DISEÑO DEL PROCESO DE COPIAS DE SEGURIDAD DE TI DE LA SUBDIRECCIÓN DE INNOVACIÓN Y SERVICIOS TECNOLOGICOS QUE APOYE EL MODELO GRC PARA EL INSTITUTO NACIONAL DE METROLOGÍA-INM

DAVID HERNAN BALLEN VARGAS
JHON ALEXANDER DÍAZ MORENO

UNIVERSIDAD CATÓLICA DE COLOMBIA
FACULTAD DE INGENIERIA
PROGRAMA DE ESPECIALIZACIÓN EN AUDITORÍA DE SISTEMAS DE INFORMACIÓN
BOGOTÁ D.C.
JULIO DE 2015

DISEÑO DEL PROCESO DE COPIAS DE SEGURIDAD DE TI DE LA SUBDIRECCIÓN DE INNOVACIÓN Y SERVICIOS TECNOLOGICOS QUE APOYE EL MODELO GRC PARA EL INSTITUTO NACIONAL DE METROLOGÍA-INM

DAVID HERNAN BALLEN VARGAS
JHON ALEXANDER DÍAZ MORENO

Trabajo de Grado para optar al título de
Especialista en auditoría de sistemas de información

DIRECTOR
CESAR ORLANDO DIAZ BENITO
Ingeniero de Sistemas

UNIVERSIDAD CATÓLICA DE COLOMBIA
FACULTAD DE INGENIERIA
PROGRAMA DE ESPECIALIZACIÓN EN AUDITORÍA DE SISTEMAS DE INFORMACIÓN
BOGOTÁ D.C.
JULIO DE 2015

Nota de Aceptación.

_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Bogotá D.C., Julio de 2015

creative commons

Atribución-NoComercial-SinDerivadas 2.5 Colombia (CC BY-NC-ND 2.5)

La presente obra está bajo una licencia:
Atribución-NoComercial-SinDerivadas 2.5 Colombia (CC BY-NC-ND 2.5)
Para leer el texto completo de la licencia, visita:
http://creativecommons.org/licenses/by-nc-nd/2.5/co/

Usted es libre de:

Compartir - copiar, distribuir, ejecutar y comunicar públicamente la obra

Bajo las condiciones siguientes:

Atribución — Debe reconocer los créditos de la obra de la manera especificada por el autor o el licenciante (pero no de una manera que sugiera que tiene su apoyo o que apoyan el uso que hace de su obra).

No Comercial — No puede utilizar esta obra para fines comerciales.

Sin Obras Derivadas — No se puede alterar, transformar o generar una obra derivada a partir de esta obra.

DEDICATORIA

Gracias a Dios por guiar mi vida y permitirme cumplir las metas que me propongo, por poner en mi vida personas tan especiales como mi madre de la cual solo recibo apoyo incondicional y buenos consejos y a mi padre quien desde el cielo cuida de mí. David Hernán Ballén Vargas

A Dios por permitirme concluir una etapa más de mi vida y a mis padres por su apoyo incondicional y ejemplo de perseverancia. Jhon Alexander Díaz Moreno.

TABLA DE CONTENIDO

LISTA DE GRAFICAS

LISTA DE TABLAS

ANEXOS

ANEXO 1. ESTRUCTURA ORGANIZACIONAL

ANEXO 2. REGISTRO FOTOGRAFICO DE

DIAGNOSTICO ANEXO 3. ENCUESTA DIAGNOSTICO 1

ANEXO 4. ENCUESTA DIAGNOSTICO 2

ANEXO 5. FORMATO DE SOLICITUD DE INFORMACION A RESPALDAR

ANEXO 6. CARACTERIZACION DEL PROCESO

ANEXO 7. FORMATO ENTREGA DE BACKUPS

ANEXO 8. DISEÑO DEL PROCESO DE COPIAS DE SEGURIDAD

ANEXO 9. CARTA DE APOYO AL DESARROLLO DEL

PROYECTO ANEXO 10. REGISTRO FIRMA SOCIALIZACION.

GLOSARIO

Activo: En relación con la seguridad de la información, se refiere a cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización. (ISO/IEC 13335-1:2004).

Alcance: Ámbito de la organización que queda sometido al SGSI. Debe incluir la identificación clara de las dependencias interfaces y limites con el entorno, sobre todo si solo incluye una parte de la organización.

Alta dirección: Persona o grupo de personas que dirigen y controlan al más alto nivel una entidad. (NTCGP 1000:2004).

Amenaza: Una causa potencial de un incidente no-deseado, el cual puede resultar en daño a un sistema u organización (ISO/IEC 13335-1:2004).

Análisis del riesgo: Proceso general del análisis del riesgo y la evaluación del riesgo (ISO/IEC Guía 73:2002).

BACK-UP: Copia de seguridad de los archivos, aplicaciones y/o bases de datos disponibles en un soporte magnético (generalmente discos extraíbles, unidades de cinta), con el fin de poder recuperar la información en caso de un daño, borrado accidental o un accidente imprevisto.

Base de Datos: Conjunto de datos que pertenecen al mismo contexto almacenados sistemáticamente. En una base de datos, la información se organiza en campos y registros. Los datos pueden aparecer en forma de texto, números, gráficos, sonido o vídeo.

Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados. (NTC 5411-1:2006).

Control: Medios para manejar el riesgo; incluyendo políticas, procedimientos, lineamientos, practicas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas, de gestión o de naturaleza legal. El control también se utiliza como sinónimo de salvaguarda o contramedida. (ISO/IEC 17799-2:2005).

Copia de Respaldo o Seguridad: Acción de copiar archivos o datos de forma que estén disponibles en caso de que un fallo produzca la pérdida de los originales.

Custodio: encargado de resguardar la información, debe seguir los lineamientos definidos por el dueño de la información para su protección.

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada. (NTC 5411-1:2006).

Efectividad: Medida del impacto de la gestión tanto en el logro de los resultados planificados, como en el manejo de los recursos utilizados y disponibles. La medición de la efectividad se denomina en la Ley 872 de 2003 como una medición del impacto. (NTCGP 1000:2004).

Eficacia: Grado en el que se realizan las actividades planificadas y se alcanzan los resultados planificados. La medición de la eficacia se denomina en la Ley 872 de 2003 como una medición de resultado. (NTCGP 1000:2004).

Eficiencia: Relación entre el resultado alcanzado y los recursos utilizados. (NTCGP 1000:2004).

Estructura de la entidad: Disposición de responsabilidades, autoridades y relaciones entre el personal. Dicha disposición es, generalmente, ordenada. En entidades del Estado la estructura organizacional está definida, normalmente, por la ley. (NTCGP 1000:2004).

Evaluación del riesgo: Proceso de comparar el riesgo estimado con un criterio de riesgo dado para determinar la importancia del riesgo (ISO/IEC Guía 73: 2002).

Evento de seguridad de la información: Cualquier evento de seguridad de la información es una ocurrencia identificada del estado de un sistema, servicio o red

indicando una posible falla en la política de seguridad de la información o falla en las salvaguardas, o una situación previamente desconocida que puede ser relevante para la seguridad. (ISO/IEC TR 18044:2004).

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con relación al riesgo. La gestión del riesgo normalmente incluye la evaluación del riesgo, tratamiento del riesgo, aceptación del riesgo y comunicación del riesgo. (ISO/IEC Guía 73: 2002).

Impacto: El coste para la empresa de un incidente - de la escala que sea-, que puede o no ser medido en términos estrictamente financieros.

Incidente de seguridad de la información: Un incidente de seguridad de la información es indicado por un solo evento o una serie de eventos inesperados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar la seguridad de la información (ISO/IES TR 18044:2004).

Infraestructura: Sistema de instalaciones, equipos y servicios necesarios para el funcionamiento de una entidad. (NTCGP 1000:2004).

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos. (NTC 5411-1:2006).

Lineamiento: Una descripción que aclara qué se debiera hacer y como, para lograr los objetivos establecidos en las políticas (ISO/IEC 1335-1:2004).

Medios de procesamiento de información: Cualquier sistema, servicio o infraestructura de procesamiento de la información, o los locales físicos que los alojan. (ISO/IEC 17799-2:2005).

Política: Intención y dirección general expresada formalmente por la gerencia. (ISO/IEC 17799-2:2005).

Procedimiento: Forma especificada para llevar a cabo una actividad o un proceso. (NTCGP 1000:2004).

Proceso: Conjunto de actividades relacionadas mutuamente o que interactúan para generar valor y las cuales transforman elementos de entrada en resultados. Los elementos de entrada para un proceso son generalmente salidas de otros procesos. Los procesos de una entidad son, generalmente, planificados y puestos en práctica bajo condiciones controladas, para generar valor. (NTCGP 1000:2004).

Propietario/responsable: Define el criterio de clasificación de la información, indica que se puede hacer con el activo, autoriza privilegios y define ciclo de vida. Riesgo residual: Nivel restante de riesgo después del tratamiento del riesgo. (ISO/IEC Guía 73:2002).

Riesgo: Combinación de la probabilidad de un evento y su ocurrencia. (ISO/IEC Guía 73:2002).

Seguridad de la información: Preservación de confidencialidad, integración y disponibilidad de la información; además, también puede involucrar otras propiedades como autenticidad, responsabilidad, no-repudiación y confiabilidad. (ISO/IEC 17799-2:2005).

Tercera persona: Esa persona u organismo que es reconocido como independiente de las partes involucradas, con relación al ítem en cuestión. (ISO/IEC Guía 2: 1996).

Tratamiento del riesgo: Proceso de selección e implementación de medidas para modificar el riesgo. (ISO/IEC Guía 73: 2002).

Usuario: Quien usa la información, responsable de su buena utilización.

Valoración del riesgo: Proceso global de análisis y evaluación del riesgo. (ISO/IEC Guía 73: 2002).

Vulnerabilidad: La debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas. (ISO/IEC 13335-1:2004).

INTRODUCCIÓN

Hemos elaborado el presente trabajo, no solo como la opción para optar al título como Especialistas en Auditoria de Sistemas de Información, sino con el fin de poner en práctica los conocimientos impartidos por nuestros docentes y que fueron adquiridos a lo largo de nuestra formación, buscando con ellos desarrollar habilidades que contribuyan a un mejor desempeño para nuestras vidas laborales y profesionales engrandeciendo así el nombre de la universidad que nos acogió. Del mismo buscamos que las organizaciones se concienticen de la importancia de los Sistemas de Información y se acojan estrategias de buenas prácticas para proteger su información más sensible e importante de los diferentes eventos que las pueden afectar.

De acuerdo a la NTC-ISO-IEC27002 “La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la organización y, en consecuencia, necesita una protección adecuada”, así las cosas el proteger la información y los sistemas que la soportan de las perdidas, el deterioro y las catástrofes que los pueden afectar (como lo son las naturales, o causados por el hombre) los convierte en recursos de gran importancia para las organizaciones independientemente del tamaño o de su naturaleza, por ende una de las máximas prioridades, razón por la cual se hace énfasis en esta investigación al mismo, adaptando una propuesta que mejore las políticas, procesos, procedimientos y las prácticas en los procesos de TI especialmente al respaldo de información y el restablecimiento de la operación, generando el mayor beneficio al Instituto Nacional de Metrología INM y que apoyen la implementación del modelo de Gobierno, Riesgo y cumplimiento GRC en la entidad.

Para tal fin se realizo inicialmente, un acercamiento a la organización, mediante la verificación de manuales de procesos y procedimientos, al igual que entrevistas con los responsables de los procesos que permitieron la obtención de información sobre las estrategias y practicas establecidas en el INM en sus procesos de TI, relacionados especialmente con las copias de seguridad y la continuidad del servicio, con los que se pudo evidenciar las oportunidades de mejora que se pueden implementar en la organización.

1 ANTECEDENTES

1.1 RIESGOS, CONTROL INTERNO Y GOBIERNO CORPORATIVO A TRAVÉS DEL TIEMPO

Acuerdo de Basilea I. Este conjunto de recomendaciones publicado en 1988 "era una medida de objetivos limitados dirigida a un pequeño grupo de bancos activos internacionalmente que competían en los mismos mercados, para eliminar ventajas competitivas injustas resultantes de discrepancias relacionadas a los regímenes reguladores". Este acuerdo "era simple y establecía que los supervisores nacionales debían exigir a los bancos activos internacionalmente que mantuvieran un valor neto (capital propio) en la proporción de un 8% de sus activos considerados de alto riesgo (el riesgo era determinado por el comité mismo, y añadido al anexo del acuerdo)".

"A pesar de que Basilea I fue creado para ser aplicado, a los países más ricos, se convirtió en norma habitual de todos los bancos en (casi) todos los países (...) A mediados de la década de los 1990, más de 120 países habían adherido a Basilea I o tenían la intención de hacerlo después de un cierto período de transición.

