde se detallen los requisitos de seguridad de la información individualizadas para cada proveedor
17	Cadena de suministro en tecnologías de la información y las comunicaciones control 15.1.3	NC-11	Existen acuerdos de seguridad con los proveedores, pero en estos no se recogen los requisitos para hacer frente a los riesgos
A.15.2 Gestión de la prestación del servicio de los proveedores			
18	Supervisión y revisión de los servicios prestados por los terceros control 15.2.1	NC-12	Aunque se llevan a cabo revisiones esporádicas del servicio prestado por terceros, debería prodecimentar y extender a todos los servicios
19	_Gestión De cambios en los servicios de terceros control 15.2.2	NC-13	No existe un proceso definido para administrar los cambios en la provisión de servicio, se lleva un cierto control manual con hoja de excel
A.16 Gestión de incidentes			
	Nada que destacar		
A.17 Aspectos de la SI en la gestión de la continuidad de negocio			
A.17.1 Continuidad de la seguridad de la información			
20	_Planificación De la continuidad Implantación de la continuidad Verificación, revisión y evaluación de la continuidad Control 17.1.1 _ 17.1. 2 _ 17. 1. 3	NC-14	Los planes de continuidad de negocio en materia de seguridad están documentados en algunos departamentos, pero no en todos, pero no existen métricas
A.17.2 Redundancias			
	Nada que destacar		
A.18 Cumplimiento			
A.18.1 Continuidad de la seguridad de la información			
21	_Identificación De la legislación aplicable control 18.1.1	OBS-7	Se han encontrado documentos desactualizados a nivel de legislación aplicable
22	_Derechos De la PI Control 18.1.2	NC-15	No se ha documentado ningún procedimiento que garantice los requisitos de cumplimiento en materia de PI
23	_Riego. los controles criptográficos control 18.1.5	NC-16	Los controles criptográficos no se dan a todos los departamentos
A.18.2 Revisiones de la seguridad de la Información			
24	_Revisión independiente de la seguridad de la información control 18.2.1	OBS-8	No existe una planificación de revisiones independientes

ANEXO M. FASE 5 - AUDITORIA DE CUMPLIMIENTO.pdf

ANEXO N. FASE 5 - NIVEL DE MADUREZ DE LOS CONTROLES - CMM_ISO_27002_2013

Nivel madurez respecto a los controles definidos en la ISO 27002:2013 tras la implantación completa de todos los proyectos propuestos y pos-auditoria

Dominio	% de conformidad	# NC menores	# NC mayores	# NC OK	% de conformidad INICIAL	% de conformidad DESEADO
A.5 -POLÍTICAS DE SEGURIDAD.	90%	0	2	0	5%	90%
A.6 -ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION.	18%	4	2	0	0%	90%
A.7 -SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	90%	0	6	0	3%	90%
A.8 -GESTIÓN DE ACTIVOS.	61%	4	4	1	0%	90%
A.9 -CONTROL DE ACCESOS.	64%	2	12	0	3%	90%
A.10 -CIFRADO.	0%	0	0	0	0%	90%
A.11 -SEGURIDAD FÍSICA Y AMBIENTAL.	71%	2	10	0	1%	90%
A.12 -SEGURIDAD EN LA OPERATIVA.	64%	5	9	0	5%	90%
A.13 -SEGURIDAD EN LAS TELECOMUNICACIONES.	13%	4	1	0	0%	90%
A.14 -ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.	30%	9	2	0	0%	90%
A.15 -RELACIONES CON SUMINISTRADORES.	62%	1	4	0	0%	90%
A.16 -GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	93%	0	1	6	0%	90%
A.17 -ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.	45%	1	3	0	3%	90%
A.18 -CUMPLIMIENTO.	75%	1	5	0	2%	90%

