ESTANDARIZACIÓN DE POLÍTICAS Y CONTROLES DE SEGURIDAD DE LA INFORMACIÓN PARA EL PROCESO "GESTIONAR LA SEGURIDAD INFORMÁTICA Y LA CONTINUIDAD DE LAS SOLUCIONES DE TIC" (M11P4)

JOSÉ LUIS JARAMILLO PARRA

UNIVERSIDAD AUTÓNOMA DE OCCIDENTE
FACULTAD DE INGENIERÍA
DEPARTAMENTO DE OPERACIONES Y SISTEMAS
PROGRAMA INGENIERÍA INFORMÁTICA
SANTIAGO DE CALI
2013

ESTANDARIZACIÓN DE POLÍTICAS Y CONTROLES DE SEGURIDAD DE LA INFORMACIÓN PARA EL PROCESO "GESTIONAR LA SEGURIDAD INFORMÁTICA Y LA CONTINUIDAD DE LAS SOLUCIONES DE TIC" (M11P4)

JOSÉ LUIS JARAMILLO PARRA

Proyecto de Grado para optar por el título de Ingeniero Informático

Director
Armando García Hernández
Ingeniero de Sistemas, MBA

UNIVERSIDAD AUTÓNOMA DE OCCIDENTE
FACULTAD DE INGENIERÍA
DEPARTAMENTO DE OPERACIONES Y SISTEMAS
PROGRAMA INGENIERÍA INFORMÁTICA
SANTIAGO DE CALI
2013

Nota de aceptación:

Aprobado por el Comité de Grado en cumplimiento de los requisitos exigidos por la Universidad Autónoma de Occidente para optar al título de Ingeniero Informático.

MIGUEL JOSÉ NAVAS

Jurado

MARIO WILSON CASTRO

Jurado

Santiago de Cali, 22 de Julio de 2013

AGRADECIMIENTOS

Es difícil agradecer a todos aquellos que de una u otra forma me han acompañado en el desarrollo de este proyecto, ya que nunca alcanza el tiempo, el papel o la memoria para mencionar o dar justicia a todos los créditos y méritos a quienes lo merecen, deseo agradecerles a todos los que me han colaborado para que este trabajo de grado salga de la mejor manera posible.

Doy infinitas gracias a Dios por haberme guiado a lo largo de mi vida, por ser mi apoyo, mi luz y mi camino, por darme la fortaleza para seguir adelante en aquellos momentos de debilidad y por brindarme una vida llena de aprendizajes, experiencias y sobre todo felicidad.

Gracias Dios por darme los mejores padres, **José María Jaramillo Vallejo** y **Luz Dary Parra Mejía**, ellos siempre me han dado su apoyo incondicional, inculcándome valores y dándome la oportunidad de tener una excelente educación en el transcurso de mi vida.

Mi abuelita **Elena**, muchísimas gracias por ser mi segunda madre, siempre brindándome amor y colaboración.

A mi hermana **Lina María Jaramillo Parra** que ha ocupado un lugar muy importante en mi corazón, gracias por el apoyo y la confianza.

Agradezco a la Universidad Autónoma de Occidente, a los docentes que me impartieron sus valiosos conocimientos con paciencia y dedicación para formarme como profesional, a el Director del Programa de Ingeniería Informática **Miguel José Navas Jaime**, quien me brindo apoyo y herramientas indispensables para mi formación profesional y a mi director de proyecto de grado **Armando García Hernández**, quien me guío en el desarrollo de este proyecto.

De igual manera agradezco al Departamento Administrativo de TIC de la Gobernación del Valle del Cauca, especialmente al Ingeniero **Diego Mauricio Peña Bolaños** por aportarme conocimientos para mi vida profesional y brindarme la confianza para el desarrollo de este proyecto.

En general quiero agradecer a todas las personas, compañeros y amigos que me han brindado apoyo, ánimo, cariño y amistad, para que mis sueños, metas y propósitos hoy en día se conviertan en la realidad más enriquecedora y valiosa.

CONTENIDO

	Pág.
RESUMEN	**13**
INTRODUCCIÓN	**14**
2. ANTECEDENTES	**16**
3. PROBLEMA DE INVESTIGACIÓN	**22**
3.1. PLANTEAMIENTO DEL PROBLEMA	**22**
4. JUSTIFICACIÓN	**24**
5. OBJETIVOS	**25**
5.1. OBJETIVO GENERAL	**25**
5.2. OBJETIVOS ESPECÍFICOS	**25**
6. MARCOS DE REFENCIA	**26**
6.1. MARCO TEÓRICO	**26**
6.2. ESTANDARES	**28**
6.3. RIESGOS	**36**
6.4. MICROSOFT SECURITY ASSESSMENT TOOL – MSAT.	**45**
7. DESARROLLO DEL PROYECTO	**50**
7.1. ESTABLECIMIENTO DEL CONTEXTO (T.1)	**51**
7.1.1. Recopilar y analizar documentos de la organización referentes a seguridad de la información (T.1.1)	**52**
7.1.2. Definir política de seguridad (T.1.2)	**53**
7.1.3. Obtener aprobación y compromiso de los directivos (T.1.3)	**54**
7.1.4. Socializar el proceso (T.1.4)	**55**
7.2. ANÁLISIS DE RIESGOS (T.2)	**56**
7.2.1. Establecer criterios de valoración (T.2.1)	**58**
7.2.2. Establecer escalas de valoración (T.2.2)	**59**
7.2.3. Identificación de activos (T.2.3)	**60**
7.2.4. Identificación y valoración de amenazas y vulnerabilidades (T.2.4)	**60**

7.2.5. Valoración del impacto (T.2.5) 61
7.2.6. Estimación del riesgo inherente (T.2.6) 62
7.2.7. Valorar los controles existentes (T.2.7) 63
7.2.8. Estimación del riesgo residual (neto) (T.2.8) 63
7.2.9. Priorizar los riesgos críticos (T.2.9) 64
7.3. GESTIÓN DE RIESGOS (T.3) 65
7.3.1. Asignar responsables de los planes de respuesta a riesgos (T.3.1) 66
7.3.2. Tomar decisiones para el tratamiento del riesgo (T.3.2) 67
7.4. MONITOREO (T.4) 68
7.4.1. Asignar responsables del monitoreo (T.4.1) 68
7.4.2. Chequeo de controles y medidas tomadas (T.4.2) 69
7.5. MEJORAMIENTO CONTINUO (T.5) 70
7.5.1. Registro de acciones de mejora e incidentes (T.5.1) 70
7.5.2. Evaluar modificaciones en los procesos (T.5.2) 71
7.6. COMUNICACIÓN (T.6) 72
7.6.1. Comunicación con la alta gerencia (T.6.1) 73
7.6.2. Comunicación con los funcionarios de la organización (T.6.2) 73
7.7. ROLES Y RESPONSABILIDADES 73
7.8. PLANTILLAS 74
7.9. CUADRO DE DESCRIPCIÓN HERRAMIENTAS (PLANTILLAS) 90
7.10. CRITERIOS DE VALORACIÓN 91
7.11. ESCALAS DE VALORACIÓN 96
7.12. EJEMPLOS 100

8. METODOLOGÍA DE LA INVESTIGACIÓN 106

9. RESULTADOS 109
9.1. RECOMENDACIONES A PARTIR DEL ANÁLISIS 109
9.2. POLÍTICAS ESTABLECIDAS 112
9.2.1. Políticas de administración de credenciales de acceso. 112
9.2.2. Políticas de software licenciado 114
9.2.3. Políticas para el uso aceptable del internet 116
9.2.4. Políticas para el uso de los recursos informáticos 119
9.2.5. Políticas para el uso del correo electrónico 121

10. CONCLUSIONES 124

11. RECOMENDACIONES 126

BIBLIOGRAFÍA 127

ANEXOS **131**

LISTA DE FIGURAS

Pág.

Figura 1. Seguridad de la información según la norma ISO/IEC 17799 26

Figura 2. Planos de actuación en la Seguridad Informática 27

Figura 3. Dominios de la Norma ISO 27002 31

Figura 4. Tipos de documentos de la ISO 27002 32

Figura 5. Controles ISO/IEC 27002 34

Figura 6. Modelo PHVA para los procesos del SGSI. NTC-ISO/IEC 27001 36

Figura 7. Estructura de gestión de riesgos – principios y directrices, ISO 31000 37

Figura 8. Guía de análisis y gestión de riesgos, ISO 27005 41

Figura 9. Descripción del proceso de análisis y gestión de riesgos 44

Figura 10. Guía de desarrollo metodológico 50

Figura 11. Guía de establecimiento del contexto 52

Figura 12. Guía de análisis de riesgos 57

Figura 13. Guía de gestión de riesgos 66

Figura 14. Guía de monitoreo 68

Figura 15. Guía mejoramiento continuo 70

Figura 16. Guía comunicación 72

Figura 17. Plantilla 01, establecimiento del contexto 75

Figura 18. Plantilla 02, Identificación de activos 77

Figura 19. Plantilla 03, análisis de riesgos 81

Figura 20. Plantilla 04, gestión de riesgos 84

Figura 21. Plantilla 05, monitoreo **86**

Figura 22. Plantilla 06, mejoramiento continuo **89**

Figura 23. Esquema de las fases del proceso unificado ágil (AUP) **107**

LISTA DE CUADROS

Pág.

Cuadro 1. Cuadro de Registro Internacional SGSI 16

Cuadro 2. Cuadro de Registro Nacional SGSI 17

Cuadro 3. Familia de normas 27000 29

Cuadro 4. Cuadro de áreas incluidas dentro de la evaluación de riesgos de seguridad – MSAT. 46

Cuadro 5. Cuadro descriptivo de la tarea T.1.1 53

Cuadro 6. Cuadro descriptivo de las tareas T.1.2.1, T.1.2.2, T.1.2.3, T.1.2.4 54

Cuadro 7. Cuadro descriptivo de la tarea T.1.3 55

Cuadro 8. Cuadro descriptivo de la tarea T.1.4 55

Cuadro 9. Cuadro descriptivo de las tareasT.2.1.1, T.2.1.2, T.2.1.3 58

Cuadro 10. Cuadro descriptivo de las tareas T.2.2.1, T.2.2.2 59

Cuadro 11. Cuadro descriptivo de la tarea T.2.3 60

Cuadro 12. Cuadro descriptivo de las tareas T.2.4.1, T.2.4.2 61

Cuadro 13. Cuadro descriptivo de la tarea T.2.5 61

Cuadro 14. Cuadro descriptivo de la tarea T.2.6 62

Cuadro 15. Cuadro descriptivo de la tarea T.2.7 63

Cuadro 16. Cuadro descriptivo de la tarea T.2.8 64

Cuadro 17. Cuadro descriptivo de la tarea T.2.9 65

Cuadro 18. Cuadro descriptivo de la tarea T.3.1 66

Cuadro 19. Cuadro descriptivo de la tarea T.3.2 67

Cuadro 20. Cuadro descriptivo de la tarea T.4.1 69

Cuadro 21. Cuadro descriptivo de la tarea T.4.2 **69**

Cuadro 22. Cuadro descriptivo de la tarea T.5.1 **71**

Cuadro 23. Cuadro descriptivo de la tarea T.5.2 **72**

Cuadro 24. Cuadro descriptivo de la tarea T.6.1 **73**

Cuadro 25. Cuadro descriptivo de la tarea T.6.2 **73**

Cuadro 26. Cuadro descriptivo de los activos de información **76**

Cuadro 27. Cuadro descriptivo de amenazas **78**

Cuadro 28. Cuadro descriptivo de herramientas (plantillas) **90**

Cuadro 29. Cuadro descriptivo de valoración de una amenaza **91**

Cuadro 30. Cuadro descriptivo de valoración de una vulnerabilidad **92**

Cuadro 31. Cuadro descriptivo de valoración de confidencialidad **93**

Cuadro 32. Cuadro descriptivo de valoración de integridad **94**

Cuadro 33. Cuadro descriptivo de valoración de disponibilidad **95**

Cuadro 34. Cuadro descriptivo de valoración de un control **96**

Cuadro 35. Cuadro descriptivo de riesgo inherente **97**

Cuadro 36. Cuadro descriptivo de riesgo residual **99**

Cuadro 37. Cuadro descriptivo de gestión de riesgos del negocio **100**

Cuadro 38. Cuadro de ejemplos de activos de Información **100**

Cuadro 39. Cuadro de ejemplos de amenazas informáticas **102**

Cuadro 40. Cuadro de ejemplos de vulnerabilidades informáticas **105**

LISTA DE ANEXOS

	Pág.
Anexo A. Establecimiento del Contexto	**131**
Anexo B. Listado de Activos	**132**
Anexo C. Análisis de Riesgos	**135**
Anexo D. Gestión de Riesgos	**139**
Anexo E. Controles de la ISO 27002 seleccionados	**142**

RESUMEN

La información es uno de los activos más importantes que se encuentra presente en una organización, por esto se hace necesario que los procesos y sistemas que la gestionan a diario deban ser protegidos de amenazas que afectan la continuidad del negocio y/o la no consecución de los objetivos organizacionales.

Hoy en día la mayor parte de la información vital se encuentra en los diferentes equipos informáticos y redes de datos, esto hace que dichos equipos y redes se encuentren sujetos a diferentes riegos e inseguridades, que en últimas pueden ser aprovechadas de forma ilícita por diferentes personas afectando directamente la disponibilidad, integridad y/o confidencialidad de la información.

Para proteger a las organizaciones de estos riesgos es necesario conocerlas y afrontarlas de una manera adecuada, para ello se debe establecer unos procedimientos adecuados e implementar controles de seguridad de la información basados en la evaluación de los riesgos y en la medición de su eficacia.

En el presente documento se ilustra el proceso que se debe llevar a cabo en una organización para conocer los riesgos a los que se encuentran expuestos sus activos de información, para luego determinar una serie de políticas, procedimientos y controles de seguridad de la información, que permitirán mantener el riesgo en un nivel aceptable por la dirección de la organización.

Palabras Claves; Seguridad de la información, Seguridad Informática, Análisis de Riesgos, Políticas de seguridad de la información, Amenazas, Vulnerabilidades, Gestión de riesgos, ISO 27000.

INTRODUCCIÓN

En la actualidad se ha ido incrementando la dependencia que existe entre la sociedad y las tecnologías de la información y comunicación (TIC), esto ha hecho que tanto ciudadanos como las diferentes organizaciones queden expuestas a diferentes amenazas presentes en el entorno. Esta tendencia hacia la interconectividad y la interoperabilidad por medio de redes de sistemas informáticos, ha hecho que las diferentes organizaciones soporten gran parte de su actividad de negocio sobre dicha tecnología, por lo tanto es necesario contar con una serie de medidas que garanticen que la información, los sistemas y la infraestructura computacional se encuentren asegurados y de esta manera se genere desarrollo y sostenibilidad en la actividad de negocio de las organizaciones.

La información es catalogada como uno de los activos más importantes presente hoy en día en todas las organizaciones, es la pieza fundamental en la actividad de negocio ya que permite tomar las diferentes decisiones para el continuo desarrollo de las organizaciones.

Actualmente la seguridad de la información ha tomado mucho auge debido al continuo crecimiento de los diferentes riesgos asociados a ésta y principalmente al continuo incremento y difusión de herramientas, malvare o programas maliciosos que contienen en su código prácticas mal intencionadas que conllevan a poner en peligro la información vital de las organizaciones.

Debido a estos riesgos las organizaciones deben realizar una correcta gestión en el campo de la seguridad de la información, para reducir las vulnerabilidades presentes y evitar de esta manera que las amenazas se materialicen y generen impactos negativos en el ámbito económico, social, legal, etc.
La implementación de políticas y controles adecuados en el campo de la seguridad de la información son de gran importancia, ya que además de garantizar la continuidad del negocio, permite a las organizaciones preservar la disponibilidad, integridad y confidencialidad de la información, los cuales son puntos clave para el éxito de ésta.

Existen diferentes organismos o entidades que se centran en desarrollar y difundir diferentes normas o estándares en el campo de la seguridad de la información. Entre estas organizaciones se encuentra la ISO (International Organization for Standardization) con la serie ISO/IEC 27000 y sus normas asociadas en el área de la seguridad de la información, dicha norma contiene un conjunto de estándares

que proporcionan un marco de gestión de la seguridad de la información, utilizable por cualquier tipo de organización y es la base para el desarrollo de este proyecto. Con la estandarización de políticas y controles de seguridad de la información en el Departamento Administrativo de las TIC de la Gobernación del Valle, lo que se quiere lograr es que la organización cumpla con sus objetivos de negocio, considerando los diferentes riesgos que están relacionados con las TIC de la organización y de esta manera se reduzcan las vulnerabilidades, evitando posibles daños provenientes de amenazas externas.

En este documento se dará a conocer el contenido teórico y metodológico para el desarrollo del proyecto y al finalizar se presentan las respectivas recomendaciones.

2. ANTECEDENTES

Existen varias organizaciones que trabajan en proyectos similares relacionados con la seguridad de la información, sin embargo son pocas las que cuentan con una certificación en la ISO/IEC 27001.

Trabajar bajo la ISO/IEC 27001 garantiza que se están tomando medidas para tratar los riesgos asociados a la disponibilidad, confidencialidad e integridad de la información, contar con la certificación en dicha norma ratifica la adaptación de buenas prácticas de seguridad de la información mundialmente aceptadas.

A nivel mundial son 7940 organizaciones que se encuentran certificadas en la ISO/IEC 27001 (Agosto 2012), que se encuentran distribuidas de la siguiente manera:

Cuadro 1. Cuadro de Registro Internacional SGSI

PAIS	CERTIFICADAS	PAIS	CERTIFICADAS	PAIS	CERTIFICADAS
Japan	4152	Netherlands	24	Belgium	3
UK	573	Saudi Arabia	24	Gibraltar	3
India	546	UAE	19	Lithuania	3
Taiwan	461	Bulgaria	18	Macau	3
China	393	Iran	18	Albania	3
Germany	228	Portugal	18	Bosnia Herzegovina	2
C. Republic	112	Argentina	17	Cyprus	2
Korea	107	Philippines	16	Ecuador	2
USA	105	Indonesia	15	Jersey	2
Italy	82	Pakistan	15	Kazakhstan	2
Spain	72	Colombia	14	Luxembourg	2
Hungary	71	Russian F.	14	Macedonia	2
Malaysia	66	Vietnam	14	Malta	2
Poland	61	Iceland	13	Mauritius	2
Thailand	59	Kuwait	11	Ukraine	2
Greece	50	Canada	10	Armenia	1
Ireland	48	Norway	10	Bangladesh	1
Austria	42	Sweden	10	Belarus	1
Turkey	35	Switzerland	9	Bolivia	1
Turkey	35	Bahrain	8	Denmark	1
France	34	Peru	7	Estonia	1
Hong Kong	32	Chile	5	Kyrgyzstan	1
Australia	30	Egypt	5	Lebanon	1
Singapore	29	Oman	5	Moldova	1
Croatia	27	Qatar	5	New Zealand	1
Slovenia	26	Sri Lanka	5	Sudan	1
Mexico	25	South Africa	5	Uruguay	1
Slovakia	25	Dom. Republic	4	Yemen	1
Brazil	24	Morocco	4	**Total**	**7940**

Fuente: International Register of ISMS Certificates, ISMS International User Group, [en línea], [consultado 06 de Noviembre, 2012]. Disponible en Internet: http://www.iso27001certificates.com/

A nivel nacional, Colombia cuenta con 14 organizaciones certificadas en la ISO/IEC 27001, las cuales son:

Cuadro 2. **Cuadro de Registro Nacional SGSI**

Nombre de la Organización	Alcance SGSI
ACH Colombia SA	La Dirección de Seguridad de la Información para los procesos que soportan el servicio de ACH (transacciones de crédito y débito) para la transferencia electrónica de fondos, SOI - Servicio de Información sobre el Funcionamiento de los pagos por el sistema de seguridad social integral y el PSE - Proveedor de Servicios Electrónicos (botón de pago) para los pagos y compras a través de Internet, incluyendo los recursos tecnológicos, administrativos, financieros y humanos de apoyo a los procesos en los dos sitios de administración, de conformidad con la declaración de Aplicabilidad de la Versión 2 de fecha 20 de noviembre de 2007.
ComBanc SA	El SGSI cubrirá toda la Organización de ComBanc S.A., por lo tanto, estarán bajo este sistema todos los activos de información y las personas ubicadas en las Oficinas en Huérfanos 770 OF 1601, la oficina remota en Augusto Leguía 79, Of. 1206, el site de producción en Huérfanos 770 piso 12 y el site remoto de contingencias en Huérfanos 1052 piso 11. De esta manera, el SGSI cubrirá los activos de información, controlados en el sistema Táctica, en los cuales se destacan: el sistema AIPAC (Cámara de compensación de altos montos y Switch DVP-LBTR), el sistema Swift para ComBanc, servidores, aparatos de telecomunicaciones, la red interna de ComBanc, la información producida para los Participantes de la Cámara (clientes) y la documentación asociada a las actividades de control. Incluye políticas, procedimientos, manuales y controles específicos de acuerdo con SoA, versión 1. 01/30/2008.
Concesión RUNT SA	Oficina administrativa: la seguridad del sistema de información de gestión de los datos de validación, autorización, registro y seguridad de las transacciones relacionadas con el tráfico y el transporte en régimen de concesión en Colombia. Incluyendo el diseño e implementación de procesos único Sistema Nacional de Registro de tráfico (HQ-RUNT) … (Continua1)

Cuadro 2 (Continuación)

Nombre de la Organización	Alcance SGSI
Concesión RUNT SA	(Continua1)… y los activos de información gestionados por Concesión RUNT SA y de terceros. Alternativa Centro de Datos locativas: Infraestructura Crítica y procesamiento de datos. De acuerdo a la Declaración de Aplicabilidad Versión 3 de 22 de febrero de 2012.
DIGISOC SAS	Prestación del servicio de gestión de incidentes de seguridad en la ciudad de Bogotá.
Dirección de inteligencia policial – DIPOL	Seguridad de la información en el sistema de gestión de la producción de operativa, estratégica y la inteligencia SERVICIO Y contrainteligencia a nivel central, garantizando la seguridad de los activos críticos. Declaración de la versión aplicabilidad 1 de 16 de enero 2012
Etek International Holding Corp.	La gestión del Sistema de Gestión de Seguridad (SGSI) en las instalaciones de Colombia, en relación con la infraestructura interna de tecnología de la información en apoyo de las actividades de las operaciones de negocios, de acuerdo con la Declaración de Aplicabilidad V4, 31 de enero de 2008 como se define en la norma ISO27001:2005. La Gestión de la Seguridad de la Información en la sucursal de Colombia, relacionada a la infraestructura interna de Tecnología de la Información para soportar las Operaciones del Negocio, de acuerdo con la Declaración de Aplicabilidad V4, 31 de Enero de 2008 Que Se refiere a la ISO 27001:2005.
Financial Systems Company Ltda.	La seguridad de la información del sistema de gestión de Financial Systems Company Ltda aplicado al "análisis, diseño, desarrollo y mantenimiento de software de gestión de cobros y recuperación, y servicios relacionados de consultoría en el proceso de cobro" en relación con la información y recursos tecnológicos utilizados para apoyar el "negocio operaciones en sus oficinas centrales corporativas en Chía, Cundinamarca, Colombia, de acuerdo con la declaración de aplicabilidad versión 8.0.
FLUIDO DE SEÑAL GROUP SA	Gestión del diseño, desarrollo, implantación, consultoría y formación en tecnologías de información, seguridad de la información y soluciones de riesgos estado de aplicación de fecha 09/09/2010.
Ricoh Colombia SA	La Seguridad de la Información del Sistema de Gestión de Ricoh Colombia SA incluidas las actividades empresariales relacionadas con los activos de información de los siguientes procesos / procedimientos: crédito y cobranza, el departamento de TI y gestión de recursos humanos ubicada en la carrera 85d no. 51-65, complejo logístico San Cayetano, Bogotá dc, Colombia, de conformidad con la declaración de aplicabilidad rev.2 desde 22 de enero 2008.

Cuadro 2 (Continuación)

Nombre de la Organización	Alcance SGSI
SETECSA SA	Seguridad de la Información del Sistema de Gestión para los siguientes servicios: almacenaje, custodia, administración y transferencia de archivo físico, los soportes magnéticos y garantías, con las siguientes actividades: recibir, inventario, validación, verificación, clasificación, naturaleza y creación de bases de datos, atención consultoría, gestión de información , incluyendo la creación y puesta en un sistema de inventario, valoración y creación de tablas de retenciones de documentos, reprografía, microfilmes, digitalización, centro alternativo de proceso y de gestión del centro de la correspondencia. En Bogotá DC City en la sede de la siguiente: - Calle 18 No. 69b-73 - Calle 18A No. 69b-79 - Calle 21 No. 69b-57 - Calle 18A No. 69F-45 De acuerdo con la declaración de aplicabilidad de fecha 2009 -11-26 versión 1.
SYNAPSIS COLOMBIA LTDA SYNAPSIS COLOMBIA LTDA	•Datos del centro zona franca: Proporcionar servicios de collocation, hospedaje y la informática bajo demanda. •Datos del centro calle 128: Proporcionar servicios de co-ubicación, hospedaje y la informática bajo demanda. •Sede Administrativa: Protección de la información SYNAPSIS y su atención al cliente relacionada y la entrega de los siguientes servicios de outsourcing de TI: Servicios de administración, Infraestructura de TI, soporte y mantenimiento, incluyendo el hardware y la plataforma de software, telecomunicaciones, automatización y control, sistema de seguridad de la información, los activos de información y Proveedores administraciones. • Administración de servicios, operación y mantenimiento de aplicaciones que incluyen soporte técnico y / o funcional y la mejora correctivo, mantenimiento preventivo y adaptativo. • Los servicios de usuario final, incluyendo contact center, centro de servicio y soporte en el sitio. Declaración de Aplicabilidad de la Versión 7, fechada el 13 de enero 2012
TELMEX COLOMBIA SA	•Data center triara: Proporcionar servicios de Collocationy Secure Mail para el segmento de clientes corporativos. •Oficina administrativa: Apoyar procesos de gestión de TI y la gestión de procesos, incluidos los sistemas de información corporativos, empresas plataforma de correo electrónico y repositorios de información corporativos. Declaración de Aplicabilidad de la Versión 1 de fecha 08 de septiembre 2010

Cuadro 2 (Continuación)

Nombre de la Organización	Alcance SGSI
UNE EPM Telecomunicaciones. SA ESP	Gestión de seguridad de la información aplicada a los procesos y actividades que apoyen las instalaciones y las TIC (Tecnologías de la Información y la Comunicación) infraestructura necesarios para prestar el servicio de hosting dedicado en el Centro de Datos de Internet ubicado en Medellín.
UNISYS Global Outsourcing y Servicios de Infraestructura (GOIS) / Servicios de Mantenimiento de apoyo (MSS)	Atención al cliente y servicios administrados de soporte, con los siguientes procesos: SGSI Gestión, Gestión de Red, Gestión de Sistemas y Gestión de Seguridad, con el apoyo de la gestión de activos, recursos humanos, infraestructura de TI y funciones llevadas a cabo en el Centro de Comando. Esto está de acuerdo con la Declaración de Aplicabilidad Versión 3.0 con fecha 03 de julio 2007.

Fuente: International Register of ISMS Certificates, ISMS International User Group, [en línea], [consultado 06 de Noviembre, 2012]. Disponible en Internet: http://www.iso27001certificates.com/

A nivel del Valle del Cauca se tiene conocimiento que se han adelantado dos proyectos orientados a la seguridad informática, los cuales son:

El primero se desarrolló en la Alcaldía de Santiago de Cali en el año 2006, el objetivo de este proyecto fue "Evaluar los controles a nivel informático, analizar la seguridad de los sistemas, realizar la evaluación de las políticas e seguridad informática propuestas para la Alcaldía de Santiago de Cali"[1].