Sin embargo, se reconoció la necesidad de una modificación profunda de Basilea I que permitiera crear regulaciones apropiadas para ser adoptadas por un gran número de países

Committee of the Treadway Commission of the Sponsoring Organization (COSO). 1992. Marco para el diseño, evaluación y monitoreo del control interno, es una iniciativa conjunta de las siguientes organizaciones:

- ✓ Asociación de Contadores Públicos Norteamericanos (“AAA”).
- ✓ Instituto Norteamericanos de Contadores Públicos Certificados (“AICPA”)
- ✓ Asociación Internacional de Ejecutivos de Finanzas (“FEI”)
- ✓ Instituto de Gerentes de Contabilidad (“IMA”)
- ✓ Instituto de Auditores Internos (“IIA”).

Misión COSO “…proporcionar liderazgo de pensamiento a través de la creación de estructuras y orientaciones generales sobre la gestión del riesgo empresarial, el control interno y la disuasión del fraude diseñado para mejorar el desempeño

organizacional, la gestión y reducir el alcance del fraude en las organizaciones.” (www.coso.org/aboutus.htm).

COBIT Marco de Control Interno para Procesos y aplicaciones de tecnología de información. 1996.

Este marco de referencia describe las mejores prácticas que pueden utilizar las compañías para controlar la información mediante la Tecnología de información (TI) y los riesgos que conllevan.

El Cobit fue divulgado por Information System Audit and Control Foundation (ISACA), en 1996, y ha sido actualizado en 1998, 2000, 2005, habiéndose divulgado la versión 4.1 del Cobit en el 2007.

PGC Principios de Gobierno Corporativo de la Organización para la Cooperación y Desarrollo Económico (OCDE) 2004. El concepto de gobierno corporativo se refiere al conjunto de principios y normas que regulan el diseño, integración y funcionamiento de los órganos de gobierno de la empresa, como son los tres poderes dentro de una sociedad:

Los Accionistas, Directorio y Alta Administración. En español se utiliza también gobernanza corporativa, gobernanza societaria y gobierno societario. (Salvochea, Ramiro. Mercados y Gobernancia. La revolución del "Corporate Governance", 2012).

Un buen Gobierno Corporativo provee los incentivos para proteger los intereses de la compañía y los accionistas, monitorizar la creación de valor y uso eficiente de los recursos brindando una transparencia de información.

La Organización para la Cooperación y el Desarrollo Económicos (OCDE), emitió en mayo de 1999 y revisó en 2004 sus “Principios de Gobierno Corporativo” en los que se encuentran las ideas básicas que dan forma al concepto que es utilizado por los países miembros y algunos otros en proceso de serlo. (http://www.confecamaras.org.co/gobierno-corporativo/165-que-es-gobierno-corporativo)

Interno SOX (S. 404). Requerimientos de control interno sobre los procesos con impacto en la información financiera. 2002

COSO ERM Marco para la administración integral de riesgos y oportunidades. 2004.

Basilea II Riesgos Sector Financiero: Estándar internacional respecto del capital necesario frente a los riesgos de cada Institución.

El propósito de este acuerdo, publicado inicialmente en 2004, es "la creación de un estándar internacional que sirva de referencia a los reguladores bancarios, con objeto de establecer los requerimientos de capital necesarios, para asegurar la protección de las entidades frente a los riesgos financieros y operativos".

Además de determinar requisitos de capital diferenciados para diferentes clases de bancos, también dirige la acción de supervisores y define los requisitos de acceso a la información.

Basilea II depende de tres pilares: coeficientes de capitales basados en riesgo, supervisión y disciplina de mercado. La sección más importante del nuevo texto se refiere a los requisitos de capital. Los supervisores realizan más funciones. Evalúan la calificación de riesgo, los sistemas gerenciales, y la estructura administrativa del banco para implementar la estrategia de riesgo y para manejar aquellos riesgos que no hayan sido tratados explícitamente en el nuevo acuerdo, como los riesgos de liquidez.

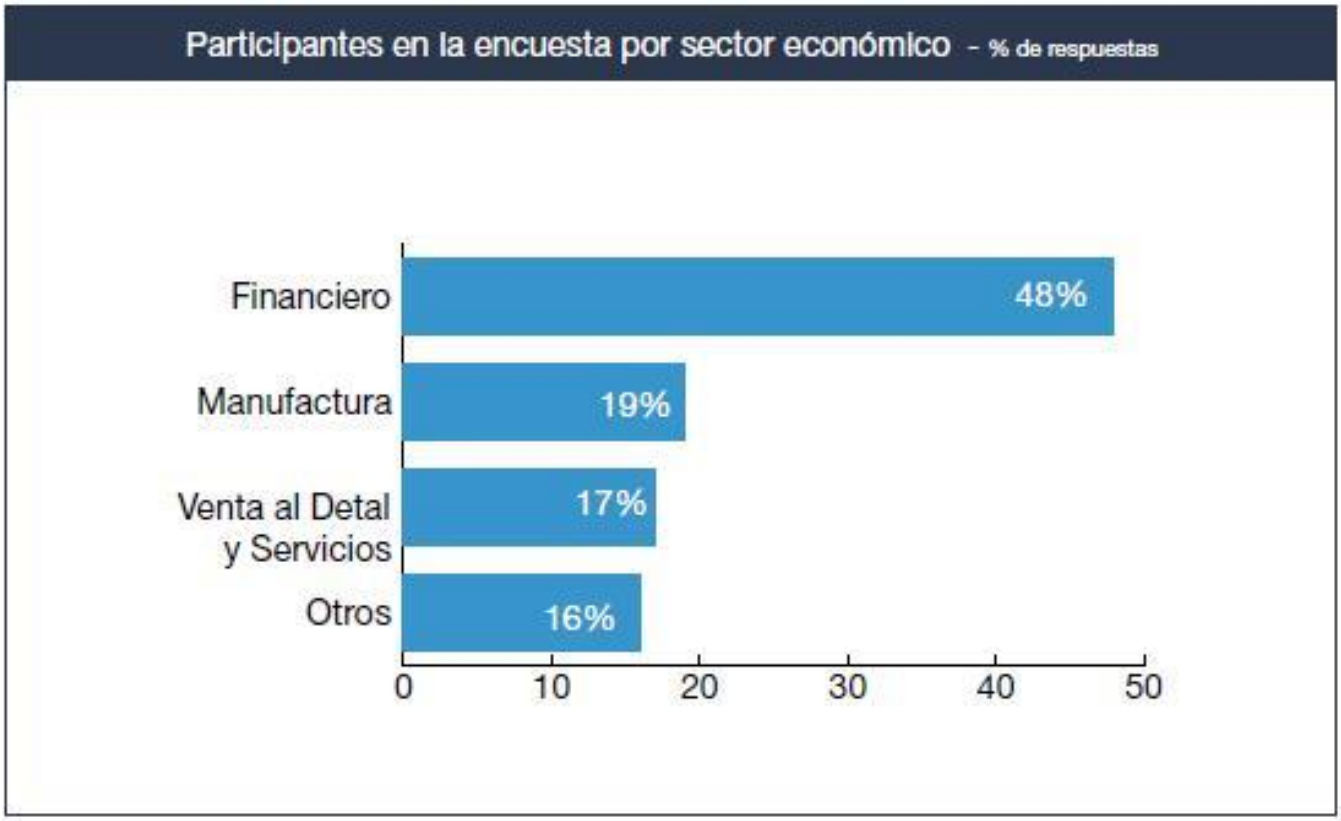
1.2 PLANTEAMIENTO Y DESCRIPCIÓN DEL PROBLEMA

La evolución de las organizaciones desde el punto de vista estratégico ha sido un factor determinante para el éxito en los últimos tiempos, ya que los esfuerzos de la dirección y la conciencia del riesgo han generado nuevas exigencias que basadas en experiencias cotidianas requieren la aplicación de controles que garanticen el cumplimiento de los códigos éticos, políticas corporativos, y demás procedimientos necesarios para el buen desarrollo y cumplimiento de los objetivos de una determinada organización.

Por lo anterior es posible afirmar que los esfuerzos continuos por alcanzar una Inteligencia de gobierno corporativo capaz de determinar los factores de riesgo brindando acciones en tiempo real, continúan siendo limitadas ya que constantemente se generan nuevos factores de riesgo adicionales que según la

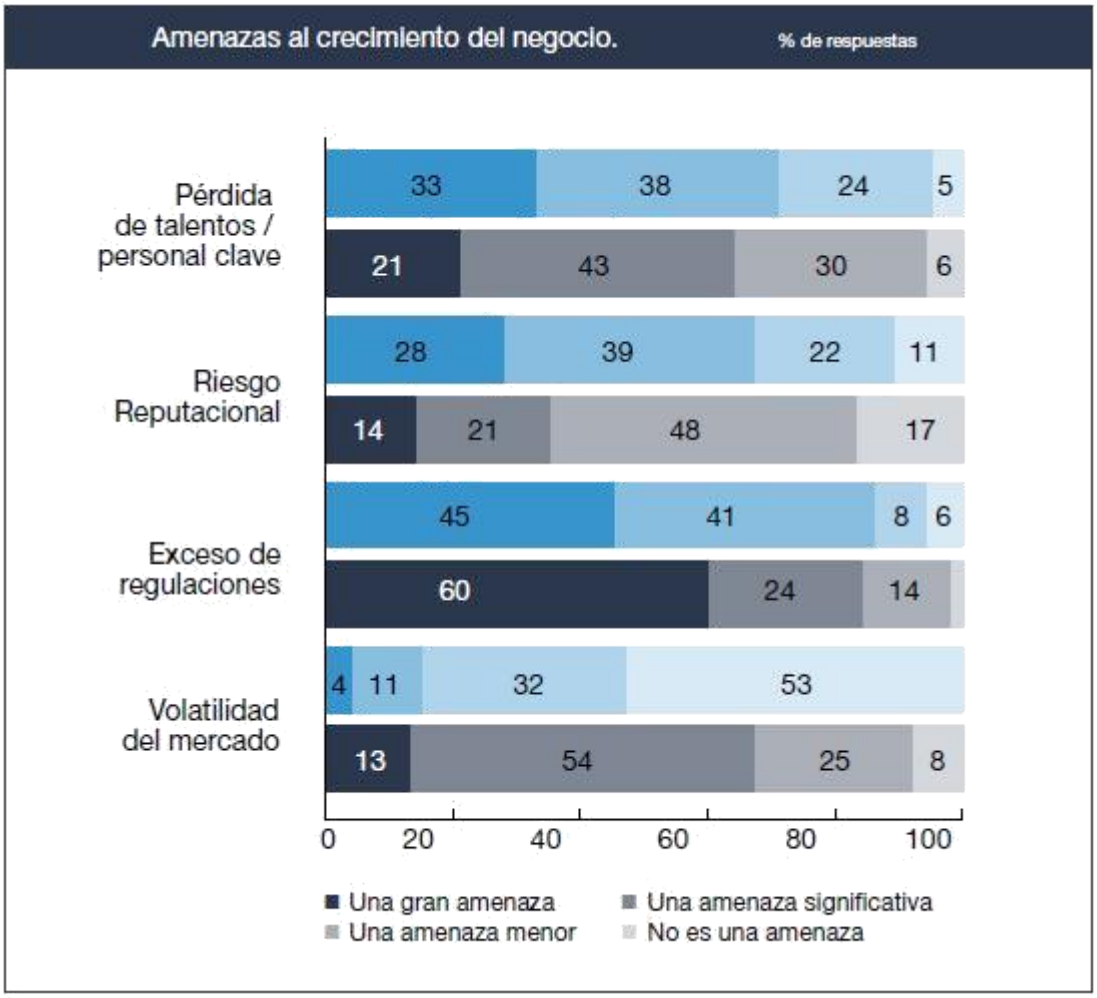
industria evidencian falencias, lo anterior teniendo en cuenta estudios como los realizados por "*Espiñeira, Sheldon y Asociados,* Firma miembro de PricewaterhouseCoopers, la cual está enfocada en áreas críticas de interés para líderes del negocio *a* nivel mundial donde se afirma que factores como el exceso de regulaciones encabeza la lista de las amenazas potenciales que afectan con mayor impacto a las empresas originando una gestión no fiable demostrando la baja tolerancia al riesgo sin priorizar mecanismos y controles internos que aporten a las diversas iniciativas del negocio.

El estudio realizado por Espiñera, Sheldon y asociados realizo sus investigaciones para los siguientes sectores:



Gráfica 1Encuestas riesgo controlado.