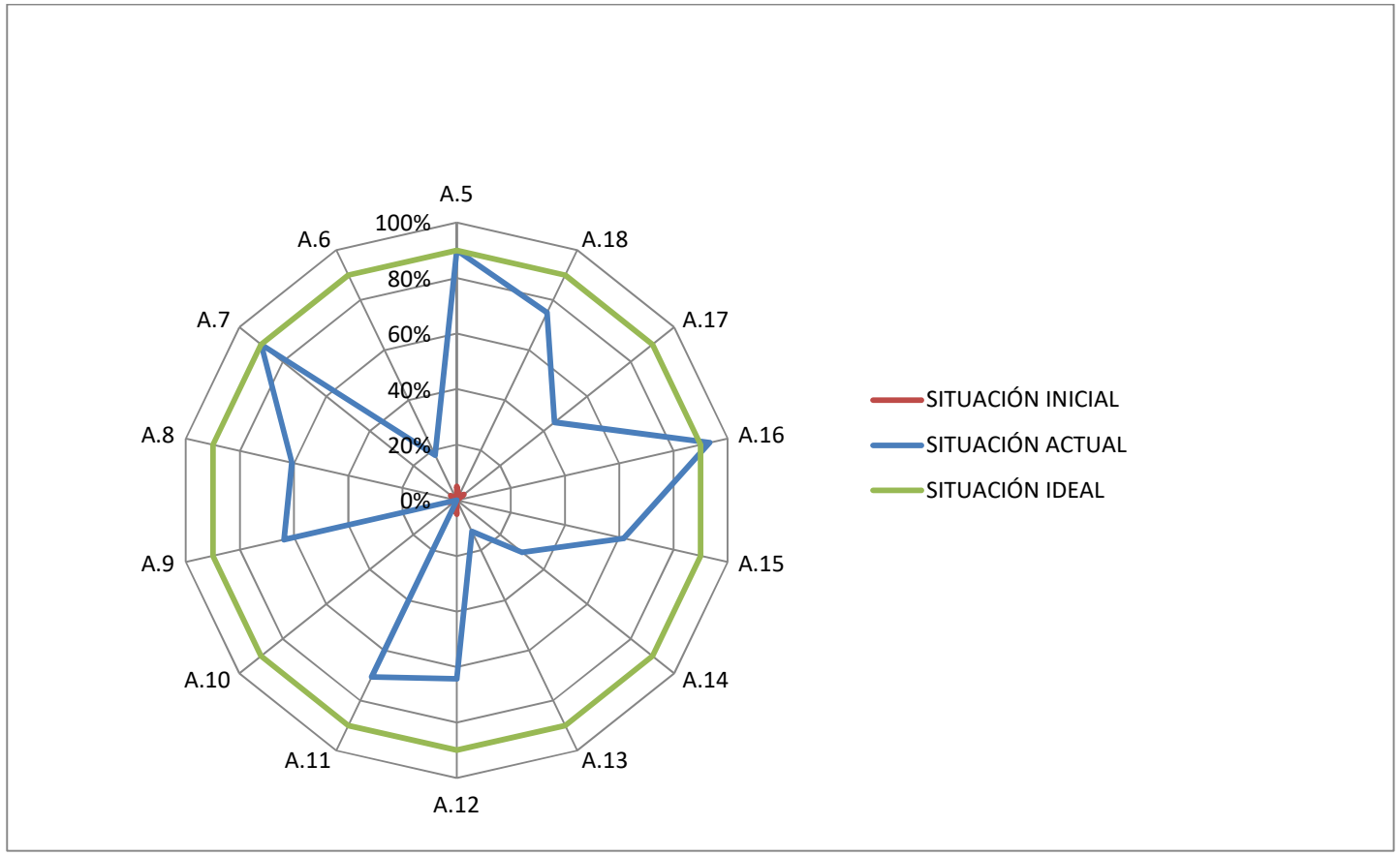
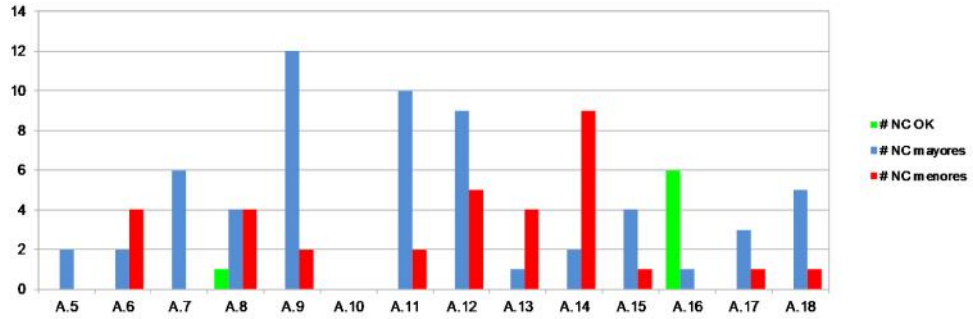
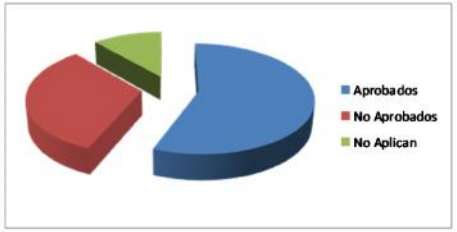

A.5
A.18
A.17
A.16
A.15
A.14
A.13
A.12
A.11
A.10
A.9
A.8
A.7
A.6
100%
80%
60%
40%
20%
0%
SITUACIÓN INICIAL
SITUACIÓN ACTUAL
SITUACIÓN IDEAL