El segundo se desarrolló en la Alcaldía del municipio de Candelaria en el año 2008, en dicho proyecto se planteó lo siguiente: "elaboración de un análisis de riegos que permitirá a la organización realizar un manejo eficiente de los recursos involucrados en el proceso tomado como referencia, identificando sus vulnerabilidades y las amenazas a las que se encuentran expuestos los activos

1 ANDRADE, Ivert, ESTRADA, Erich, RODRÍGUEZ, Debray. Evaluación e implementación de políticas de seguridad informática en la alcaldía de Santiago de Cali. Trabajo de grado Profesional en Ingeniería Electrónica. . Santiago de Cali: Universidad Autónoma de Occidente. Facultado de Ingeniería. Departamento de Electrónica, Septiembre, 2006.

para que de esta forma se puedan aprovechar mejor y permitan un buen funcionamiento de la organización"[2.]

Por ultimo vale la pena recalcar la estrategia de "Seguridad y Privacidad en las Tecnologías de Información" que se encuentra desarrollando el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, la cual consiste en brindar los lineamientos necesarios para implementar un modelo de seguridad de la información al interior de las entidades del estado y así proporcionar confianza a los ciudadanos al realizar sus trámites en línea.

Las funciones principales de esta estrategia están enmarcadas en los siguientes puntos:

- Liderar la implementación de plataformas con estándares de seguridad en las entidades del estado.

- Elaborar una estrategia de seguridad de la información que soporte un marco normativo específico.

- Definir los lineamientos y estándares de protección de la información pública, para su preservación en situaciones de desastre.

- Fomentar y reforzar la cooperación internacional en materia de Ciberseguridad.

- Promover una cultura de ciberresponsabilidad en el estado, basada en la concientización y formación continua en ciberseguridad.

- Apoyar en la identificación de la infraestructura crítica del país.

- Definir los lineamientos y estándares de seguridad que se deben tener en cuenta con los dispositivos móviles corporativos y personales.

- Estructurar la estrategia de capacitación de funcionarios del departamento de TI y/o Seguridad.

- Definir la estrategia de sensibilización para altos directivos de las entidades y para los funcionarios públicos en general[3].

---

2 MOLINA, Lina. Modelo de seguridad para el procedimiento no. 19 del manual de procesos y procedimientos de la alcaldía de Candelaria "legalización de pago y contabilización de cuentas y contratos". Trabajo de grado Profesional Ingeniería Informática. Santiago de Cali: Universidad Autónoma de Occidente. Facultado de Ingeniería. Departamento de Operaciones y Sistemas, Febrero, 2008.

3 Seguridad para el acceso a la información de las entidades del Estado, Ministerio de Tecnologías de la Información y las Comunicaciones Republica de Colombia - Gobierno en Línea, Abril 2013, [en línea], [consultado 24 de Julio, 2013]. Disponible en Internet: http://programa.gobiernoenlinea.gov.co/apc-aa-files/da4567033d075590cd3050598756222c/ResumenEjecutivo_Seguridad.pdf

3. PROBLEMA DE INVESTIGACIÓN

3.1. PLANTEAMIENTO DEL PROBLEMA

Debido al continuo desarrollo y expansión de las tecnologías de la información y la comunicación sobre todo el mundo, ha ocasionado que tanto las personas como las organizaciones las hayan aceptado como parte fundamental en el desarrollo de sus actividades cotidianas.

Hoy en día la mayor parte de la información vital se encuentra en los diferentes equipos informáticos, esto hace que dichos equipos se encuentren sujetos a diferentes riegos e inseguridades, que en últimas pueden ser aprovechadas de forma ilícita por diferentes personas afectando directamente la disponibilidad (la información debe estar lista para acceder cuando se necesite), integridad (la información debe ser completa y correcta en cualquier momento) y/o confidencialidad (la información solo debe ser accedida por personas autorizadas) de la información.

Actualmente se están presentando ataques virtuales externos hacia la Gobernación del Valle del Cauca registrados por el firewall; este hecho ocurre debido a que no se cuentan con suficientes medidas tecnológicas que garanticen que la información se encuentre disponible en todo momento, sea correcta y accedida solo por personas autorizadas, además los procedimientos y políticas de seguridad de la información no se encuentran claramente definidos dentro de la organización. Teniendo en cuenta que estos tres factores (tecnológicos, procedimientos y políticas) presentan falencias en la organización, sería poco eficiente la respuesta frente algún tipo de fallo en la seguridad de la información.

Por lo tanto, es necesario establecer un conjunto de políticas, procedimientos y controles que permita a la Gobernación del Valle Del Cauca garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos y gestionados, manteniendo así el riesgo de los sistemas de información dentro de unos niveles mínimos que sean asumibles por la organización, para ello se cuenta con una serie de estándares propuestos por la ISO (International Organization for Standardization e IEC (International Electrotechnical Commission), mas puntualmente se trata de la ISO/IEC 27000, que en pocas palabras es un conjunto de estándares que proporcionan un marco de gestión de la seguridad de la información.

Lo que se busca con el desarrollo de este proyecto es brindar respuesta a la pregunta ¿Qué políticas, procedimientos y controles de seguridad de la información con base en la ISO/IEC 27001, son aplicables para el proceso "Gestionar la seguridad informática y la continuidad de las soluciones de TIC" en el Departamento Administrativo de las TIC de la Gobernación del Valle Del Cauca?

4. JUSTIFICACIÓN

La seguridad de la información es una parte vital que se debe considerar en todas las organizaciones. Al no contar con buenas prácticas frente a la seguridad de la información, permitirá que diferentes atacantes o amenazas utilicen la organización para sus fines lucrativos y delictivos, los equipos informáticos podrán contener diferentes códigos maliciosos que conllevaran a poner en riesgo la información vital. Por consiguiente, la organización se verá afectada y no se cumpliría con los objetivos de negocio, los cuales son su razón de ser.

La seguridad de la información es una disciplina que se encuentra en continua evolución se debe llevar el correcto monitoreo de los controles aplicados para determinar si están cumpliendo con su labor o si es necesario actualizarlos, para alcanzar los objetivos previamente previstos.

Con la implementación de un sistema de gestión de seguridad de la información (SGSI) basado en la ISO/IEC 27001, se podrá contar con un sistema actualizado (siempre y cuando se haga una correcta gestión sobre el), que permitirá reducir de manera considerable las diferentes vulnerabilidades presentes en los activos de información del Departamento Administrativo de las TIC de la Gobernación del Valle. De este modo, se podrá evitar que las amenazas se materialicen, se generará confianza entre los funcionarios presentes en el Departamento Administrativo de las TIC, se cumplirá con los objetivos del negocio teniendo en consideración los riesgos asociados y se preservará la confidencialidad, integridad y disponibilidad de la información.

5. OBJETIVOS

5.1. OBJETIVO GENERAL

Establecer políticas y controles de seguridad de la información con base en la ISO/IEC 27001 para el proceso "Gestionar la seguridad informática y la continuidad de las soluciones de TIC" (M11P4)[4], que le permitan al Departamento Administrativo de las TIC de la Gobernación del Valle Del Cauca adoptar buenas prácticas de seguridad de la información mundialmente aceptadas.

5.2. OBJETIVOS ESPECÍFICOS

- Examinar la situación actual del Departamento Administrativo de las TIC de la Gobernación del Valle del Cauca entorno a los activos de información.
- Establecer el contexto del proceso (alcance, objetivos, justificación, etc.).
- Establecer metodología para la gestión de riesgos de seguridad de la información.
- Realizar un análisis de riesgos y gestión del riesgo de seguridad de la información.
- Estandarizar políticas de seguridad de la información.
- Establecer objetivos de control y controles de Seguridad de la Información presentes en el Anexo A de la ISO/IEC 27001:2005.
- Generar la documentación pertinente en referente a la seguridad de la información del Departamento Administrativo de las TIC.
- Informar y concienciar a los funcionarios del Departamento Administrativo de las TIC sobre la importancia del cumplimiento de las políticas de la seguridad de la información planteadas.

4 M11P4= Marco proceso número 11, proceso número 4, Departamento Administrativo TIC – Gobernación del Valle del Cauca

6. MARCOS DE REFENCIA

6.1. MARCO TEÓRICO

6.1.1. Seguridad de la información. La norma ISO/IEC 27001 define la seguridad de la Información como la preservación de su confidencialidad,[5] su integridad [6] y su disponibilidad, [7] así como de los sistemas implicados en su tratamiento, dentro de una organización.

Figura 1. Seguridad de la información según la norma ISO/IEC 17799

Fuente: GÓMEZ, Álvaro, Enciclopedia de la Seguridad Informática, Primera edición, Mexico: Editorial Alfaomega, 2007, p. 4.

6.1.2. Seguridad informática. La seguridad informática es abarcada por la seguridad de la información. La seguridad informática se puede definir como: "…cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos pueden conllevar daños sobre la información, comprender su confidencialidad, autenticidad o integridad, disminuir

5 Según la ISO/IEC 13335-1:2004]: característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.

6 Según [ISO/IEC 13335-1:2004]: propiedad/característica de salvaguardar la exactitud y completitud de los activos.

7 Según [ISO/IEC 13335-1:2004]: característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.

el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema"[8].

6.1.3. Objetivos de la seguridad informática. Entre los principales objetivos que debe velar la seguridad informática se encuentran:

- **"**Minimizar y gestionar los riesgos y detectar los posibles problemas y amenazas a la seguridad.

- Garantizar la adecuada utilización de los recursos y de las aplicaciones del sistema"[9].

Para cumplir con lo anterior se deben contemplar cuatro planos de acción (Figura 2), en el primero denominado organización se establecen las políticas y procedimientos que deben ser cumplidos dentro de la organización, a partir de este plano surge el segundo denominado humano en el cual se da a conocer lo planteado en el plano anterior, además se sensibilizan y concientizan a las personas presentes en la organización, el tercero denominado técnico se establecen las diferentes medidas tecnológicas (Hardware y Software) que brindaran apoyo a la seguridad de la información, por último se encuentra el denominado legislación donde se establecen las medidas legales que deben ser cumplidas por la organización en el ámbito de seguridad de la información.

Figura 2. **Planos de actuación en la Seguridad Informática**

8 GÓMEZ, Álvaro, Enciclopedia de la Seguridad Informática, Primera edición, Mexico: Editorial Alfaomega, 2007, p. 4.

9 Ibíd., p. 7.

Fuente: GÓMEZ, Álvaro, Enciclopedia de la Seguridad Informática, Primera edición, Mexico: Editorial Alfaomega, 2007, p. 8.

6.1.4. Gestión de seguridad de la información. "El Sistema de Gestión de la Seguridad de la Información (SGSI) en las empresas ayuda a establecer estas políticas, procedimientos y controles en relación a los objetivos de negocio de la organización, con objeto de mantener siempre el riesgo por debajo del nivel asumible por la propia organización"[10].

Por medio de un SGSI se le brinda a la organización una visión global sobre el estado de sus sistemas de información, los controles que tienen asociados y la manera como operan, para poder determinar si se están obteniendo los resultados deseados, permitiendo así, tomar decisiones para garantizar la seguridad de la información.

"En definitiva, con un SGSI, la organización conoce los riesgos a los que está sometida su información y los gestiona mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente"[11].

6.2. ESTANDARES

6.2.1. Estándar de seguridad de la información. Para llevar a cabo la gestión de la seguridad de la información es aconsejable basarse en las diferentes normas y estándares que están aprobados mundialmente; dichas normas y estándares permiten llevar a cabo el proceso de seguridad de la información de manera estructurada, documentada y basándose en los diferentes controles y políticas que se establecen. Entre las diferentes normas y estándares se encuentra la ISO/IEC 27000 la cual es:

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

10 Concepto de un SGSI, Instituto Nacional de Tecnologías de la Comunicación - INTECO. [en línea], [consultado 09 de Noviembre, 2012]. Disponible en Internet: http://cert.inteco.es/Formacion/SGSI/Conceptos_Basicos/Concepto_SGSI/

11 Ibíd., Disponible en Internet: http://cert.inteco.es/Formacion/SGSI/Conceptos_Basicos/Concepto_SGSI/

seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña"[12].

En el cuadro 3 se puede observar cómo se encuentra distribuida la familia del estándar ISO/IEC 27000.

Cuadro 3. Familia de normas 27000

Familia de normas 27000	
Norma ISO/IEC	**Título**
ISO 27000	Gestión de la Seguridad de la Información: Fundamentos y vocabulario.
ISO 27001	Especificaciones para un **SGSI**.
ISO 27002	Código de Buenas Prácticas.
ISO 27003	Guía de Implantación de un **SGSI**.
ISO 27004	Sistema de Métricas e Indicadores.
ISO 27005	Guía de Análisis y Gestión de Riesgos.
ISO 27006	Especificaciones para Organismos Certificadores de **SGSI**.
ISO 27007	Guía para auditar un **SGSI**.
ISO 2701X	Guías sectoriales.
ISO 27XXX	Futuras normas.

Fuente: Normativa de un SGSI, Instituto Nacional de Tecnologías de la Comunicación, INTECO - España, [en línea], [consultado 09 de Noviembre, 2012]. Disponible en Internet: http://cert.inteco.es/Formacion/SGSI/Conceptos_Basicos/Normativa_SGSI

Aunque cada norma de la familia de la ISO 27000 se encarga de diferentes puntos para la seguridad de la información, se destacan dos normas relevantes, la ISO 27001y la ISO 27002.

6.2.1.1. ISO 27001. "Esta norma es la definición de los procesos de gestión de la seguridad, por lo tanto, es una especificación para un SGSI y, en este momento, es la única norma Certificable, dentro de la familia ISO 27000.

12 Sistema de Gestión de la Seguridad de la Información, ISO, 2005 [en línea], [consultado 04 de Noviembre, 2012]. Disponible en Internet: http://www.iso27000.es/sgsi.html

En su Anexo A aparecen los objetivos de control y los controles que se desarrollan con más profundidad en la Norma ISO 27002"[13].

6.2.1.2. ISO 27002. "La ISO 27002 viene a ser un código de buenas prácticas en el que se recoge un catálogo de los controles de seguridad y una guía para la implantación de un SGSI. Al igual que el Anexo A de la ISO 27001, se compone de 11 dominios, 39 objetivos de seguridad y 133 controles de seguridad. Cada uno de los dominios conforma un capítulo de la norma y se centra en un determinado aspecto de la seguridad de la información"[14].

La primera parte de la norma la conforma lo siguiente:

- Introducción a los conceptos de seguridad de la información y SGSI.
- Campo de aplicación de la norma.
- Términos y definiciones de la norma.
- Estructura del estándar de la norma.
- Indicadores de evaluación y tratamiento del riesgo.

La segunda parte la conforman los siguientes dominios:

13 Normativa de un SGSI, Instituto Nacional de Tecnologías de la Comunicación, INTECO - España, [en línea], [consultado 09 de Noviembre, 2012]. Disponible en Internet:http://cert.inteco.es/Formacion/SGSI/Conceptos_Basicos/Normativa_SGSI

14Ibíd., Disponible en Internet: http://cert.inteco.es/Formacion/SGSI/Conceptos_Basicos/Normativa_SGSI

Figura 3. Dominios de la Norma ISO 27002

Fuente: Normativa de un SGSI, Instituto Nacional de Tecnologías de la Comunicación, INTECO - España, [en línea], [consultado 09 de Noviembre, 2012]. Disponible en Internet:http://cert.inteco.es/Formacion/SGSI/Conceptos_Basicos/Normativa_SGSI

6.2.1.2.1. ISO 27002 (Documentación). Todas las medidas que se hayan decidido implantar para la protección de la información deben quedar documentadas, la estructura de la documentación generada seguirá la siguiente forma:

Figura 4. Tipos de documentos de la ISO 27002

Fuente: Normativa de un SGSI, Instituto Nacional de Tecnologías de la Comunicación, INTECO - España, [en línea], [consultado 09 de Noviembre, 2012]. Disponible en Internet:http://cert.inteco.es/Formacion/SGSI/Conceptos_Basicos/Normativa_SGSI

Donde las Políticas sientan las bases de la seguridad constituyendo la redacción de los objetivos generales y las implantaciones que ha llevado a cabo la organización. Pretenden indicar las líneas generales para conseguir los objetivos marcados sin entrar en detalles técnicos. Deben ser conocidas por todo el personal de la organización.

Los Procedimientos desarrollan los objetivos marcados en la Políticas. En ellos sí que aparecerían detalles más técnicos y se concreta cómo conseguir los objetivos expuestos en las Políticas. No es necesario que los conozcan todas las personas de la organización sino, únicamente, aquellas que lo requieran para el desarrollo de sus funciones.

Las Instrucciones constituyen el desarrollo de los Procedimientos. En ellos se llega hasta describir los comandos técnicos que se deben realizar para la ejecución de dichos Procedimientos.

Y por último los Registros evidencian la efectiva implantación del SGSI y el cumplimiento de los requisitos. En este punto también es importante el contar con

una serie de indicadores o métricas de seguridad que permitan evaluar la consecución de los objetivos de seguridad establecidos[15].

6.2.1.3. Anexo A (ISO 27001 - ISO 27002). "El Anexo A es donde se juntan las normas ISO 27001 e ISO 27002. Los controles de la norma ISO 27002 tienen los mismos nombres que en el Anexo A de la norma ISO 27001; pero la diferencia se encuentra en el nivel de detalle: la ISO 27001 sólo proporciona una breve descripción de un control, mientras que la ISO 27002 ofrece lineamientos detallados sobre cómo implementar el control"[16].

15 Normativa de un SGSI, Instituto Nacional de Tecnologías de la Comunicación, INTECO - España, [en línea], [consultado 09 de Noviembre, 2012]. Disponible en Internet:http://cert.inteco.es/Formacion/SGSI/Conceptos_Basicos/Normativa_SGSI

16 KOSUTIC, Dejan, Controles del Anexo A de la norma ISO 27001, 20 de octubre de 2010, [en línea], [consultado 08 de Noviembre, 2012]. Disponible en Internet: http://blog.iso27001standard.com/es/tag/anexo-a/

Figura 5. Controles ISO/IEC 27002

ISO/IEC 27002:2005. Dominios (11), Objetivos de control (39) y Controles (133)

CLIC SOBRE CADA CONTROL PARA MÁS INFORMACIÓN

Versión actualizada de esta lista en: http://www.iso27000.es/download/ControlesISO27002-2005.pdf

5. POLÍTICA DE SEGURIDAD.
- 5.1 Política de seguridad de la información.
  - 5.1.1 Documento de política de seguridad de la información.
  - 5.1.2 Revisión de la política de seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
- 6.1 Organización interna.
  - 6.1.1 Compromiso de la Dirección con la seguridad de la información.
  - 6.1.2 Coordinación de la seguridad de la información.
  - 6.1.3 Asignación de responsabilidades relativas a la seg. de la informac.
  - 6.1.4 Proceso de autorización de recursos para el tratamiento de la información.
  - 6.1.5 Acuerdos de confidencialidad.
  - 6.1.6 Contacto con las autoridades.
  - 6.1.7 Contacto con grupos de especial interés.
  - 6.1.8 Revisión independiente de la seguridad de la información.
- 6.2 Terceros.
  - 6.2.1 Identificación de los riesgos derivados del acceso de terceros.
  - 6.2.2 Tratamiento de la seguridad en la relación con los clientes.
  - 6.2.3 Tratamiento de la seguridad en contratos con terceros.

7. GESTIÓN DE ACTIVOS.
- 7.1 Responsabilidad sobre los activos.
  - 7.1.1 Inventario de activos.
  - 7.1.2 Propiedad de los activos.
  - 7.1.3 Uso aceptable de los activos.
- 7.2 Clasificación de la información.
  - 7.2.1 Directrices de clasificación.
  - 7.2.2 Etiquetado y manipulado de la información.

8. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
- 8.1 Antes del empleo.
  - 8.1.1 Funciones y responsabilidades.
  - 8.1.2 Investigación de antecedentes.
  - 8.1.3 Términos y condiciones de contratación.
- 8.2 Durante el empleo.
  - 8.2.1 Responsabilidades de la Dirección.
  - 8.2.2 Concienciación, formación y capacitación en seg. de la informac.
  - 8.2.3 Proceso disciplinario.
- 8.3 Cese del empleo o cambio de puesto de trabajo.
  - 8.3.1 Responsabilidad del cese o cambio.
  - 8.3.2 Devolución de activos.
  - 8.3.3 Retirada de los derechos de acceso.

9. SEGURIDAD FÍSICA Y DEL ENTORNO.
- 9.1 Áreas seguras.
  - 9.1.1 Perímetro de seguridad física.
  - 9.1.2 Controles físicos de entrada.
  - 9.1.3 Seguridad de oficinas, despachos e instalaciones.
  - 9.1.4 Protección contra las amenazas externas y de origen ambiental.
  - 9.1.5 Trabajo en áreas seguras.
  - 9.1.6 Áreas de acceso público y de carga y descarga.
- 9.2 Seguridad de los equipos.
  - 9.2.1 Emplazamiento y protección de equipos.
  - 9.2.2 Instalaciones de suministro.
  - 9.2.3 Seguridad del cableado.
  - 9.2.4 Mantenimiento de los equipos.
  - 9.2.5 Seguridad de los equipos fuera de las instalaciones.
  - 9.2.6 Reutilización o retirada segura de equipos.
  - 9.2.7 Retirada de materiales propiedad de la empresa.

10. GESTIÓN DE COMUNICACIONES Y OPERACIONES.
- 10.1 Responsabilidades y procedimientos de operación.
  - 10.1.1 Documentación de los procedimientos de operación.
  - 10.1.2 Gestión de cambios.
  - 10.1.3 Segregación de tareas.
  - 10.1.4 Separación de los recursos de desarrollo, prueba y operación.
- 10.2 Gestión de la provisión de servicios por terceros.
  - 10.2.1 Provisión de servicios.
  - 10.2.2 Supervisión y revisión de los servicios prestados por terceros.
  - 10.2.3 Gestión del cambio en los servicios prestados por terceros.
- 10.3 Planificación y aceptación del sistema.
  - 10.3.1 Gestión de capacidades.
  - 10.3.2 Aceptación del sistema.
- 10.4 Protección contra el código malicioso y descargable.
  - 10.4.1 Controles contra el código malicioso.
  - 10.4.2 Controles contra el código descargado en el cliente.
- 10.5 Copias de seguridad.
  - 10.5.1 Copias de seguridad de la información.
- 10.6 Gestión de la seguridad de las redes.
  - 10.6.1 Controles de red.
  - 10.6.2 Seguridad de los servicios de red.
- 10.7 Manipulación de los soportes.
  - 10.7.1 Gestión de soportes extraíbles.
  - 10.7.2 Retirada de soportes.
  - 10.7.3 Procedimientos de manipulación de la información.
  - 10.7.4 Seguridad de la documentación del sistema.
- 10.8 Intercambio de información.
  - 10.8.1 Políticas y procedimientos de intercambio de información.
  - 10.8.2 Acuerdos de intercambio.
  - 10.8.3 Soportes físicos en tránsito.
  - 10.8.4 Mensajería electrónica.
  - 10.8.5 Sistemas de información empresariales.
- 10.9 Servicios de comercio electrónico.
  - 10.9.1 Comercio electrónico.
  - 10.9.2 Transacciones en línea.
  - 10.9.3 Información públicamente disponible.
- 10.10 Supervisión.
  - 10.10.1 Registros de auditoría.
  - 10.10.2 Supervisión del uso del sistema.
  - 10.10.3 Protección de la información de los registros.
  - 10.10.4 Registros de administración y operación.
  - 10.10.5 Registro de fallos.
  - 10.10.6 Sincronización del reloj.

11. CONTROL DE ACCESO.
- 11.1 Requisitos de negocio para el control de acceso.
  - 11.1.1 Política de control de acceso.
- 11.2 Gestión de acceso de usuario.
  - 11.2.1 Registro de usuario.
  - 11.2.2 Gestión de privilegios.
  - 11.2.3 Gestión de contraseñas de usuario.
  - 11.2.4 Revisión de los derechos de acceso de usuario.
- 11.3 Responsabilidades de usuario.
  - 11.3.1 Uso de contraseñas.
  - 11.3.2 Equipo de usuario desatendido.
  - 11.3.3 Política de puesto de trabajo despejado y pantalla limpia.
- 11.4 Control de acceso a la red.
  - 11.4.1 Política de uso de los servicios en red.
  - 11.4.2 Autenticación de usuario para conexiones externas.
  - 11.4.3 Identificación de los equipos en las redes.
  - 11.4.4 Protección de los puertos de diagnóstico y configuración remotos.
  - 11.4.5 Segregación de las redes.
  - 11.4.6 Control de la conexión a la red.
  - 11.4.7 Control de encaminamiento (routing) de red.
- 11.5 Control de acceso al sistema operativo.
  - 11.5.1 Procedimientos seguros de inicio de sesión.
  - 11.5.2 Identificación y autenticación de usuario.
  - 11.5.3 Sistema de gestión de contraseñas.
  - 11.5.4 Uso de los recursos del sistema.
  - 11.5.5 Desconexión automática de sesión.
  - 11.5.6 Limitación del tiempo de conexión.
- 11.6 Control de acceso a las aplicaciones y a la información.
  - 11.6.1 Restricción del acceso a la información.
  - 11.6.2 Aislamiento de sistemas sensibles.
- 11.7 Ordenadores portátiles y teletrabajo.
  - 11.7.1 Ordenadores portátiles y comunicaciones móviles.
  - 11.7.2 Teletrabajo.

12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN.
- 12.1 Requisitos de seguridad de los sistemas de información.
  - 12.1.1 Análisis y especificación de los requisitos de seguridad.
- 12.2 Tratamiento correcto de las aplicaciones.
  - 12.2.1 Validación de los datos de entrada.
  - 12.2.2 Control del procesamiento interno.
  - 12.2.3 Integridad de los mensajes.
  - 12.2.4 Validación de los datos de salida.
- 12.3 Controles criptográficos.
  - 12.3.1 Política de uso de los controles criptográficos.
  - 12.3.2 Gestión de claves.
- 12.4 Seguridad de los archivos de sistema.
  - 12.4.1 Control del software en explotación.
  - 12.4.2 Protección de los datos de prueba del sistema.
  - 12.4.3 Control de acceso al código fuente de los programas.
- 12.5 Seguridad en los procesos de desarrollo y soporte.
  - 12.5.1 Procedimientos de control de cambios.
  - 12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
  - 12.5.3 Restricciones a los cambios en los paquetes de software.
  - 12.5.4 Fugas de información.
  - 12.5.5 Externalización del desarrollo de software.
- 12.6 Gestión de la vulnerabilidad técnica.
  - 12.6.1 Control de las vulnerabilidades técnicas.

13. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
- 13.1 Notificación de eventos y puntos débiles de seguridad de la información.
  - 13.1.1 Notificación de los eventos de seguridad de la información.
  - 13.1.2 Notificación de puntos débiles de seguridad.
- 13.2 Gestión de incidentes y mejoras de seguridad de la información.
  - 13.2.1 Responsabilidades y procedimientos.
  - 13.2.2 Aprendizaje de los incidentes de seguridad de la información.
  - 13.2.3 Recopilación de evidencias.

14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
- 14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio.
  - 14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.
  - 14.1.2 Continuidad del negocio y evaluación de riesgos.
  - 14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información.
  - 14.1.4 Marco de referencia para la planificación de la cont. del negocio.
  - 14.1.5 Pruebas, mantenimiento y reevaluación de planes de continuidad.

15. CUMPLIMIENTO.
- 15.1 Cumplimiento de los requisitos legales.
  - 15.1.1 Identificación de la legislación aplicable.
  - 15.1.2 Derechos de propiedad intelectual (DPI).
  - 15.1.3 Protección de los documentos de la organización.
  - 15.1.4 Protección de datos y privacidad de la información de carácter personal.
  - 15.1.5 Prevención del uso indebido de recursos de tratamiento de la información.
  - 15.1.6 Regulación de los controles criptográficos.
- 15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico.
  - 15.2.1 Cumplimiento de las políticas y normas de seguridad.
  - 15.2.2 Comprobación del cumplimiento técnico.
- 15.3 Consideraciones sobre las auditorías de los sistem. de información.
  - 15.3.1 Controles de auditoría de los sistemas de información.
  - 15.3.2 Protección de las herramientas de auditoría de los sist. de inform.