Donde se detectaron los siguientes factores como amenazas que estarían en calidad de ser controlables con un modelo GRC:

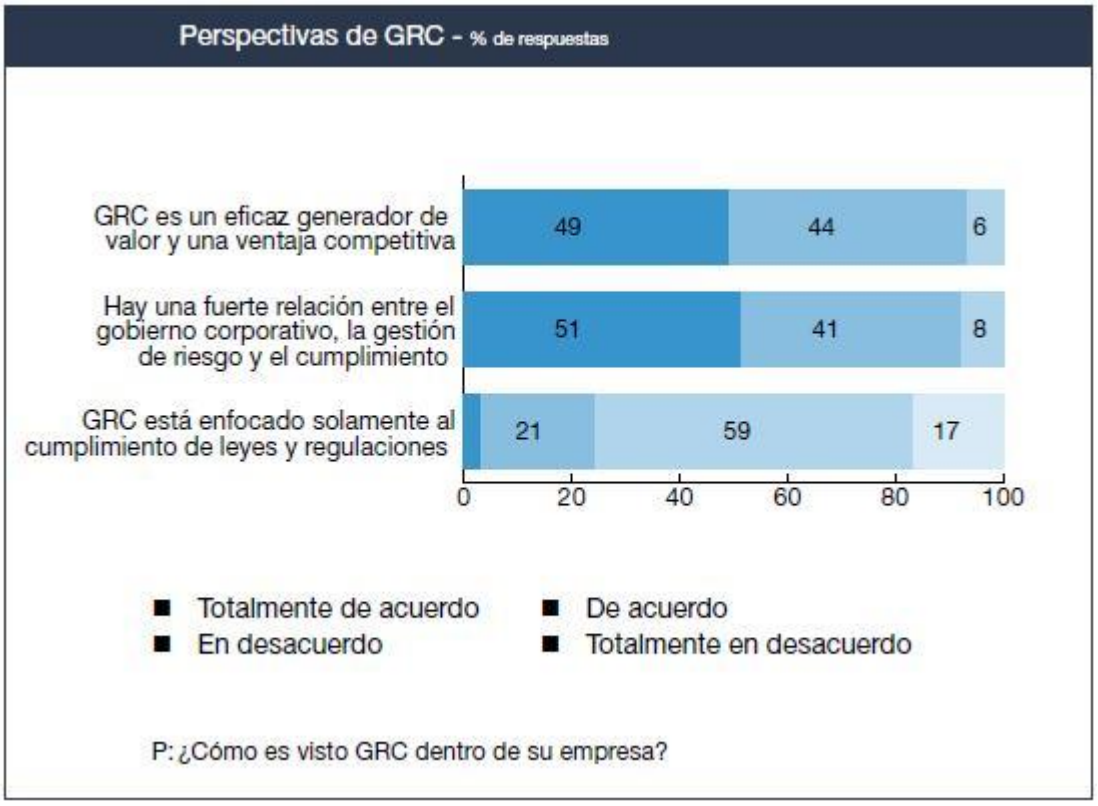


Gráfica 2 Amenazas al crecimiento del negocio.

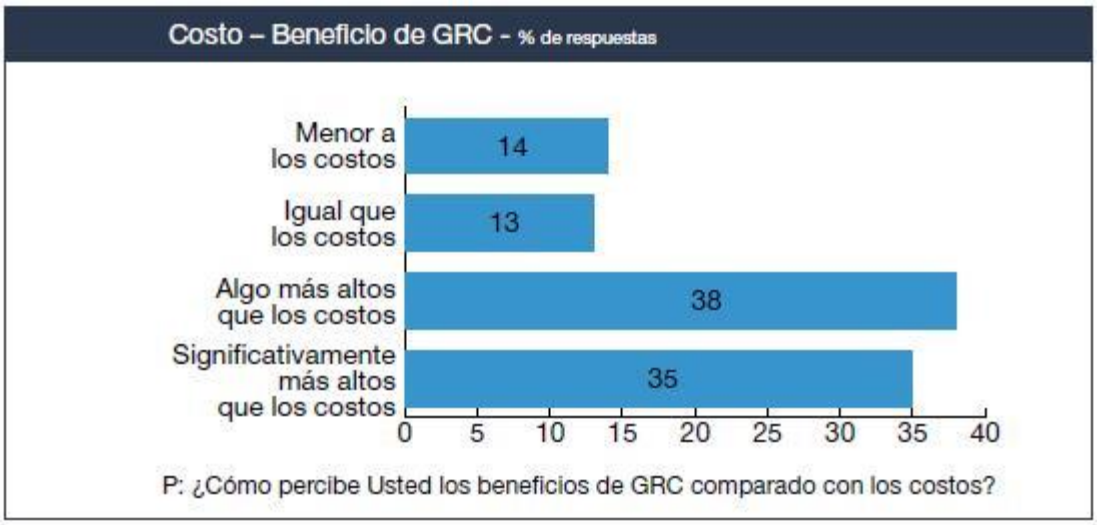
Es importante aclarar que el éxito de las organizaciones se basa en la búsqueda de objetivos de manera hábil teniendo en cuenta los obstáculos que de ellos mismos se pudieran originar, además el concepto de riesgo para las organizaciones debe representar no solo los escenarios de crisis económica y social sino todo tipo de situaciones improbables e inesperadas ajenas a las políticas internas de la empresa.

Si hablamos de las pequeñas y medianas empresas en Colombia es claro que no solo las limitaciones de carácter económico son el factor determinante para la problemática de resultados deseados frente a la realidad de logros no alcanzados, ya que en múltiples escenarios encontramos marcos de política de control e indicadores de seguimiento y cumplimiento débiles donde no existen procesos de autoevaluación de riesgos y marcos de reportes y responsabilidades que permitan establecer una adecuada alineación estratégica.

Sin embargo también es evidente que en gran parte del sector industrial se tiene conocimiento de GRC y su alcance según estudios realizados por "*Espiñeira, Sheldon y Asociados como se observa en la siguiente imagen:*



Gráfica 3. Perspectivas de GRC



Gráfica 4. Costo - Beneficio de GRC

Lo anterior evidencia que el limitante económico sigue siendo un factor importante para mostrar poco interés en la adopción de un modelo de éxito empresarial basado en diferentes disciplinas que abarcan la integración de la administración, la gestión de riesgos, y el cumplimiento, sin dejar de lado la asignación puntual de roles y responsabilidades, desconociendo los beneficios de contar con una práctica eficaz como lo es el modelo de Gobernabilidad, Riesgo y Cumplimiento lo cual representa el punto de partida de este estudio basado también en normatividad aplicable al campo de los procesos de copias de seguridad de TI como lo es la norma ISO/IEC 27001 y el conjunto de buenas prácticas que esta enmarca para el respaldo de información aplicable a cualquier organización interesada en permitir la integración de procesos clave para convertirse en una entidad más fiable, íntegra y reconocida mientras es consciente de los riesgos del medio y desee aprovechar las oportunidades que presenta el mercado actual.

1.3 OBJETIVO GENERAL.

Diseñar el proceso del respaldo de información y copias de seguridad de TI de la subdirección de innovación y servicios tecnológicos del instituto nacional de metrología - INM que apoye el desarrollo de un modelo GRC.

1.4 OBJETIVOS ESPECÍFICOS

- Diagnosticar el estado actual de la organización en cuento las políticas, procesos, procedimientos y las prácticas en los procesos de TI especialmente al respaldo de información y el restablecimiento de la operación.

- Planear y definir el alcance del proceso de copias de seguridad de TI y de la Subdirección de Innovación y Servicios Tecnológicos del INM que apoye el modelo GRC en la entidad.

- Diseñar el proceso de copias de seguridad de TI, estableciendo roles y responsabilidades.

- Validar que el modelo propuesto este enfocado y sea acorde a las necesidades del INM.

1.5 JUSTIFICACIÓN

La gobernabilidad corporativa es estricta, y los requerimientos regulatorios han incrementado el reto para lograr un nivel de cumplimiento satisfactorio teniendo en cuenta al estudio de los riesgos asociados a cada organización, hace **viable** la realización de este proyecto ya que todas las organizaciones, independiente de su tamaño, se esfuerzan con dificultad para lograr cumplir con esas regulaciones y al mismo tiempo administrar efectivamente sus riesgos corporativos.

El desarrollo de este proyecto **beneficia** inicialmente al Instituto Nacional de Metrología –INM, y específicamente a los procesos de TI de la subdirección de innovación y Servicios Tecnológicos ya que busca establecer, mantener y demostrar una continua mejora en el crecimiento del negocio asociado a TI y más específicamente al proceso de copias de seguridad el cual resulta de gran importancia ya que esta área es la encargada de administrar y gestionar el centro de cómputo de la entidad y sus políticas asociadas.

El beneficio se verá también representado en las diferentes organizaciones que decidan aplicar un modelo de mejores prácticas que permita encontrar la unificación de criterios y la coordinación de esfuerzos mediante una adecuada gestión de riesgos y una la adecuada administración de recursos físicos y humanos.

Por lo anterior es evidente que la **contribución** al crecimiento empresarial con calidad y cumplimiento, se verá reflejada al poco tiempo de hacer uso de las buenas prácticas destacadas en las primeras fases del modelo GRC mencionado en este proyecto, estableciendo bases sólidas con enfoques de riesgo que finalmente brindaran mayor calidad de vida a cada uno de los integrantes existentes en un determinado ciclo de consumo.

En la década de los años 80 existió una gran difusión de las metodologías que propugnaban la mejora continua de los procesos de las organizaciones, en una lucha sin fin para incrementar la productividad, la competitividad, la cuota de mercado y el beneficio. Sin embargo, a principios del siglo XXI se produjeron una serie de escándalos financieros, con gran repercusión mediática mundial, que cuestionaron cómo se estaban gestionando las empresas así como la calidad de las informaciones que transmitían a la sociedad.

A partir de ahí ganaron reconocimiento aquellos modelos de gestión empresarial que ponían énfasis en el control interno. Más adelante se comprobó que el mero control en el seno de la organización tampoco era suficiente para garantizar un desarrollo saludable de los negocios, incrementándose notablemente los seguidores de aquellos modelos que abogan por una gestión coordinada de los aspectos de gobernanza, gestión del riesgo y cumplimiento.

Por esta razón y con el fin de continuar enriqueciendo la línea de investigación de la Facultad de Ingenieria, de la Universidad de Colombia, definida como “Software inteligente y convergencia tecnológica”, ya que se identifican diferentes aspectos que posibilitan tomar acciones preventivas y correctivas en el ámbito técnico, tecnológico y financiero para buscar en un proceso de mejora la satisfacción del cliente y el posicionamiento competitivo.

De igual forma buscamos que la aplicación de las mejores prácticas en los procesos encamine a la entidad hacia la implementación del modelo GRC, el cual contribuirá a que la organización mejore la confiabilidad y calidad de sus procesos no solamente en los procesos de TI si no en los demás desarrollados en la entidad.

2 MARCOS DE REFERENCIA

2.1 MARCO TEORICO

2.1.1 Sistema de gestión de la seguridad de la información

El SGSI (Sistema de Gestión de Seguridad de la Información) es el concepto central sobre el que se construye ISO 27001. La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

Este proceso es el que constituye un SGSI, que podría considerarse, por analogía con una norma tan conocida como ISO 9001, como el sistema de calidad para la seguridad de la información.

Garantizar un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado. El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

2.1.2 Definición de SGSI

SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System.

En el contexto aquí tratado, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres

términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:

- Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

- Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

- Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Para garantizar que la seguridad de la información es gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI.

2.1.3 Funcionalidad del SGSI

La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización. La confidencialidad, integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos.

Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos, el “hacking” o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por catástrofes naturales y fallos técnicos.