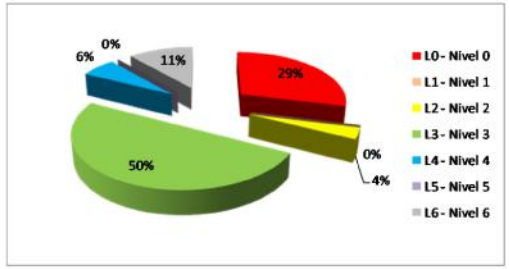
Tabla de Valores

Valor	Efectividad	Significado	Descripción	Número
L0	0%	Inexistente	Carencia completa de cualquier proceso conocido.	33
L1	10%	Inicial / Ad-hoc	Procedimientos inexistentes o localizados en áreas concretas. El éxito de las tareas se debe a esfuerzos personales.	0
L2	50%	Reproducible, pero intuitivo	Existe un método de trabajo basado en la experiencia, aunque sin comunicación formal. Dependencia del conocimiento individual	4
L3	90%	Proceso definido	La organización en su conjunto participa en el proceso. Los procesos están implantados, documentados y comunicados.	57
L4	95%	Gestionado y medible	Se puede seguir la evolución de los procesos mediante indicadores numéricos y estadísticos. Hay herramientas para mejorar la calidad y la eficiencia	7
L5	100%	Optimizado	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos	0
L6	N/A	No aplica		13



Valor	Número
Aprobados	64
No Aprobados	37
No Aplican	13





L0 - Nivel 0	33
L1 - Nivel 1	0
L2 - Nivel 2	4
L3 - Nivel 3	57
L4 - Nivel 4	7
L5 - Nivel 5	0
L6 - Nivel 6	13

Control de ISO /IEC 27002:2013	Controles y objetivos de control	Valoración	Observaciones				
A.5	**POLÍTICAS DE SEGURIDAD**			0,9		**L0**	0
A.5.1	**Directrices de la Dirección en seguridad de la información**			**0,9**		**L1**	0
A.5.1.1	Conjunto de políticas para la seguridad de la información	L3		0,9		**L2**	0
A.5.1.2	Revisión de las políticas para la seguridad de la información	L3		0,9		**L3**	2
						L4	0
						L5	0
						L6	0
						NC Mayores	0
						NC Menores	2
						Observaciones	0

Control de ISO /IEC 27002:2013	Controles y objetivos de control	Valoración	Anotaciones				
A.6	**ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INF.**			0,2		**L0**	4
A.6.1	**Organización interna**			**0,4**		**L1**	0
A.6.1.1	Asignación de responsabilidades para la segur. de la información.	L3		0,9		**L2**	0
A.6.1.2	Segregación de tareas.	L3		0,9		**L3**	2
A.6.1.3	Contacto con las autoridades	L0		0		**L4**	0
A.6.1.4	Contacto con grupos de interés especial	L0		0		**L5**	0
A.6.1.5	Seguridad de la información en la gestión de proyectos	L0		0		**L6**	1
A.6.2	**Dispositivos para movilidad y teletrabajo.**			**0,0**			
A.6.2.1	Política de uso de dispositivos para movilidad.	L0		0			
A.6.2.2	Teletrabajo.	L6		N/A			
						NC Mayores	4
						NC Menores	2
						Observaciones	0

Control de ISO /IEC 27002:2013	Controles y objetivos de control	Valoración	Anotaciones				
A.7	**SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.**			0,9000		**L0**	0
A.7.1	**Organización interna**			**0,9**		**L1**	0
A.7.1.1	Investigación de antecedentes.	L3		0,9		**L2**	0
A.7.1.2	Términos y condiciones de contratación.	L3		0,9		**L3**	6
A.7.2	**Durante la contratación.**			**0,9000**		**L4**	0
A.7.2.1	Responsabilidades de gestión.	L3		0,9		**L5**	0
A.7.2.2	Concienciación, educación y capacitación en segur. de la informac.	L3		0,9		**L6**	0
A.7.2.3	Proceso disciplinario.	L3		0,9			
A.7.3	**Cese o cambio de puesto de trabajo.**			**0,9**			
A.7.3.1	Cese o cambio de puesto de trabajo.	L3		0,9			
						NC Mayores	0
						NC Menores	6
						Observaciones	0

Control de ISO /IEC 27002:2013	Controles y objetivos de control	Valoración	Anotaciones				
A.8	**GESTIÓN DE ACTIVOS.**			0,6083		**L0**	4
A.8.1	**Responsabilidad sobre los activos.**			**0,5**		**L1**	0
A.8.1.1	Inventario de activos.	L4		0,95		**L2**	0
A.8.1.2	Propiedad de los activos.	L0				**L3**	4
A.8.1.3	Uso aceptable de los activos.	L0				**L4**	1
A.8.1.4	Devolución de activos.	L0		0		**L5**	0
A.8.2	**Clasificación de la información.**			**0,9**		**L6**	1
A.8.2.1	Directrices de clasificación.	L3		0,9			
A.8.2.2	Etiquetado y manipulado de la información.	L3		0,9			
A.8.2.3	Manipulación de activos.	L3		0,9			
A.8.3	**Manejo de los soportes de almacenamiento.**			**0,5**			
A.8.3.1	Gestión de soportes extraíbles.	L0		0			
A.8.3.2	Eliminación de soportes.	L3		0,9			
A.8.3.3	Soportes físicos en tránsito	L6		N/A			
						NC Mayores	4
						NC Menores	4
						Observaciones	1