Documento sólo para uso didáctico. La norma oficial debe adquirirse en entidades autorizadas para su venta

Ver. 4.0, 16-1-2011

Fuente: Controles ISO/IEC 27002:2005, ISO, [en línea], [consultado 09 de Noviembre, 2012]. Disponible en Internet: http://www.iso27000.es/download/ControlesISO27002-2005.pdf

6.2.2. Modelo PDCA ("Plan-Do-Check-Act"). El Sistema de Gestión de la Seguridad de la Información se basa en la continua monitorización y mejoramiento del sistema, para ello se basa en el modelo PDCA ("Plan-Do-Check-Act") o en español PHVA (Planear-Hacer-Verificar-Actuar). En cada una de las fases se realizan diferentes actividades, las cuales son:

En la fase denominada establecer el SGSI (PLANEAR) la norma da las pautas para determinar el alcance del modelo en la empresa, identificar los activos de información y tasarlos, luego hacer el análisis y la evaluación del riesgo y determinar que activos de información están sujetos a riesgo. Seguidamente, en esta fase, se deben determinar las opciones para el tratamiento del riesgo, se debe determinar el alcance que se desea y realizar un análisis y gestión de riesgos referente a los activos de información.

En la segunda fase denominada Implementar y operar el SGSI (HACER) "se debe elaborar el plan de tratamiento del riesgo, detallando las acciones que deben emprenderse para implantar las opciones de tratamiento del riesgo escogidas, se deben implantar las diferentes políticas y controles en la organización.

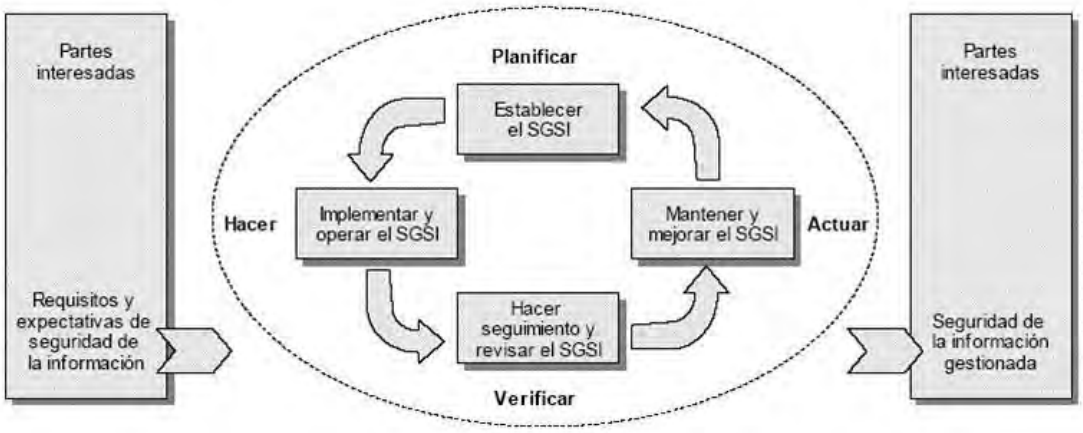
En la tercera fase denominada Hacer seguimiento y revisar el SGSI (VERIFICAR) "la empresa debe tener los procedimientos y rutinas establecidas para con ayuda de métrica, revisar el desempeño del SGSI", se deben verificar los diferentes controles implementados para así comprobar que son los suficientes y que están funcionando de manera correcta.

En la cuarta y última fase denominada mantener y mejorar el SGSI (ACTUAR) "se toman las acciones pertinentes para reaccionar a incidentes y tomar también las acciones preventivas de lugar"[13], se deben llevar a cabo labores de mejora y de corrección para garantizar la correcta gestión de la seguridad de la información[17].

En la figura 6 se ilustra las fases del modelo PHVA para un Sistema de Gestión de Seguridad de la Información.

17 ALEXANDER, Alberto. Diseño de un sistema de gestión de seguridad de información Optica ISO 27001:2005, Primera Edición, Bogota: Editorial Alfaomega, 2007, p. 22.

Figura 6. Modelo PHVA para los procesos del SGSI. NTC-ISO/IEC 27001



Fuente: La Norma ISO 27001 y La Gestión Documental fundamentales en la Implementación, AyC Ltda, Bogotá, 10 de enero de 2012, [en línea], [consultado 03 de Noviembre, 2012]. Disponible en Internet: http://www.aycltda.com.co/wp-content/uploads/2012/01/Modelo-PHVA-SGSI.jpg

6.3. RIESGOS

Una de las partes más importantes para establecer un SGSI es la relacionada con la gestión de riesgos, los riesgos según la ISO 73:2002 es la combinación de la probabilidad de un evento y sus consecuencias. En nuestro caso, los riesgos es la probabilidad de que una amenaza explote alguna vulnerabilidad de un activo de información y conlleve a la pérdida de la confidencialidad, integridad o disponibilidad del mismo.

6.3.1. Gestión de riesgos. La gestión de riesgos es la que va a permitir que estos sean conocidos, gestionados y asumidos por la organización, se define como: "…proceso que se encargar de identificar y cuantificar la probabilidad de que se produzcan amenazas y de establecer un nivel aceptable de riesgo para la organización, considerando el impacto potencial de un incidente no deseado"[18].

Para llevar a cabo el proceso de gestión de riesgos, la ISO 27001 estipula que se debe adoptar una metodología que va a permitir analizar los riesgos asociados a

18AREITIO, Javier. Seguridad de la información, redes, informática y sistemas de información, España: Editorial Paraninfo, 2008, p.7.

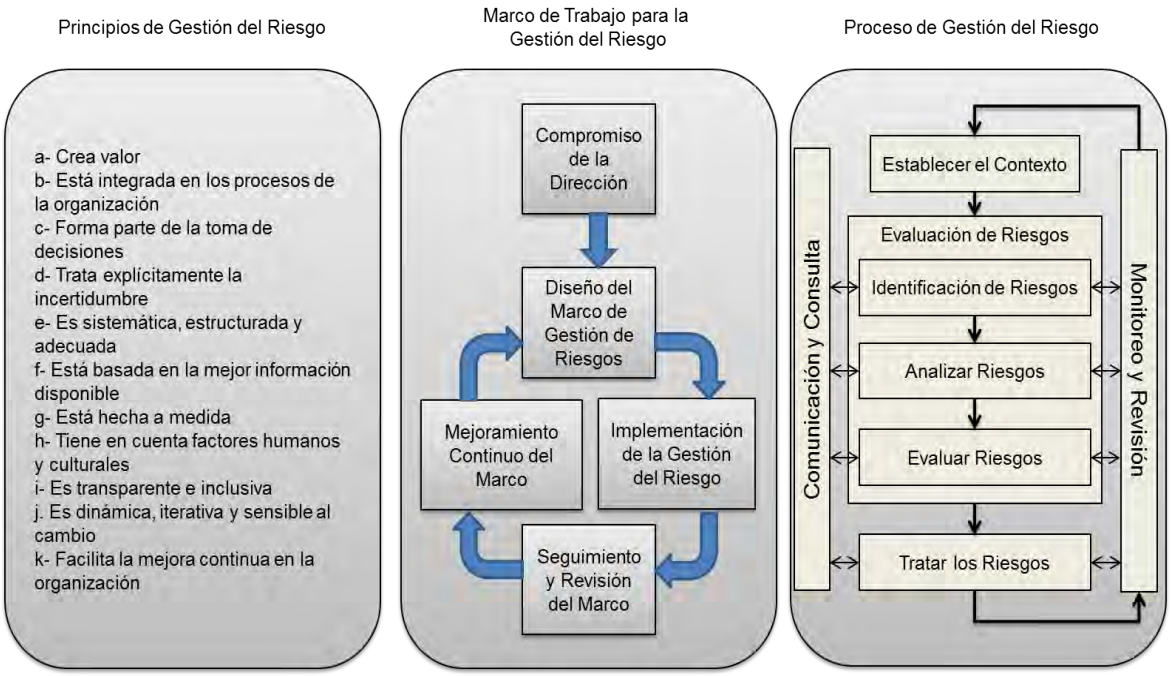
los activos de información y de esta manera brindarle a la dirección un nivel de riesgo aceptable y/o asumible.

Para este proyecto se decidió trabajar bajo la metodología ***MAGERIT***. (En el numeral "6.3.4. Metodología MAGERIT" se determina en qué consiste esta metodología planteada).

6.3.2. ISO 31000. La norma ISO 31000 está destinada para la gestión de riesgos, el propósito es proporcionar principios y directrices genéricas para los profesionales y las empresas que emplean procesos de gestión de riesgos.

En la Figura 7 se ilustra la estructura que propone la ISO 31000:

Figura 7. Estructura de gestión de riesgos – principios y directrices, ISO 31000



Fuente: Avantium business consulting, Gestión de riesgos (ISO 31000), 2011 [en línea], [consultado el 12 de Marzo, 2013]. Disponible en Internet: http://www.avantium.es/index.php/gestion-de-riesgos-iso-31000

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

- Los principios para la gestión de riesgos.
- Marco de trabajo para la gestión del riesgo.
- El proceso de gestión de riesgos.

Para una mayor eficacia, la gestión del riesgo en una organización debe tener en cuenta los siguientes principios:

- Crea valor. Contribuye a la consecución de objetivos así como la mejora de aspectos tales como la seguridad y salud laboral, cumplimiento legal y normativo, protección ambiental, etc.
- Está integrada en los procesos de una organización. No debe ser entendida como una actividad aislada sino como parte de las actividades y procesos principales de una organización.
- Forma parte de la toma de decisiones. La gestión del riesgo ayuda a la toma de decisiones evaluando la información sobre las distintas alternativas.
- Trata explícitamente la incertidumbre. La gestión del riesgo trata aquellos aspectos de la toma de decisiones que son inciertos, la naturaleza de esa incertidumbre y como puede tratarse.
- Es sistemática, estructurada y adecuada. Contribuye a la eficiencia y, consecuentemente, a la obtención de resultados fiables.
- Está basada en la mejor información disponible. Los inputs del proceso de gestión del riesgo están basados en fuentes de información como la experiencia, la observación, las previsiones y la opinión de expertos.
- Está hecha a medida. La gestión del riesgo está alineada con el contexto externo e interno de la organización y con su perfil de riesgo.
- Tiene en cuenta factores humanos y culturales. Reconoce la capacidad, percepción e intenciones de la gente, tanto externa como interna, que puede facilitar o dificultar la consecución de los objetivos de la organización.
- Es transparente e inclusiva. La apropiada y oportuna participación de los grupos de interés (stakeholders) y, en particular, de los responsables a todos los niveles, asegura que la gestión del riesgo permanece relevante y actualizada.
- Es dinámica, iterativa y sensible al cambio. La organización debe velar para que la gestión del riesgo detecte y responda a los cambios de la empresa.

- Facilita la mejora continua de la organización. Las organizaciones deberían desarrollar e implementar estrategias para mejorar continuamente, tanto en la gestión del riesgo como en cualquier otro aspecto de la organización.

El diseño e implantación de un modelo de gestión del riesgo, permitirá a la organización:

- Fomentar la gestión proactiva en lugar de la reactiva.
- Ser consciente de la necesidad de identificar y tratar el riesgo en todos los niveles de la organización.
- Mejorar la identificación de oportunidades y amenazas.
- Cumplir con los requisitos legales y normativos aplicables así como las normas internacionales.
- Mejorar la información financiera.
- Mejorar la gestión empresarial.
- Mejorar la confianza de los grupos de interés (stakeholders).
- Establecer una base fiable para la toma de decisiones y planificación.
- Mejorar los controles.
- Repartir y utilizar de forma efectiva los recursos para la gestión de riesgos.
- Mejorar la eficacia y la eficiencia operacional.
- Aumentar la seguridad y salud.
- Mejorar la prevención así como la gestión de incidentes.
- Minimizar las pérdidas.
- Mejorar el aprendizaje organizativo.
- Mejorar la resistencia organizativa." [19]

19 Avantium business consulting, Gestión de riesgos (ISO 31000), 2011 [en línea], [consultado el 12 de Marzo, 2013]. Disponible en Internet: http://www.avantium.es/index.php/gestion-de-riesgos-iso-31000

6.3.3. ISO 27005. La norma ISO/IEC 27005 propone una guía para la gestión de los riesgos de seguridad de la información, basándose en los principios definidos en las diferentes normas de la serie 27000. La norma ISO 27005 es aplicable en todo tipo de organización y no proporciona o recomienda una metodología específica.

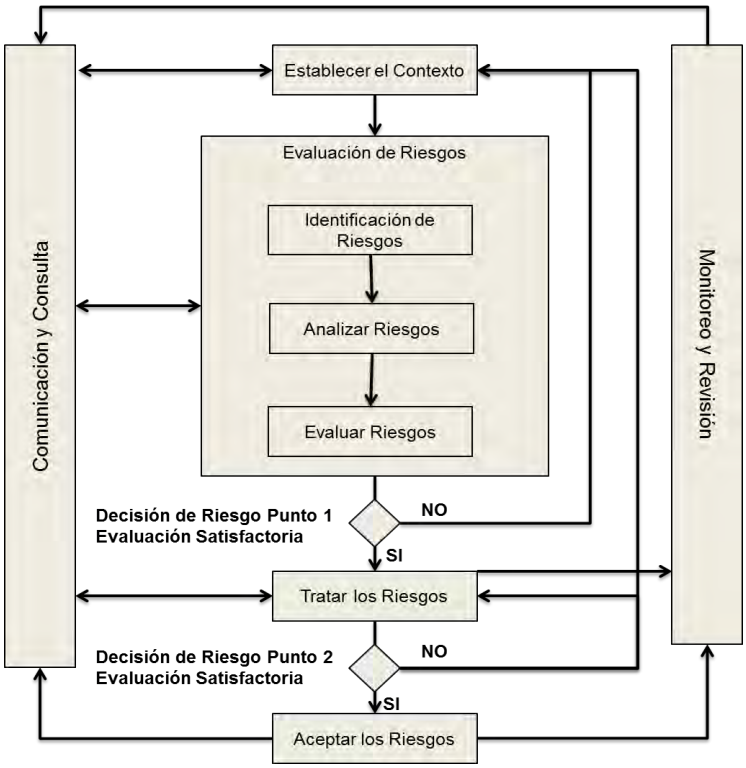
Las secciones de contenido son:

- Prefacio
- Introducción
- Referencias normativas
- Términos y definiciones
- Estructura
- Fondo
- Descripción del proceso de ISRM
- Establecimiento del contexto
- Seguridad de la Información - Evaluación de riesgos (ISRA)
- Seguridad de la Información - Tratamiento de riesgos
- Seguridad de la información - Aceptación del riesgo
- Seguridad de la información - Comunicación de riesgos
- Seguridad de la información - Seguimiento del riesgo y revisión
- Anexo A: Definición del alcance del proceso
- Anexo B: Valoración de activos y evaluación de impacto
- Anexo C: Ejemplos de amenazas típicas
- Anexo D: Vulnerabilidades y métodos de evaluación de la vulnerabilidad
- Anexo E: Enfoques ISRA [20].

20 The ISO 27000 Directory, Introduction To ISO 27005 (ISO27005), 2008 [en línea], [consultado el 12, Marzo, 2013]. Disponible en Internet: http://www.27000.org/iso-27005.htm

En la siguiente figura 8 se ilustra la estructura y las fases que propone la ISO/IEC 27005:

Figura 8. Guía de análisis y gestión de riesgos, ISO 27005



Fuente: CORREA, Ricardo, CALDANA, Daniella, LOBOS, Carlos, OLEA, Leonardo, Serie de normas ISO 27000 e ISO 31000: Implicancias para el auditor interno gubernamental, ISO, Montevideo – Uruguay, 2011, [en línea], [consultado 12 de Marzo, 2013]. Disponible en Internet:http://www.iuai.org.uy/iuai/documentos/noticias/Ricardo%20Correa%20ISO%2027000%20Y%2031000.pdf

- Establecer el contexto: Lo primero que se debe tener claro es a dónde se quiere llegar y que se puede llegar a tolerar, por lo tanto se establecer el alcance y los objetivos.

- Evaluación de riesgos: El proceso de evaluar riesgos consta de dos partes bien diferenciadas. En la primera se analiza el riesgo al que se está sujeto. Mientras que en la segunda se priorizaran los riesgos para saber a qué se debe prestar más atención y destinar el mayor número de recursos.

- Identificación de Riesgos: Identificar las posibles amenazas, vulnerabilidades y sus posibles consecuencias (impacto).

- Analizar Riesgos: Basándose en las posibles consecuencias y su probabilidad de ocurrencia, se estima cuál es el nivel de riesgo al que se encuentra expuesta la organización.

- Evaluar Riesgos: Se decide en base a los criterios establecidos en el establecimiento del contexto, qué riesgos son más importantes.

- Tratamiento del Riesgo: Se determina que tratamiento se le va a dar al riesgo (mitigar, evitar, transferir, aceptar).

- Aceptación del Riesgo: ¿Son aceptables los riesgos residuales propuestos?

- Comunicación y consulta: Este proceso es continuo y busca mantener informado a las partes interesadas.

- Monitoreo y revisión: En este proceso se verifican que los tratamientos de riesgos propuestos estén cumpliendo su objetivo[21].

6.3.4. Metodología MAGERIT. MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, como respuesta a la percepción de que la Administración, y, en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión.

La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de las tecnologías de la información, que supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza.

MAGERIT interesa a todos aquellos que trabajan con información digital y sistemas informáticos, si dicha información, o los servicios que se prestan gracias a ella, son valiosos, MAGERIT les permitirá saber cuánto valor está en juego y les ayudará a protegerlo; conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos.

Con MAGERIT se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista[22].

21 HERNANDEZ RUIZ, Miguel Ángel, Pinceladas sobre ISO 27005, 4 Octubre 2010, [en línea], [consultado 12 de Marzo, 2013]. Disponible en Internet: http://www.27000.org/iso-27005.htm

6.3.4.1. Objetivos de la metodología MAGERIT. MAGERIT establece los siguientes objetivos:

- Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos
- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)
- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control
- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso[23].

6.3.4.2. Elementos de MAGERIT. Los elementos más significativos en la metodología MAGERIT para el estudio de la Seguridad en Sistemas de Información son los siguientes:

- Activos: recursos del sistema de información o relacionados con éste, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por la dirección.
- Amenazas: eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.
- Vulnerabilidad de un activo: potencialidad o posibilidad de ocurrencia de la materialización de una amenaza sobre dicho activo.
- Impacto en un activo: consecuencia sobre éste de la materialización de una amenaza.
- Riesgo: posibilidad de que se produzca un impacto determinado en un activo, en un dominio o en toda la organización.

---

22 ESPAÑA. MAGERIT versión 3, Portal de Administración Electrónica, [en línea], [consultado 09 de Noviembre, 2012]. Disponible en Internet: http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_General&langPae=es&iniciativa=184

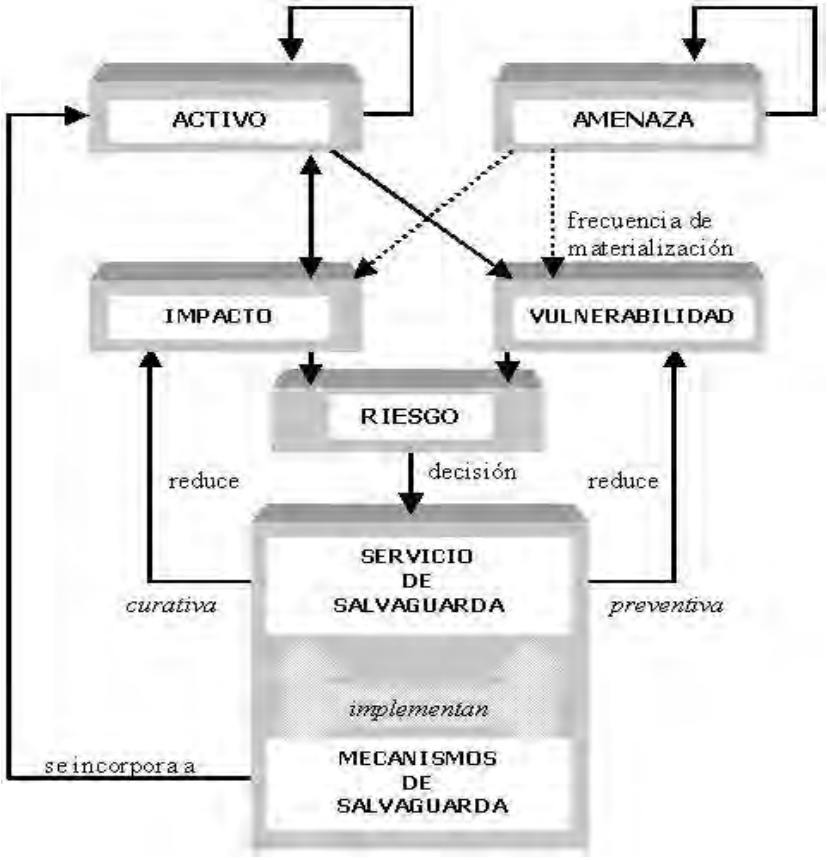
23 Ibíd., Disponible en internet: http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_General&langPae=es&iniciativa=184

- Servicio de salvaguarda: acción que reduce el riesgo.

- Mecanismo de salvaguarda: procedimiento, dispositivo, físico o lógico, que reduce el riesgo[24].

En la figura 9 se muestra la interrelación con los diferentes elementos anteriormente nombrados:

Figura 9. Descripción del proceso de análisis y gestión de riesgos



24 CAO, Javier, Análisis y gestión de riesgos de la seguridad de los sistemas de la información, InforMAS - Revista de Ingeniería Informática del Colegio de Ingenieros en Informática de la Región de Murcia, España, 7 de Marzo de 2005, [en línea], [consultado 10 de Noviembre, 2012]. Disponible en Internet: http://www.ciimurcia.es/informas/abr05/articulos/Analisis_gestion_riesgos_seguridad_sistemas_informacion.php

Fuente: CAO, Javier, Análisis y gestión de riesgos de la seguridad de los sistemas de la información, InforMAS - Revista de Ingeniería Informática del Colegio de Ingenieros en Informática de la Región de Murcia, España, 7 de Marzo de 2005, [en línea], [consultado 10 de Noviembre, 2012]. Disponible en Internet: http://www.ciimurcia.es/informas/abr05/articulos/Analisis_gestion_riesgos_seguridad_sistemas_informacion.php

6.3.4.3. Etapas para el proceso de análisis y gestión de riesgos con la metodología MAGERIT. En los procesos de análisis y gestión de riesgos de la seguridad en los sistemas de información la metodología MAGERIT se contemplan las siguientes fases:

- Planificación: En esta etapa se debe establecer el objetivo del proyecto, el dominio de estudio, las restricciones generales y además definir las métricas para valorar los diferentes elementos de seguridad.

- Análisis de riesgos: En esta etapa se realizan una serie de entrevistas al personal de la organización para poder identificar los activos con sus amenazas y vulnerabilidades, además se cuantifica el impacto en caso de que una amenaza se materialice.

- Gestión de riesgos: En esta etapa se procede a la interpretación del riesgo, se identifican los puntos débiles y los mecanismos de salvaguarda que están actualmente implantados, además se analiza cuales salvaguardas podrían llegar a implantarse para disminuir los niveles del riesgo a los valores deseados.

- Selección de mecanismos de salvaguarda: En esta etapa se procede a analizar todos los resultados anteriormente obtenidos y se establece un plan para la implantación de los salvaguardas[25].

6.4. MICROSOFT SECURITY ASSESSMENT TOOL – MSAT.

La Herramienta de Evaluación de Seguridad de Microsoft - MSAT está diseñada para identificar y abordar los riesgos de seguridad de un entorno informático. La herramienta utiliza un enfoque integral para medir el nivel de seguridad y cubre aspectos tales como usuarios, procesos y tecnología. Sus conclusiones incluyen orientaciones y recomendaciones para mitigar los

25 MASSELLI, Carlos, CAVALLER, Daniel, "Seguridad, estandarización, objetivos de control y su cuantificación económica para el sistema transaccional de gestión presupuestaria GEPRE – UNCuyo, en el marco de la gestión de calidad", [en línea], [consultado el 10 de Noviembre, 2012]. Disponible en Internet: http://bdigital.uncu.edu.ar/objetos_digitales/693/Masselli_seguridad.pdf

esfuerzos además de enlaces a información adicional sobre cuestiones propias del sector.

La evaluación se compone de 200 preguntas distribuidas en cuatro categorías:

- Infraestructura
- Aplicaciones
- Operaciones
- Usuarios

Las preguntas que conforman el cuestionario de la herramienta y las respuestas asociadas se derivan de las prácticas recomendadas de seguridad más comúnmente aceptadas, tanto de manera general como específica.

El siguiente cuadro 4 especifica las áreas incluidas dentro de la evaluación de riesgos de seguridad:

Cuadro 4. Cuadro de áreas incluidas dentro de la evaluación de riesgos de seguridad – MSAT.

Infraestructura	Importancia para la seguridad
Defensa perimetral	La defensa perimetral se centra en la seguridad de los límites de la red, ahí donde la red interna conecta con el mundo exterior. Constituye la primera línea de defensa contra los intrusos.
Autentificación	Unos procesos rigurosos en la autentificación de usuarios, administradores y usuarios remotos pueden ayudar a prevenir que alguien ajeno a la red obtenga acceso no autorizado a ella a través de ataques locales o remotos.
Gestión y monitorización	La gestión, monitorización y recogida de datos adecuada son críticas para el mantenimiento y análisis de entornos tecnológicos. Estas herramientas son incluso más importantes si se ha producido un ataque y se requiere un análisis del incidente.
Estaciones de trabajo	La seguridad de las estaciones de trabajo individuales es un factor clave en la defensa de cualquier entorno, especialmente si se permite el acceso remoto. Las estaciones de trabajo deberían disponer de protección para resistir un ataque común.

Cuadro 4 (Continuación)

Aplicaciones	Importancia para la seguridad
Implementación y uso	Cuando las aplicaciones de negocio críticas se encuentran implementadas en producción, se debe proteger la seguridad y disponibilidad de dichas aplicaciones y de los servidores que las alojan. Es esencial un mantenimiento continúo que asegure que se resuelvan los problemas de seguridad y que no se producen nuevas vulnerabilidades en el entorno.
Diseño de aplicaciones	Un diseño que no cumple adecuadamente los mecanismos de autentificación, autorización y validación de datos puede permitir que un atacante aproveche una vulnerabilidad de seguridad y obtenga acceso a información confidencial.
Aplicaciones	**Importancia para la seguridad**
Diseño de aplicaciones	Las metodologías de desarrollo de aplicaciones seguras son clave para cerciorarse de que tanto las aplicaciones desarrolladas internamente como las desarrolladas por terceros cumplen los modelos de seguridad y no dejan a la empresa abierta a posibles ataques.
	La integridad y la confidencialidad de los datos son dos de las grandes preocupaciones de cualquier empresa. La pérdida o robo de datos puede influir negativamente en sus beneficios y reputación. Es importante comprender cómo las aplicaciones gestionan los datos críticos y cómo esos datos son protegidos
Operaciones	**Importancia para la seguridad**
Entorno	La seguridad de una organización depende de las operaciones, procesos y directrices que se aplican en su entorno. Permiten acentuar la seguridad siempre que incluyan algo más que las propias defensas tecnológicas. Es indispensable disponer de una documentación precisa del entorno para que el equipo de operaciones sepa cómo gestionarlo y mantenerlo.
Política de seguridad	La política de seguridad corporativa se refiere al conjunto de políticas y directrices individuales existentes que permiten dirigir la seguridad y el uso adecuado de tecnología y procesos dentro de la organización. Esta área cubre políticas de seguridad de todo tipo, como las destinadas a usuarios, sistemas o datos.