El cumplimiento de la legalidad, la adaptación dinámica y puntual a las condiciones variables del entorno, la protección adecuada de los objetivos de negocio para asegurar el máximo beneficio o el aprovechamiento de nuevas

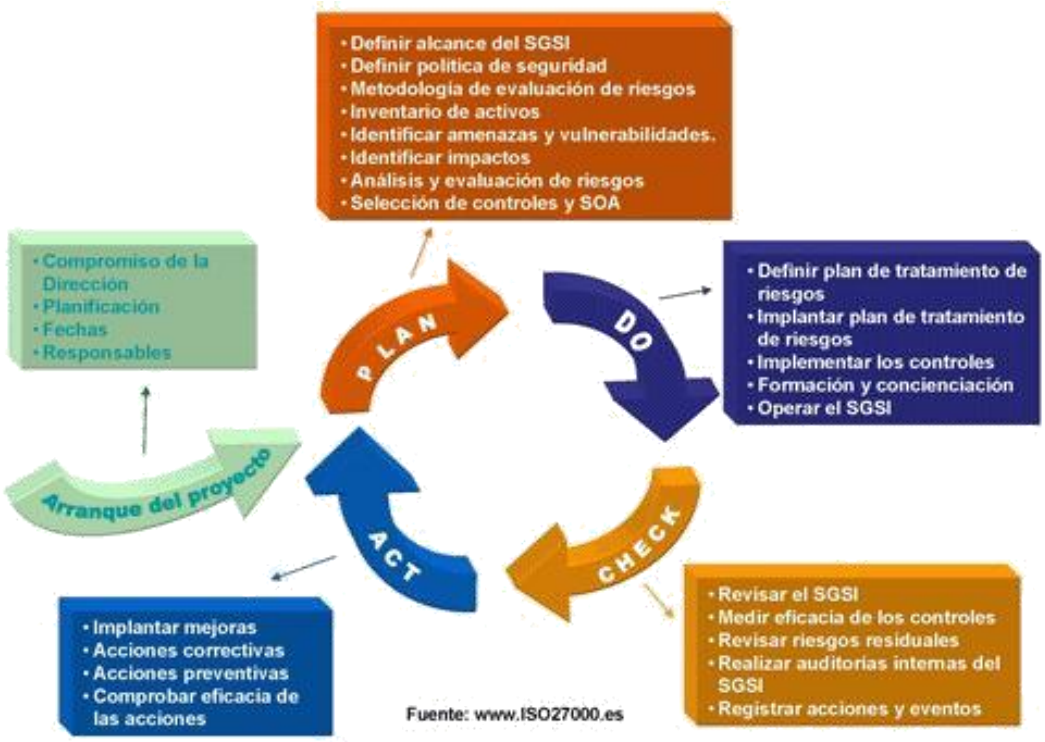
oportunidades de negocio, son algunos de los aspectos fundamentales en los que un SGSI es una herramienta de gran utilidad y de importante ayuda para la gestión de las organizaciones.

El nivel de seguridad alcanzado por medios técnicos es limitado e insuficiente por sí mismo. En la gestión efectiva de la seguridad debe tomar parte activa toda la organización, con la gerencia al frente, tomando en consideración también a clientes y proveedores de bienes y servicios. El modelo de gestión de la seguridad debe contemplar unos procedimientos adecuados y la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos.

El Sistema de Gestión de la Seguridad de la Información (SGSI) ayuda a establecer estas políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir.

Con un SGSI, la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente.

2.1.4 ¿Cómo adaptarse?



Gráfica 5. ISO27000

2.1.5 Planificación

Planificación, fechas, responsables, conceptos que como en todo proyecto de envergadura, representan el éxito, el tiempo y el esfuerzo invertidos en esta fase multiplican sus efectos positivos sobre el resto de fases.

En función de características de la entidad objeto de esta investigación y en busca de una mejora teniendo en cuenta localización, activos y tecnología, definiendo el alcance y los límites del proyecto el cual se inicia con un alcance limitado.

Definir política de seguridad: incluyendo el marco general y los objetivos de seguridad de la información de la organización, teniendo en cuenta los requisitos, legales y contractuales en cuanto a seguridad, buscando una alineación con la gestión de riesgo general, estableciendo criterios de evaluación de riesgo y que a su vez sea aprobada por la Dirección para lo cual se ha socializada en varias ocasiones el objetivo de esta investigación, contando con la aprobación de los jefes de área y en este caso el Subdirector de Innovación y Servicios tecnológicos Ingeniero Carlos Eduardo Porras.

Definir el enfoque de evaluación de riesgos: definir una metodología de evaluación de riesgos apropiada acorde a las necesidades de la organización, desarrollar criterios de aceptación de riesgos y determinar el nivel de riesgo aceptable son elementos desarrollados para el cumplimiento de los objetivos propuestos. Existen muchas metodologías de evaluación de riesgos aceptadas internacionalmente; en este caso se opta por una combinación de varias. Es importante recordar que el riesgo nunca es totalmente eliminable ni sería rentable hacerlo, por lo que es necesario definir una estrategia de aceptación de riesgo.

Inventario de activos: todos aquellos activos de información que tienen algún valor para la organización y que quedan dentro del alcance del SGSI.

Gráfica 6. Fases ISO27000

Identificar amenazas y vulnerabilidades: todas las que afectan a los activos del inventario.

Identificar los impactos: los que podría suponer una pérdida de la confidencialidad, la integridad o la disponibilidad de cada uno de los activos.

Análisis y evaluación de los riesgos: evaluar el daño resultante de un fallo de seguridad (es decir, que una amenaza explote una vulnerabilidad) y la probabilidad de ocurrencia del fallo; estimar el nivel de riesgo resultante y determinar si el riesgo es aceptable (en función de los niveles definidos previamente) o requiere tratamiento.

Identificar y evaluar opciones para el tratamiento del riesgo: el riesgo puede reducido (mitigado mediante controles), eliminado (p. ej., eliminando el activo), aceptado (de forma consciente) o transferido (p. ej., con un seguro o un contrato de outsourcing).

Selección de controles: seleccionar controles para el tratamiento el riesgo en función de la evaluación anterior. Utilizar para ello los controles del Anexo A de ISO 27001 (teniendo en cuenta que las exclusiones habrán de ser justificadas) y otros controles adicionales si se consideran necesarios.

Aprobación por parte de la Dirección del riesgo residual y autorización de implantar el SGSI: hay que recordar que los riesgos de seguridad de la información son riesgos de negocio y sólo la Dirección puede tomar decisiones sobre su aceptación o tratamiento. El riesgo residual es el que queda, aún después de haber aplicado controles, también es importante recordar que el "riesgo cero" no existe prácticamente en ningún caso.

Confeccionar una Declaración de Aplicabilidad: la llamada SOA (Statement of Applicability) es una lista de todos los controles seleccionados y la razón de su elección, los controles actualmente implementados y la justificación de cualquier control. Es, en definitiva, un resumen de las decisiones tomadas en cuanto al tratamiento del riesgo.

2.1.6 Norma ISO 27000

La información es un activo vital para el éxito y la continuidad en el mercado de cualquier organización. El aseguramiento de dicha información y de los sistemas que la procesan es, por tanto, un objetivo de primer nivel para la organización.

Para la adecuada gestión de la seguridad de la información, es necesario implantar un sistema que aborde esta tarea de una forma metódica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización.

ISO/IEC 27000 es un conjunto de estándares desarrollados en fase de desarrollo- por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la

seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

En este apartado se resumen las distintas normas que componen la serie ISO 27000 y se indica cómo puede una organización implantar un sistema de gestión de seguridad de la información (SGSI) basado en ISO 27001.

2.1.6.1 Beneficios

- Establecimiento de una metodología de gestión de la seguridad clara y estructurada.
- Reducción del riesgo de pérdida, robo o corrupción de información.
- Los clientes tienen acceso a la información a través medidas de seguridad.
- Los riesgos y sus controles son continuamente revisados.
- Confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial.
- Las auditorías externas ayudan cíclicamente a identificar las debilidades del sistema y las áreas a mejorar.
- Posibilidad de integrarse con otros sistemas de gestión (ISO 9001, ISO 14001,OHSAS 18001L).
- Continuidad de las operaciones necesarias de negocio tras incidentes de gravedad.
- Conformidad con la legislación vigente sobre información personal, propiedad intelectual y otras.
- Imagen de empresa a nivel internacional y elemento diferenciador de la competencia.
- Confianza y reglas claras para las personas de la organización.
- Reducción de costes y mejora de los procesos y servicio.
- Aumento de la motivación y satisfacción del personal.
- Aumento de la seguridad en base a la gestión de procesos en vez de en la compra sistemática de productos y tecnologías.

2.1.7 Norma ISO/IEC 17799-2:2005 ahora ISO/IEC 27002

Proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.

ISO 17799 define la información como un activo que posee valor para la organización y requiere por tanto de una protección adecuada. El objetivo de la seguridad de la información es proteger adecuadamente este activo para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocio.

La norma UNE-ISO/IEC 17799 establece diez dominios de control que cubren por completo la Gestión de la Seguridad de la Información:

1. Política de seguridad.
2. Aspectos organizativos para la seguridad.
3. Clasificación y control de activos.
4. Seguridad ligada al personal.
5. Seguridad física y del entorno.
6. Gestión de comunicaciones y operaciones.
7. Control de accesos.
8. Desarrollo y mantenimiento de sistemas.
9. Gestión de continuidad del negocio.
10. Conformidad con la legislación.

La adopción de la norma ISO 17799 proporciona diferentes ventajas a cualquier organización:

- Aumento de la seguridad efectiva de los sistemas de información.
- Correcta planificación y gestión de la seguridad.
- Garantías de continuidad del negocio.
- Mejora continua a través del proceso de auditoría interna.
- Incremento de los niveles de confianza de nuestros clientes y partners.
- Aumento del valor comercial y mejora de la imagen de la organización.

2.1.8 Norma NTC-ISO 31000:2009.

Tiene como finalidad ayudar a las organizaciones de todo tipo y tamaña a gestionar el riego con efectividad. Establece una serie de principios que deben ser satisfechos para hacer gestión eficaz del riesgo.

Esta norma recomienda que las organizaciones desarrollen, implementen y mejoren continuamente un marco de trabajo o estructura de soporte cuyo objetivo es integrar el proceso de gestión de riesgos en el gobierno corporativo de la organización, planificación y estrategia, gestión, procesos de información, políticas, valores y cultura.

Esta ISO no es específica a alguna industria o sector, puede ser utilizada en entidades públicas, privadas, organizaciones sin fines de lucro, asociaciones, grupo o individuos.

La norma ISO 31000:2009 establece los principios y directrices de carácter genérico sobre la gestión del riesgo.

2.1.8.1 Principios Básicos para la Gestión de Riesgos

La gestión del riesgo en una organización debe tener en cuenta los siguientes principios que contribuirán a una mayor eficacia:

a. Crea valor
b. Está integrada en los procesos de la organización
c. Forma parte de la toma de decisiones.
d. Trata explícitamente la incertidumbre.
e. Es sistemática, estructurada y adecuada.
f. Está basada en la mejor información disponible.
g. Está hecha a medida.
h. Tiene en cuenta factores humanos y culturales.
i. Es transparente e inclusiva.
j. Es dinámica, iterativa y sensible al cambio.
k. Facilita la mejora continua de la organización.

El enfoque está estructurado en tres elementos claves para una efectiva gestión de riesgos:

1. Los principios de gestión del riesgo.
2. El marco de trabajo para la gestión del riesgo.
3. El proceso de gestión de riesgo.

2.1.8.2 Beneficios de la norma.

La norma ISO 31000 está diseñada para ayudar a las organizaciones a:

- Aumentar la probabilidad de lograr los objetivos.
- Fomentar la gestión proactiva.
- Ser consientes de la necesidad de identificar y tratar el riesgo en toda la organización.
- Mejorar en la identificación de oportunidades y amenazas.

- Cumplir con las exigencias legales y reglamentarias pertinentes, así como las normas internacionales.
- Mejorar la información financiera.
- Mejorar la gobernabilidad.
- Mejorar la confianza de los grupos de interés (stakeholder).
- Establecer una base confiable para la toma de decisiones y la planificación.
- Mejorar los controles.
- Asignar y utilizar con eficiencia operacional.
- Mejorar la salud y de seguridad, así como la protección del medio ambiente.
- Mejorar la prevención de perdida, así como la gestión de incidentes.
- Minimizar las perdidas.
- Mejorar el aprendizaje organizacional.
- Mejorar capacidad de recuperación de la organización.

2.1.9 ISO/IEC 20000-2.

Es el primer conjunto de normativa internacional específica para la gestión de los servicios basados en las Tecnologías de la Información (TI). Presentan una organización cabal de las principales actividades necesarias para gestionar estos servicios, agrupadas en un conjunto de procesos considerados esenciales para la creación, prestación y evolución de los servicios de las TI. Al aplicar sus requisitos y recomendaciones, las organizaciones de TI emprenderán un camino indudable de mejora en el control y la calidad de su actividad.

Se pueden considerar como normas “troncales” en la gestión de las TI, pues estructuran en torno a procesos las actividades más esenciales.

Las Normas ISO/IEC 20000 introducen en la organización de las TI una forma de trabajo metódica, integrada y orientada a los procesos, haciendo especial énfasis en garantizar la calidad del servicio a los distintos clientes de las TI. Además, articulan su implantación con un sistema de gestión específico, que incorpora la disciplina y el rigor de ISO 90000 en la implantación del modelo de trabajo en las TI.

Su adopción como normas internacionales surge a raíz de la iniciativa de elevar a ISO e IEC las normas británicas BS 15000 relativas a la gestión del servicio de las TI. Las Normas ISO/IEC 20000 hoy vigentes se tramitaron en ISO a través del procedimiento rápido denominado procedimiento fasttrack.