Control de ISO /IEC 27002:2013	Controles y objetivos de control	Valoración	Anotaciones				
A.9	**CONTROL DE ACCESOS.**			0,6375		**L0**	2
A.9.1	**Requisitos de negocio para el control de accesos.**			**0,90**		**L1**	0
A.9.1.1	Política de control de accesos.	L3		0,9		**L2**	0
A.9.1.2	Control de acceso a las redes y servicios asociados.	L3		0,9		**L3**	12
A.9.2	**Gestión de acceso de usuario.**			**0,75**		**L4**	0
A.9.2.1	Gestión de altas/bajas en el registro de usuarios.	L3		0,9		**L5**	0
A.9.2.2	Gestión de los derechos de acceso asignados a usuarios.	L3		0,9		**L6**	0
A.9.2.3	Gestión de los derechos de acceso con privilegios especiales.	L3		0,9			
A.9.2.4	Gestión de información confidencial de autenticación de usuarios.	L0		0			
A.9.2.5	Revisión de los derechos de acceso de los usuarios.	L3		0,9			
A.9.2.6	Retirada o adaptación de los derechos de acceso	L3		0,9			
A.9.3	**Responsabilidades del usuario.**			**0,00**			
A.9.3.1	Uso de información confidencial para la autenticación.	L0		0			
A.9.4	**Control de acceso a sistemas y aplicaciones.**			**0,90**			
A.9.4.1	Restricción del acceso a la información.	L3		0,9			
A.9.4.2	Procedimientos seguros de inicio de sesión.	L3		0,9			
A.9.4.3	Gestión de contraseñas de usuario.	L3		0,9			
A.9.4.4	Uso de herramientas de administración de sistemas.	L3		0,9			
A.9.4.5	Control de acceso al código fuente de los programas.	L3		0,9			
						NC Mayores	2
						NC Menores	12
						Observaciones	0

Control de ISO /IEC 27002:2013	Controles y objetivos de control	Valoración	Anotaciones				
A.10	**CIFRADO.**			0,0000		**L0**	0
A.10.1	**Controles criptográficos.**			**0,0**		**L1**	0
A.10.1.1	Política de uso de los controles criptográficos.	L6		N/A		**L2**	0
A.10.1.2	Gestión de claves.	L6		N/A		**L3**	0
						L4	0
						L5	0
						L6	2
						NC Mayores	0
						NC Menores	0
						Observaciones	0

Control de ISO /IEC 27002:2013	Controles y objetivos de control	Valoración	Anotaciones				
A.11	**SEGURIDAD FÍSICA Y AMBIENTAL.**			0,7063		**L0**	2
A.11.1	**Áreas seguras.**			**0,68**		**L1**	0
A.11.1.1	Perímetro de seguridad física.	L3		0,9		**L2**	1
A.11.1.2	Controles físicos de entrada.	L3		0,9		**L3**	9
A.11.1.3	Seguridad de oficinas, despachos y recursos.	L0		0		**L4**	0
A.11.1.4	Protección contra las amenazas externas y ambientales.	L3		0,9		**L5**	0
A.11.1.5	El trabajo en áreas seguras.	L6		N/A		**L6**	3
A.11.1.6	Áreas de acceso público, carga y descarga.	L6		N/A			
A.11.2	**Seguridad de los equipos.**			**0,73750**			
A.11.2.1	Emplazamiento y protección de equipos.	L3		0,9			
A.11.2.2	Instalaciones de suministro.	L3		0,9			
A.11.2.3	Seguridad del cableado.	L2		0,5			
A.11.2.4	Mantenimiento de los equipos.	L3		0,9			
A.11.2.5	Salida de activos fuera de las dependencias de la empresa.	L0		0			
A.11.2.6	Seguridad de los equipos y activos fuera de las instalaciones.	L6		N/A			
A.11.2.7	Reutilización o retirada segura de dispositivos de almacenamiento.	L3		0,9			
A.11.2.8	Equipo informático de usuario desatendido.	L3		0,9			
A.11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla.	L3		0,9			
						NC Mayores	2
						NC Menores	10
						Observaciones	0