Cuadro 4 (Continuación)

Operaciones	Importancia para la seguridad
Copias de seguridad y recuperación	Las copias de seguridad y recuperación de datos son esenciales para asegurar la continuidad del negocio en caso de que ocurra un desastre o un fallo de hardware o software. No disponer de ellas puede suponer una pérdida significativa de datos y productividad. La reputación de la compañía y de la marca podría ser puesta en entredicho.
Gestión de actualizaciones	Una buena gestión de actualizaciones es importante para la seguridad del entorno tecnológico de la organización. Es necesario llevar a cabo actualizaciones periódicas y programadas para evitar que alguien aproveche vulnerabilidades conocidas.
Usuarios	**Importancia para la seguridad**
Requisitos y evaluación	Los requisitos de seguridad deberían ser entendidos por todas las personas con capacidad de decisión, ya sea en cuestiones de negocio como en cuestiones técnicas, de forma que tanto unos como otros contribuyan a mejorar la seguridad en lugar de pelearse con ella. Llevar a cabo regularmente una evaluación por parte de terceras partes puede ayudar a la compañía a revisar, evaluar e identificar las áreas que necesitan mejorar.
Políticas y procedimientos	Disponer de unos procedimientos claros y prácticos en la gestión de relaciones con vendors o partners puede evitar que la compañía se exponga a posibles riesgos. Si se aplican también estos procedimientos en los procesos de contratación y terminación de contrato de empleados se puede proteger a la empresa de posibles empleados poco escrupulosos o descontentos.
Formación y concienciación	Los empleados deberían recibir formación y ser conscientes de las políticas de seguridad existentes y de cómo la aplicación de esas políticas puede ayudarles en sus actividades diarias. De esta forma no expondrán inadvertidamente a la compañía a posibles riesgos.

Fuente: MICROSOFT, Herramienta de evaluación de seguridad Microsoft (MSAT), [en línea], [consultado 12 de Marzo, 2013]. Disponible en Internet: http://technet.microsoft.com/es-es/library/cc185712.aspx

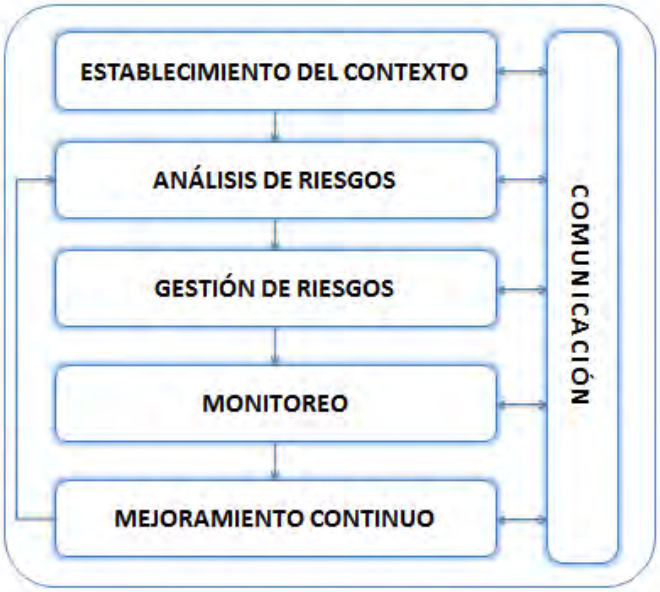
MSAT proporciona:

- Un conocimiento constante, completo y fácil de utilizar del nivel de seguridad.
- Un marco de defensa en profundidad con análisis comparativos del sector.
- Informes detallados y actuales comparando su plan inicial con los progresos obtenidos.
- Recomendaciones comprobadas y actividades prioritarias para mejorar la seguridad.
- Consejos estructurados de Microsoft y de la industria[26].

26 MICROSOFT, Herramienta de evaluación de seguridad Microsoft (MSAT), [en línea], [consultado 12 de Marzo, 2013]. Disponible en Internet: http://technet.microsoft.com/es-es/library/cc185712.aspx

7. DESARROLLO DEL PROYECTO

Figura 10. Guía de desarrollo metodológico



Teniendo en cuenta que un proceso es una secuencia de procedimientos interrelacionados y ordenados que permiten la consecución de un objetivo determinado, se propone un marco de trabajo orientado a procesos que sea fácil de entender, se le dé continuidad y permita cubrir la necesidad identificada en la organización. Además, la organización cuenta con un mapa de procesos, lo ideal es que este modelo planteado se ingrese a dicho mapa como un nuevo proceso y de esta manera se le dé continuidad a la gestión de la seguridad informática dentro de la organización.

El marco de trabajo cuenta con seis procesos en los cuales se llevan a cabo una serie de tareas para el cumplimiento del mismo. Inicia con el establecimiento del contexto, seguido del análisis de riesgos, la gestión de riesgos, el monitoreo, el mejoramiento continuo y por ultimo un proceso que se lleva a cabo en todas las instancias denominado la comunicación.

Debido a que se plantea el mejoramiento continuo el modelo está ajustado a seguir un ciclo, se pueden generar variedad de iteraciones siempre y cuando el contexto que se está manejando no manifieste cambios relevantes, en la figura 10 se puede observar gráficamente.

En cada una de las tareas se proponen una serie de herramientas que pueden ser tenidas en cuenta o ajustadas de acuerdo a la necesidad que se presente y así optimizar el desarrollo de las mismas.

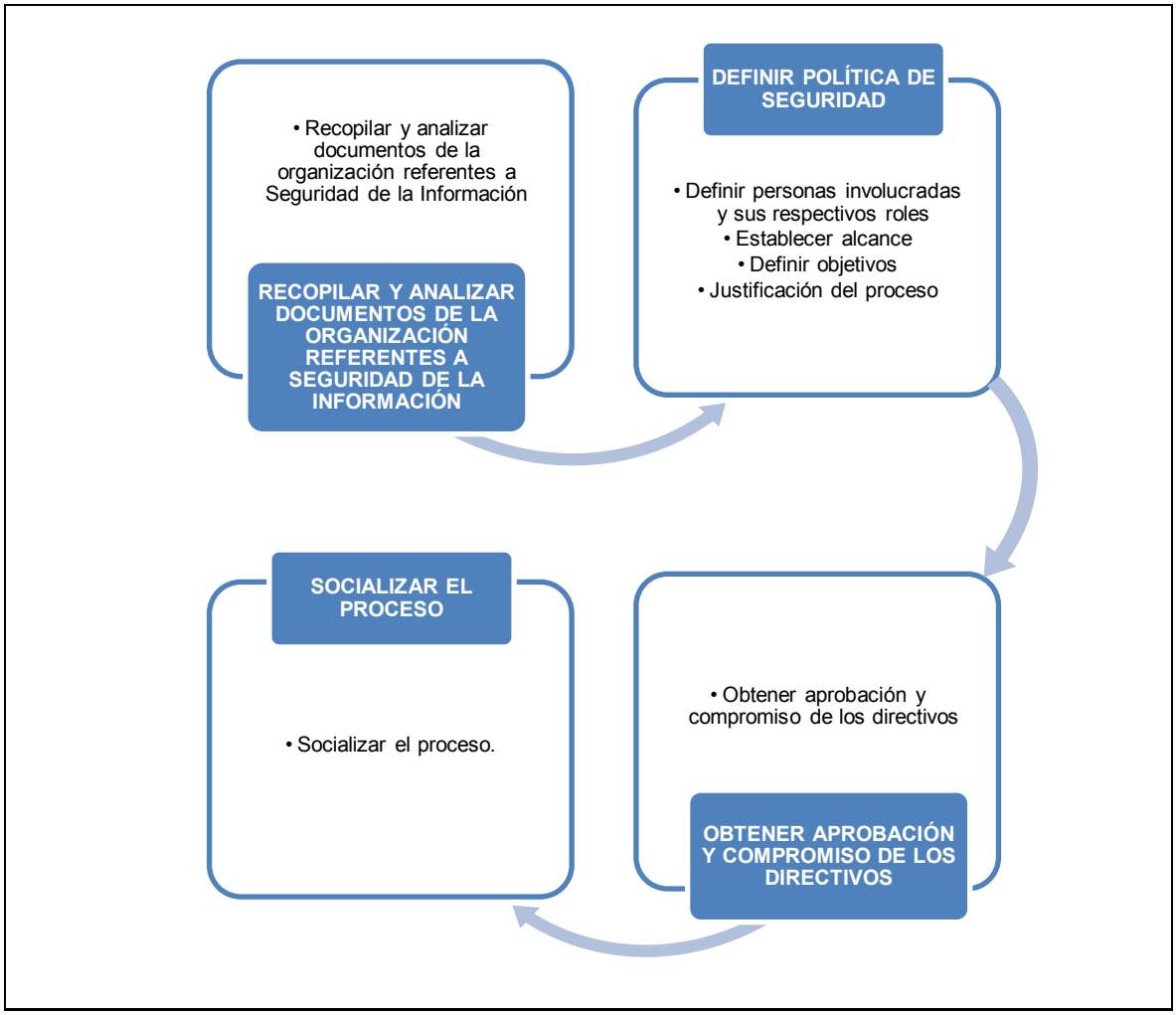
- Las tareas se identifican con “T.#”, donde “T” hace referencia a Tarea y “#” es el número de la tarea

7.1. ESTABLECIMIENTO DEL CONTEXTO (T.1)

En esta fase se analiza la situación actual desde el punto de vista de la seguridad para hacerse una idea de lo que se tiene en el momento, se plantea el alcance, los objetivos, la justificación del proceso que se va a realizar, las personas que van a estar involucradas en cada una de las fases y por ultimo busca obtener la aprobación de la alta gerencia para luego ser socializado con todos los funcionarios de la organización.

En el establecimiento del contexto se detallan las siguientes tareas:

Figura 11. Guía de establecimiento del contexto



7.1.1. Recopilar y analizar documentos de la organización referentes a seguridad de la información (T.1.1). En esta tarea se recopilan todos los documentos en los que se ve involucrada de alguna manera la seguridad de la información dentro de la organización.

Una vez reunida toda la información relevante, se analiza para observar que aspectos contempla de manera correcta, cuales se pueden mejorar y los que definitivamente requieren un cambio inmediato, esto se realiza con el fin de tenerlos en cuenta en el proceso que se va a dar inicio.
Si la organización no cuenta con nada establecido referente a la seguridad de la información se procede a la siguiente tarea.

Cuadro 5. Cuadro descriptivo de la tarea T.1.1

Tareas	• T.1.1. Recopilar y analizar documentos de la organización referentes a seguridad de la información.
Objetivo	• Analizar la situación actual de la organización frente al tema de seguridad de la información.
Responsable	• Funcionarios de la organización
Entradas	• Documentos relacionados con seguridad de la información
Salidas	• Conocimiento y análisis de la situación actual de la organización

7.1.2. Definir política de seguridad (T.1.2). En esta tarea se establece de manera clara las líneas generales que la organización desea seguir en aspectos de seguridad de acuerdo al contexto dado por la misión, visión, objetivos y estrategias de la organización.

Se deben definir los siguientes aspectos:

- ✓ **Definir personas involucradas y sus respectivos roles (T.1.2.1):** se debe definir un líder o director de seguridad que conozca los diferentes aspectos que se van a llevar a cabo en el proceso, el será el encargado de coordinar las tareas a realizar y además de poner en consideración posibles sugerencias de los funcionarios de la organización. También es necesario designar un comité de seguridad encargado de buscar soluciones y brindar apoyo a las decisiones que se tomen frente a los temas de seguridad, por lo general son personas del área de infraestructura, soporte, servicios generales, etc.

- ✓ **Establecer alcance (T.1.2.2):** permitirá identificar que se va a proteger en la organización.

- ✓ **Definir Objetivos (T.1.2.3):** especifica lo que se quiere lograr con el proceso.

- ✓ **Justificación del proceso (T.1.2.4):** se debe plasmar lo que se va hacer, como se va hacer y la importancia de llevar a cabo el proceso.

Cuadro 6. Cuadro descriptivo de las tareas T.1.2.1, T.1.2.2, T.1.2.3, T.1.2.4

Tareas	• T.1.2.1. Definir personas involucradas y sus respectivos roles • T.1.2.2. Establecer alcance • T.1.2.3. Definir Objetivos • T.1.2.4. Justificación del proceso
Objetivo	• Definir el alcance, objetivos, personas involucradas y justificación del proceso, para tener claro las líneas generales que la organización desea seguir en el ámbito de la seguridad.
Responsable	• Funcionario encargado del proyecto
Entradas	• Documentación pertinente de la organización (visión, misión, objetivos, etc.…)
Salidas	• Definición de roles • Especificaciones generales del proyecto • Registro de la Plantilla 01: Establecimiento del contexto

❖ **Herramienta:** En esta tarea se propone la Plantilla 01: Establecimiento del contexto, para llevar el registro de la política de seguridad.

7.1.3. Obtener aprobación y compromiso de los directivos (T.1.3). En esta tarea se debe obtener la aprobación de los directivos de la organización, exponiéndoles la política de seguridad (los objetivos, alcance, personas involucradas y justificación del proceso) anteriormente establecida, esto se realiza con el fin de contar con el apoyo en caso de necesitar diferente recursos para poder afrontar los riesgos de manera adecuada y además de contar con el respaldo de la alta gerencia para las diferentes actividades que se tienen que realizar más adelante.

En esta tarea también se tienen en cuenta posibles sugerencias de la alta gerencia y en caso de tener que ajustar algún aspecto de la política de seguridad, se procede a su revisión y se presenta de nuevo a los directivos involucrados.

Cuadro 7. Cuadro descriptivo de la tarea T.1.3

Tareas	• T.1.3. Obtener aprobación y compromiso de los directivos
Objetivo	• Obtener el compromiso de los directivos de la organización para proceso que se va a llevar a cabo.
Responsable	• Director de seguridad
Entradas	• Registro de la Plantilla 01: Establecimiento del contexto
Salidas	• Aprobación del proyecto por parte de la alta gerencia • Registro de aprobación de la Plantilla 01: Establecimiento del contexto

❖ **Herramienta:** En esta tarea se propone la Plantilla 01: Establecimiento del contexto, para registrar de la aprobación de la alta gerencia.

7.1.4. Socializar el proceso (T.1.4). Una vez obtenida la aprobación por parte de los directivos de la gerencia, se procede a comunicar a los diferentes funcionarios los aspectos que se plantearon en la política de seguridad, esta tarea se realiza con el fin de concientizar a las diferentes personas involucradas y para invitarlas a que participen con sugerencias que permitan reducir los riesgos de la organización frente al tema de seguridad de la información.

La tarea de socialización se puede llevar a cabo mediante reuniones, circulares o los diferentes medios de comunicación presentes en la organización.

Cuadro 8. Cuadro descriptivo de la tarea T.1.4

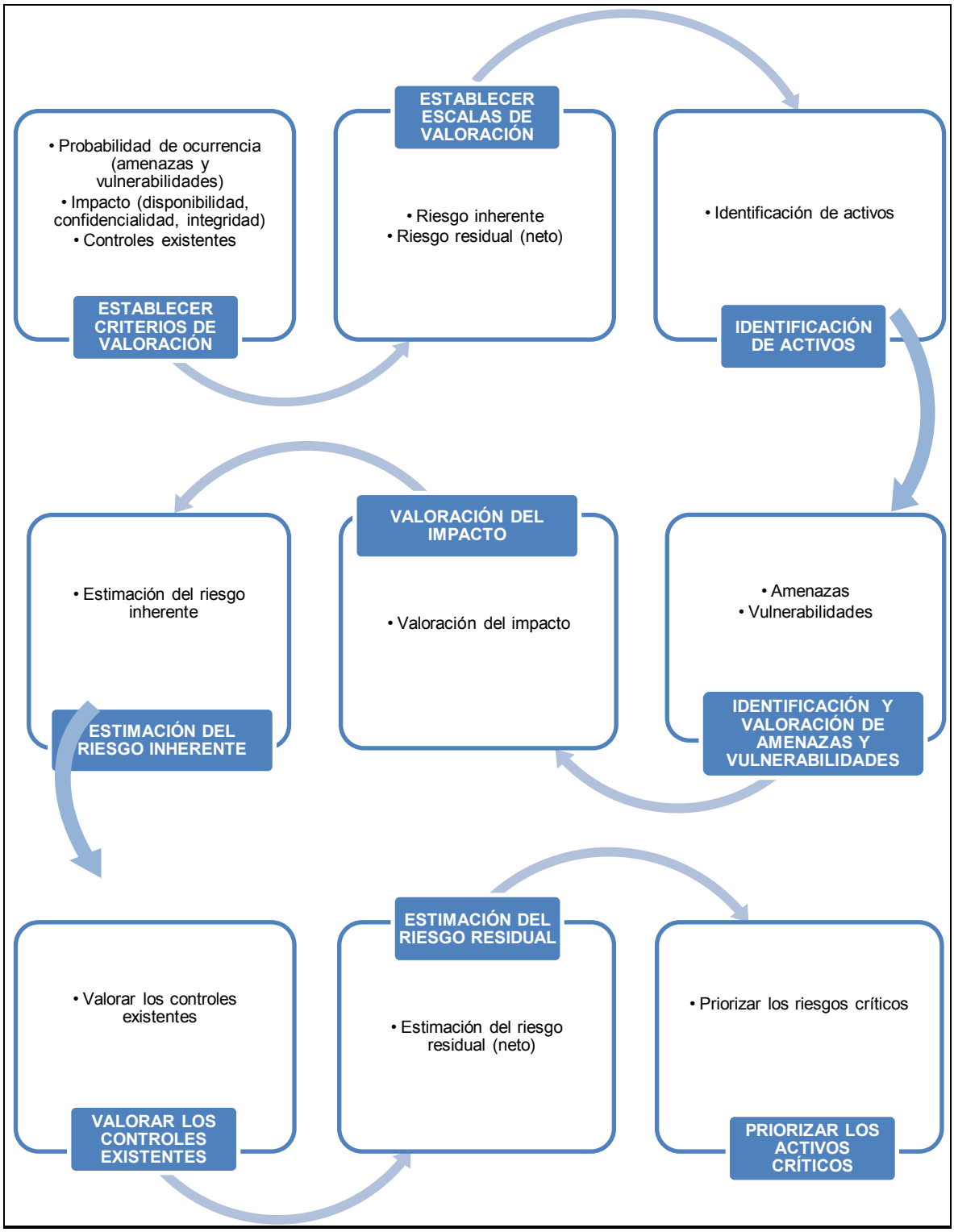
Tareas	• T.1.4. Socializar el proceso
Objetivo	• Comunicar, concienciar y explicar a los diferentes funcionarios de la organización el proceso que se va a llevar a cabo.
Responsable	• Director de seguridad • Comité de seguridad
Entradas	• Registro de la Plantilla 01: Establecimiento del contexto
Salidas	• Los funcionarios adquieren con conocimientos generales sobre el proyecto que se va a realizar.

7.2. ANÁLISIS DE RIESGOS (T.2)

En esta fase se establecen todos los criterios de valoración que se van a tener en cuenta en el proceso, se recopilan los activos de información y luego se procede a su respectiva valoración teniendo en cuenta amenazas, vulnerabilidades, impacto y controles asociados. Este proceso es necesario ya que todos los activos de información no tienen el mismo valor, ni están expuestos a los mismos riesgos. Al final del análisis se priorizan los riesgos más críticos que enfrenta la organización.

En el análisis de riesgos se detallan las siguientes tareas:

Figura 12. Guía de análisis de riesgos



7.2.1. Establecer criterios de valoración (T.2.1). En esta tarea el líder y el comita de seguridad establecen los criterios de valoración, los cuales van a permitir identificar la importancia de cada uno de los activos a evaluar.

Se deben establecer criterios de valoración para:

- ✓ **Probabilidad de ocurrencia (amenazas y vulnerabilidades) (T.2.1.1):** considera la existencia de una amenaza, la cual pueda llegar a explotar una determinada vulnerabilidad de la organización. En este caso es necesario establecer dos criterios de valoración, el primero para medir la probabilidad de ocurra una amenaza y el segundo para medir la probabilidad de que se explote una vulnerabilidad.

- ✓ **Impacto (disponibilidad, confidencialidad, integridad) (T2.1.2):** considera cual puede ser el daño causado a la organización en caso de que un activo se vea comprometido. En este caso es necesario establecer tres criterios de valoración, el primero que permitirá identificar el daño causado en cuanto a la confidencialidad, el segundo a la integridad y por último la disponibilidad.

- ✓ **Controles existentes (T.2.1.3):** considera que tan efectivos son los controles que se están utilizando. En este caso es necesario establecer un criterio de valoración que permita identificar si existe un control y si este cumple su función correctamente.

Cuadro 9. Cuadro descriptivo de las tareasT.2.1.1, T.2.1.2, T.2.1.3

Tareas	• T.2.1.1. Probabilidad de ocurrencia (amenazas y vulnerabilidades) • T.2.1.2. Impacto (disponibilidad, confidencialidad, integridad) • T.2.1.3. Controles existentes
Objetivo	• Definir criterios de valoración que permitan analizar la probabilidad de ocurrencia, el impacto y los controles existentes, frente a los riesgos de la organización.
Responsable	• Director de seguridad • Comité de seguridad
Entradas	• Documentación generada en la tarea T.1.2.Definir política de seguridad
Salidas	• Criterios de valoración de probabilidad de ocurrencia, impacto y controles.

❖ **Herramienta:** En esta tarea se propone los cuadros de criterios de valoración (Cuadro 29. Cuadro de criterios de valoración de una amenaza , Cuadro 30. Cuadro de criterios de valoración de una vulnerabilidad, Cuadro 31. Cuadro de criterios de valoración de confidencialidad, Cuadro 32. Cuadro de criterios de valoración de integridad, Cuadro 33. Cuadro de criterios de valoración de disponibilidad, Cuadro34. Cuadro de criterios de valoración de un control), en ellas se encuentra registrados los criterios de valoración anteriormente nombrados, basándose en un enfoque semicuantitativo.

7.2.2. Establecer escalas de valoración (T.2.2). En esta tarea el líder y el comité de seguridad establecen las escalas de valoración, las cuales van a permitir identificar cual es la respuesta que se le debe dar al riesgo que se está evaluando.

Se deben establecer dos escalas de valoración para:

✓ **Riesgo inherente (T.2.2.1):** identifica la valoración del riesgo existente en la organización antes de tomar acciones o establecer controles que permitan a la organización reducir su probabilidad de ocurrencia.

✓ **Riesgo residual (neto) (T.2.2.2):** identifica la valoración del riesgo existente en la organización después de que se han tomado acciones o establecido controles que permiten a la organización reducir su probabilidad de ocurrencia.

El rango de las escalas de valoración debe ser acorde a los criterios de evaluación anteriormente establecidos en la tarea T.2.1. Establecer criterios de valoración.

Cuadro 10. Cuadro descriptivo de las tareas T.2.2.1, T.2.2.2

Tareas	• T.2.2.1. Riesgo inherente • T.2.2.2.Riesgo residual (neto)
Objetivo	• Definir escalas de valoración de riesgo inherente y riesgo residual, para identificar la respuesta adecuada al riesgo.
Responsable	• Director de seguridad • Comité de seguridad
Entradas	• Criterios de valoración planteados en la tarea T.2.1. Establecer criterios de valoración.
Salidas	• Escalas de valoración del riesgo inherente y riesgo residual

- **Herramienta:** En esta tarea se propone los cuadros de escalas de riesgos (Cuadro 35. Cuadro de la escala de riesgo inherente, Cuadro 36. Cuadro de la escala de riesgo residual), en ella se encuentran registradas las escalas de valoración correspondientes.

7.2.3. Identificación de activos (T.2.3). En esta tarea el director de seguridad y el comité de seguridad, se reúnen con las personas encargadas de los activos de información de la organización, para obtener un listado con una serie de características específicas de cada activo identificado, se debe tener en cuenta el alcance.

Cuadro 11. **Cuadro descriptivo de la tarea T.2.3**

Tareas	• T.2.3. Identificación de activos
Objetivo	• Definir un listado de activos de información de la organización sobre los cuales se va a llevar el proceso.
Responsable	• Director de seguridad • Comité de seguridad
Entradas	• Documentación generada en la tarea T.1.2.Definir política de seguridad
Salidas	• Listado de características específicas de los activos de información. • Registro de la Plantilla 02: Identificación de activos

- **Herramienta:** En esta tarea se propone la Plantilla 02: Identificación de activos, en ella se llevara a cabo el registro de cada uno de los activos de información identificados, como base se plantean una serie de activos que pueden ser tenidos en cuenta si consideran pertinentes para la organización.

7.2.4. Identificación y valoración de amenazas y vulnerabilidades (T.2.4). Las tareas "**Amenazas (T.2.4.1)"** y **"Vulnerabilidades (T.2.4.2)"** se realizan con cada una de las personas responsables de los activos de información, se identifican las posibles amenazas y las vulnerabilidades que puedan presentar los activos. Luego de identificar las amenazas y vulnerabilidades, se procede a valorarlas de acuerdo a los criterios establecidos en la tarea T.2.1.1 Probabilidad de ocurrencia (amenazas y vulnerabilidades).

Cuadro 12. Cuadro descriptivo de las tareas T.2.4.1, T.2.4.2

Tareas	• T.2.4.1. Amenazas • T.2.4.2. Vulnerabilidades
Objetivo	• Identificar y valorar las posibles amenazas y vulnerabilidades que afecten a los activos de información.
Responsable	• Comité de seguridad
Entradas	• Criterios de valoración de probabilidad de ocurrencia, tarea T.2.1.1 Probabilidad de ocurrencia (amenazas y vulnerabilidades).
Salidas	• Identificación de amenazas y vulnerabilidades • Valoración de amenazas y vulnerabilidades • Registro parcial de la Plantilla 03: Análisis de riesgos

❖ **Herramienta:** En esta tarea se propone la Plantilla 03: Análisis de riesgos, en ella se registraran las amenazas y vulnerabilidades con sus respectivas valoraciones.

7.2.5. Valoración del impacto (T.2.5). Esta tarea se realiza con cada una de las personas responsables de los activos de información, se valora el impacto generado de acuerdo a los criterios establecidos en la tarea T.2.1.2. Impacto (disponibilidad, confidencialidad, integridad).

Cuadro 13. **Cuadro descriptivo de la tarea T.2.5**

Tareas	• T.2.5. Valoración del impacto
Objetivo	• Valorar el impacto causado en los aspectos de disponibilidad, confidencialidad e integridad.
Responsable	• Comité de seguridad
Entradas	• Criterios de valoración de impacto, tarea T.2.1.2. Impacto (disponibilidad, confidencialidad, integridad). • Registro parcial de la Plantilla 03: Análisis de riesgos
Salidas	• Valoración de impacto • Registro parcial de la Plantilla 03: Análisis de riesgos

❖ **Herramienta:** En esta tarea se propone la Plantilla 03: Análisis de riesgos, en ella se registrara la valoración obtenida en cada uno de los aspectos del impacto (disponibilidad, confidencialidad, integridad).

7.2.6. Estimación del riesgo inherente (T.2.6). En esta tarea se calcula el riesgo inherente, para realizar esta tarea se necesita la valoración obtenidos en las tareas T.2.4.1. Amenazas, T.2.4.2. Vulnerabilidades y T.2.5. Valoración del impacto, los valores permitirán calcular el valor del riesgo inherente con ayuda de su respectiva ecuación.

Una vez calculado el valor del riesgo inherente se procede a utilizar la escala establecida en la tarea T.2.2.1. Riesgo inherente, y se procede a analizar la situación.