Las Normas ISO/IEC 20000 se componen de dos partes: la primera es la especificación para la gestión del servicio y tiene un carácter preceptivo, y la segunda se establece como un código de buenas prácticas o recomendaciones.

Ambas partes forman un marco para definir las características de los procesos implicados en la gestión del servicio, que son esenciales para la prestación de los mismos con la calidad requerida.

2.1.10 Gobierno, Riesgo y Cumplimiento (GRC)

Ha sido un tema que hasta en los últimos años no se le había dado la importancia que requiere. Si bien el término GRC es nuevo, en lo individual las organizaciones han mostrado poco interés en su adopción, desconociendo quizá los beneficios de contar con esta eficaz práctica.

No debe entenderse al Gobierno Corporativo como cumplimiento regulatorio y como mejor práctica solamente, se tendrá que dar la importancia que realmente tiene para el establecimiento de una estructura de vigilancia que asegure la adecuada conducción de la empresa.

El establecer un modelo de GRC es una necesidad para las empresas, sin embargo, no se puede decir que al establecer este modelo se incrementarán las ventas de una compañía o que su crecimiento se realizará en un tiempo determinado, los resultados dependerán del grado de importancia que se le dé al modelo pues como tal, éste no es un bien tangible sino una inversión reflejada en el fortalecimiento de la estructura de cualquier empresa.

2.1.11 Copias de respaldo o de back-up.

El objetivo de las copias de respaldo o de Back-Up es mantener la integridad y disponibilidad de la información y los medios de procesamiento de información, basándose en procedimientos de rutina para implementar la política de respaldo acordada y la estrategia para tomar copias de respaldo de la data y practicar su restauración oportuna.

Se debieran hacer copias de respaldo de la información y software probarlas regularmente en concordancia con la política de copias de respaldo acordada.

La ISO/IEC 17799-2:2005 realiza las siguientes consideraciones que se deberían tener en cuenta para el respaldo de la información:

a) Se debiera definir el nivel necesario de respaldo de la información.
b) Se debieran producir registros exactos y completos de las copias de respaldo y procedimientos documentados de la restauración.

c) La extensión (por ejemplo, respaldo completo o diferencial) y la frecuencia de los respaldos debiera reflejar los requerimientos comerciales de la organización, los requerimientos de seguridad de la información involucrada, y el grado crítico de la información para la operación continúa de la organización.
d) Las copias de respaldo se debieran almacenar en un lugar apartado, a la distancia suficiente como para escapar de cualquier daño por un desastre en el local principal.
e) A la información de respaldo se le debiera dar el nivel de protección física y ambiental apropiado consistente con los estándares aplicados en el local principal; los controles aplicados a los medios en el local principal se debiera extender para cubrir la ubicación de la copia de respaldo.
f) Los medios de respaldo se debieran probar regularmente para asegurar que se puedan confiar en ellos para usarlos cuando sea necesaria en caso de emergencia.
g) Los procedimientos de restauración se debieran chequear y probar regularmente para asegurar que sean efectivos y que pueden ser completados dentro del tiempo asignado en los procedimientos operacionales para la recuperación.
h) En situaciones cuando la confidencialidad es de importancia, las copias de respaldo debieran ser protegidas por medios de una codificación.

2.1.11.1 Identificar los datos críticos para el negocio.

En un equipo informático se almacenan inmensas cantidades de información pero no toda es importante. A la hora de planificar una copia de seguridad es importante que tengamos muy claro que información es la más importante, para no gastar tiempo, esfuerzo y espacio en copiar datos que no son relevantes.

2.1.11.2 Inventario de los activos.

Se debieran identificar todos los activos y se debiera elaborar y mantener un inventario de todos los activos importantes. Una organización debiera identificar todos los activos y documentar la importancia de estos activos. El inventario de los activos debiera incluir toda la información necesaria para poder recuperarse de un desastre; incluyendo el tipo de activo, formato, ubicación, información de respaldo, información de licencias y un valor comercial. El inventario no debiera duplicar innecesariamente otros inventarios, pero se debiera asegurar que el contenido esté alineado. Además, se debiera acordar y documentar la propiedad y la clasificación de la propiedad para cada uno de los activos. Basados en la importancia del activo, su valor comercial y su clasificación de seguridad, se

debieran identificar los niveles de protección que se conmensuran con la importancia de los activos.

Existen muchos tipos de activos, incluyendo:

- Información: bases de datos y archivos de data, contratos y acuerdos, documentación del sistema, información de investigaciones, manuales del usuario, material de capacitación, procedimientos operacionales o de soporte, planes de continuidad del negocio, acuerdos para contingencias, rastros de auditoría e información archivada.
- Activos de software: software de aplicación, software del sistema, herramientas de desarrollo y utilidades;
- Activos físicos: equipo de cómputo, equipo de comunicación, medios removibles y otro equipo
- Servicios: servicios de computación y comunicación, servicios generales; por ejemplo, calefacción, iluminación, energía y aire acondicionado;
- Personas, y sus calificaciones, capacidades y experiencia;
- Intangibles, tales como la reputación y la imagen de la organización. Los inventarios de los activos ayudan a asegurar que se realice una protección efectiva de los activos, y también puede requerir de otros propósitos comerciales; como planes de salud y seguridad, seguros o razones financieras (gestión de activos). El proceso de compilar un inventario de activos es un pre-requisito importante de la gestión del riesgo.

2.1.11.3 Determinar la frecuencia adecuada para backups.

Este es un punto muy importante a la hora de crear una buena política de copias de seguridad. Hay que determinar la periodicidad de los backup, teniendo en cuenta cada cuánto tiempo cambia la información.

2.1.11.4 Copia continua

Aun teniendo en cuenta lo anterior, lo ideal es que el backup esté permanentemente actualizado, es decir, que en caso de pérdida de la información podamos recuperar todo, incluso lo que haya sucedido sólo unos segundos antes del incidente.

2.1.11.5 Verificar los backups para garantizar que se pueden restaurar.

Los procedimientos de respaldo para los sistemas individuales debieran ser probados regularmente para asegurar que cumplan con los requerimientos de los planes de continuidad del negocio. Para sistemas críticos, los procedimientos de respaldo debieran abarcar toda la información, aplicaciones y data de todos los sistemas, necesarios para recuperar el sistema completo en caso de un desastre.

2.1.11.6 Destrucción de los backups

Se debiera determinar el período de retención para la información esencial, y también cualquier requerimiento para que las copias de archivo se mantengan permanentemente.

2.1.11.7 Seguridad física y ambiental

El objetivo de tener áreas seguras es evitar el acceso físico no autorizado, daño e interferencia con la información y los locales de la organización.

Los medios de procesamiento de información crítica o confidencial debieran ubicarse en áreas seguras, protegidas por los perímetros de seguridad definidos, con las barreras de seguridad y controles de entrada apropiados. Debieran estar físicamente protegidos del acceso no autorizado, daño e interferencia.

Se debieran utilizar perímetros de seguridad (barreras tales como paredes, rejas de entrada controladas por tarjetas o recepcionistas) para proteger las áreas que contienen información y medios de procesamiento de información.

Cuando sea apropiado, se debieran considerar e implementar los siguientes lineamientos para los perímetros de seguridad físicos:

a. Los perímetros de seguridad debieran estar claramente definidos, y la ubicación y fuerza de cada uno de los perímetros dependerá de los requerimientos de seguridad de los activos dentro del perímetro y los resultados de la evaluación del riesgo.

b. Los perímetros de un edificio o local que contienen los medios de procesamiento de información debieran ser físicamente sólidos (es decir, no debieran existir brechas en el perímetro o áreas donde fácilmente pueda ocurrir un ingreso no autorizado); las paredes externas del local debieran

ser una construcción sólida y todas las puertas externas debieran estar adecuadamente protegidas contra accesos no autorizados mediante mecanismos de control; por ejemplo, vallas, alarmas, relojes, etc.; las puertas y ventanas debieran quedar aseguradas cuando están desatendidas y se debiera considerar una protección externa para las ventas, particularmente en el primer piso.

c. Se debiera contar con un área de recepción con un(a) recepcionista u otros medios para controlar el acceso físico al local o edificio; el acceso a los locales y edificios debieran restringirse solamente al personal autorizado
d. Cuando sea aplicable, se debieran elaborar las barreras físicas para prevenir el acceso físico no autorizado y la contaminación ambiental.

e. Todas las puertas de emergencia en un perímetro de seguridad debieran contar con alarma, debieran ser monitoreadas y probadas en conjunción con las paredes para establecer el nivel de resistencia requerido en concordancia con los adecuados estándares regionales, nacionales e internacionales; debieran operar en concordancia con el código contra-incendios local de una manera totalmente segura.

f. Se debieran instalar adecuados sistemas de detección de intrusos según estándares nacionales, regionales e internacionales y debieran ser probados regularmente para abarcar todas las puertas externas y ventanas accesibles; las áreas no ocupadas debieran contar con alarma en todo momento; también se debiera proveer protección para otras áreas; por ejemplo, el cuarto de cómputo o cuarto de comunicaciones.

g. Los medios de procesamiento de información manejados por la organización debieran estar físicamente separados de aquellas manejadas por terceros.

2.1.11.8 Otra información

La protección física se puede lograr creando una o más barreras físicas alrededor de los locales de la organización y los medios de procesamiento de información. El uso de las múltiples barreras proporciona protección adicional, para que la falla de una barrera no signifique que la seguridad se vea comprometida inmediatamente.

Un área segura puede ser una oficina con llave, o varias habitaciones rodeadas por una barrera de seguridad física interna continua. Pueden ser necesarios barreras y perímetros adicionales para controlar el acceso físico entre las áreas con diferentes requerimientos de seguridad dentro del perímetro de seguridad.

Se debiera prestar consideración especial a la seguridad de acceso físico que se debiera dar a los edificios donde se alojan múltiples organizaciones.

2.1.11.9 Controles de ingreso físico

Las áreas seguras debieran protegerse mediante controles de ingreso apropiados para asegurar que sólo se le permita el acceso al personal autorizado.

Se debieran considerar los siguientes lineamientos:

a. Se debiera registrar la fecha y la hora de entrada y salida de los visitantes, y todos los visitantes debieran ser supervisados a no ser que su acceso haya sido previamente aprobado; sólo se les debiera permitir acceso por propósitos específicos y autorizados y se debieran emitir las instrucciones sobre los requerimientos de seguridad del área y sobre los procedimientos de emergencia.

b. El acceso a áreas donde se procesa o almacena información sensible se debiera controlar y restringir sólo a personas autorizadas.

c. Se debieran utilizar controles de autenticación; por ejemplo, tarjeta de control de acceso más PIN; para autorizar y validar todo los accesos.

d. Se debiera mantener un rastro de auditoría de todos los accesos

e. Se debiera requerir que todos los usuarios empleados, contratistas y terceras personas y todos los visitantes usen alguna forma de identificación visible y se debiera notificar inmediatamente al personal de seguridad si se encuentra a un visitante no acompañado y cualquiera que no use una identificación visible.

f. Al personal de servicio de apoyo de terceros se le debiera otorgar acceso restringido a las áreas seguras o los medios de procesamiento de información confidencial, solo cuando sea necesario; este acceso debiera ser autorizado y monitoreado.

g. Los derechos de acceso a áreas seguras debieran ser revisados y actualizados regularmente, y revocados cuando sea necesario.

2.1.12 Clasificación de activos de información.

Los activos de información deben ser clasificados para señalar su sensibilidad y criticidad de acuerdo a la confidencialidad, integridad y disponibilidad, de la información que contienen o bien de acuerdo a la funcionalidad que cumplen y rotulados en función a ello, con el objeto de señalar cómo ha de ser tratada y protegida dicha información.

Generalmente, la información deja de ser sensible o crítica después de un cierto período de tiempo, por ejemplo, cuando la información se ha hecho pública. Estos aspectos deben tenerse en cuenta, puesto que la clasificación por exceso puede traducirse en gastos adicionales innecesarios para la organización.

Las pautas de clasificación deben prever y contemplar el hecho de que la clasificación de un ítem de información determinado no necesariamente debe mantenerse invariable por siempre, y que ésta puede cambiar de acuerdo con una Política predeterminada. Se debe considerar la cantidad de categorías a definir para la clasificación dado que los esquemas demasiado complejos pueden tornarse engorrosos y antieconómicos o resultar poco prácticos.

La información adopta muchas formas, tanto en los sistemas informáticos como fuera de ellos. Puede ser almacenada (en dichos sistemas o en medios portátiles), transmitida (a través de redes o entre sistemas) e impresa o escrita en papel. Cada una de estas formas debe contemplar todas las medidas necesarias para asegurar la confidencialidad, integridad y disponibilidad de la información.