Control de ISO /IEC 27002:2013	Controles y objetivos de control	Valoración	Anotaciones				
A.12	**SEGURIDAD EN LA OPERATIVA.**			0,6429		**L0**	5
A.12.1	**Responsabilidades y procedimientos de operación.**			**0,2**		**L1**	0
A.12.1.1	Documentación de procedimientos de operación.	L0		0		**L2**	0
A.12.1.2	Gestión de cambios.	L0		0		**L3**	9
A.12.1.3	Gestión de capacidades.	L3		0,9		**L4**	0
A.12.1.4	Separación de entornos de desarrollo, prueba y producción.	L0		0		**L5**	0
A.12.2	**Protección contra código malicioso.**			**0,90000**		**L6**	0
A.12.2.1	Controles contra el código malicioso.	L3		0,9			
A.12.3	**Copias de seguridad.**			**0,90000**			
A.12.3.1	Copias de seguridad de la información.	L3		0,9			
A.12.4	**Registro de actividad y supervisión.**			**0,67500**			
A.12.4.1	Registro y gestión de eventos de actividad.	L3		0,9			
A.12.4.2	Protección de los registros de información.	L3		0,9			
A.12.4.3	Registros de actividad del administrador y operador del sistema.	L3		0,9			
A.12.4.4	Sincronización de relojes.	L0		0			
A.12.5	**Control del software en explotación.**			**0,90000**			
A.12.5.1	Instalación del software en sistemas en producción.	L3		0,9			
A.12.6	**Gestión de la vulnerabilidad técnica.**			**0,90000**			
A.12.6.1	Gestión de las vulnerabilidades técnicas.	L3		0,9			
A.12.6.2	Restricciones en la instalación de software.	L3		0,9			
A.12.7	**Consideraciones de las auditorías de los sistemas de información.**			**0,00000**			
A.12.7.1	Controles de auditoría de los sistemas de información.	L0		0			
						NC Mayores	5
						NC Menores	9
						Observaciones	0

Control de ISO /IEC 27002:2013	Controles y objetivos de control	Valoración	Anotaciones				
A.13	**SEGURIDAD EN LAS TELECOMUNICACIONES.**			0,1250		**L0**	4
A.13.1	**Gestión de la seguridad en las redes.**			**0,25**		**L1**	0
A.13.1.1	Controles de red.	L2		0,5		**L2**	1
A.13.1.2	Mecanismos de seguridad asociados a servicios en red.	L0		0		**L3**	0
A.13.1.3	Segregación de redes.	L6		N/A		**L4**	0
A.13.2	**Intercambio de información con partes externas.**			**0,00000**		**L5**	0
A.13.2.1	Políticas y procedimientos de intercambio de información.	L0		0		**L6**	2
A.13.2.2	Acuerdos de intercambio.	L6		N/A			
A.13.2.3	Mensajería electrónica.	L0		0			
A.13.2.4	Acuerdos de confidencialidad y secreto.	L0		0			
						NC Mayores	4
						NC Menores	1
						Observaciones	0

Control de ISO /IEC 27002:2013	Controles y objetivos de control	Valoración	Anotaciones				
A.14	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.**			0,3000		**L0**	9
A.14.1	**Requisitos de seguridad de los sistemas de información.**			**0,90**		**L1**	0
A.14.1.1	Análisis y especificación de los requisitos de seguridad.	L3		0,9		**L2**	0
A.14.1.2	Seguridad de las comunicaciones en servicios accesibles por redes públicas.	L6		N/A		**L3**	2
A.14.1.3	Protección de las transacciones por redes telemáticas.	L3		0,9		**L4**	0
A.14.2	**Seguridad en los procesos de desarrollo y soporte.**			**0,00000**		**L5**	0
A.14.2.1	Política de desarrollo seguro de software.	L0		0		**L6**	2
A.14.2.2	Procedimientos de control de cambios en los sistemas.	L0		0			
A.14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	L0		0			
A.14.2.4	Restricciones a los cambios en los paquetes de software.	L0		0			
A.14.2.5	Uso de principios de ingeniería en protección de sistemas.	L0		0			
A.14.2.6	Seguridad en entornos de desarrollo.	L0		0			
A.14.2.7	Externalización del desarrollo de software.	L6		N/A			
A.14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas.	L0		0			
A.14.2.9	Pruebas de aceptación.	L0		0			
A.14.3	**Datos de prueba.**			**0,00000**			
A.14.3.1	Protección de los datos utilizados en pruebas.	L0		0			
						NC Mayores	9
						NC Menores	2
						Observaciones	0

Control de ISO /IEC 27002:2013	Controles y objetivos de control	Valoración	Anotaciones				
A.15	**RELACIONES CON SUMINISTRADORES.**			0,6167		**L0**	1
A.15.1	**Seguridad de la información en las relaciones con suministradores.**			**0,33**		**L1**	0
A.15.1.1	Política de seguridad de la información para suministradores.	L2		0,5		**L2**	2
A.15.1.2	Tratamiento del riesgo dentro de acuerdos de suministradores.	L2		0,5		**L3**	2
A.15.1.3	Cadena de suministro en tecnologías de la información y comunicaciones.	L0		0		**L4**	0
A.15.2	**Gestión de la prestación del servicio por suministradores.**			**0,90000**		**L5**	0
A.15.2.1	Supervisión y revisión de los servicios prestados por terceros.	L3		0,9			
A.15.2.2	Gestión de cambios en los servicios prestados por terceros.	L3		0,9			
						NC Mayores	1
						NC Menores	4
						Observaciones	0