Cuadro 14. Cuadro descriptivo de la tarea T.2.6

Tareas	• T.2.6. Estimación del riesgo inherente
Objetivo	• Calcular el valor del riesgo inherente.
Responsable	• Comité de seguridad
Entradas	• Resultado de valoración de amenazas, tarea T.2.4.1. Amenazas • Resultado de valoración de vulnerabilidades, tarea T.2.4.2. Vulnerabilidades • Resultado de valoración de impacto, tarea T.2.5. Valoración del impacto • Escala de valoración del riesgo inherente, tarea T.2.2.1. Riesgo inherente • Ecuación de riesgo inherente • Registro parcial de la Plantilla 03: Análisis de riesgos
Salidas	• Resultado de valoración del riesgo inherente • Registro parcial de la Plantilla 03: Análisis de riesgos

Para calcular el riesgo inherente es necesario utilizar la ecuación planteada en la ISO 31000, la ecuación es la siguiente:

$$\boldsymbol{Riesgo\ Inherente} = (Probabilidad\ de\ Ocurrencia\ \times Impacto)$$

Donde la probabilidad de ocurrencia basándose en la metodología de análisis de riesgos de seguridad de la información es:

$$\boldsymbol{Probabilidad\ de\ Ocurrencia} = \left(\frac{Amenaza + Vulnerabilidad}{2}\right)$$

Y el impacto es:

$$\boldsymbol{Impacto} = \left(\frac{Confidencialdiad + Integridad + Disponibilidad}{3}\right)$$

❖ **Herramienta:** En esta tarea se propone la Plantilla 03: Análisis de riesgos, en ella se registrara la valoración del riesgo inherente y se analiza la situación.

7.2.7. Valorar los controles existentes (T.2.7). Esta tarea se realiza con cada una de las personas responsables de los activos de información, se valora el control existente de acuerdo a los criterios establecidos en la tarea T.2.1.3. Controles existentes.

Cuadro 15. Cuadro descriptivo de la tarea T.2.7

Tareas	• T.2.7. Valorar los controles existentes
Objetivo	• Valorar el control existente para mitigar el riesgo.
Responsable	• Comité de seguridad
Entradas	• Criterios de valoración de los controles existentes, tarea T.2.1.3. Controles existentes. • Registro parcial de la Plantilla 03: Análisis de riesgos
Salidas	• Resultado de valoración de los controles existentes • Registro parcial de la Plantilla 03: Análisis de riesgos

❖ **Herramienta:** En esta tarea se propone la Plantilla 03: Análisis de riesgos, en ella se registrara la valoración obtenida con respecto a los controles existentes.

7.2.8. Estimación del riesgo residual (neto) (T.2.8). En esta tarea se calcula el riesgo residual, para realizar esta tarea se necesita la valoración obtenidos en las tareas T.2.6. Estimación del riesgo inherente y T.2.7. Valorar los controles existentes, los valores permitirán calcular el valor del riesgo residual con ayuda de su respectiva ecuación.

Una vez calculado el valor del riesgo residual se procede a utilizar la escala establecida en la tarea T.2.2.2. Riesgo residual (neto) y se procede a analizar la situación.

Cuadro 16. Cuadro descriptivo de la tarea T.2.8

Tareas	• T.2.8. Estimación del riesgo residual (neto)
Objetivo	• Calcular el valor del riesgo neto.
Responsable	• Comité de seguridad
Entradas	• Resultado de valoración del riesgo inherente, tarea T.2.6. Estimación del riesgo inherente • Resultado de valoración de los controles existentes, tarea T.2.7. Valorar los controles existentes • Escala de valoración del riesgo residual, tarea T.2.2.1. Riesgo residual • Ecuación de riesgo residual • Registro parcial de la Plantilla 03: Análisis de riesgos
Salidas	• Resultado de valoración del riesgo residual • Registro de la Plantilla 03: Análisis de riesgos

Para calcular el riesgo residual es necesario utilizar la ecuación planteada en la ISO 31000, la ecuación es la siguiente:

$$\boldsymbol{Riesgo\ Residual} = \left(\frac{Riesgo\ Inherente}{Control}\right)$$

- **Herramienta:** En esta tarea se propone la Plantilla 03: Análisis de riesgos, en ella se registrara la valoración del riesgo residual y se analiza la situación.

7.2.9. Priorizar los riesgos críticos (T.2.9). En esta tarea se establece la priorización de los riesgos teniendo en cuenta los resultados obtenidos en la tarea T.2.8.Estimación del riesgo residual (neto),se espera obtener un orden para empezar a tomar medidas frente los riesgos más críticos que afecten a los activos.

Cuadro 17. Cuadro descriptivo de la tarea T.2.9

Tareas	• T.2.9. Priorizar los riesgos críticos
Objetivo	• Determinar el orden para el tratamiento de riesgos, teniendo en cuenta principalmente los riesgos más críticos.
Responsable	• Director de seguridad • Comité de seguridad
Entradas	• Resultado de valoración del riesgo residual, tarea T.2.8. Estimación del riesgo residual (neto) • Registro parcial de la Plantilla 03: Análisis de riesgos
Salidas	• Priorización de riesgos • Registro de la Plantilla 03: Análisis de riesgos • Registro de la Plantilla 04: Gestión de riesgos

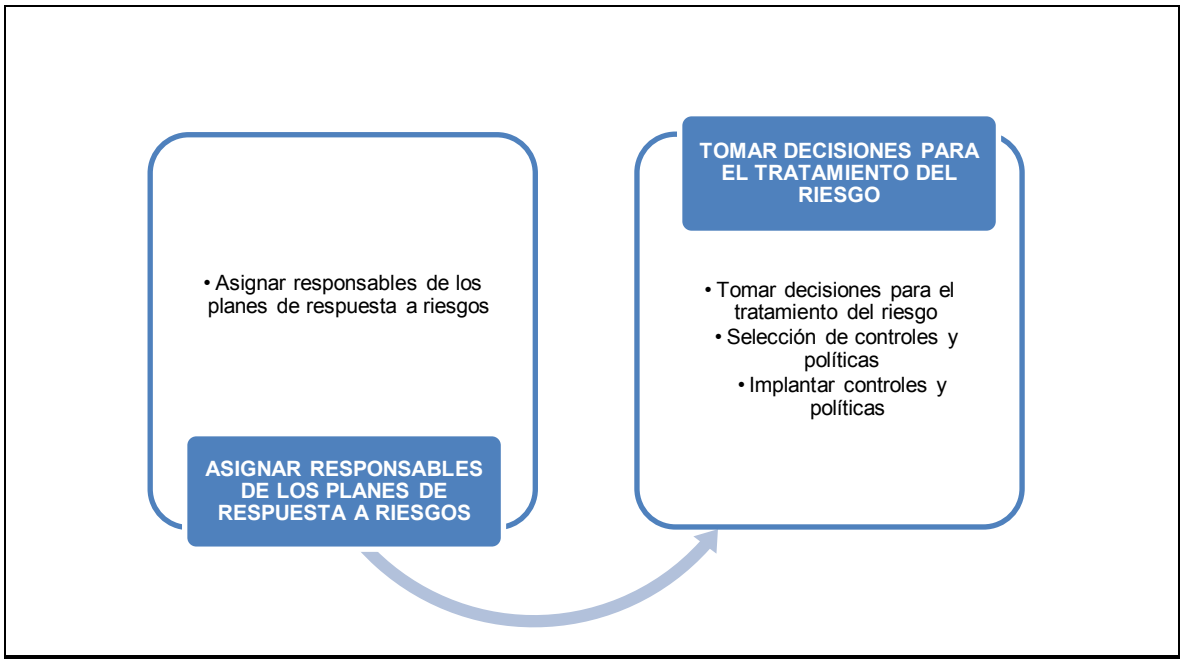
❖ **Herramienta:** En esta tarea se propone la Plantilla 03: Análisis de riesgos, se registrará el orden para el tratamiento de los riesgos.

7.3. GESTIÓN DE RIESGOS (T.3)

Esta fase busca reducir los riesgos anteriormente identificados, implantando controles y medidas adecuadas. También se asignan personas responsables a cada tratamiento de riesgo.

En la gestión de riesgos se detallan las siguientes tareas:

Figura 13. Guía de gestión de riesgos



7.3.1. Asignar responsables de los planes de respuesta a riesgos (T.3.1). En esta tarea se debe determinar la persona responsable de cada riesgo identificado, con el fin de que sea el líder en el proceso que se va a llevar a cabo en el tratamiento del riesgo, deben ser personas que conozcan y entiendan del tema que se está tratando para así tomar las mejores decisiones.

La persona que sea asignada puede ser seleccionada del comité de seguridad previamente establecido.

Cuadro 18. Cuadro descriptivo de la tarea T.3.1

Tareas	• T.3.1. Asignar responsables de los planes de respuesta a riesgos.
Objetivo	• Designar personas responsables para llevar a cabo el tratamiento de los riesgos
Responsable	• Director de seguridad • Comité de seguridad
Entradas	• Registro de la Plantilla 03: Análisis de riesgos
Salidas	• Registro parcial de la Plantilla 04: Gestión de riesgos • Registro parcial de la Plantilla 05: Monitoreo

❖ **Herramienta:** En esta tarea se propone la Plantilla 04: Gestión de riesgos, en ella se registrara la persona encargada de llevar a cabo el tratamiento de cada uno de los riesgos identificados.

7.3.2. Tomar decisiones para el tratamiento del riesgo (T.3.2). En esta tarea se reúne el director de seguridad, el comité de seguridad y las personas anteriormente asignadas en la tarea T.3.1. Asignar responsables de los planes de respuesta a riesgos, para tomar la decisión más adecuada en el tratamiento del riesgo, esta tarea se debe realizar con respecto a lo establecido en la escala de valoración de la tarea T.2.2.2. Riesgo residual (neto), recordemos que el riesgo se puede evitar, asumir, transferir, mitigar, en todos los casos debe quedar el registro y una explicación de la decisión tomada.

Por último se debe recordar obtener la aprobación de la alta gerencia mediante el proceso de comunicación.

Se debe tener en cuenta que para cada decisión de tratamiento del riesgo, se deben realizar las siguientes tareas:

➢ **Selección de controles y políticas**: se deben tomar una serie de medidas que actúen de salvaguarda para los activos, se tendrá en cuenta los controles expuestos en la guía de buenas prácticas ISO/IEC 27002 y de ser necesario se completaran con otros estándares o metodologías, como por ejemplo, los presentes en el catálogo de elementos de MAGERIT.

➢ **Implantar controles y políticas:** se deben documentar y socializar todas las medidas implantadas, para que los funcionarios estén informados y conozcan los diferentes controles y políticas, con el fin de que sean cumplidas y se logre mitigar el riesgo.

Cuadro 19. Cuadro descriptivo de la tarea T.3.2

Tareas	• T.3.2. Tomar decisiones para el tratamiento del riesgo
Objetivo	• Determinar la decisión adecuada para el tratamiento del riesgo
Responsable	• Director de seguridad • Comité de seguridad
Entradas	• Registro parcial de la Plantilla 04: Gestión de riesgos • Registro parcial de la Plantilla 05: Monitoreo
Salidas	• Registro parcial de la Plantilla 04: Gestión de riesgos • Registro parcial de la Plantilla 05: Monitoreo

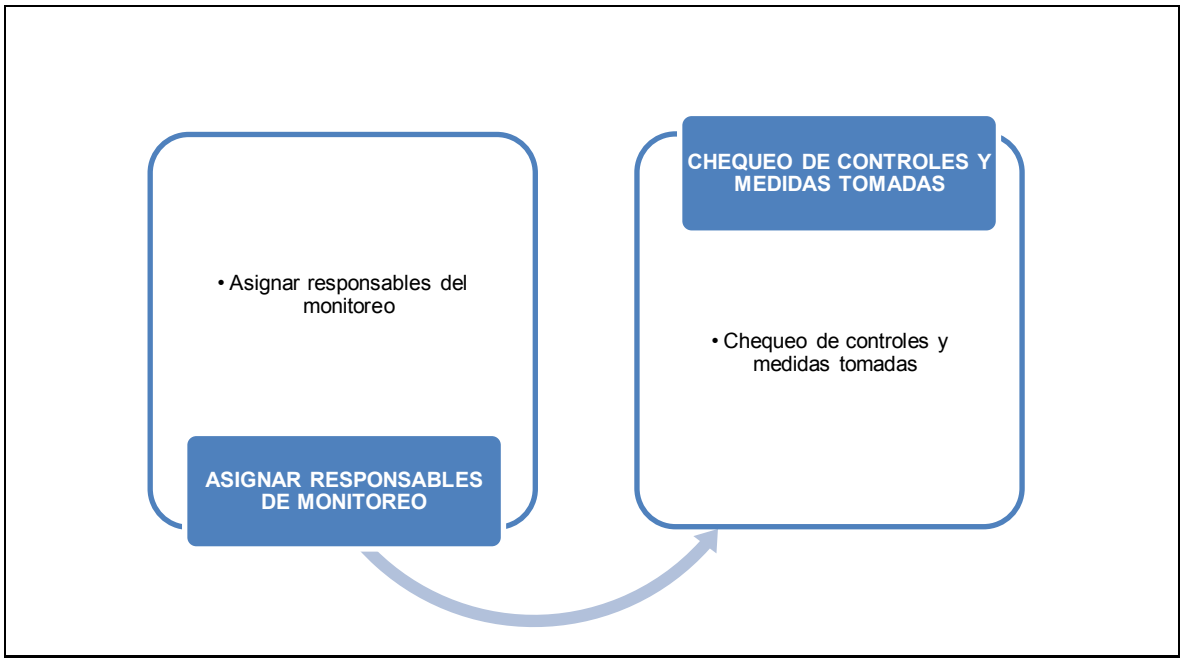
- **Herramienta:** En esta tarea se propone la Plantilla 04: Gestión de riesgos, en ella se registrara el tratamiento que se llevara a cabo con de cada uno de los riesgos identificados.

7.4. MONITOREO (T.4)

Esta fase se debe realizar periódicamente, el objetivo es monitorear que los controles se hayan implementado y que estén cumpliendo con su tarea, además promueve que se realicen posibles sugerencias para un mejor tratamiento del riesgo.

En el monitoreo se detallan las siguientes tareas:

Figura 14. Guía de monitoreo



7.4.1. Asignar responsables del monitoreo (T.4.1). En esta tarea se debe determinar la persona responsable del monitoreo de cada tratamiento riesgo identificado, con el fin de que sea el líder en el proceso que se está llevando a cabo en el tratamiento del riesgo, deben ser personas que conozcan y entiendan del tema que se está tratando.

La persona encargada del monitoreo no debe ser la misma que se encuentra asignada para el tratamiento del riesgo, se debe llevar a cabo de esta manera para que las personas adquieran el compromiso adecuadamente y se cumplan con los objetivos planteados.

Cuadro 20. Cuadro descriptivo de la tarea T.4.1

Tareas	• T.4.1. Asignar responsables del monitoreo
Objetivo	• Designar personas responsables para llevar a cabo el monitoreo del tratamiento de los riesgos
Responsable	• Director de seguridad • Comité de seguridad
Entradas	• Registro parcial de la Plantilla 04: Gestión de riesgos • Registro parcial de la Plantilla 05: Monitoreo
Salidas	• Registro parcial de la Plantilla 04: Gestión de riesgos • Registro parcial de la Plantilla 05: Monitoreo

❖ **Herramienta:** En esta tarea se propone la Plantilla 04: Gestión de riesgos, en ella se registrara la persona encargada de llevar a cabo el monitoreo de cada uno de los riesgos identificados.

7.4.2. Chequeo de controles y medidas tomadas (T.4.2). En esta tarea la persona asignada para el monitoreo del tratamiento del riesgo, se basa en lo establecido y verifica que se esté cumpliendo de manera acorde a lo previamente planteado, además debe reportar si las medidas tomadas son las más adecuadas.

Estos chequeos deberán hacerse periódicamente y llevar su respectivo registro.

Cuadro 21. Cuadro descriptivo de la tarea T.4.2

Tareas	• T.4.2. Chequeo de controles y medidas tomadas
Objetivo	• Verificar que se estén llevando a cabo las medidas tomadas y que sean las adecuadas.
Responsable	• Persona encargada del monitoreo
Entradas	• Registro parcial de la Plantilla 04: Gestión de riesgos • Registro parcial de la Plantilla 05: Monitoreo
Salidas	• Registro de la Plantilla 05: Monitoreo

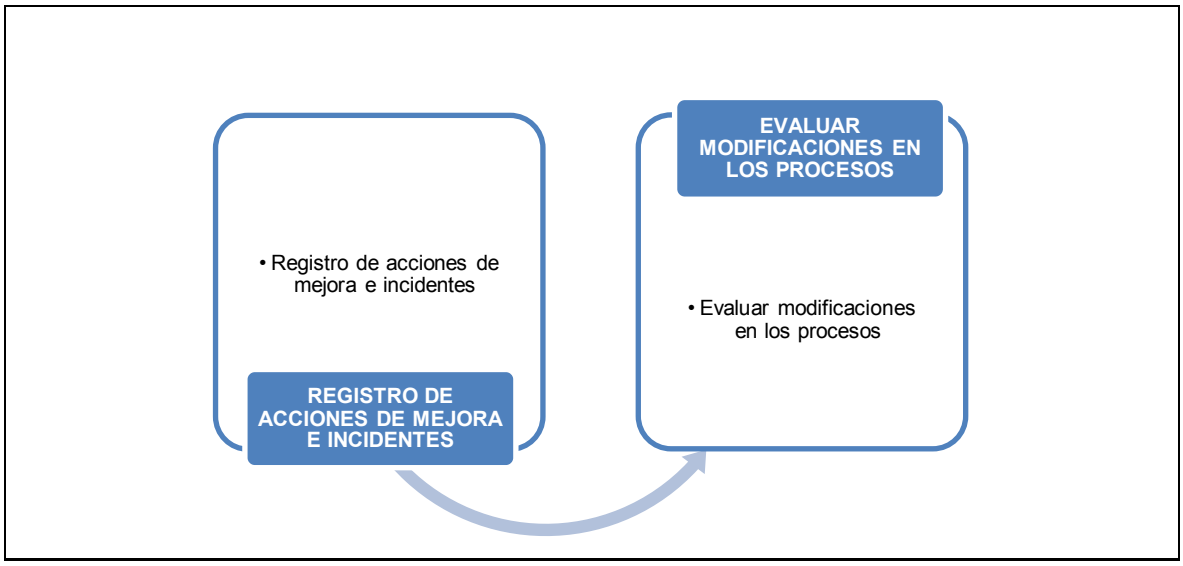
❖ **Herramienta:** En esta tarea se propone la Plantilla 05: Monitoreo, en ella se registrara el monitoreo que se llevara a cabo con de cada uno de los riesgos identificados.

7.5. MEJORAMIENTO CONTINUO (T.5)

En esta fase se registran los incidentes ocurridos, las acciones correctivas y posibles eslabones débiles que necesitan ser mejorados o corregidos. Todos los registros se ponen en consideración en busca de tomar las mejores decisiones y luego proceder a ser aprobados.

En el mejoramiento continuo se detallan las siguientes tareas:

Figura 15. Guía mejoramiento continuo



7.5.1. Registro de acciones de mejora e incidentes (T.5.1). En esta tarea se debe llevar el registro de acciones de mejora o posibles incidentes que se presente en la organización, se debe reportar que fallo y que solución se tomó en el momento, esta tarea se realiza con el fin de tener en cuenta lo sucedido y realizar posibles modificaciones en los procesos.

El registro del incidente debe ser hecho por la persona que estuvo a cargo en ese momento y las acciones de mejora pueden ser registradas por cualquier funcionario dentro de la organización.

Cuadro 22. Cuadro descriptivo de la tarea T.5.1

Tareas	• T.5.1. Registro de acciones de mejora e incidentes
Objetivo	• Registrar acciones de mejora e incidentes que se presenten dentro de la organización
Responsable	• Funcionarios de la organización
Entradas	• Plantilla 06: Mejoramiento continuo
Salidas	• Registro parcial de la Plantilla 06: Mejoramiento continuo

Se pueden consolidar los siguientes tipos de acciones:

- ✓ **Preventivas:** son aquellas acciones que se plantean para prevenir que algo no deseado ocurra en la organización, la idea que se tiene con este tipo de acciones es la prevenir un posible problema, en vez de solucionarlo en el momento que se origina, lo cual podría traer impactos negativos a la organización.

- ✓ **Correctivas:** son aquellas acciones que se toman para corregir cuando algo no deseado afecto a la organización, estas decisiones están basadas en los problemas que se originan y buscan dar solución provisionalmente a un incidente.

- ✓ **Mejora:** son aquellas acciones que se plantean para hacer las cosas de manera más eficaz y eficiente, consiguiendo los resultados esperados con menor esfuerzo, estas decisiones no están basadas en la necesidad de solucionar un problema sino de ayudar en el mejoramiento continuo del proceso.

- ❖ **Herramienta:** En esta tarea se propone la Plantilla 06: Mejoramiento continuo, en ella se registrara los incidentes y la manera como se asumió, además se plantearan posibles acciones de mejora con su respectivo tipo y justificación.

7.5.2. Evaluar modificaciones en los procesos (T.5.2). En esta tarea se reúne el director de seguridad y el comité de seguridad, para poner en consideración las acciones preventivas, correctivas y de mejora. Básicamente lo que se busca es evaluar si son viables para presentarlas a la alta gerencia en busca respectiva aprobación y proceder a efectuar los cambios pertinentes.

Se debe recordar informar los posibles cambios que se presenten a todas las personas involucradas en los procesos.

Cuadro 23. Cuadro descriptivo de la tarea T.5.2

Tareas	• T.5.2. Evaluar modificaciones en los procesos
Objetivo	• Evaluar las acciones preventivas, correctivas y de mejora
Responsable	• Director de seguridad • Comité de seguridad
Entradas	• Registro parcial de la Plantilla 06: Mejoramiento continuo
Salidas	• Registro de la Plantilla 06: Mejoramiento continuo

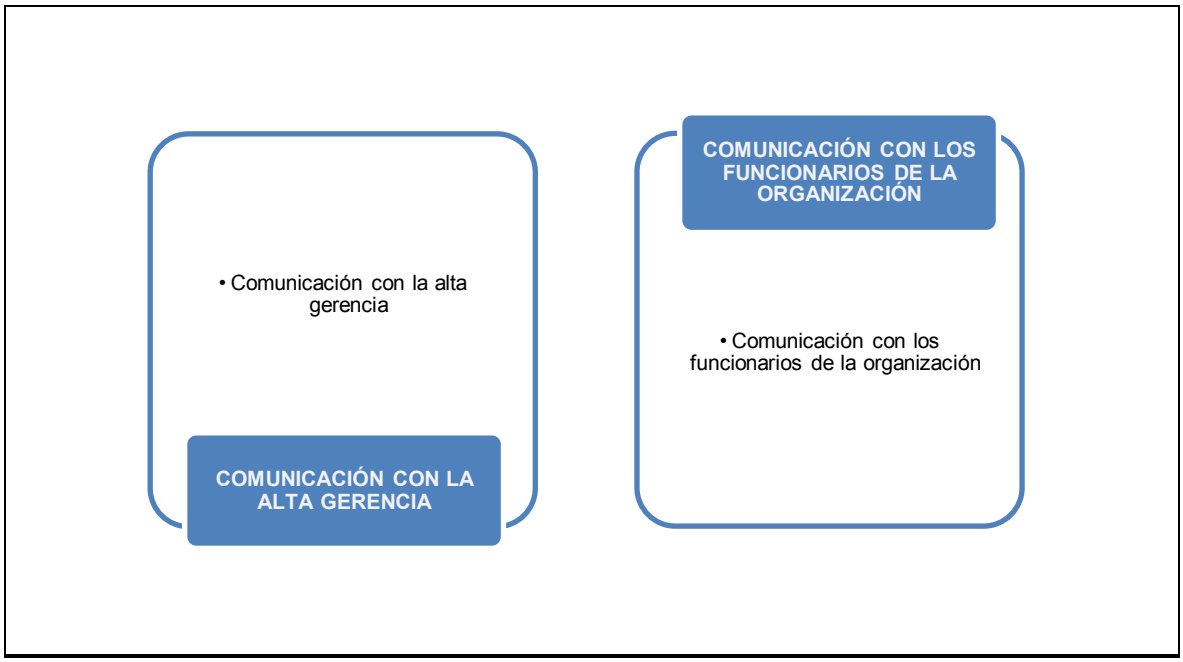
❖ **Herramienta:** En esta tarea se propone la Plantilla 06: Mejoramiento continuo, en ella se registrara la posible aprobación de las acciones preventivas, correctivas y de mejora.

7.6. COMUNICACIÓN (T.6)

En esta fase básicamente lo que se maneja es la continua comunicación con la alta gerencia y con los funcionarios de la organización, para que todos estén comprometidos con el proceso y puedan aportar en el desarrollo del mismo.

En la comunicación se detallan las siguientes tareas:

Figura 16. Guía comunicación



7.6.1. Comunicación con la alta gerencia (T.6.1). En esta tarea continua se busca que la alta gerencia conozca lo que se está llevando a cabo en cada una de las fases del proceso, para que de esta manera mantengan informados y se facilite la aprobación en cada una de las toma de decisiones.

Cuadro 24. Cuadro descriptivo de la tarea T.6.1

Tareas	• T.6.1. Comunicación con la alta gerencia
Objetivo	• Informar y Comprometer a la alta gerencia en la toma de decisiones
Responsable	• Director de seguridad
Entradas	• Documentación generada en las tareas • Registro de las plantillas generadas en las tareas
Salidas	• Plantillas aprobadas

7.6.2. Comunicación con los funcionarios de la organización (T.6.2). En esta tarea continua se busca que los funcionarios de la organización estén informados sobre el proceso que se está llevando a cabo, para que de esta manera sean conscientes de la importancia del proceso y faciliten su colaboración en el proceso.

Cuadro 25. Cuadro descriptivo de la tarea T.6.2

Tareas	• T.6.2. Comunicación con los funcionarios de la organización
Objetivo	• Concientizar a los funcionarios de la organización
Responsable	• Director de seguridad • Comité de seguridad
Entradas	• Documentación generada en las tareas • Plantillas generadas en las tareas
Salidas	• Funcionarios informados y concientizados sobre el proceso.

7.7. ROLES Y RESPONSABILIDADES

- **Alta gerencia:** directivos encargados de tomar y aprobar las decisiones que se tomen dentro la organización.

- **Director de seguridad:** persona encargada de coordinar y brindar apoyo en cada una de las tareas a realizar, además es el encargado de presentar lo realizado en cada fase a la alta gerencia.

- **Comité de seguridad:** grupo de personas encargadas de realizar diferentes tareas y brindar apoyo en el proceso.

- **Persona responsable del plan de respuesta a riesgos:** persona encargada de realizar el acompañamiento en el momento de la implementación del tratamiento del riesgo y además verifica que los funcionarios estén cumpliendo con lo planteado.

- **Persona responsable del monitoreo:** persona encargada de monitorear que se implantaron las medidas propuestas para el tratamiento de los riesgos.

- **Funcionarios:** las diferentes personas que de alguna manera u otra influyen en las labores de la organización.

7.8. PLANTILLAS

A continuación se presentan las diferentes plantillas empleadas para el desarrollo del proceso:

7.8.1. Plantilla 01: Establecimiento del contexto. Esta plantilla está compuesta por los siguientes campos:

- **PERSONAS INVOLUCRADAS:**

- **NOMBRE:** identifica nombre del funcionario.

- **ROL:** identifica la función que va a desempeñar.

- **ALCANCE:** identifica que se va a proteger en la organización.

- **OBJETIVO:** identifica lo que se quiere lograr con el proceso.

- **JUSTIFICACIÒN DEL PROCESO:** identifica lo que se va hacer, como se va hacer y la importancia de llevar a cabo el proceso.

- **APROBACIÒN:**

- **FECHA DE PRESENTACIÒN:** identifica la fecha en la que se presentó el establecimiento del contexto a la alta gerencia.

- **FECHA DE APROBACIÒN:** identifica la fecha de aprobación establecimiento del contexto por parte de la alta gerencia.

- **NOMBRE (Jefe de la Organización):** identifica el nombre del jefe que aprobó el establecimiento del contexto.