2.1.13 Roles frente a los activos de información.

Un sistema de clasificación de la información ayuda a asegurar aquellas decisiones que satisfacen a toda la compañía y no solo a la protección de información individual.

Antes de que la clasificación de la información se lleve a cabo se tienen en cuenta unos pasos claves:

1. Identificar todos los recursos de información que necesitan ser protegidos: En este paso es importante tener en cuenta los siguientes aspectos para cada uno de los recursos de información.

- Localización de la información
- Cómo se protege la información actualmente

- Propietario de los datos
- Custodio de los datos.
- Formato de la información (base de datos, archivos, aplicación)

2. Identificar las medidas de protección de la información teniendo en cuenta la necesidad del negocio y objetivos de la protección de la información:

- Autenticación: Donde se puede utilizar la autenticación sencilla (identificador y contraseña) y la autenticación doble (identificador, contraseña y secreto clave).
- Acceso basado en roles: Basado generalmente en necesidades del negocio y funciones del trabajo. En este caso se maneja una Lista de control de acceso.
- (ACL) la cual contiene el nivel de acceso para cada persona (leer, editar y borrar).
- Cifrado: Se utiliza para asegurar la privacidad de información sensible o personal, también para que la información no sea vista o alterada sin detección alguna.
- Controles administrativos: Sirven para asegurar la integridad de la información.
- Controles tecnológicos: Protección de virus, redundancia del disco, sistema y aplicaciones, al igual que segregación de la red.
- Garantía: Validación de la protección del sistema. Con la ayuda de monitoreo.

El criterio de clasificación de la información se da en función a:

2.1.13.1 Confidencialidad

Impacto que tendría para la organización la pérdida de confidencialidad sobre el activo de información. Que sea conocido por personas no autorizadas

2.1.13.2 Integridad

Impacto que tendría la pérdida de integridad. Si la exactitud y estado completo de la información y métodos de procesamiento fueran alterados.

2.1.13.3 Disponibilidad

Impacto que tendría la pérdida de disponibilidad. Si los usuarios autorizados no tuvieran acceso a los activos de información en el momento que lo requieran.

2.1.13.4 Criticidad

Establece la importancia total del activo de información, de acuerdo a la valoración en cada una de las propiedades.

La información puede pasar a ser obsoleta y por lo tanto, ser necesario eliminarla. La destrucción de la información es un proceso que debe asegurar la confidencialidad de la misma hasta el momento de su eliminación.

Los responsables de los Activos de información son los encargados de clasificarlos de acuerdo con su grado de sensibilidad y criticidad, de documentar y mantener actualizada la clasificación efectuada, de definir las funciones que deben tener permisos de acceso a los activos y son responsables de mantener los controles adecuados para garantizar su seguridad.

El Responsable de Seguridad de la Información es el encargado de asegurar que los lineamientos para la utilización de los recursos de la tecnología de información contemplen los requerimientos de seguridad establecidos según la criticidad de la información que procesan.

Cada Propietario de la Información supervisará que el proceso de clasificación y rótulo de información de su área de competencia sea cumplimentado de acuerdo a lo establecido.

3 METODOLOGÍA DE LA INVESTIGACIÓN

3.1 ENFOQUE

Esta investigación cuenta con un enfoque de carácter mixto, ya que se hace uso de métodos de recolección y análisis de datos basados en diferentes estudios con impacto en los factores que son mejorables con la aplicación de un modelo GRC para las diferentes organizaciones, así como el uso de descripciones y observaciones sin medición numérica pero que a su vez permiten obtener un marco general de las tres primeras fases a proponer por parte de los autores de esta investigación identificando claramente el mecanismo adecuado para su exitosa implementación.

3.2 TIPO DE INVESTIGACIÓN

El tipo de investigación que definimos para este proyecto hace referencia a un marco descriptivo y analítico ya que inicialmente buscamos la identificación de los mecanismos de administración y gestión con que se cuenta actualmente para el proceso de copias de seguridad y backups de TI realizadas a cargo de la Subdirección de Innovación y Servicios Tecnológicos de la entidad, y analítica porque una vez identificado el estado actual del proceso de copias de seguridad y su gestión, es posible determinar factores de mejora y optimización orientadas según los lineamientos del modelo GRC en sus tres primeras fases.

4 DISEÑO METODOLOGICO

4.1 GENERALIDADES DE LA ORGANIZACIÓN

El 16 de junio de 2011 se emite la ley 1450 por la cual se expide el Plan Nacional de Desarrollo, en el cual se incluye la necesidad de la existencia de una ley de metrología y del Instituto Nacional de Metrología para Colombia.

Mediante el Decreto 4175 de 2011 fue creado el Instituto Nacional de Metrología, entidad encargada de la coordinación nacional de la metrología científica e industrial, y la ejecución de actividades que permiten la innovación y soportan el desarrollo económico, científico y tecnológico del país, por medio de la investigación, la prestación de servicios metrológicos, el apoyo a las actividades de control metrológico y la diseminación de mediciones trazables al Sistema Internacional de unidades. Esta entidad es regida por el Ministerio de Comercio, Industria y Turismo de Colombia.

4.1.1 Misión del INM:

Coordinar en el territorio nacional la metrología científica e industrial y ejecutar actividades que permitan la innovación y soporten el desarrollo económico, científico y tecnológico del país.

4.1.2 Visión del INM:

En el 2020 seremos el centro de investigación, desarrollo e innovación líder en materia Metrológica en Colombia, con proyección internacional y capacidades de medición reconocidas, actuando con responsabilidad social.

4.1.3 Objetivos del INM

La coordinación nacional de la metrología científica e industrial, y la ejecución de actividades que permitan la innovación y soporten el desarrollo económico, científico y tecnológico del país, mediante la investigación, la prestación de servicios metrológicos, el apoyo a las actividades de control metrológico y la diseminación de mediciones trazables al Sistema Internacional de unidades (SI).

4.1.4 Funciones

De acuerdo a lo estipulado en el Artículo 6 del Decreto 4175 el Instituto Nacional de Metrología, tendrá como Funciones Generales las siguientes:

Participar en la formulación de las políticas en materia metrológica y ser el articulador y ejecutor de la metrología científica e industrial del país.

Desarrollar las actividades de metrología científica e industrial para el adelanto de la innovación y el desarrollo económico, científico y tecnológico del país, en coordinación con otras entidades y organismos.

Asegurar la trazabilidad internacional de los patrones nacionales de medida y representar los intereses del país en los foros nacionales e internacionales de metrología científica e industrial.

Fortalecer las actividades de control metrológico que adelanten las autoridades competentes para asegurar la confiabilidad de las mediciones.

Actuar como centro de desarrollo tecnológico de la metrología científica e industrial y en tal calidad, apoyar y asesorar al Gobierno Nacional y a otras entidades o personas en el desarrollo científico y tecnológico del país.

Establecer, custodiar y conservar los patrones nacionales de medida correspondientes a cada magnitud, salvo que su conservación o custodia sea más conveniente en otra institución, caso en el cual el Instituto Nacional de Metrología - INM establecerá los requisitos aplicables y, con base en ellos, designará a la entidad competente.

Establecer y operar los laboratorios de referencia de metrología científica e industrial que requiera el país, de acuerdo con las políticas del Estado y designar los laboratorios primarios de metrología que requiera.

Asegurar la trazabilidad de las mediciones al Sistema Internacional de unidades (SI) definido por la 'Conferencia General de Pesas y Medidas de la Oficina Internacional de Pesas y Medidas (BIPM) y hacer su divulgación.

Establecer, coordinar y articular, la Red Colombiana de Metrología (RCM).

Fijar las tasas a que hace referencia el artículo 70 de la Ley 1480 de 2011 y para los servicios de metrología que preste el Instituto Nacional de Metrología -INM incluidas las calibraciones, las verificaciones iníciales y subsiguientes, los programas de capacitación y los servicios de asistencia técnica.

Proporcionar servicios de calibración a los patrones de medición de los laboratorios, centros de investigación, a la industria u otros interesados, cuando así se solicite de conformidad con las tasas que establezca la ley para el efecto, así como expedir los certificados de calibración y de materiales de referencia correspondientes.

Realizar las calibraciones de patrones para metrología legal y los ensayos para la aprobación de modelo o prototipo de los instrumentos de medida de acuerdo con las normas vigentes.

Asesorar y prestar servicios de asistencia técnica a las entidades que lo soliciten, en aspectos científicos y tecnológicos de las mediciones y sus aplicaciones.

Mantener, coordinar y difundir la hora legal de la República de Colombia.

Producir, de acuerdo con su capacidad y con referencia a estándares internacionales, materiales de referencia requeridos por él para e importar aquellos materiales de referencia confiables e insumos de laboratorios que requiera para su actividad; así como establecer mecanismos de homologación de los materiales de referencia que se utilizan en el país de acuerdo con estándares internacionales.

Realizar estudios técnicos necesarios para establecer los patrones de medida y solicitar a la Superintendencia de Industria y Comercio su oficialización.

Promover y participar de las comparaciones inter- Laboratorios y desarrollos de la metrología científica e industrial a nivel nacional e internacional.

Realizar estudios sobre las necesidades de medición de los diferentes sectores de la economía que se requieran y publicar documentos de consulta.

Apoyar y desarrollar actividades de ciencia, tecnología e innovación en lo de su competencia, como integrante del Sistema Nacional de Ciencia, Tecnología e Innovación.

Establecer y mantener la jerarquía de los patrones de medida, de acuerdo con las recomendaciones técnicas internacionales.

Obtener, proteger, registrar y explotar las patentes y otros derechos de propiedad intelectual que el INM desarrolle o produzca en ejercicio de sus actividades científicas y tecnológicas,

Las demás funciones que se le asignen por ley.

4.1.5 Valores institucionales

Los valores expresados en el Código de Ética y Buen Gobierno, constituyen la expresión y sentir institucional, que son compartidos por todo el personal, valores que no son negociables y deben observarse en forma transversal en todas las gestiones y actividades que adelanten los trabajadores en sus diferentes procesos.

De esta manera el comportamiento ético de los funcionarios del Instituto Nacional de Metrología se expresa y se fundamenta a través del siguiente decálogo de valores institucionales:

4.1.5.1 Compromiso

El Director del Instituto Nacional de Metrología y su equipo directivo se comprometen a orientar sus actuaciones en el ejercicio de la función pública hacia el logro de los objetivos y el cumplimiento de la visión y la misión institucional.

Para el efecto las actuaciones y esfuerzos institucionales se dirigen al cumplimiento de las funciones y responsabilidades asignadas al INM desarrollando lo previsto por la Constitución Política en cuanto a los principios de la función administrativa: igualdad, moralidad, eficacia, economía, celeridad, imparcialidad y publicidad, puestos al servicio del interés general, buscando que los funcionarios vayan más allá de cumplir con una norma, una ley, reglamento u obligación, poniendo a disposición de la institución todas sus capacidades actitudes, conocimientos y habilidades, de acuerdo a su propia convicción y voluntad.

Este valor tiene diferentes expresiones en el servicio público, sin embargo para fines prácticos y de orientación se citan algunas pautas concretas, sin pretender que con ello se limite el campo de acción y significado.

Respecto al compromiso, se espera que los funcionarios del Instituto Nacional de Metrología tengan sentido de pertenencia y por voluntad propia pongan a disposición de la entidad, todo su conocimiento, iniciativas, habilidades y creatividad para alcanzar las metas individuales e institucionales.

Son requisitos del compromiso la autorregulación, autocontrol y disciplina, por lo tanto se excluyen controles de tipo coercitivo.

4.1.5.2 Honestidad

Es una forma de vivir congruente entre lo que se piensa y la conducta que se observa hacia el prójimo, que junto a la justicia, exige en dar a cada quien lo que le es debido. El funcionario del INM declarará todo interés privado que tenga respecto de las labores del oficio y hará lo necesario para evitar que los conflictos personales deterioren el interés público.

La persona honesta busca con ahínco lo recto, lo honrado, lo razonable y lo justo; no pretende jamás aprovecharse de la confianza, la inocencia o la ignorancia de otros. Es en pocas palabras realizar el trabajo con dignidad, honradez y decoro.

El servidor público no deberá utilizar su cargo público para obtener algún provecho o ventaja personal o a favor de terceros. Tampoco deberá buscar o aceptar compensaciones o prestaciones de cualquier persona u organización que puedan comprometer su desempeño como servidor público.

4.1.5.3 Respeto

Manifestaciones de consideración y tolerancia hacia los demás en beneficio de un buen clima organizacional. El Respeto es el reconocimiento del valor inherente y los derechos innatos de los individuos y de la sociedad, con dignidad, el cual exige un trato atento en condiciones de equidad y justicia.