Control de ISO /IEC 27002:2013	Controles y objetivos de control	Valoración	Anotaciones				
A.16	**GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.**			0,9333		**L0**	0
A.16.1	**Gestión de incidentes de seguridad de la información y mejoras.**			**0,93**		**L1**	0
A.16.1.1	Responsabilidades y procedimientos.	L3		0,9		**L2**	0
A.16.1.2	Notificación de los eventos de seguridad de la información.	L4		0,95		**L3**	1
A.16.1.3	Notificación de puntos débiles de la seguridad	L4		0,95		**L4**	6
A.16.1.4	Valoración de eventos de seguridad de la información y toma de decisiones.	L4		0,95		**L5**	0
A.16.1.5	Respuesta a los incidentes de seguridad.	L4		0,95		**L6**	0
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información.	L4		0,95			
A.16.1.7	Recopilación de evidencias.	L4		0,95			
					NC Mayores		0
					NC Menores		1
					Observaciones		6

Control de ISO /IEC 27002:2013	Controles y objetivos de control	Valoración	Anotaciones				
A.17	**ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.**			0,4500		**L0**	1
A.17.1	**Continuidad de la seguridad de la información.**			**0,9**		**L1**	0
A.17.1.1	Planificación de la continuidad de la seguridad de la información.	L3		0,9		**L2**	0
A.17.1.2	Implantación de la continuidad de la seguridad de la información.	L3		0,9		**L3**	3
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la Seguridad de la información.	L3		0,9		**L4**	0
A.17.2	**Redundancias.**			**0,00000**		**L5**	0
A.17.2.1	Disponibilidad de instalaciones para el procesamiento de la información.	L0		0		**L6**	0
					NC Mayores		1
					NC Menores		3
					Observaciones		0

Control de ISO /IEC 27002:2013	Controles y objetivos de control	Valoración	Anotaciones				
A.18	**CUMPLIMIENTO.**			0,7500		**L0**	1
A.18.1	**Cumplimiento de los requisitos legales y contractuales.**			**0,90**		**L1**	0
A.18.1.1	Identificación de la legislación aplicable.	L3		0,9		**L2**	0
A.18.1.2	Derechos de propiedad intelectual (DPI).	L6		N/A		**L3**	5
A.18.1.3	Protección de los registros de la organización.	L3		0,9		**L4**	0
A.18.1.4	Protección de datos y privacidad de la información personal.	L3		0,9		**L5**	0
A.18.1.5	Regulación de los controles criptográficos.	L6		N/A		**L6**	2
A.18.2	**Revisiones de la seguridad de la información.**			**0,60000**			
A.18.2.1	Revisión independiente de la seguridad de la información.	L0		0			
A.18.2.2	Comprobación del cumplimiento	L3		0,9			
A.18.2.3	Disponibilidad de instalaciones para el procesamiento de la información.	L3		0,9			
					NC Mayores		1
					NC Menores		5
					Observaciones		0