- **FIRMA:** identifica la firma del jefe que aprobó el establecimiento del contexto.

- **OBSERVACIONES:** campo libre para algún comentario adicional.

Figura 17. Plantilla 01, establecimiento del contexto

PERSONAS INVOLUCRADAS	
Nombre	**Rol**
ALCANCE	
OBJETIVOS	
JUSTIFICACIÓN DEL PROCESO	
APROBACIÓN	
FECHA PRESENTACIÓN	
FECHA APROBACIÓN	
NOMBRE (Jefe de la organización)	
FIRMA	

OBSERVACIONES	

NOTA: El desarrollo planteado para esta plantilla se encuentra en el inciso de Anexos con el nombre de “Anexo A. Establecimiento del contexto”

7.8.2. Plantilla 02: Identificación de activos. Activo se denomina activo a cualquier cosa que tiene valor para la organización y por lo tanto debe protegerse (ISO/IEC 13335-1:2004). De tal manera que un activo de información es un elemento que contiene o manipula información de valor para la organización.

Algunos activos de información generales pueden ser encontrados en la Cuadro 38. Cuadro de ejemplos de activos de Información.

Esta plantilla está compuesta por los siguientes campos:

- **IDENTIFICADOR ACTIVO:** identificación única de cada activo.
- **ACTIVO:** identifica el nombre del activo.
- **CATEGORÍA**: identifica clasificación del activo.

Los activos se pueden distinguir diferentes categorías, las categorías más relevantes presentadas en la metodología MAGERIT son:

Cuadro 26. Cuadro descriptivo de los activos de información

Categoría	Descripción
Datos	Elementos de información que, de forma singular o agrupada de alguna forma, representan el conocimiento que se tiene de algo.
Aplicaciones	Con múltiples denominaciones (programas, aplicativos, desarrollos, etc.) este epígrafe se refiere a tareas que han sido automatizadas para su desempeño por un equipo informático.
Servicios	Función que satisface una necesidad de los usuarios (del servicio).
Infraestructura	Dícese de bienes materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, siendo pues depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos.
Equipamiento Auxiliar	En este epígrafe se consideran otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.

Fuente: ESPAÑA. Metodología de análisis y gestión de Riesgos de los sistemas de información – II Catalogo de Elementos, MAGERIT- Versión 2, Ministerio de administraciones públicas, Madrid, 20 de Junio, 2006.

- **RESPONSABLE:** identifica la persona a cargo del activo.

- **RESPONSABLE POR LA SEGURIDAD:** identifica a el responsable por la seguridad del activo (que en algunos casos es la misma persona indicada como responsable por el activo) y quien aprueba la asociación de controles para reducir el riesgo.

- **DESCRIPCIÓN:** campo libre para describir el activo.

- **LOCALIZACIÓN:** identifica dónde se encuentra físicamente el activo. En el caso de información en formato electrónico, en qué equipo se encuentra.

- **QUÉ SUCEDE SI FALTA EL ACTIVO (IMPACTO**): Campo para describir brevemente el impacto generado sobre el activo.

❖ Impacto: consecuencia de la materialización de una amenaza, lo que podría suponer en caso de una pérdida de la confidencialidad, la integridad o la disponibilidad con el activos de información.

- **OBSERVACIONES:** campo libre para algún comentario adicional.

Figura 18. Plantilla 02, Identificación de activos

		FECHA:					
		NOMBRE:					
		CARGO:					
IDENTIFICADOR ACTIVO	**ACTIVO**	**CATEGORÍA ACTIVO**	**RESPONSABLE DEL ACTIVO**	**RESPONSABLE POR LA SEGURIDAD**	**DESCRIPCIÓN**	**LOCALIZACIÓN**	**¿QUÉ SUCEDE SI FALTA EL ACTIVO? (IMPACTO)**
OBSERVACIONES							

NOTA: El desarrollo parcial planteado para esta plantilla se encuentra en el inciso de Anexos con el nombre de “Anexo B. Listado de activos”

7.8.3. Plantilla 03: Análisis de riesgos. Esta plantilla está compuesta por los siguientes campos:

- **FECHA:** identifica la fecha en la que se llevó a cabo la identificación de los activos.

- **NOMBRE:** identifica el nombre del funcionario que realizo la identificación de los activos

- **CARGO:** identifica el cargo del funcionario que realizo la identificación de los activos.

- **IDENTIFICADOR RIESGO:** número de identificación asignado al riesgo.

- **DESCRIPCIÓN AMENAZA:** identifica las posibles amenazas que afectan el activo.

❖ Según [ISO/IEC 13335-1:2004]: una amenaza es la causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

Algunas amenazas generales pueden ser encontradas en la Cuadro 39. Cuadro de ejemplos de amenazas informáticas.

- **CATEGORÍA AMENAZA:** identifica la categoría de la amenaza que afecta al activo.

Cuadro 27. Cuadro descriptivo de amenazas

CATEGORÍA AMENAZA	DESCRIPCIÓN
Fraude Interno / Externo	Fallas que provienen de un engaño para sacar provecho o beneficio.
Cumplimiento	Fallas que provienen de una actuación en contra de una obligación, una política y/o procedimiento.
Interrupción y Falla del Sistema	Fallas que provienen de un evento provocado directamente o indirectamente produciendo la paralización de los sistemas.
Soporte y Entrega del Servicio	Fallas que provienen de la prestación del servicio de asistencia a software o hardware.
Otra	Fallas que no se encuentran estipuladas en ninguna de las categorías anteriores.

Fuente: ESPAÑA. Metodología de análisis y gestión de Riesgos de los sistemas de información – II Catalogo de Elementos, MAGERIT- Versión 2, Ministerio de administraciones públicas, Madrid, 20 de Junio, 2006.

- **VALORACIÓN AMENAZA:** identifica la valoración que se asigna teniendo en cuenta la posibilidad de que ocurra la amenaza identificada.

- **DESCRIPCIÓN VULNERABILIDAD:** Identifica las vulnerabilidades que presenta el activo.
- Vulnerabilidad es una debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISO/IEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

Algunas vulnerabilidades generales pueden ser encontradas en el cuadro 40. Cuadro de ejemplos de vulnerabilidades informáticas.

- **VALORACIÓN VULNERABILIDAD:** identifica la valoración que se asigna teniendo en cuenta la posibilidad de que una amenaza explote la vulnerabilidad identificada.

- **RELEVANCIA DEL ACTIVO (IMPACTO):**
  - **VALORACIÒN CONFIDENCILIDAD:** identifica la valoración que se asigna teniendo en cuenta el impacto generado frente a la confidencialidad.

  - **VALORACIÒN DISPONIBILIDAD:** identifica la valoración que se asigna teniendo en cuenta el impacto generado frente a la disponibilidad.

  - **VALORACIÒN INTEGRIDAD:** identifica la valoración que se asigna teniendo en cuenta el impacto generado frente a la integridad.

- **RIESGO INHERENTE:** identifica la valoración del riesgo existente en la organización antes de tomar acciones o establecer controles

- **DESCRIPCIÒN CONTROL:** identifica los controles aplicados sobre el activo.

- Según [ISO/IEC 27000]: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo aceptable. (Nota: Control es también utilizado como sinónimo de salvaguarda o contramedida).

- **VALORACIÓN CONTROL:** identifica la valoración que se asigna teniendo en cuenta la efectividad del control asociado.

- **RIESGO RESIDUAL:** identifica la valoración del riesgo existente en la organización después de que se han tomado acciones o establecido controles

- **PRIORIZACIÒN:** identifica el orden de prioridades para el tratamiento de los riesgos.

Figura 19. Plantilla 03, análisis de riesgos

FECHA:	
NOMBRE:	
CARGO:	

IDENTIFICADOR AMENAZA	ACTIVO	INDICADOR RIESGO	DESCRIPCIÓN AMENAZA	CATEGORÍA AMENAZA	VALORACIÓN AMENAZA	DESCRIPCIÓN VULNERABILIDAD	VALORACIÒN VULNERABILIDAD	RELEVANCIA DEL ACTIVO (IMPACTO)			RIESGO INHERENTE	DESCRIPCIÓN CONTROL	VALORACIÓN CONTROL	RIESGO RESIDUAL	PRIORIZACIÓN
								VALORACIÓN CONFIDENCIALIDAD	VALORACIÓN DISPONIBILIDAD	VALORACIÓN INTEGRIDAD					

NOTA: El desarrollo parcial planteado para esta plantilla se encuentra en el inciso de Anexos con el nombre de “Anexo C. Análisis de riesgos”

7.8.4. Plantilla 04: Gestión de riesgos. Esta plantilla está compuesta por los siguientes campos:

- **FECHA:** identifica la fecha en la que se llevó a cabo la valoración de los activos.
- **NOMBRE:** identifica el nombre del funcionario que realizo la valoración de los activos
- **CARGO:** identifica el cargo del funcionario que realizo la valoración de los activos.
- **IDENTIFICADOR RIESGO:** número de identificación asignado al riesgo.
- **RIESGO RESIDUAL:** identifica la valoración del riesgo existente en la organización después de que se han tomado acciones o establecido controles.
- **PRIORIZACIÒN:** identifica el orden de prioridades para el tratamiento de los riesgos.
- **RESPONSABLE DEL TRATAMIENTO DEL RIESGO:** identifica al funcionario encargado de liderar el proceso para el tratamiento del riesgo identificado.
- **TRATAMIENTO DEL RIESGO:** identifica el tipo de tratamiento de riesgo que se va a llevar a cabo (evitar, transferir, mitigar, asumir).
- **ACCIONES TOMADAS:** identifica las diferentes acciones tomadas para el tratamiento del riesgo.
- **RESPONSABLE DEL MONITOREO DEL RIESGO:** identifica al funcionario encargado de monitorear el tratamiento del riesgo identificado.
- **FECHA:** identifica la fecha en la se determinó el tratamiento del riesgo y sus responsables.
- **APROBACIÒN:**

  - **FECHA DE PRESENTACIÒN:** identifica la fecha en la que se presentó el tratamiento de los riesgos y los responsables.
  - **FECHA DE APROBACIÒN:** identifica la fecha de aprobación del tratamiento de los riesgos y los responsables.
  - **NOMBRE (Jefe de la Organización):** identifica el nombre del jefe que aprobó el tratamiento de los riesgos y los responsables.

- **FIRMA:** identifica la firma del jefe que aprobó el tratamiento de los riesgos y los responsables.

- **OBSERVACIONES:** campo libre para algún comentario adicional.

Figura 20. Plantilla 04, gestión de riesgos

IDENTIFICADOR RIESGO	RIESGO RESIDUAL	PRIORIZACIÒN	RESPONSABLE DEL TRATAMIENTO DEL RIESGO	TRATAMIENTO DEL RIESGO	ACCIONES TOMADAS	RESPONSABLE DEL MONITOREO DEL RIESGO	FECHA

APROBACIÓN	
FECHA PRESENTACIÓN	
FECHA APROBACIÓN	
NOMBRE (Jefe de la organización)	
FIRMA	

NOTA: El desarrollo parcial planteado para esta plantilla se encuentra en el inciso Anexos con el nombre de “Anexo D. Gestión de riesgos”, las decisiones tomadas se realizaron a partir de las recomendaciones establecidas en el numeral “9.2. Recomendaciones a partir del análisis”.

7.8.5. Plantilla 05: Monitoreo. Esta plantilla está compuesta por los siguientes campos:

- **IDENTIFICADOR RIESGO:** número de identificación asignado al riesgo.
- **RESPONSABLE DEL TRATAMIENTO DEL RIESGO:** identifica al funcionario encargado de liderar el proceso para el tratamiento del riesgo identificado.
- **TRATAMIENTO DEL RIESGO:** identifica el tipo de tratamiento de riesgo que se va a llevar a cabo (evitar, transferir, mitigar, asumir)
- **ACCIONES TOMADAS:** identifica todas medidas tomadas para el tratamiento del riesgo, políticas, controles, etc.
- **RESPONSABLE DEL MONITOREO:** identifica al funcionario encargado de monitorear el tratamiento del riesgo identificado.
- **FECHA MONITOREO:** identifica la fecha en la se llevó a cabo el monitoreo.
- **CHEQUEO:** identifica si se está cumpliendo con el tratamiento del riesgo, se registra aprobado o no aprobado.
- **OBESERVACIONES:** campo libre para algún comentario adicional.

Figura 21. Plantilla 05, monitoreo

IDENTIFICADOR RIESGO	RESPONSABLE DEL TRATAMIENTO DEL RIESGO	TRATAMIENTO DEL RIESGO	ACCIONES TOMADAS	RESPONSABLE DEL MONITOREO DEL RIESGO	FECHA MONITOREO	CHEQUEO	OBSERVACIONES

7.8.6. Plantilla 06: Mejoramiento continuo. Esta plantilla está compuesta por los siguientes campos:

- **INCIDENTE:** identifica una breve descripción del incidente
- **ACCIONES TOMADAS:** identifica todas aquellas acciones correctivas que se realizaron para superar el incidente
- **NOMBRE FUNCIONARIO:** identifica al funcionario que estuvo a cargo del incidente
- **FECHA INCIDENTE:** identifica la fecha en la que se presentó el incidente
- **OBESERVACIONES:** campo libre para algún comentario adicional.
- **IDENTIFICADOR MEJORA:** número de identificación asignado a la acción de mejora propuesta.
- **TIPO DE ACCIÓN:** identifica el tipo de acción propuesta, puede ser correctiva, preventiva o mejora.
- **CAMBIO:** identifica cual es el cambio propuesto, puede ser para una tarea, un tratamiento de riesgo u otra.
- **JUSTIFICACIÓN:** identifica una breve justificación del cambio propuesto.
- **NOMBRE FUNCIONARIO:** identifica el nombre del funcionario que propone la acción de mejora
- **FECHA ENTREGA:** identifica la fecha en la que se presentó la acción de mejora
- **FECHA REVISIÓN:** identifica la fecha en la que se revisó la acción de mejora propuesta.
- **DECISIÓN:** identifica si el director de seguridad aprobó o no la acción de mejora propuesta.
- **OBESERVACIONES:** campo libre para algún comentario adicional.
- **APROBACIÒN:**
  - **FECHA DE PRESENTACIÒN:** identifica la fecha en la que se presentó la plantilla de mejora continua a la alta gerencia.

- **FECHA DE APROBACIÒN:** identifica la fecha de aprobación de la plantilla de mejora continua.

- **NOMBRE (Jefe de la Organización):** identifica el nombre del jefe que aprobó la plantilla de mejora continua.

- **FIRMA:** identifica la firma del jefe que aprobó la plantilla de mejora continua.

Figura 22. Plantilla 06, mejoramiento continuo

INCIDENTE	ACCIONES TOMADAS	NOMBRE FUNCIONARIO	FECHA INCIDENTE	OBSERVACIONES

IDENTIFICARDOR MEJORA	TIPO DE ACCIÓN	CAMBIO	JUSTIFICACIÓN	NOMBRE FUNCIONARIO	FECHA ENTREGA	FECHA REVISIÓN	DECISIÓN	OBSERVACIONES

APROBACIÓN	
FECHA PRESENTACIÓN	
FECHA APROBACIÓN	
NOMBRE (Director de seguridad)	
FIRMA	

7.9. CUADRO DE DESCRIPCIÓN HERRAMIENTAS (PLANTILLAS)

Cuadro 28. Cuadro descriptivo de herramientas (plantillas)

NOMBRE	DESCRIPCIÓN
Plantilla 01: Establecimiento del contexto.	En esta plantilla se define la política de seguridad de la información, en donde se deja claro lo que se va a proteger y lo que se quiere lograr, en su parte inferior se hace referencia a una serie de campos para llevar el registro de aprobación por parte de la alta gerencia.
Plantilla 02: Identificación de activos.	En esta plantillase registran cada uno de los activos presentes en la organización, además de sus características más relevantes.
Plantilla 03: Análisis de riesgos.	En esta plantilla se registran las amenazas, vulnerabilidades y los controles aplicados para cada uno de los activos anteriormente identificados, además se realiza una valoración por cada uno de los conceptos y se priorizan los riesgos dependiendo de la valoración obtenida.
Plantilla 04: Gestión de riesgos.	En esta plantillase registran tanto las acciones tomadas para el tratamiento del riesgo, como las personas encargadas de gestionar el tratamiento y el monitoreo del mismo.
Plantilla 05: Monitoreo.	En esta plantilla se lleva el chequeo del tratamiento del riesgo anteriormente propuesto, se realiza con el objetivo de que se cumplan todas las acciones tomadas.
Plantilla 06: Mejoramiento continuo.	En esta plantillase registran los diferentes incidentes que se presenten en la organización y además, las acciones de mejora propuestas para su posterior aprobación. En su parte inferior se hace referencia a una serie de campos para llevar el registro de aprobación por parte de la alta gerencia.

7.10. CRITERIOS DE VALORACIÓN

Los siguientes criterios de valoración permitirán analizar la probabilidad de ocurrencia, el impacto y los controles existentes, frente a los riesgos de la secretaria TIC.

7.10.1. Probabilidad de ocurrencia. Se determina mediante la probabilidad de que una amenaza explote una vulnerabilidad.

7.10.1.1. Amenaza. Según [ISO/IEC 13335-1:2004]: una amenaza es la causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

Probabilidad de que una amenaza afecte al activo:

Cuadro 29. Cuadro descriptivo de valoración de una amenaza

CRITERIO DE VALORACIÓN DE AMENAZA	
VALOR AMENAZA	**DESCRIPCIÓN**
1- Muy bajo	Una vez cada cinco años
2- Bajo	Una vez cada tres años
3- Moderado	Una ó dos veces al año
4- Alta	Tres ó cuatro veces al año
5- Muy alta	Una o más veces al mes

7.10.1.2. Vulnerabilidad. Según [ISO/IEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

Probabilidad de que se explote una vulnerabilidad del activo:

Cuadro 30. Cuadro descriptivo de valoración de una vulnerabilidad

CRITERIO DE VALORACIÓN DE VULNERABILIDAD	
VALOR VULNERABILIDAD	**DESCRIPCIÓN**
1- Muy bajo	Es muy poco probable que pueda ser explotada por una amenaza, los daños causados son insignificantes
2- Bajo	Es poco probable que pueda ser explotada por una amenaza, los daños causados pueden llegar a ser significativos
3 - Moderado	Es probable que pueda ser explotada por una amenaza, los daños causados son significativos pero no impiden la continuidad de las labores
4 – Alta	Es muy probable que pueda ser explotada por una amenaza, se causan daños dentro del área afectada, impidiendo la continuidad de las labores en el área
5- Muy Alta	Es muy probable que pueda ser explotada por una amenaza, se causan daños dentro y fuera del área afectada, impidiendo la continuidad en más áreas

7.10.2. Relevancia de activo. Determina como se ve afectado un activo de información, de acuerdo a las características de la información.

7.10.2.1. Confidencialidad. Acceso a la información únicamente por personas autorizadas. ([ISO/IEC 13335-1:2004]: característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados).

Grado en que afecta la confidencialidad:

Cuadro 31. Cuadro descriptivo de valoración de confidencialidad

CRITERIO DE VALORACIÓN DE CONFIDENCIALIDAD		
VALORACIÓN	**CLASE**	**DESCRIPCIÓN**
1- No relevante	No aplica	No aplica
2- Bajo	Disponible al publico	La información no sensible, las instalaciones de procesamiento de información y los recursos del sistema están disponibles para el público. Los daños son insignificantes ó nulos.
3- Medio	Para uso interno exclusivamente	La información no sensible está restringida para uso interno exclusivamente, es decir, no está disponible para el público. El incidente no trascendería del área afectada.
4- Alto	Uso restringido solamente	La información sensible está restringida para uso interno exclusivamente, es decir, no está disponible para el público. El incidente trascendería del área afectada.
5- Muy alto	Estrictamente confidencial	La información sensible solo estará disponible para las necesidades del negocio. Los daños serian catastróficos, la reputación y la imagen de la organización se vería comprometida.

Fuente: ISO 27005: Tecnologia de la información, Técnicas de seguridad - Gestión del riesgo de seguridad de la información, ISO/IEC, 2011.

7.10.2.2. Integridad. Mantenimiento de la exactitud y completitud de la información. ([ISO/IEC 13335-1:2004]: propiedad/característica de salvaguardar la exactitud y completitud de los activos).

Grado en que afecta la integridad:

Cuadro 32. Cuadro descriptivo de valoración de integridad

CRITERIO DE VALORACIÓN DE INTEGRIDAD		
VALORACIÓN	**CLASE**	**DESCRIPCIÓN**
1- No relevante	No aplica	No aplica
2- Bajo	Integridad baja	El daño o modificación no autorizada no es crítico para las aplicaciones empresariales. El impacto en la empresa es insignificante o nulo
3- Medio	Integridad media	El daño o modificación no autorizada no es crítico, pero si notorio para las aplicaciones empresariales. El impacto en la empresa podría llegar a ser significativo
4- Alto	Integridad alta	El daño o modificación no autorizada es crítico y notorio para las aplicaciones empresariales. El impacto en la empresa es significativo
5- Muy alto	Integridad intacta	El daño o modificación no autorizada es crítico para las aplicaciones empresariales. El impacto en la empresa es importante y podría conllevar a una falla grave o total de la aplicación empresarial

Fuente: ISO 27005: Tecnologia de la información, Técnicas de seguridad - Gestión del riesgo de seguridad de la información, ISO/IEC, 2011.

7.10.2.3. Disponibilidad. Acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran. ([ISO/IEC 13335-1:2004]: característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada).

Grado en que afecta la disponibilidad:

Cuadro 33. Cuadro descriptivo de valoración de disponibilidad

CRITERIO DE VALORACIÓN DE DISPONIBILIDAD		
VALORACIÓN	**CLASE**	**DESCRIPCIÓN**
1- No relevante	No aplica	No aplica
2- Bajo	Disponibilidad baja	Se puede tolerar que el activo no esté disponible por varios días
3- Medio	Disponibilidad media	Se puede tolerar que el activo no esté disponible máximo un día
4- Alto	Disponibilidad alta	Se puede tolerar que el activo no esté disponible por máximo de media día
5- Muy alto	Disponibilidad permanente	No se puede tolerar que el activo no esté disponible por más de unas cuantas horas o incluso menos

Fuente: ISO 27005: Tecnologia de la información, Técnicas de seguridad - Gestión del riesgo de seguridad de la información, ISO/IEC, 2011.

7.10.3. Controles existentes. Determina que tan efectivo es un control o salvaguarda.

7.10.3.1. Control. Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. (Nota: Control es también utilizado como sinónimo de salvaguarda o contramedida).

Valoración del control:

Cuadro 34. Cuadro descriptivo de valoración de un control

CRITERIO DE VALORACIÓN DECONTROL	
VALORACIÓN	**DESCRIPCIÓN**
1- Nulo	No tiene control asociado
2- Bajo	Tiene control asociado y no funciona correctamente
3- Moderado	El control asociado funciona, pero puede presentar fallas en algún momento
4- Alto	El control asociado funciona correctamente, pero se puede mejorar
5- Muy alto	El control asociado es efectivo y funciona correctamente

7.11. ESCALAS DE VALORACIÓN

Las siguientes escalas de valoración permitirán analizar e identificar cual es la respuesta más acertada para el tratamiento del riesgo que se está evaluando.

7.11.1. Riesgo inherente. Identifica la valoración del riesgo existente en la organización antes de tomar acciones o establecer controles que permitan a la organización reducir su probabilidad de ocurrencia.

Cuadro 35. Cuadro descriptivo de riesgo inherente

VALORACIÓN	RIESGO INHERENTE	DESCRIPCIÒN
1 2 3 4 5	ACEPTAR / ARCHIVAR	La criticidad es insignificante: se recomienda aceptar y archivar el riesgo ya que puede ser más costoso ejecutar acciones para mitigarlo.
6 7 8 9 10 11 12	REVISAR	La criticidad es considerable: aunque los riesgos no son críticos se debe hacer una revisión y seguimiento para evaluar si posteriormente cambian las características del riesgo.
13 14 15 16 17 18 19 20 21 22 23 24 25	EVALUAR	La criticidad es alta: se debe realizar la valoración del riesgo residual y determinar qué acciones se deben tomar para que la organización no se vea afectada.

7.11.2. Riesgo residual. Identifica la valoración del riesgo existente en la organización después de que se han tomado acciones o establecido controles que permiten a la organización reducir su probabilidad de ocurrencia.

La siguiente matriz es una representación gráfica para ilustrar la priorización de los riesgos de acuerdo a la probabilidad de ocurrencia contra el impacto.
Los que se encuentran en la zona roja son los más críticos e involucran el más alto grado de riesgo, la zona anaranjada implica riesgos medios y requieren atención continua. Las áreas amarillas son riesgos bajos y es recomendable asumirlos.

IMPACTO		1- NO RELEVANTE	2- BAJO	3- MEDIO	4- ALTO	5- MUY ALTO
	1- NO RELEVANTE	1	2	3	4	5
	2 -BAJO	2	4	6	6	10
	3 - MEDIO	3	6	9	12	15
	4 - ALTO	4	8	12	16	20
	5 - MUY ALTO	5	10	15	20	25
	PROBABILIDAD DE OCURRENCIA					

Escala:

Cuadro 36. Cuadro descriptivo de riesgo residual

VALORACIÓN	RIESGO RESIDUAL	DESCRIPCIÒN
1 2 3 4 5	ASUMIR	La criticidad es insignificante: se recomienda asumir el riesgo ya que puede ser más costoso ejecutar acciones que reduzcan el riesgo.
6 7 8 9 10 11 12	ASUMIR / MITIGAR	La criticidad es considerable: aunque los riesgos no son tan críticos se debe hacer seguimiento para evaluar si posteriormente cambian las características del riesgo y se hace necesario implementar controles que mitiguen el riesgo.
13 14 15 16 17 18 19 20 21 22 23 24 25	ELIMINAR / TRANSFERIR / MITIGAR	La criticidad es alta: se deben tomar acciones inmediatas, ya que es demasiado probable de que una amenaza se materialice y cause daños considerables en la organización.

Cuadro 37. Cuadro descriptivo de gestión de riesgos del negocio

Asumir	Asumir un riesgo significa no hacer nada para evitarlo, en caso de presentarse una pérdida, esta es aceptada por la organización. Además se puede tomar esta decisión en caso de que el tratamiento del riesgo tenga costos elevados en comparación a los beneficios obtenidos.
Transferir	Transferir un riesgo significa reducir la probabilidad del riesgo transfiriendo la responsabilidad, la administración y gestión del mismo a otra parte. Ejemplos de esta respuesta está comprando seguros y outsourcing (tercerización).
Mitigar	Mitigar el riesgo significa reducir tanto la probabilidad de ocurrencia y como la magnitud de su impacto, se deben establecer acciones y gestionarlas para mantener el riesgo en un rango aceptable por la organización.
Evitar	Evitar el riesgo significa no permitir la ejecución de actividades y/o eliminación del activo, porque no hay otra respuesta para reducir los riesgos de negocio a un nivel aceptable de una manera costo-efectiva.

Fuente: PRICE, Laura, SMITH, Abby, Managing Cultural Assets from a Business Perspective - Appendix I: The Business Risk Model, Marzo de 2000 [en línea], [consultado 15 de Febrero, 2013]. Disponible en Internet: http://www.clir.org/pubs/reports/pub90/appendix1.html

7.12. EJEMPLOS

Para el desarrollo del proceso se tuvieron en cuenta como base los siguientes activos, amenazas y vulnerabilidades.