El valor del respeto, se manifiesta a través de la relación, comunicación y convivencia que surge entre los diferentes grupos de trabajo en el Instituto Nacional de Metrología y el trato con los usuarios en el cumplimiento del servicio. Este valor tiene diferentes expresiones en el servicio público, sin embargo para

fines prácticos y de orientación se citan algunas pautas concretas, sin pretender que con ello se limite el campo de acción y significado de respeto.

a. El punto de partida para fortalecer este valor será el Auto respeto que cada funcionario debe tener por sí mismo.
b. Los funcionarios y servidores del Instituto Nacional de Metrología observarán el respeto a todos los ciudadanos y atenderán sus inquietudes y solicitudes sin ningún tipo de discriminación en virtud de factores físicos, clase social, el color, la raza, la religión, sexo o estatus.
c. Aceptar la individualidad y la diferencia que existe entre los diferentes funcionarios con el fin de construir un conceso que facilite la convivencia y la comunicación.
d. La alta dirección y los líderes de los procesos deben promover en la Institución, el valor del respeto facilitando la expresión de pensamiento, criterios y el discernimiento.
e. Este valor se expresará además a través del respeto por los recursos físicos, financieros que el Estado pone a disposición de la institución y la responsabilidad y el respeto que se debe tener frente a los recursos del medio ambiente.
f. El trato cortés, los buenos modales, la tolerancia y el respeto por el buen nombre y reputación de los demás, son condiciones fundamentales para expresar el respeto a nivel organizacional y con los ciudadanos.

4.1.5.4 Solidaridad

En general, aquel sentimiento que lleva a las personas a apoyarse y ayudarse mutuamente.

En filosofía se refiere a aquella relación humana en la que un ser basa su felicidad y por ende, la hace depender del grado de felicidad que sienten las demás personas.

Los servidores públicos deben ser solidarios en su trabajo, en el cumplimiento de sus funciones. La ayuda mutua crea el espíritu de cuerpo, pero no debe confundirse con la complicidad o el encubrimiento.

4.1.5.5 Responsabilidad

Capacidad de asumir las consecuencias que se deriven de los actos que realizan o ejecutan en cumplimiento de las funciones como servidor público.

El valor de la Responsabilidad, se manifiesta a través de múltiples expresiones en el cumplimiento del servicio público, a través de este valor confluyen una serie de comportamientos y principios éticos. La responsabilidad se expresa, a través del autocontrol y la disciplina de las tareas asignadas, que deben asumir todos los funcionarios del Instituto Nacional de Metrología, así mismo:

a. La forma de planear responsablemente el tiempo, las acciones y los recursos empleados en cada una de las actividades encomendadas.
b. Asumir con responsabilidad las consecuencias que por error u omisión se puedan generar producto de las gestiones o actividades desempeñadas.
c. La celeridad y eficiencia con que se actué con acciones correctivas y preventivas frente a situaciones que pueden entorpecer la misión institucional.
d. Antes de tomar decisiones estableciendo el impacto de las mismas sobre los usuarios y partes de interés.

4.1.5.6 Justicia

Reconocer equitativamente lo que a cada uno le corresponde y le pertenece. Se refiere a la intención, la acción y los medios empleados para instaurar y preservar el orden dentro de una comunidad, al establecer una ordenación que permita y garantice la realización del bien común. Es actuar con equidad, tomar decisiones regidas por principios de igualdad y celeridad para buscar el beneficio general.

Sinónimo de equilibrio en el buen obrar, para que todas las personas puedan recibir lo que les corresponde sin discriminaciones y con sujeción a sus derechos y deberes.

4.1.5.7 Lealtad

Actuar con fidelidad y sinceridad ante la institución y los compañeros de trabajo. La lealtad es un corresponder, una obligación que se tiene al haber obtenido algo provechoso. Es un compromiso a defender lo que creemos y en quien creemos. Por eso el concepto de la lealtad se da en temas como la Patria, el trabajo, la familia o la amistad. Cuando algo o alguien nos han dado algo bueno, le debemos mucho más que agradecimiento. El servidor público responderá por la confianza que han depositado en él y no utilizará de mala manera la información confidencial.

4.1.6 Estructura organizacional.

Según el organigrama (Ver Anexo Nº 1) la organización presenta una estructura funcional, en donde se proponen Sub Direcciones, que son regulados por una dirección general. El área de Tics no tiene organigrama, solo se aplica lo estipulado en el manual de funciones de cada uno de los integrantes del grupo de acuerdo al Decreto 4175 de 2009 de creación del INM.

4.1.6.1 Subdirección de Innovacion y Servicios Tecnologicos.

La Subdirección de Innovación y Servicios Tecnológicos del INM se encarga de coordinar los servicios que ofrece el Instituto. Así como también, facilitar la comunicación entre los clientes y las áreas encargadas de la prestación de servicio, descritos de manera general como:

- Servicios de calibración de equipos en metrología física y los servicios de metrología química.
- Servicios especiales de medición.
- Suministro y producción de materiales de referencia y materiales de referencia certificados.
- Servicios de capacitación (cursos cortos y estadías) en Bogotá y otras ciudades.
- Servicios de Asesoría Metrológica (SAM) a la industria.

Entre sus funciones se encuentran además:

- Organizar y coordinar ensayos de aptitud, comparaciones inter-laboratorios y estudios colaborativos en coordinación con la Subdirecciones del INM.
- Proponer a la Dirección general del INM la realización de convenios, acuerdos y demás instrumentos de intercambio científico y tecnológico y coordinar las acciones derivadas de los mismos.

- Establecer y apoyar programas de capacitación técnica y propiciar formación en materia metrológica.

- Evaluar la viabilidad técnica de prestación de servicios de calibración y de capacitación y otros de naturaleza técnica, así como de nuevas propuestas que demanden los usuarios.

- Dirigir, proponer y coordinar las líneas de investigación científica, los proyectos de investigación, innovación y servicios tecnológicos del INM.

- Prestar servicios tecnológicos de apoyo relacionados con mediciones y asesoría metrológica al usuario, para el favorecimiento de la transformación productiva y científica, con el apoyo de las otras dependencias.

A través de esta Subdirección el INM ejerce la función de coordinar de la Red Colombiana de Metrología (RCM) establecida para apoyar el desarrollo de la metrología en los diversos sectores económicos del país.

5 DISEÑO DEL PROCESO DE COPIAS DE SEGURIDAD.

Empresa: INSTITUTO NACIONAL DE METROLOGIA INM.

Dirigido a: SUBDIRECCION DE INNOVACION Y SERVICIOS TECNOLOGICOS SIST.

5.1 DETECCIÓN DE NECESIDADES.

El propósito de revisión es analizar y evaluar la estructura organizacional, las políticas, los procedimientos operativos, el control, el uso de los recursos materiales y técnicos de la organización para conseguirlo se realizo un proceso de verificación interna, a través de instrumentos que permitieron conocer de primera mano la información requerida para sustentar las necesidades reales del proceso objeto de este proyecto. Como lo fueron visitas de inspección, entrevistas con el personal responsable y encuestas de verificación. (Ver anexos Nº 1 y 2).

Fuente: Administrador de infraestructura tecnológica. Se realizo entrevista Semi-Estructurada con preguntas abiertas que permiten ampliar algunos aspectos de las condiciones actuales de los procesos que se realizan para resguardar la información más sensible de la organización. (Ver anexo Nº3).

Fuente: Administrador de seguridad. Entrevista Semi Estructurada con preguntas abiertas que permite ampliar la información en algunos aspectos. (Ver Anexo Nº4).

Otra ayuda para establecer el diagnostico de la entidad fue la observación de personal realizando sus tareas y labores cotidianas, en donde se pudo establecer las funciones reales que se llevan a cabo en el area de TI de la organización la percepción de seguridad las relaciones de comunicación en el grupo de trabajo.

A continuación se muestra la descripción e interpretación de hallazgos que se pudieron establecer mediante la aplicación de los instrumentos descritos anteriormente.

- La entidad cuenta con Manual de Infraestructura Tecnológica y Redes, pero en este no se menciona información específica acerca de cómo se deberían realizar las copias de seguridad.

- La entidad no tiene establecido políticas, manuales y procedimientos relacionados a las copias de seguridad de TI, solo cuentan con el documento antes mencionado. Del cual no se realiza seguimiento, tan solo se verifica que las actividades de las cuales depende la continuidad de los servicios de TI se realicen.

- El documento se actualiza siempre y cuando surge la necesidad de agregarle información generada por los cambios de software o hardware, estas actualizaciones son actualizadas por el área de TI según sus necesidades.

- En la entidad se realizan copias de seguridad completas e incrementales de manera manual para los principales recursos compartidos y servidores, cuenta con una herramienta principal denominada Symantec Backup.

- La entidad no tiene establecido formalmente a que servidores ni equipos de cómputo debe realizar copias de seguridad. Actualmente se respaldan los principales servidores con información o aplicaciones criticas, no existe una matriz donde se maneje la información detallada de bases de datos o servidores, a los servidores seleccionados se realizan copias completas semanales e incrementales diarias de manera individual, el proceso se realiza de forma manual.

- No se tiene establecido frecuencias ni horarios específicos para hacer las copias de seguridad. Los respaldos de información no son probados ya que no existe ningún proceso que indique la obligatoriedad de realizarlo, ni con que frecuencias se debe realizar. Se verifica que no se genere alertas por errores en la copia en caso de presentarlo se repite el procedimiento.

- Los backups generados no son duplicados ya que no se cuentan con los recursos para realizarlo.

- La herramienta utilizada para realizar los backup tiene un registro de los backups generados, pero solo se verifica que las copias estén generadas

sin errores, por el déficit de personal no se puede realizar mayor gestión sobre estos reportes.

- El almacenamiento no cuenta con las condiciones optimas, ni mínimas de seguridad ya que se realiza en un archivador ubicado en el área de TICS de baja seguridad donde se puede presentar un flujo medio de personal. No se realiza almacenamiento externo.

- Las cintas son etiquetadas a mano y no existe un formato estandarizado para el etiquetado, el cual no se registra en ningún documento adicional.

- Es evidente el déficit de personal para definir roles y responsabilidades para los procesos a cargo de la subdirección. Solo se cuenta con dos administradores que cuentan con los privilegios para realizar las copias de seguridad.

- No se cuenta con un administrador principal que esté al tanto de la programación, ejecución y validación de funcionamiento de las copias realizadas.

- No se verifica que la información a respaldar sea realmente sensible para la organización.

- No se lleva un registro de las solicitudes de copia de seguridad realizadas a la subdirección.

- Los activos más afectados en el último año son los recursos compartidos donde se cuenta con más de un administrador de información almacenada.

- Recientemente la entidad adquirió dentro de su proceso de modernización de infraestructura tecnológica, una unidad de almacenamiento tipo SAN con capacidad efectiva de cerca de 18 Teras efectivas, según lo conversado con los administradores de infraestructura este almacenamiento puede ofrecer hasta 1 año de retención.

5.2 IDENTIFICACION DE ACTIVOS DE INFORMACION INM.

SERVIDORES				
Ítem	**Nombre**	**Descripción**	**S.O.**	**Observaciones**
1	Andromeda	Servidor de dominio Active Directory y recursos compartidos	Windows server 2008R2	
2	Pegaso	Servidor de impresión	S.O Windows server 2012	instalado en un equipo tipo Desktop
3	Aplicaciones1	Servidor de intranet y aplicaciones internas,	Linux, Fedora 19	instalado en un equipo tipo Desktop
4	Zeus	Servidor Host de virtualización.	Windows server 2012R2	Almacena 4 servidores virtuales
5	Hora Legal1	Almacena una de las aplicaciones más críticas de la entidad, la hora legal colombina consultada y sincronizada por todo el país	Linux Red Hat	Originada en el laboratorio de tiempo y frecuencia del INM.
6	Hades	Servidor cluster de virtualización.	Windows server 2012R2	
7	Orion	servidor principal de recursos compartidos y almacenamiento critico	Windows server 2012	
8	Orion Motor	Aplicación critica de la red colombiana de metrología consultada a nivel nacional y con miras a ser consultada fuera del país	Windows server 2012	virtual
9	Orioncenam	aplicaciones internas desarrolladas por el instituto de metrología de México	Windows server 2012	
10	Labtics	servidor de prueba	Windows server 2012	instalado en un equipo tipo Desktop
11	Fénix	Servidor encargado de realizar las copias de		Instalado en un equipo tipo

		seguridad.		Desktop, conectado a la unidad robótica.
12	Orion DC	servidorreplicade controlador de dominio,	Windows server 2012-virtual.	