ANEXO N. FASE 5 - NIV MADU CONTR CMM_ISO27002_2013.mht

RESUMEN ANALITICO ESPECIALIZADO R.A.E

Título de Documento.	PLAN DE IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA UNIDAD ADMINISTRATIVA PARQUES NACIONALES NATURALES DE COLOMBIA, SEGÚN NORMA ISO 27001:2013
Autor	GONZALEZ TABARES Eduin Gildardo
Fuentes Bibliográficas	-Implantación de un SGSI en la entidad incibe [en línea]. Disponible en: <https://www.incibe.es/extfrontinteco/img/file/intecocert/sgsi/img/guia_apoyo_sgsi.pdf> -INTECO. Curso de sistemas de gestión de la seguridad de la información según la norma une iso iec 27001 [en línea]. Disponible en: <https://formacion-online.inteco.es/curso/index.php> -Sistema de gestión de seguridad de la información en una organización [en línea]. Disponible en: <http://cert.inteco.es/extfrontinteco/img/file/intecocert/sgsi/> ma.%20ntc-iso-iec%2027001.pdf> [citado en 10 de octubre de 2015] -PORTAL DE ISO 27001 EN ESPAÑOL. El anexo de iso 27001 en español [en línea]. Disponible en: <http://iso27002.wiki.zoho.com/> -PORTAL SENA. Estándares para la seguridad de la información [en línea]. Disponible en: <https://senaintro.blackboard.com/bbcswebdav/1/oa_estandarseguridad/oc.pdf> -SEGU-INFO . Políticas de seguridad de la información [en línea]. Disponible en: <http://www.segu-info.com.ar/politicas/polseginf.htm> -Certificación ISO-27001 [en línea]. Disponible en: <http://www.segu-info.com.ar/foro/?q=certificacion>
Año	2018
Resumen	El presente tiene como objetivo la implementación de un sistema de gestión de seguridad de la información para la UNIDAD ADMINISTRATIVA PARQUES NACIONALES NATURALES DE COLOMBIA, SEGÚN NORMA ISO 27001:2013. El plan de implementación de la ISO / IEC 27001: 2013 es un aspecto clave en cualquier organización que quiera alinear sus procedimientos con esta norma. Así pues, para conseguir el objetivo final del proyecto con éxito, este se ha estructurado en seis fases. En primer lugar, se ha realizado una descripción de los objetivos, alcance y expectativas a cumplir, partiendo de un análisis de la situación inicial a nivel de seguridad de la información. En tanto que todo Sistema de Gestión de Seguridad de la Información se apoya en un cuerpo documental para el cumplimiento normativo, se han desarrollado los principales documentos del SGSI para PARQUES NACIONALES NATURALES DE COLOMBIA: política de seguridad, procedimiento de auditorías internas, gestión de indicadores, procedimiento de revisión por dirección, gestión de roles y responsabilidades, comité de seguridad, SOA y análisis de riesgos. Llegados a este punto, se ha elaborado un análisis de riesgos aplicando la metodología Magerit v.3, para cuantificar la importancia de los activos. Y a partir de esta información, se definieron un conjunto de iniciativas y proyectos necesarios para conseguir el nivel de seguridad que PARQUES NACIONALES NATURALES DE COLOMBIA requiere. Una vez implementados los proyectos y con el objetivo de evaluar la madurez de la seguridad, se ha realizado una auditoría de cumplimiento de la norma. Para determinar la madurez de los controles una vez implementados los nuevos procesos.
Palabras claves	Autenticidad, Confidencialidad, Controles, Disponibilidad, Integridad, ISO/IEC 27001:2013, ISO/IEC 27002:2013, Magerit, Políticas De Seguridad, Proceso, Riesgos,

	Sistema De Gestión De Seguridad De La Información (Sgsi), Trazabilidad, Vulnerabilidades.
Contenidos	Enfoque y método para seguir. ❯ **FASE I: Situación actual.** Contextualización, objetivos y análisis diferencial, Contextualización y objetivos, Objetivos y alcance del plan director de seguridad, Análisis diferencial de la situación inicial respecto a la norma ISO/IEC 27001:2013, Análisis diferencial de la situación inicial respecto a la norma ISO/IEC 27002:2013. ❯ **FASE II: Sistema de Gestión Documental.** política de seguridad, procedimiento de auditorías internas, gestión de indicadores, procedimiento de revisión por dirección., gestión de roles y responsabilidades., comité de seguridad del SGSI. declaración de aplicabilidad, metodología del análisis de riesgos. ❯ **FASE III: Análisis de riesgos**. inventario y valoración de los activos, análisis de amenazas, impacto potencial, riesgo potencial, riesgos a tratar. ❯ **FASE IV: Propuesta de Proyectos**. propuestas de mejora, planificación temporal de ejecución, evaluación del riesgo tras la implantación de los proyectos, nivel de cumplimientos de la norma ISO/IEC 27002:2013- ❯ **FASE V: Auditoría de Cumplimiento de la ISO IEC 27002: 2013** plan de auditoria, alcance, evolución del análisis diferencial. ❯ **FASE VI:** Presentación de resultados y entrega de informes
Descripción del problema	La entidad PARQUES NACIONALES NATURALES DE COLOMBIA desea tener una propuesta que permita identificar, disminuir y mitigar los riesgos al que se encuentra expuesta actualmente, Desea contar con un modelo de Gestión de Seguridad de la Información (SGSI) permitiendo proteger la confidencialidad, integridad y disponibilidad de la información. Esta propuesta será de gran importancia para la entidad, teniendo en cuenta que no ha definido políticas que tengan que ver con seguridad informática, otro aspecto inexistente es la asignación de responsabilidades en materia de seguridad, no se cuenta con procedimientos en materia de seguridad física y desastres de origen natural que afecten los activos de la entidad, entre los problemas más graves se encuentra el uso inadecuado de los recursos tecnológicos, falta de control en navegación por la internet y uso inadecuado del correo electrónico.
Objetivos	OBJETIVO GENERAL. Planear la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) para la Unidad Administrativa Parques Nacionales Naturales de Colombia, según la norma ISO 27001:2013, para gestionar la seguridad de la información poder reducir los riesgos, amenazas y vulnerabilidades que pueden afectar a los activos del área. OBJETIVOS ESPECÍFICOS. Localizar los puntos más vulnerables dentro del área. Identificar las amenazas y los riesgos de que ocurran éstas. Seleccionar los controles de la norma ISO 27002 para la reducción de riesgos y amenazas en el área. Identificar el estado actual de los activos informáticos que serán objeto de protección por el SGSI Describir los fundamentos de un SGSI y Diseñar un SGSI acorde a las necesidades de la entidad Elaborar una guía básica con políticas y procedimientos, en base a las normas internacionales.
Metodología	La propuesta de investigación es de tipo exploratoria y descriptiva.