7.12.1. Cuadro de ejemplos de activos. En el siguiente cuadro se plantean una serie de activos que pueden llegar a ser tenidos en cuenta en la selección de los mismos:

Cuadro 38. Cuadro de ejemplos de activos de Información

ACTIVO	CATEGORIA
Multimedia	Datos
Base de datos	Datos
Condigo fuente	Datos
Datos de configuración	Datos
Registro de actividad (Log)	Datos

Cuadro 38 (Continuación)

ACTIVO	CATEGORIA
Datos financieros	Datos
Contraseñas de funcionarios	Datos
Datos de contacto de empleados	Datos
Datos personales de empleados	Datos
Procesos y Procedimientos	Datos
Archivos organizacionales	Datos
Internet	Servicios
Correo electrónico	Servicios
Transferencia de archivos (FTP)	Servicios
Almacenamiento de ficheros	Servicios
Mensajería instantánea	Servicios
Sistema de nombres de dominio (DNS)	Servicios
Servicio telefónico	Servicios
Uso compartido de archivos	Servicios
Acceso a red privada virtual (VPN)	Servicios
Servicio de autenticación de usuario	Servicios
Servicios inalámbricos (WiFi)	Servicios
Servicios web	Servicios
Dynamic Host Configuration Protocol (DHCP)	Servicios
Browser	Aplicaciones
Cliente de correo electrónico	Aplicaciones
Sistema de gestión de base de datos	Aplicaciones
Antivirus	Aplicaciones
Sistema operativo	Aplicaciones
Software licenciado	Aplicaciones
Sistema de backup	Aplicaciones
Centro de datos	Infraestructura
Computador de escritorio	Infraestructura
Computador Portátil	Infraestructura
Servidor de aplicación	Infraestructura
Servidor de archivos (data)	Infraestructura
Switch	Infraestructura
Router	Infraestructura

Cuadro 38 (Continuación)

ACTIVO	CATEGORIA
Modem	Infraestructura
Firewall	Infraestructura
Medios extraíbles (usb, cd-room, disco duro)	Infraestructura
Red de cableado	Infraestructura
Cintas de Backup	Infraestructura
Servidor proxy	Infraestructura
Servidor DHCP	Infraestructura
Central telefónica	Infraestructura
Red telefónica	Infraestructura
Fuentes de alimentación	Equipamiento Auxiliar
Sistemas de alimentación ininterrumpida (UPS)	Equipamiento Auxiliar
Equipos de climatización	Equipamiento Auxiliar
Sistema contra incendio	Equipamiento Auxiliar

Fuente: MICROSOFT, Guía de administración de riesgos de seguridad, 15 Octubre 2004, [en línea], [consultado 15 de Febrero, 2013]. Disponible en Internet: http://www.microsoft.com/spain/technet/recursos/articulos/srsgch00.mspx

7.12.2. Cuadro de ejemplos de amenazas. En el siguiente cuadro se plantean una serie de amenazas que pueden llegar a ser tenidas en cuenta en la selección de las mismas:

Cuadro 39. Cuadro de ejemplos de amenazas informáticas

AMENAZAS	CATEGORÍA
Acceso no autorizado al centro de datos	Cumplimiento
Incumplimiento en el mantenimiento/ chequeo del sistema de información	Cumplimiento
Uso no autorizado del equipo informático	Cumplimiento
Uso de software sin licencia	Cumplimiento
Uso de software prohibido	Cumplimiento
Uso de software infectado por malware	Cumplimiento
Descargas de malware con/sin intención	Cumplimiento
Creación de cuentas de usuario sin autorización	Cumplimiento
Hurto de documentos	Cumplimiento
Hurto de equipos informáticos	Cumplimiento

Cuadro 39 (Continuación)

AMENAZAS	CATEGORÍA
Destrucción de información	Cumplimiento
Divulgación de información	Cumplimiento
Fugas de información	Cumplimiento
Hurto de información	Fraude Interno/Externo
Espionaje remoto	Fraude Interno/Externo
Abuso de privilegios / derechos	Fraude Interno/Externo
Falsificación de privilegios / derechos	Fraude Interno/Externo
Inserción/Alteración accidental de información	Fraude Interno/Externo
Inserción/Alteración de información incorrecta	Fraude Interno/Externo
Suplantación de identidad del usuario	Fraude Interno/Externo
Uso no previsto de recursos del sistema	Fraude Interno/Externo
Repudio	Fraude Interno/Externo
Difusión de software dañino	Fraude Interno/Externo
Acceso no autorizado al sistema	Fraude Interno/Externo
Accesos forzados al sistema (Intrusión)	Fraude Interno/Externo
Ingeniería social	Fraude Interno/Externo
Manipulación con software	Fraude Interno/Externo
Inyección de código mal intencionado	Fraude Interno/Externo
Sabotaje al sistema	Fraude Interno/Externo
Interceptación de tráfico en la red	Fraude Interno/Externo
Análisis de tráfico de la red	Fraude Interno/Externo

Cuadro 39 (Continuación)

AMENAZAS	CATEGORÍA
Interrupción de la red	Interrupción y Fallas del Sistema
Denegación de servicio	Interrupción y Fallas del Sistema
Falla suministro eléctrico	Interrupción y Fallas del Sistema
Falla de servicios de comunicaciones	Interrupción y Fallas del Sistema
Falla del equipo informático	Interrupción y Fallas del Sistema
Caída del sistema por agotamiento de recursos	Interrupción y Fallas del Sistema
Saturación del sistema de información	Interrupción y Fallas del Sistema
Mal funcionamiento de software	Interrupción y Fallas del Sistema
Errores de hardware	Interrupción y Fallas del Sistema
Errores de software	Interrupción y Fallas del Sistema
Errores de administrador	Interrupción y Fallas del Sistema
Errores de los funcionarios	Interrupción y Fallas del Sistema
Errores de configuración	Interrupción y Fallas del Sistema
Errores de encaminamiento de mensajes	Interrupción y Fallas del Sistema
Errores de secuencia de mensajes	Interrupción y Fallas del Sistema
Degradación de los soportes de almacenamiento de información	Soporte y Entrega del Servicio
Errores de actualización y/o mantenimiento de software	Soporte y Entrega del Servicio
Errores de actualización y/o mantenimiento de equipos (hardware)	Soporte y Entrega del Servicio

Fuente: MICROSOFT, Guía de administración de riesgos de seguridad, 15 Octubre 2004, [en línea], [consultado 15 de Febrero, 2013]. Disponible en Internet: http://www.microsoft.com/spain/technet/recursos/articulos/srsgch00.mspx

7.12.3. Cuadro de ejemplos de vulnerabilidades. En el siguiente cuadro se plantean una serie de vulnerabilidades que pueden llegar a ser tenidas en cuenta en la selección de las mismas:

Cuadro 40. Cuadro de ejemplos de vulnerabilidades informáticas

VULNERABILIDADES
Tablas de contraseñas sin protección
Gestión deficiente de las contraseñas
Habilitación de servicio innecesarios
Software nuevo
Falta de copias de respaldo
Falta de protección física en puertas
Trafico sensible sin protección
Conexión deficiente de los cables
Falta de identificación y autentificación de emisor y receptor
Transferencia de contraseñas autorizadas
Conexiones de red pública sin protección
Falta de mecanismos de monitoreo de actividades
Falta de políticas para el uso correcto de los medios informáticos
Falta de conciencia acerca de la seguridad
Red energética inestable
Falta de procedimientos
Falta de asignación de responsabilidades en la seguridad de la información
Falta de planes de continuidad
Falta de políticas sobre el uso de recursos informáticos
Falta de procesos disciplinarios referentes a los incidentes de seguridad de la información
Falta de políticas sobre el uso de computadores portátiles
Falta de revisiones regulares por parte de la gerencia
Falta de revisiones de hardware
Falta de revisiones de software
Sistemas contra incendios insuficientes
Software antivirus obsoleto
Protocolo innecesario habilitado

Fuente ISO 27005: Tecnologia de la información, Técnicas de seguridad - Gestión del riesgo de seguridad de la información, Anexo D: Vulnerabilidades y métodos para la evaluación de la vulnerabilidad ISO/IEC, 2011.

8. METODOLOGÍA DE LA INVESTIGACIÓN

La metodología para el desarrollo y seguimiento de este proyecto es Agile Unified Process (AUP).

AUP es una adaptación de UP (marco de desarrollo software iterativo e incremental), formalizada por Scott Ambler. AUP se preocupa especialmente de la gestión de riesgos. Propone que aquellos elementos con alto riesgo obtengan prioridad en el proceso de desarrollo y sean abordados en etapas tempranas del mismo. Para ello, se crean y mantienen listas identificando los riesgos desde etapas iniciales del proyecto. Especialmente relevante en este sentido es el desarrollo de prototipos ejecutables durante la base de elaboración del producto, donde se demuestre la validez de la arquitectura para los requisitos clave del producto y que determinan los riesgos técnicos.

En AUP se establecen cuatro fases que transcurren de manera consecutiva y que acaban con hitos claros alcanzados:

- **Concepción:** El objetivo de esta fase es obtener una comprensión común cliente-equipo de desarrollo del alcance del nuevo sistema y definir una o varias arquitecturas candidatas para el mismo.

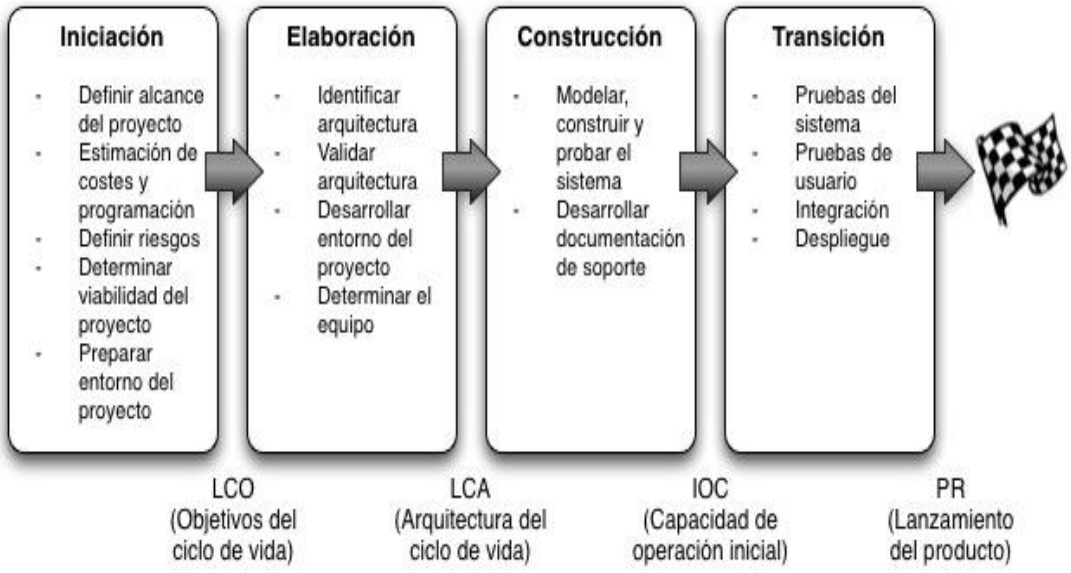
- **Elaboración:** El objetivo es que el equipo de desarrollo profundice en la comprensión de los requisitos del sistema y en validar la arquitectura.

- **Construcción:** Durante la fase de construcción el sistema es desarrollado y probado al completo en el ambiente de desarrollo.

- **Transición:** el sistema se lleva a los entornos de preproducción donde se somete a pruebas de validación y aceptación y finalmente se despliega en los sistemas de producción[27].

[27] Agile UP, AESIS – Software para soluciones empresariales, [en línea], [consultado 04 de Noviembre, 2012]. Disponible en Internet: http://www.aesist.com/metodologias/aguile-up

Figura 23. Esquema de las fases del proceso unificado ágil (AUP)



Fuente: Agile UP, AESIS – Software para soluciones empresariales, [en línea], [consultado 04 de Noviembre, 2012]. Disponible en Internet: http://www.aesist.com/metodologias/aguile-up

Las fases a contemplar para el desarrollo de este proyecto son:

Fase de Concepción

- Identificar y analizar los requerimientos del proyecto del Departamento Administrativo de las TIC de la Gobernación del Valle.
- Conocer el modelo de negocio del Departamento Administrativo de las TIC.
- Definir el alcance del proyecto.
- Recopilar documentos de seguridad de la información presentes en el Departamento Administrativo de las TIC.
- Estimación de costos y cronograma del proyecto.
- Asegurar el compromiso de la Dirección con el proyecto.

Fase de Elaboración

- Planificación del proyecto.
- Análisis de riesgos asociados al entorno del proyecto.
- Definir una metodología para la clasificación de los riesgos asociados a los activos del Departamento Administrativo de las TIC.
- Llevar a cabo la gestión de activos del Departamento Administrativo de las TIC.
- Definir activos a ser protegidos del Departamento Administrativo de las TIC.
- Identificar y evaluar las amenazas y vulnerabilidades de los activos.
- Calcular el valor del riesgo asociado a cada activo.

Fase de Construcción

- Identificar y evaluar alternativas posibles para el tratamiento de los riesgos.
- Establecer políticas y procedimientos referentes a la seguridad de la información del Departamento Administrativo de las TIC.
- Seleccionar los controles correctos que permitan al Departamento Administrativo de las TIC reducir el riesgo a un nivel aceptable.
- Generar la documentación pertinente referente a la seguridad de la información del Departamento Administrativo de las TIC.
- Informar y concienciar a los funcionarios del Departamento Administrativo de las TIC frente a la importancia del cumplimiento de políticas y procedimientos de la Seguridad de la Información.

Fase de Transición

- Entregar el proyecto estandarización de política y controles de seguridad de la información para el proceso gestionar la seguridad informática y la continuidad de las soluciones de TIC" con la documentación pertinente.

9. RESULTADOS

Teniendo en cuenta el análisis realizado es indispensable tener en cuenta una serie de medidas y políticas que permitan gestionar de manera adecuada la seguridad de la información en el Departamento Administrativo de TIC de la Gobernación del Valle del Cauca.

9.1. RECOMENDACIONES A PARTIR DEL ANÁLISIS

Basándose en el análisis realizado, los controles seleccionados de la norma ISO/IEC 27002 (Presente en el inciso de Anexos con el nombre de "Anexo E. Controles de la ISO 27002 seleccionados"), los resultados obtenidos a partir del software Microsoft Security Assessment Tool y los conocimientos del autor, se recomienda tener en cuenta los siguientes aspectos para complementar la seguridad de la información en el Departamento Administrativo de las TIC:

- ✓ Proporcionar a los jefes y funcionarios formación en materia de seguridad de la información, teniendo en cuenta que debe ser un proceso permanente ya que cada vez hay nuevas personas vinculadas a la Gobernación del Valle del Cauca.

- ✓ Crear y establecer las diferentes políticas que permitan garantizar las características de la información (disponibilidad, integridad, confidencialidad). (Basarse en el modelo estándar de políticas planteado en el numeral 9.13)

- ✓ Estar informando de manera activa a todos los jefes, funcionarios y usuarios de las políticas y mecanismos que deben cumplir y utilizar para proteger los activos de información de la Gobernación del Valle del Cauca.

- ✓ Establecer y aplicar correctivos o sanciones para las "violaciones" en el ámbito de la seguridad de la información.

- ✓ Estar en continua actualización de las diferentes políticas de seguridad de la información, con el fin de mantenerlas y mejorarlas.

- ✓ Estar en continua supervisión sobre las medidas tomadas, para verificar que si se están cumpliendo de manera acorde a lo estipulado.

- ✓ Establecer canales de comunicación abiertos con los diferentes funcionarios vinculados a la Gobernación del Valle del Cauca para conocer posibles fallas en la seguridad de la información y de esta manera tomar las medidas pertinentes.

- ✓ Realizar auditorías internas con el fin de reunir aportes para mejorar la seguridad de la información.

- ✓ Llevar el registro de los posibles incidentes que afecten la seguridad de la información, con sus respectivas acciones tomadas.

- ✓ Llevar el registro de las acciones de mejora que sean planteadas.

- ✓ Realizar reuniones periódicas con las personas encargadas de la seguridad de la información y la alta gerencia, para conocer resultados y de igual manera establecer posibles cambios que mejoren el aspecto de la seguridad de la información.

- ✓ Establecer medidas para controlar el SPAM en los correos electrónicos.

- ✓ Establecer políticas para el uso de antivirus de usuario final. (Basarse en el modelo estándar de políticas planteado en el numeral 9.13)

- ✓ Establecer políticas para el uso de VPNs para determinar los métodos de autenticación adecuados para el control del acceso remoto de los funcionarios.
- ✓ Establecer políticas para la protección de los recursos de informática móvil y las telecomunicaciones. (Basarse en el modelo estándar de políticas planteado en el numeral 9.13)

- ✓ Establecer políticas para el uso de las redes inalámbricas (Wi-Fi) internas a la Gobernación del Valle del Cauca y externas. (Basarse en el modelo estándar de políticas planteado en el numeral 9.13)

- ✓ Establecer parámetros de seguridad en las redes inalámbricas (Wi-Fi) de la Gobernación del Valle del Cauca, las cuales permitan controlar el acceso a dichas redes por medio de autenticación y cifrado WPA para evitar que el tráfico de la red inalámbrica sea leído como texto sin formato.

- ✓ Establecer criterios de aceptación para nuevos sistemas de información, actualizaciones y versiones nuevas, con el fin de que estos sistemas no afecten la seguridad de la información de la Gobernación del Valle del Cauca.

- ✓ Obtener el licenciamiento comercial necesario para poder establecer conexión a través de las VPN, que permita a los funcionarios del exterior trabajar como si estuvieran en la misma red local, garantizando un entorno de carácter confidencial y privado.

- ✓ Obtener una mejor solución para bloquear el acceso no autorizado a la red y de igual manera controlar el flujo de una red a otra, permitiendo solamente el tráfico necesario. (Firewall)

- ✓ Obtener una solución para supervisar el acceso a las bases de datos, de igual manera que permita identificar posibles anomalías y las proteja contra ataques internos y externos, además de garantizar que los datos de entrada sean correctos y apropiados. (Data bases Firewall)

- ✓ Obtener una solución de seguridad para proteger contra ataques internos y externos las aplicaciones web, además de garantizar que los datos de entrada sean correctos y apropiados. (Web application Firewall)

- ✓ Obtener una solución que sea capaz de alivianar las cargas de las aplicaciones web, con el fin de optimizar el performance (velocidad/resultado) de dichas aplicaciones.

- ✓ Obtener una solución para asegurar la disponibilidad de los servicios, evitando de esta manera la denegación de servicio. (DDoS protector appliance)

- ✓ Implementar un canal de redundancia para el servicio de internet, con el fin de asegurar la disponibilidad del servicio en caso de que se vea comprometido el canal principal.

- ✓ Obtener el licenciamiento comercial necesario para los antivirus de los equipos informáticos de escritorio para garantizar detección y/o eliminar malwares. Es de vital importancia que no se espere a que las licencias expiren para luego adquirirlas y se debe procurar tener la base de firmas actualizada chequeándola por lo menos una vez por semana.

- ✓ Actualizar los sistemas de alimentación ininterrumpida (UPS), con el fin de proteger los equipos informáticos contra fallos en el suministro de energía.

- ✓ Establecer políticas de escritorios limpios para evitar que los documentos impresos que contengan información confidencial sean accedidos por personas sin autorización.

- ✓ Generar un proyecto de actualización equipos los equipos informáticos obsoletos que llevan un tiempo considerable operando los sistemas de información, ya que pueden conllevar a fallas técnicas que afecten la continuidad del negocio.

- ✓ Actualizar los sistemas de Backup para realizar las copias de seguridad de toda la información esencial del negocio y del software, se deberá probar con

regularidad el proceso de recuperación de datos para asegurar que las copias de seguridad funcionan óptimamente.

- ✓ Las copias de seguridad realizadas a los servidores deben ser almacenadas en un lugar distinto a las instalaciones de la Gobernación del Valle del Cauca.

- ✓ Establecer un proceso para deshabilitar a tiempo las cuentas del personal que ya no está vinculado a la organización para garantizar que no se produzcan accesos no autorizados y además generar espacio para el ingreso de nuevas cuentas.

- ✓ Compromiso adecuado de la dirección en los temas relacionados con seguridad de la información, ya que los sistemas de información son de vital importancia para la Gobernación del Valle del Cauca.

- ✓ Adecuado seguimiento y monitoreo de los controles para garantizar que se está cumpliendo con las medidas establecidas y de esta manera garantizar la seguridad de la información en la Gobernación del Valle del Cauca.

9.2. POLÍTICAS ESTABLECIDAS

A continuación se presentan una serie de política establecidas para el Departamento Administrativo de las TIC, se debe tener en cuenta que la dirección debe determinar quién revisa que se esté cumpliendo, el momento que entra a ser efectiva y además cada cuanto se examinará la política con el fin de identificar posibles mejoras.

Las políticas son las siguientes:

9.2.1. Políticas de administración de credenciales de acceso. Las contraseñas o credenciales de acceso son utilizadas para autentificar el acceso a diferentes recursos, el uso indebido de las contraseñas podría llegar a causar impactos negativos para la organización.

Esta política de administración de credenciales de acceso provisto para la Gobernación del Valle del Cauca tiene la intención de asegurar el acceso a los sistemas de información de la organización.

Objetivo y propósito:

Definir políticas que permitan la correcta selección y uso de contraseñas, para asegurar los sistemas de información de la Gobernación del Valle del Cauca.

Alcance:

La política de administración de credenciales de acceso aplica para todos los funcionarios, contratistas y/o empleados temporales que usen los sistemas de información de la Gobernación del Valle del Cauca.

Políticas para las contraseñas de usuario final:

Toda persona que deba acceder a los sistemas de información de la Gobernación del Valle del Cauca, debe obtener la autorización para generar su respectiva credencial de acceso (usuario y contraseña).

- ✓ Cada usuario debe tener su propia cuenta de acceso a los sistemas de información.

- ✓ Si la cuenta no es usada debe encontrarse deshabilitada.

- ✓ Cada cuenta debe de estar asociada a una contraseña.

- ✓ Las contraseñas deben mantenerse privadas y confidenciales en todo momento.

- ✓ Las cuentas que no sean utilizadas por un periodo de 60 días deben ser bloqueadas y se debe realizar la respectiva investigación para su eliminación.

- ✓ Una contraseña valida no debe ser menor a 8 caracteres.

- ✓ Una contraseña valida debe cumplir con un mínimo de 3 o 4 reglas de complejidad, las cuales son las siguientes:
- La contraseña debe contener caracteres mayúsculos (A – Z)
- La contraseña debe tener caracteres minúsculos (a – z)
- La contraseña debe contener números (0 – 9)
- La contraseña debe contener caracteres especiales (Ejemplo: @, #, $, %, etc.)

- ✓ La contraseña tiene validez de # días y luego debe cambiarse.

- ✓ La contraseña no se puede re utilizar por un plazo de un año.

- ✓ Las contraseñas no pueden ser escritas en ningún documento.

- ✓ Las contraseñas no pueden ser almacenadas en ningún tipo de dispositivo (celular, tablet, computador, etc.)

- ✓ Las contraseñas no deben ser las mismas entre sistemas y aplicaciones.

- ✓ No se deben utilizar contraseñas que puedan adivinarse fácilmente (Ejemplo: nombres, meses del año, nombre de usuario de red, etc.)

- ✓ No utilice palabras en idiomas extranjeros — Los programas de descifrado de contraseñas a menudo verifican contra listas de palabras que abarcan diccionarios de muchos idiomas. No es seguro confiarse en un idioma extranjero para asegurar una contraseña.

- ✓ Los usuarios son forzados a cambiar su contraseña en el primer acceso al sistema.

- ✓ Cuide que nadie observe cuando escribe su clave.

- ✓ No observe a otros mientras escriben sus contraseñas.

- ✓ No pida las contraseñas de otra persona.

- ✓ No habilite la opción de “recordar claves” en los programas que utilice.

- ✓ No envíe su clave por correo electrónico ni la mencione en una conversación.

Consecuencias de la mala administración credenciales de acceso:

El uso indebido de credenciales de acceso permitirá que personas no autorizadas puedan acceder a los sistemas de información de la Gobernación del Valle del Cauca, afectando así la confidencialidad, disponibilidad y/o integridad de la información.

9.2.2. Políticas de software licenciado. El software licenciado es un producto de software que se caracteriza por ser comercializado con ciertos términos de uso, establecidas por el fabricante.

Esta política de software licenciado para la Gobernación del Valle del Cauca tiene la intención de asegurar que las personas que tienen acceso a los medios informáticos se adhieran a las políticas de licenciamiento y acuerdos de derecho de autor establecidos por el fabricante del software, cualquier violación al

licenciamiento de software expone a la Gobernación del Valle del Cauca a severas penalizaciones.

Objetivo y propósito:

Definir políticas que permitan cumplir con los términos de licenciamiento de software, permitiendo de esta manera asegurar los sistemas de información de la Gobernación del Valle del Cauca y evitando posibles penalizaciones.

Alcance:

La política de software licenciado aplica para todos los funcionarios, contratistas y/o empleados temporales que usen sistemas informáticos de la Gobernación del Valle del Cauca.

Políticas para el uso de software:

Únicamente software totalmente aprobado y con licencia puede ser utilizado en los equipos informáticos de la Gobernación del Valle del Cauca, para prevenir problemas de tipo legal y asegurar el correcto funcionamiento de los equipos informáticos, se debe cumplir con la política de software licenciado.

- ✓ El usuario final no se encuentra autorizado para instalar software en los equipos informáticos, la instalación debe software debe ser programada por el "Departamento Administrativo de las TIC" de la Gobernación del Valle del Cauca.

- ✓ Todo requerimiento de software por parte de los usuarios finales debe ser informado a "Departamento Administrativo de las TIC" de la Gobernación del Valle del Cauca, para proceder a obtener el licenciamiento correspondiente para su instalación.

- ✓ El "Departamento Administrativo de las TIC" de la Gobernación del Valle del Cauca se encuentra en capacidad de realizar monitoreos de control en los equipos informáticos para evitar la ejecución de software no licenciado y/o no aprobado.

- ✓ En caso de ser necesaria una desinstalación y/o actualización de software, el usuario final debe solicitarlo al "Departamento Administrativo de las TIC" de la Gobernación del Valle del Cauca.

Consecuencias del uso de software no licenciado:

- ✓ Penalizaciones para la Gobernación del Valle del Cauca.

- ✓ Al instalar software de dudosa procedencia y/o no licenciado, se podrían presentar diferentes anomalías en los equipos informáticos pudiéndose tratar de malwares (virus, gusanos, troyanos, adware, etc…) que afectaran el desempeño óptimo de estos.

- ✓ El software no licenciado no permite ser actualizarlo, al no poder actualizar el software permite que las aplicaciones mantengan sus vulnerabilidades por años, afectando así la seguridad de los sistemas de información.

- ✓ Degradación del rendimiento de la aplicación (software).

9.2.3. Políticas para el uso aceptable del internet. El acceso a internet debe ser utilizado con propósitos autorizados o con el destino por el que fue provisto, el uso indebido de internet no solo lleva a la distracción de los funcionarios en sus horas laborales o a la posibilidad de ser contagiados por algún tipo de malware (virus), sino que también degradan la conexión al servicio, lo cual conlleva a la lentitud de accesos debido a la saturación, incluso a la imposibilidad de conexión a determinada web o servicio necesario para la Gobernación del Valle del Cauca.

Estas políticas definen el uso aceptable del internet provisto para la Gobernación del Valle del Cauca con la intención de asegurar la calidad del servicio.

Objetivo y propósito:

Definir políticas que aseguren el buen funcionamiento del acceso a internet, para facilitar las labores de los funcionarios de la Gobernación del Valle del Cauca.

Alcance:

Las políticas para el uso del internet aplican para todos los funcionarios, contratistas, usuarios, empleados temporales y terceros que usen los equipos informáticos de la Gobernación del Valle del Cauca para acceder a Internet.

Uso de internet:

Privilegios: Se determinaran usuarios con privilegios a más alto nivel para la navegación en internet. La cuenta de usuario con privilegios solo debe ser utilizada por la persona encargada, sin importar la circunstancia, está prohibido compartir o revelar la contraseña a otros usuarios.

Políticas para el uso aceptable del internet:

Internet es una herramienta que debe ser utilizada estrictamente para las funciones laborales y no con otros fines, para asegurar el correcto uso, será monitoreado y controlado por el Departamento Administrativo de las TIC.