Tabla 1. Identificación de activos de información INM- servidores

EQUIPOS DE COMPUTO			
ITEM	**NOMBRE PC**	**RESPONSABLE EQUIPO**	**AREA**
1	INM085	Rene Hideki Doku Vendréis	Contabilidad
2	INM006	Marina Azucena Medina Sandoval	Contabilidad
3	INM010	Mayckol Jesid Morales Castro	Presión
4	INM118	Jhon Jaiver Escobar Soto	Masa
5	INM116	Arístides Candelario Dajer Espeleta	Fuerza
6	INM098	Alexander Martínez López	Corriente
7	INM094	Gina Paola Bustos Sáenz	Densidad
8	INM117	Pablo Cesar Solano Orduz	Longitud
9	INM011	Liz Yonaidy Giraldo Garzón	Volumen
10	INM126	Liz Catherine Hernández Forero	Tiempo
11	INM099	Stivinson Córdoba Sánchez	Volumen
12	INM109	David Alonso Plazas Hernández	Mediciones Geométricas

Tabla 2. Identificación de activos de información INM- Equipos de cómputo

NOMBRE PC	DESCRIPCION					
	PROCESADOR	**HD**	**MEM**	**IP**	**MAC**	**S.O**
INM085	INTEL CORE I5 3,4 GHZ	500 GB	8 GB	192.168.10.184	B8-CA-3A-93-09-22	Windows 8
INM006	INTEL CORE I5 3.1 GHZ	500 GB	4 GB	192.168.10.217	E8-39-35-4F-ED-46	Windows 7
INM010	INTEL CORE I5 3.1 GHZ	500 GB	4 GB	192.168.10.64	78-45-C4-1B-59-B6	Windows 7
INM118	INTEL CORE I5 3,4 GHZ	500 GB	8 GB	192.168.10.139	B8-CA-3A-90-7E-E5	Windows 8
INM116	INTEL CORE I5 3,4 GHZ	500 GB	8 GB	192.168.10.146	B8-CA-3A-90-84-18	Windows 8
INM098	INTEL CORE I5 3,4 GHZ	500 GB	8 GB	192.168.10.214	B8-CA-3A-90-80-BB	Windows 8

INM094	INTEL CORE I5 3,4 GHZ	500 GB	8 GB	192.168.10.37	B8-CA-3A-90-81-E0	Windows 8
INM117	INTEL CORE I5 3,4 GHZ	500 GB	8 GB	192.168.10.37	B8-CA-3A-90-80-8B	Windows 8
INM011	INTEL CORE I5 3.1 GHZ	500 GB	4 GB	192.168.10.138	78-45-C4-1B-59-91	Windows 7
INM126	INTEL CRE I7 3,4 GHZ	500 GB	8 GB	192.168.11.82	B8-CA-3A-90-E9-62	Windows 8
INM099	INTEL CORE I5 3,4 GHZ	500 GB	8 GB	192.168.10.41	B8-CA-3A-90-82-80	Windows 8
INM109	INTEL CORE I5 3,4 GHZ	500 GB	8 GB	192.168.10.151	B8-CA-3A-90-83-86	Windows 8

Tabla 3. Identificación de activos de información INM- Descripción equipos de cómputo

6 ALCANCE DEL PROCESO DE COPIAS DE SEGURIDAD DE TI DEL INM.

Contribuir a garantizar que los recursos informáticos de la organización se encuentren disponibles para cumplir sus propósitos, es decir, que se puedan recuperar incluso luego de alteraciones por circunstancias de fallas técnicas o factores externos.

El alcance de este proceso abarca el desarrollo de la documentación necesaria según las recomendaciones definidas en la normatividad correspondiente para el respaldo de información, precisando claramente los activos de información a respaldar, frecuencias, tipos de copias, almacenamiento adecuado, pruebas de la mismas, etiquetado, entre otros. De igual manera se busca concientizar al personal de la entidad inmerso en este proceso para garantizar la aplicación y el cumplimiento de la documentación propuesta para ser aprobada por la entidad.

Por lo ya mencionado es evidente la necesidad para el INM de implementar un proceso de copias de seguridad que coadyuve a mejorar no solo la disponibilidad, e integridad de la información sino también todo el entorno que debe manejarse para este tipo de operaciones, determinando para esto mecanismos de control efectivos.

Establecer las tareas necesarias para desarrollar y coordinar de manera eficiente y efectiva lo especificado en la caracterización del proceso de copias de seguridad de TI, y dar ejecución a los siguientes ítems.

- Definición de información crítica a respaldar
- Programación automática de copias de seguridad
- Verificación continua de copias de seguridad
- Almacenamiento seguro y controlado para el respaldo de información en cintas

6.1 DEFINICION INFORMACION A RESPALDAR

La información a respaldar debe ser la que realmente sea importante para el Instituto Nacional Metrología para lo cual se debe garantizar que las solicitudes que realicen las diferentes dependencias cumplan con las características que ameriten que sean respaldadas, para tal fin hemos definido el FORMATO DE SOLICITUD DE INFORMACIÓN A RESPALDAR (Ver ANEXO 5), el cual

contribuye a determinar que tipo de información se pretende respaldar, la cual tendrá que ser autorizada por el jefe de la dependencia solicitante.

6.2 CARACTERIZACIÓN DEL PROCESO

Según los estándares de la entidad es necesario presentar diferentes documentos que soportan la creación y definición de nuevos procesos, uno de ellos es el formato de caracterización de procesos, donde se resume los diferentes aspectos a tener en cuenta dentro de este proceso. (Ver anexo Nº 6)

Es importante que se lleve registro de la actividad realizada por el profesional a cargo una vez concluido la copia de seguridad, haciendo entrega del equipo objeto del procedimiento a su responsable. Se debe verificar las condiciones funcionales y de realizado el respaldo de información. Para tal fin se diseño el formato de entrega de backups (ver anexo Nº 7) en donde se llevara un mayor control registrando entre otro la dependencia solicitante, el tamaño total de la copia y el responsable de realizarla así como la recepción a satisfacción del dueño del equipo respaldado.

6.3 PROGRAMACION DE COPIAS AUTOMATICAS

Establecer junto con el equipo de trabajo la frecuencia en la que deberán ser realizadas las copias de seguridad de los servidores “Andrómeda, Orion, Orion-DC, Orion-Motor, Pegaso, Orion-CENAM y Fenix”, además de todos los registros de calidad y técnicos, funcionarios responsables y frecuencia en la que deberán ser realizados, el tipo de backup definiendo de la importancia de la información que alverga cada servidor..

6.4 TIPOS DE BACKUPS

Se aplicaran 2 tipos de backups dentro de este proceso:

Copia completa: se realiza mínimo una vez por semana en cada uno de los servidores existentes.

Copia incremental: Consiste en almacenar los ficheros completos que han sido únicamente modificados, la programación para estas modalidades consiste en realizar 4 copias incrementales y 3 copias completas de manera distribuida por semana para los servidores.

6.5 ALMACENAMIENTO DE CINTAS

Para el almacenamiento de cintas se sugiere mejorar las condiciones actuales, establecer un lugar más seguro donde se cuente con acceso restringido, y con custodio responsable.

6.6 MONITOREO Y VERIFICACION

Fortalecer el procedimiento realizado dando una mayor utilización a la herramienta de respaldo principal Symantec 2014, en donde se generen informes diarios del estado de actividades realizadas, pendientes y/o con errores.

Establecer un servidor de pruebas para la verificación de la información respaldada, donde se permiten descargas de archivos, ejecución de bases de datos y aplicaciones con el fin de determinar el correcto funcionamiento de los datos respaldados.

6.7 PLANES DE CONTINGENCIA

Fortalecer los mecanismos de respaldo y medios de almacenamiento adicionales para permitir la continuidad del proceso de copias de seguridad de TI así:

Debido a que los productos Microsoft están presentes en un 95% de la infraestructura de la entidad se cuenta con el asistente de copias de seguridad de Windows instalado como rol en cada uno de los servidores Windows Server, que permite respaldar la información de manera similar a la realizada con la herramienta principal de Symantec.

Los medios alternos de almacenamiento se encuentran en la unidad de almacenamiento SAN adquirida recientemente por la entidad, de igual manera existen 2 discos duros externos de 4 TB cada uno adquiridos para este fin.

6.8 ETIQUETADO DE BACKUPS

Luego del análisis de los backups generados periódicamente se evidencio que en una sola cinta tipo LTO 6 con capacidad de 2.5 TB o hasta 6.25 TB comprimidos

es posible almacenar todas las copias de los diferentes servidores hasta por 15 días, lo cual se traduce en un único etiquetado por rango de fechas en el formato legal colombiano Año-Mes-Día, tanto en la cinta como en la respectiva plantilla creada para este fin. Lo anterior teniendo en cuenta también la disponibilidad de los recursos de almacenamiento y buscando su mayor aprovechamiento.

La estructura final es la siguiente:

Cinta INM No xx: 2015-03-01 A 2015-03-16

Para el etiquetado de las copias de seguridad de equipos a respaldar se definió la siguiente estructura:

Nombre del PC + nombre de usuario + fecha realización

Ejemplo: INM018-JDIAZM-2015-05-05

7 COPIAS DE SEGURIDAD DE TI – INM.

De acuerdo al trabajo investigativo realizado se diseño el proceso de copias de seguridad para el Instituto Nacional de Metrología INM, el cual recopila y formaliza muchos de los procedimientos actualmente realizados por la organización apoyándonos en las mejores prácticas consultadas y que han sido mencionadas en el presente trabajo. (Ver anexo Nº8).

8 VERIFICACION DEL PROCESO PROPUESTO

Para verificar que el proceso propuesto se encontraba acorde a las necesidades de la organización procedimos a presentarlo y socializarlo ante el personal de la Subdirección De Innovación Y Servicios Tecnológicos del INM, encontrando una buena recepción por parte de la subdirección encargada del proceso reconociendo el trabajo realizado que contribuye a mejorar los procesos del área de TICS. (Ver anexo Nº9 y anexo 10).

CONCLUSIONES

- La implementación de un proceso de copias de seguridad de TI brinda un gran aporte para la organización ya que evita perdidas de información crítica aportando a la continuidad de la operación.

- Se pudo evidenciar que la entidad no contaba con políticas, procesos, procedimientos y las prácticas establecidos para los procesos de TI especialmente al respaldo de información y el restablecimiento de la operación.

- Durante la ejecución del proyecto se logro planear y definir el alcance del proceso de copias de seguridad de TI y de la Subdirección de Innovación y Servicios Tecnológicos del INM apoyando el modelo GRC en la entidad.

- Se diseño el proceso de copias de seguridad de TI, estableciendo roles y responsabilidades.

- Se determinó que el proceso diseñado durante esta investigación es acorde a las necesidades de la organización, como se pudo evidenciar luego de presentarlo al interior de la entidad y socializarlo en donde se encontró una buena recepción por parte de la subdirección encargada del proceso reconociendo el trabajo realizado que contribuye a mejorar los procesos del área de TICS.

RECOMENDACIONES

- El contar con el proceso establecido para las copias de seguridad no garantiza el éxito del mismo, es de vital importancia que el personal involucrado acojan el proceso propuesto, a fin que este no quede como un documento más si no que aporte integralmente a la entidad, para lo cual se tiene que brindar capacitación y concientización a los funcionarios encargados que la ejecución de estas actividades contribuyen a reducción de la pérdida de información.

- Las buenas prácticas brindaron pautas particulares para el desarrollo del diseño de las copias de seguridad, las cuales deben ser continuamente actualizadas por la organización para que el proceso aporte un mejor valor y respalde los objetivos del negocio establecidos por el INM.

- Es importante hacer monitoreo continuo a cada uno de los elementos que encierran este proceso para garantizar el éxito continuo de la operación del mismo.

- El INM debe identificar los procesos y procedimientos no formalizados, con el fin de planearlos, diseñarlos e implementarlos de una manera organizada para que le permitan determinar roles y responsabilidades que contribuyan al cumplimiento de los objetivos organizacionales.

BIBLIOGRAFIA

1. Albert G. Alexander,(2007). Diseño de un Sistema de Gestión de la Información, Colombia: Alfaomega

2. Seltiz, C. (2010).El GRC Capability Model. Estados Unidos: OCEG Editors

3. Ormella Meller. (2009). Gestión de riesgos principios y directrices. Estados Unidos: International Organization for Standardization.

4. Harrsch, C. (2005). Gestión de la seguridad de la información en una empresa. Estados Unidos: International Organization for Standardization.

5. Padrini, F y Lucheroni, M (2006) Calidad de los Servicios TI. Barcelona: De vecchi

6. Marcombo Alexander (2007). Diseño de un Sistema de Gestión de Seguridad de Información .España: AlfaOmega).

7. Winkler, Zen (2008). el arte de la Seguridad de la Información, México: Editorial Patria.