	Exploratoria: se explora y analiza la situación inicial de la entidad, se aplican las técnicas necesarias para recolectar y analizar datos con el fin de describir, generar procedimientos e implementar normas acordes con las necesidades de la Entidad, siguiendo la metodología Magerit v.3 Descriptiva: se describen y comparan los procedimientos y políticas existentes, se realiza un análisis diferencial de las medidas de seguridad y normativa en relación con la seguridad de la información que tenía la organización, tomando como referencia la norma ISO / IEC27001: 2013 y el código de buenas prácticas detallado en la ISO / IEC27002: 2013 contemplando los controles y objetivos de los dominios. Por consiguiente, el plan de implementación de la ISO / IEC 27001: 2013 es un aspecto clave en cualquier organización que quiera alinear sus procedimientos con esta norma. Para conseguir el objetivo final del proyecto con éxito, este se ha estructurado en seis fases. **FASE I: Situación actual:** **FASE II: Sistema de gestión documental.** **FASE III: Análisis de riesgos.** **FASE IV: Propuestas de proyectos.** **FASE V: Auditoria del cumplimiento.**
Resultados	Se da inicio a la elaboración e implantación de un esquema documental en la entidad, el cual no existía. Ahora se dispone de una correcta documentación, clasificada y fácilmente accesible. Esto repercute en la calidad de los procesos y en los controles de los mismos. Cabe Destacar que los dominios A6, A13 y A14 son los dominios donde se han detectado contrariedades mayores, que requieren un mayor trabajo para ser resueltos. Estos dominios recibirán proyectos específicos con mayor inversión, pues se trata de dominios que no han sido tenidos en cuenta dentro de la empresa desde hace mucho tiempo y se encuentran en niveles realmente bajos de cumplimiento (<=30%). Se aprecia notablemente la mejoría en términos generales de la seguridad dentro de la entidad. Desafortunadamente queda mucho por hacer antes de poder ser certificados en la norma ISO. Como se observa en la tabla de No Conformidades, en todos los dominios de la norma en los que PARQUES NACIONALES NATURALES DE COLOMBIA ha mejorado, existen todavía varias No Conformidades menores que impiden que se alcance el nivel mínimo de cumplimiento. Estas “no conformidades” son fácilmente subsanables mediante la creación de proyectos específicos a tal efecto complementando los existentes o generando nuevos. Como ganancia se consiguió un compromiso de la dirección con la Seguridad de la Información. Gracias a este proyecto, la dirección de la entidad que antes se mostraba distante y sin interés por todo lo relacionado con la informática, ahora se involucra activamente en la toma de decisiones apoyando procesos y proyectos. Este es el primer paso necesario para conseguir la certificación / IEC27001: 2013 en un futuro próximo.
Conclusiones	En la actualidad el tema de seguridad de la información toma cada vez mayor importancia al interior de las organizaciones, y es creciente el número de organizaciones que necesitan asegurar sus sistemas, bien sea porque quieran certificarse para garantizar que sus sistemas sean seguros o porque de alguna forma

	han sufrido ataques y pretenden desarrollar una estrategia de seguridad basándose en las mejores prácticas de aseguramiento de la información expuestas en las normas. El desarrollo e implementación del Sistema de Gestión de Seguridad de la Información (SGSI) para la Unidad Administrativa Parques Nacionales Naturales de Colombia, según la norma ISO 27001:2013, reduce los riesgos, amenazas y vulnerabilidades que pueden afectar a los activos del área, es una necesidad para todas las empresas que se preocupan por la gestión de la seguridad de la información o los riesgos relacionados con la TI. En primer lugar, se localizaron los puntos más vulnerables dentro de la entidad, se Identificaron y analizaron las amenazas y los riesgos de que ocurran éstas, Se seleccionaron los controles de la norma ISO 27002 para la reducción de riesgos y amenazas en el área, se Identificaron los activos informáticos que son objeto de protección por el SGSI, Luego de comprender los procesos críticos de organización, se desarrolló el sistema de gestión documental y posterior a esto se elaboró su análisis de riesgo. Gracias a la metodología empleada, se elabora una guía básica con políticas y procedimientos, en base a las normas internacionales y por último se diseña un SGSI acorde a las necesidades de la entidad. Gracias a esto y a una correcta aplicación de lo aquí expuesto, se cumple con el objetivo de mejorar el diagnóstico inicial del sistema de seguridad de la información, se definieron un conjunto de nuevos proyectos. y posterior a esto, se ha auditado el SGSI, verificando ISO / IEC27001: 2013 con resultados positivos para la entidad.