- ✓ El acceso a internet en horas laborales es de uso solo laboral y no personal, con el fin de no saturar el ancho de banda y así poder hacer buen uso del servicio.

- ✓ No se permite el ingreso a páginas web con cualquier tipo de transmisión vía Internet (Escuchar músicas, ver vídeos, tv en vivo, etc.)

- ✓ No se permite el uso del denominado "CHAT" en ningún horario (Página Web, Messenger, etc.)

- ✓ No se permite descargar ningún programa (software), sin la debida autorización de la secretaria TIC, tales como: Shareware, software de evaluación, etc.

- ✓ No se permite descargar archivos de música (MP3, WAV, etc.), ya que estos no poseen licencia para su uso en la Gobernación y pueden contener códigos maliciosos.

- ✓ No se permite descargar archivos de video (AVI, MOV, MP4, etc.), ya que estos no poseen licencia para su uso en la Gobernación y pueden contener códigos maliciosos.

- ✓ No se permite instalar ningún programa para escuchar música (MP3, RA, WAV, etc.), o emisoras de radio vía Internet. (WINAMP, REAL AUDIO, ARES, etc.)

- ✓ No se permite instalar ningún programa para ver vídeos (REAL PLAYER, MEDIA PLAYER, etc.)

- ✓ No se permite entrar a páginas web de redes sociales (Facebook, Twitter, etc.)

- ✓ No se permite habilitar, ni revisar correos electrónicos que no sean autorizados en la Gobernación del Valle del Cauca. Ya que estos correos pueden tener virus y afectar la red de la Gobernación (HOTMAIL, YAHOO, GMAIL7, etc.)

- ✓ No debe usarse el Internet para realizar llamadas o videoconferencias (SYPE, Dialpad, NET2PHONE, FREEPHONE, etc.)

- ✓ No se permite entrar a páginas web con contenido de entretenimiento.

- ✓ No se permite realizar ningún tipo de compra, venta u oferta vía internet, que no sean exclusivas de la Gobernación del Valle del Cauca y con su respectivo permiso.

- ✓ No se permite el ingreso a páginas web de juegos.

- ✓ No se permite descargar ningún tipo de juego.

- ✓ No se permite el uso de herramientas que permitan navegar por la web de manera anónima, ni herramientas que salten las medidas establecidas en el proxy del Departamento Administrativo de las TIC.

- ✓ No se permite enviar archivos de gran tamaño vía correo electrónico a compañeros de oficina, para eso existen otros medios.

- ✓ No se permite participar en la propagación de mensajes de correo electrónico encadenados o participar en esquemas piramidales o similares.

- ✓ Si se recibe un correo de origen desconocido, consulten inmediatamente con la Secretaria TIC sobre su seguridad. Bajo ningún aspecto se debe abrir o ejecutar archivos adjuntos a correos dudosos, ya que podrían contener códigos maliciosos (virus, troyanos, keyloogers, gusanos, etc).

- ✓ No se permite el uso del correo electrónico con fines personales.

- ✓ No abandone su computador, sin verificar que ha cerrado la sesión de correo, ya que cualquier acción que se realice quedará a su nombre.

- ✓ Al dirigirse a un sitio web, teclee directamente la dirección en el navegador.

- ✓ No se permite descargar o publicar material ilegal, con derechos de propiedad intelectual o material nocivo usando un recurso de la Gobernación del Valle del Cauca.

Consecuencias del mal uso del internet:

- ✓ Saturación de la red, lo que provoca interrupción del servicio o conexiones lentas debido al alto tráfico.

- ✓ Virus: Los virus informáticos son programas que se instalan de forma inadvertida en los ordenadores, realizan su función destructiva o intrusiva y pueden propagarse hacia otros ordenadores. Los medios más utilizados de propagación son:

- Correo electrónico: Pueden ser ejecutados con solo abrir y leer el correo electrónico o al descargar archivos adjuntos presentes en el mensaje.

- Las descargas: Hay muchas páginas web que dan la posibilidad de descargar archivos haciendo clic en un enlace, se abre un cuadro de diálogo para preguntarnos en qué carpeta de nuestro disco duro queremos dejar el archivo y comienza la descarga. Si el archivo que descargamos está infectado puede infectar nuestro ordenador.

✓ Filtraciones de información por parte de terceros, utilizando como medio herramientas como spyware u otras que pueden ser ejecutadas al descargar archivos en el computador.

9.2.4. Políticas para el uso de los recursos informáticos. Los recursos informáticos son los diferentes dispositivos tecnológicos que procesan información, por ende son parte vital para la Gobernación del Valle del Cauca, deben ser utilizados con el destino por el que fue provisto para cumplir con las diferentes actividades laborales.

Estas políticas definen el uso aceptable de los recursos informáticos previsto para la Gobernación del Valle del Cauca con la intención de un correcto funcionamiento de los mismos.

Objetivo y propósito:

Definir políticas que aseguren el uso adecuado de los recursos informáticos, para facilitar las labores de los funcionarios de la Gobernación del Valle del Cauca.

Alcance:

Las políticas para el uso adecuado de los recursos informáticos aplican para todos los funcionarios, contratistas, usuarios, empleados temporales y terceros que usen los equipos informáticos de la Gobernación del Valle del Cauca.

Políticas para el uso adecuado de los recursos informáticos:

Los dispositivos informáticos deben ser utilizados estrictamente para las funciones laborales, se considera uso adecuado:

✓ Evite almacenar o enviar información cuando no se esté completamente seguro que no se están violando las leyes de derechos de autor.

- ✓ Evite distribuir y/o instalar software sin licenciamiento en los equipos informáticos.

- ✓ Evite almacenar en los equipos informáticos material que no es estrictamente laboral, como por ejemplo: material pornográfico y/o ofensivo que atenten contra la dignidad de otra persona.
- ✓ No ejecutar intencionalmente software malicioso en los equipos informáticos y/o en la red de la Gobernación del Valle del Cauca.

- ✓ No forzar el acceso a los sistemas de información sobre el cual no tenga permisos o no se encuentra autorizado para hacerlo.

- ✓ Evite realizar escaneos de puertos o análisis de tráfico con el propósito de conocer vulnerabilidades de seguridad en la red de la Gobernación del Valle del Cauca, solo se encuentran autorizadas para realizar estas tareas el Coordinador de Seguridad Informática o una persona que sea delegada directamente por el Departamento Administrativo de las TIC.

- ✓ Evite realizar ataques informáticos para aprovechar las diferentes vulnerabilidades de los sistemas de información.

- ✓ Evite ejecutar monitoreo en la red con el fin de realizar interceptaciones de mensajes.

- ✓ Evite generar y distribuir contenido que no sea acorde y/o relevante para las acciones laborales de la Gobernación del Valle del Cauca.

- ✓ Mantenga distante todo tipo de líquidos y/o comida de los equipos informáticos, ya que dichos elementos podrían ocasionar daños irreversibles en los equipos.

- ✓ Evite asociar equipos informáticos externos a la red de la Gobernación del Valle del Cauca, de ser necesario se debe informar al Departamento Administrativo de las TIC para su debida autorización.

- ✓ Evite difundir información personal de los diferentes funcionarios sin su consentimiento.

- ✓ Evite utilizar equipos informáticos sin autorización y/o el que ha sido asignado a sus compañeros sin su consentimiento.

- ✓ Evite utilizar las cuentas de usuario de otro funcionario de la Gobernación del Valle del Cauca.

- ✓ Evite realizar cualquier actividad que vaya en contra de los objetivos laborales de la Gobernación del Valle del Cauca.

- ✓ Evite utilizar los sistemas de información con actividades que impacten la confidencialidad, integridad y disponibilidad de la información.

- ✓ Evite realizar cambios no autorizados en los sistemas de información.

Consecuencias del mal uso de los recursos informáticos:

- ✓ Fallas técnicas que inhabiliten el uso de determinado equipo informático.

- ✓ Fallas físicas que inhabiliten el uso de determinado equipo informático.

- ✓ Fallas en el rendimiento del equipo informático provocando lentitud en las tareas a realizar.

- ✓ Infección por malware.

9.2.5. Políticas para el uso del correo electrónico. El correo electrónico es una de las aplicaciones que más atrae usuarios dentro de la organización, ya que permite contactarlos y mantenerlos informados de manera electrónica.

Estas políticas definen el uso aceptable del correo electrónico para la Gobernación del Valle del Cauca con la intención de asegurar la calidad del servicio.

Objetivo y propósito:

Definir políticas que aseguren el buen funcionamiento del correo electrónico, para facilitar las labores de los funcionarios de la Gobernación del Valle del Cauca.

Alcance:

Las políticas para el uso del correo electrónico aplican para todos los funcionarios, contratistas y empleados temporales que estén vinculados con una cuenta de correo electrónico de la Gobernación del Valle del Cauca para acceder a Internet.

Políticas para el uso del correo electrónico:

El correo electrónico es una herramienta que debe ser utilizada estrictamente para las funciones laborales y no con otros fines, recuerde que usted es el único

responsable de la información presente en las comunicaciones enviadas y recibidas.

- ✓ Todos los mensajes de correo electrónico deben contener el nombre y apellidos del remitente y su cargo, con el fin de identificar rápidamente quien lo envía.

- ✓ Sea precavido con la información que envía por correo electrónico.

- ✓ Evite utilizar lenguaje inapropiado, sexista, obsceno, de acoso y palabras que puedan ofender al destinatario del correo electrónico.

- ✓ Cerciórese que la dirección de correo destino sea la indicada, para evitar que los correos electrónicos lleguen a personas no deseadas.

- ✓ Los funcionarios de la Gobernación del Valle no pueden emplear direcciones de correo electrónico diferentes a las cuentas oficiales para atender asuntos institucionales.

- ✓ No envié vía correo electrónico información confidencial que ponga en riesgo a los funcionarios y/o a la Gobernación del Valle del Cauca.

- ✓ No comparta sus credenciales de acceso de correo electrónico, ya que son personales e intransferibles.

- ✓ No se permite enviar archivos de gran tamaño vía correo electrónico a compañeros de oficina, para eso existen otros medios.

- ✓ En el momento de leer un correo electrónico, cerciórese de que la información confidencial que aparecen en la pantalla no sean vistos por personas no autorizadas.

- ✓ No se permite participar en la propagación de mensajes de correo electrónico encadenados o participar en esquemas piramidales o similares.

- ✓ Ejecute el antivirus antes de abrir cualquier adjunto que haya recibido por correo electrónico, para evitar cualquier software malicioso.

- ✓ Si se recibe un correo de origen desconocido, consulten inmediatamente con el Departamento Administrativo de las TIC sobre su seguridad. Bajo ningún aspecto se debe abrir o ejecutar archivos adjuntos a correos dudosos, ya que podrían contener códigos maliciosos (virus, troyanos, keyloogers, gusanos, etc).

- ✓ No se permite el uso del correo electrónico con fines personales.

- ✓ No abandone su computador, sin verificar que ha cerrado la sesión de correo, ya que cualquier acción que se realice quedará a su nombre.

- ✓ El funcionario encargado de la cuenta de correo electrónico debe encargarse de gestionar su cuenta, eliminando correos que no tengan relevancia para así asegurar disponibilidad del buzón de mensajes.

Consecuencias del mal uso del correo electrónico:

- ✓ Virus: Los virus informáticos son programas que se instalan de forma inadvertida en los ordenadores, realizan su función destructiva o intrusiva y pueden propagarse hacia otros ordenadores. En un correo electrónico pueden ser ejecutados con solo abrir y leer el correo electrónico o al descargar archivos adjuntos presentes en el mensaje.

- ✓ Saturación del servidor de correo electrónico con información irrelevante produciendo interrupción del servicio.

- ✓ Generación de SPAM: correo basura o mensaje basura no solicitado, no deseados o de remitente no conocido.

- ✓ Saturación de la red, lo que provoca interrupción del servicio o conexiones lentas debido al alto tráfico.

- ✓ Filtraciones de información por parte de terceros, violando la confidencialidad de la información.

10. CONCLUSIONES

- ✓ Se debe tener en cuenta que para la correcta gestión de la seguridad de la información no es suficiente con tener diferentes dispositivos informáticos como firewalls, antivirus, dispositivos antispam, etc., va más allá de esto, se debe también tener en cuenta un correcto desempeño de los procesos y una correcta formación y concientización del personal que se encuentra dentro de la organización, ya que en últimas son los encargados de manipular la información vital del negocio y son la pieza fundamental para una correcta gestión en el ámbito de la seguridad de la información.

- ✓ La seguridad de la información es un proceso continuo que debe ser apoyado y liderado constantemente por la alta dirección para poder tener el respaldo necesario e implementar las medidas adecuadas que permitan asegurar la disponibilidad, integridad y confidencialidad de la información.

- ✓ La ISO/IEC 27002 es un estándar que brinda una guía de buenas prácticas en el aspecto de seguridad de la información, para el desarrollo de este proyecto se tuvo en cuenta la norma para obtener las recomendaciones en el ámbito de la seguridad de la información.

- ✓ En el desarrollo de este proyecto se plantearon una serie de recomendaciones y medidas que permitirán mitigar los diferentes riesgos informáticos que pueden afectar de manera negativa a los sistemas de información de la Gobernación del Valle del Cauca.

- ✓ Las políticas, estándares y procedimientos de seguridad de la información deben ser dirigidas por un líder que conozca el tema y esté dispuesto a escuchar, para que pueda guiar y aclarar las inquietudes de los funcionarios al ingresar las nuevas medidas.
- ✓ Por medio de un análisis de riesgos se logró identificar las diferentes amenazas informáticas que pueden afectar a los sistemas de información y a partir de este análisis se realizó la gestión de riesgos donde se establecieron las diferentes recomendaciones pertinentes.

- ✓ Se socializó con los funcionarios del Departamento Administrativo de las TIC, dándoles a conocer el proyecto, las diferentes medidas que se han implementado y las que próximamente se espera que sean vinculadas (La evidencia se encuentra presente en el archivo digital con nombre “Lista de Asistencia - Seguridad Informática”).

- ✓ Se debe tener en cuenta que los riesgos en el aspecto de seguridad de la información siempre van a existir, sean identificados o no con un proceso de

seguridad de la información, esto implica que deben ser gestionados de la mejor manera buscando equivalencia entre costo/beneficio.

11. RECOMENDACIONES

Teniendo en cuenta una proyección a futuro en el campo de seguridad de la información se le recomienda al Departamento Administrativo de las TIC de la Gobernación del Valle del Cauca:

- ✓ Sistematizar el proceso de seguridad de la información empleando un software especializado para el desarrollo de esta actividad, con el fin de optimizar el proceso.

- ✓ Se debe estar en constante actualización en el proceso de seguridad de la información, con el fin de optimizar el proceso y estar en mejora continua, esto debido a que diariamente se conocen nuevas amenazas que afectan los sistemas de información.

- ✓ Se debe tener en cuenta los controles expuestos en la ISO/IEC 27002 en caso de identificar nuevos riesgos referentes a la seguridad de la información para mitigarlos de manera adecuada.

- ✓ Generar campañas de información, concientización y formación para funcionarios de la Gobernación del Valle del Cauca en los aspectos de seguridad de la información.

- ✓ Para mayor confianza de que se están realizando las cosas de manera adecuada, se recomienda plantearse a futuro obtener una certificación de seguridad de la información, por ejemplo: Certificación ISO/IEC 27001 – SGSI.

- ✓ Establecer un grupo o comité de dirección que guíe el proceso de seguridad de la información.

- ✓ Es de vital importancia que se continúen las charlas de seguridad de la información para los usuarios finales, con objetivo de dar a conocer las diferentes políticas y medidas que se toman para gestionar la seguridad de la información en la Gobernación del Valle del Cauca.

BIBLIOGRAFÍA

Agile UP, AESIS – Software para soluciones empresariales, [en línea], [consultado 04 de Noviembre, 2012]. Disponible en Internet: http://www.aesist.com/metodologias/aguile-up

ALEXANDER, Alberto. Diseño de un sistema de gestión de seguridad de información Optica ISO 27001:2005, Primera Edición, Bogota: Editorial Alfaomega, 2007.

ANDRADE, Ivert, ESTRADA, Erich, RODRÍGUEZ, Debray. Evaluación e implementación de políticas de seguridad informática en la alcaldía de Santiago de Cali. Trabajo de grado Profesional en Ingeniería Electrónica. . Santiago de Cali: Universidad Autónoma de Occidente. Facultado de Ingeniería. Departamento de Electrónica, Septiembre, 2006.

AREITIO, Javier. Seguridad de la información, redes, informática y sistemas de información, España: Editorial Paraninfo, 2008.

Avantium business consulting, Gestión de riesgos (ISO 31000), 2011 [en línea], [consultado el 12 de Marzo, 2013]. Disponible en Internet: http://www.avantium.es/index.php/gestion-de-riesgos-iso-31000

CAO, Javier, Análisis y gestión de riesgos de la seguridad de los sistemas de la información, InforMAS - Revista de Ingeniería Informática del Colegio de Ingenieros en Informática de la Región de Murcia, España, 7 de Marzo de 2005, [en línea], [consultado 10 de Noviembre, 2012]. Disponible en Internet: http://www.ciimurcia.es/informas/abr05/articulos/Analisis_gestion_riesgos_seguridad_sistemas_informacion.php

Concepto de un SGSI, Instituto Nacional de Tecnologías de la Comunicación - INTECO. [en línea], [consultado 09 de Noviembre, 2012]. Disponible en Internet: http://cert.inteco.es/Formacion/SGSI/Conceptos_Basicos/Concepto_SGSI/

Controles ISO/IEC 27002:2005, ISO, [en línea], [consultado 09 de Noviembre, 2012]. Disponible en Internet: http://www.iso27000.es/download/ControlesISO27002-2005.pdf

CORREA, Ricardo, CALDANA, Daniella, LOBOS, Carlos, OLEA, Leonardo, Serie de normas ISO 27000 e ISO 31000: Implicancias para el auditor interno gubernamental, ISO, Montevideo – Uruguay, 2011, [en línea], [consultado 12 de Marzo, 2013]. Disponible en Internet:http://www.iuai.org.uy/iuai/documentos/noticias/Ricardo%20Correa%20ISO%2027000%20Y%2031000.pdf

ESPAÑA. MAGERIT versión 3, Portal de Administración Electrónica, [en línea], [consultado 09 de Noviembre, 2012]. Disponible en Internet: http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_General&langPae=es&iniciativa=184

ESPAÑA. Metodología de análisis y gestión de Riesgos de los sistemas de información – II Catalogo de Elementos, MAGERIT- Versión 2, Ministerio de administraciones públicas, Madrid, 20 de Junio, 2006.

GÓMEZ, Álvaro, Enciclopedia de la Seguridad Informática, Primera edición, Mexico: Editorial Alfaomega, 2007.

HERNANDEZ RUIZ, Miguel Ángel, Pinceladas sobre ISO 27005, 4 Octubre 2010, [en línea], [consultado 12 de Marzo, 2013]. Disponible en Internet: http://www.27000.org/iso-27005.htm

International Register of ISMS Certificates, ISMS International User Group, [en línea], [consultado 06 de Noviembre, 2012]. Disponible en Internet: http://www.iso27001certificates.com/

ISO 27005: Tecnologia de la información, Técnicas de seguridad - Gestión del riesgo de seguridad de la información, ISO/IEC, 2011.

KOSUTIC, Dejan, Controles del Anexo A de la norma ISO 27001, 20 de octubre de 2010, [en línea], [consultado 08 de Noviembre, 2012]. Disponible en Internet: http://blog.iso27001standard.com/es/tag/anexo-a/

La Norma ISO 27001 y La Gestión Documental fundamentales en la Implementación, AyC Ltda, Bogotá, 10 de enero de 2012, [en línea], [consultado 03 de Noviembre, 2012]. Disponible en Internet: http://www.aycltda.com.co/wp-content/uploads/2012/01/Modelo-PHVA-SGSI.jpg

MASSELLI, Carlos, CAVALLER, Daniel, "Seguridad, estandarización, objetivos de control y su cuantificación económica para el sistema transaccional de gestión presupuestaria GEPRE – UNCuyo, en el marco de la gestión de calidad", [en línea], [consultado el 10 de Noviembre, 2012]. Disponible en Internet: http://bdigital.uncu.edu.ar/objetos_digitales/693/Masselli_seguridad.pdf

MICROSOFT, Guía de administración de riesgos de seguridad, 15 Octubre 2004, [en línea], [consultado 15 de Febrero, 2013]. Disponible en Internet: http://www.microsoft.com/spain/technet/recursos/articulos/srsgch00.mspx

--------, Herramienta de evaluación de seguridad Microsoft (MSAT), [en línea], [consultado 12 de Marzo, 2013]. Disponible en Internet: http://technet.microsoft.com/es-es/library/cc185712.aspx

MOLINA, Lina. Modelo de seguridad para el procedimiento no. 19 del manual de procesos y procedimientos de la alcaldía de Candelaria "legalización de pago y contabilización de cuentas y contratos". Trabajo de grado Profesional Ingeniería Informática. Santiago de Cali: Universidad Autónoma de Occidente. Facultado de Ingeniería. Departamento de Operaciones y Sistemas, Febrero, 2008.

Normativa de un SGSI, Instituto Nacional de Tecnologías de la Comunicación, INTECO - España, [en línea], [consultado 09 de Noviembre, 2012]. Disponible en Internet:http://cert.inteco.es/Formacion/SGSI/Conceptos_Basicos/Normativa_SGSI

POSADA, Andrés, GÓMEZ, Sergio. Propuesta de guía de implementación de mejores prácticas en gestión de riesgos de tecnologías de información en universidades privadas. Trabajo de grado Maestría en Gestión Informática y Telecomunicaciones. Santiago de Cali: Universidad ICESI. Facultad de Ingeniería, Noviembre, 2012.

PRICE, Laura, SMITH, Abby, Managing Cultural Assets from a Business Perspective - Appendix I: The Business Risk Model, Marzo de 2000 [en línea],

[consultado 15 de Febrero, 2013]. Disponible en Internet: http://www.clir.org/pubs/reports/pub90/appendix1.html

Seguridad para el acceso a la información de las entidades del Estado, Ministerio de Tecnologías de la Información y las Comunicaciones Republica de Colombia - Gobierno en Línea, Abril 2013, [en línea], [consultado 24 de Julio, 2013]. Disponible en Internet: http://programa.gobiernoenlinea.gov.co/apc-aa-files/da4567033d075590cd3050598756222c/ResumenEjecutivo_Seguridad.pdf

Sistema de Gestión de la Seguridad de la Información, ISO, 2005 [en línea], [consultado 04 de Noviembre, 2012]. Disponible en Internet: http://www.iso27000.es/sgsi.html

The ISO 27000 Directory, Introduction To ISO 27005 (ISO27005), 2008 [en línea], [consultado el 12, Marzo, 2013]. Disponible en Internet: http://www.27000.org/iso-27005.htm

TORRECILLA, Pablo, Más sobre el proceso unificado ágil: fases y disciplinas, 7, Junio, 2012 [en línea], [consultado 10 de Noviembre, 2012]. Disponible en Internet: http://nosolopau.com/2012/06/07/mas-sobre-el-proceso-unificado-agil-fases-y-disciplinas/

ANEXOS

Anexo A. Establecimiento del Contexto

A continuación se presentan la plantilla correspondiente al establecimiento del contexto:

PERSONAS INVOLUCRADAS	
Nombre	**Rol**
Diego Mauricio Peña Bolaños José Luis Jaramillo Parra	Coordinador de Seguridad Informática (Director)
ALCANCE	
Va desde la identificación de los activos de información del Departamento Administrativo de las TIC, para posteriormente identificar y valorar los riesgos dependiendo de la amenaza, hasta la propuesta de tratamiento de los riesgos que generan mayor impacto.	
OBJETIVOS	
• Identificar los activos de información que se encuentra en el Departamento Administrativo de las TIC • Identificar y valorar los riesgos a los que se encuentran expuestos los activos de información del Departamento Administrativo de las TIC • Proporcionar recomendaciones para reducir los riesgos a los que se encuentran expuestos los activos de información del Departamento Administrativo de las TIC •Gestionar la seguridad informática en el Departamento Administrativo de las TIC	
JUSTIFICACIÓN DEL PROCESO	
Las organizaciones se encuentran expuestas a un creciente índice de riesgos informáticos, esto hace que se generen planes para el tratamiento de los mismos y así reducir el riesgo a unos niveles aceptables por la organización. Con este proyecto se busca identificar y valorar los riesgos informáticos a los que se encuentra expuesto el Departamento Administrativo de las TIC de la Gobernación del Valle, para así recomendar controles, políticas y procedimientos referentes a seguridad de la información, los cuales permitirán mitigar dichos riesgos. De esta manera también se buscara concientizar a los funcionarios del Departamento Administrativo de las TIC y prolongar la continuidad del negocio.	
APROBACIÓN	
FECHA PRESENTACIÓN	
FECHA APROBACIÓN	
NOMBRE (Jefe)	
FIRMA	
OBSERVACIONES	

Anexo B. Listado de Activos

A continuación se presentan el registro parcial de la plantilla correspondiente al listado de activos teniendo en cuenta para el análisis:

	FECHA:	20/02/2013
	NOMBRE:	Diego Mauricio Peña Bolaños
	CARGO:	Coordinador de Seguridad Informática

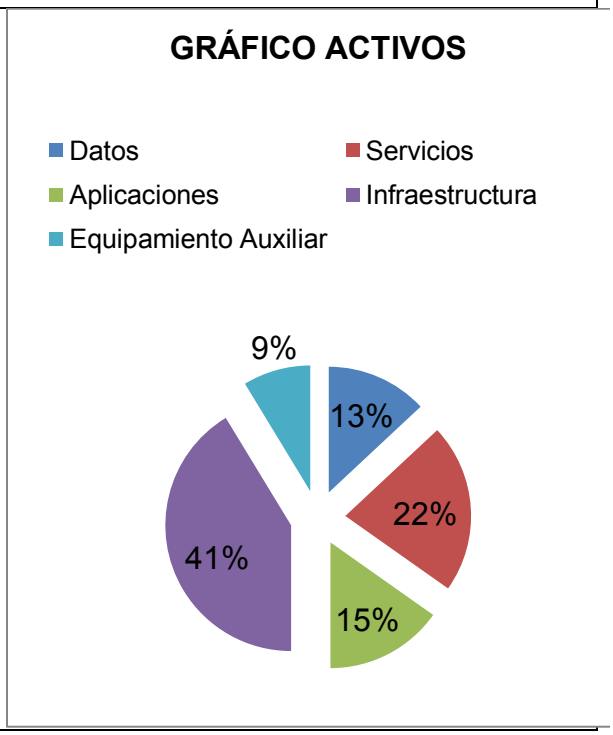
IDENTIFICADOR ACTIVO	ACTIVO	CATEGORIA	RESPONSABLE	RESPONSABLE POR LA SEGURIDAD	DESCRIPCIÓN	LOCALIZACIÓN	¿QUÉ SUCEDE SI FALTA EL ACTIVO? (IMPACTO)
1	Base de datos	Datos	Wilton Galindez	Wilton Galindez	Conjunto de datos almacenados, para su posterior uso y extracción de información	Servidor Piedechinche	Falta de disponibilidad de información
2	Código fuente	Datos	Carmen Beatriz	Carmen Beatriz	Líneas de texto en un lenguaje de programación que tienen en su estructura unas sentencias con una función específica.	Computador de Escritorio	Falta de aplicación
3	Datos de configuración	Datos	Carmen Eliza	Carmen Eliza	Contiene los pasos para el correcto funcionamiento de los dispositivos tecnológicos	Computador de Escritorio	Falta de información para configurar los dispositivos

IDENTIFICADOR ACTIVO	ACTIVO	CATEGORIA	RESPONSABLE	RESPONSABLE POR LA SEGURIDAD	DESCRIPCIÓN	LOCALIZACIÓN	¿QUÉ SUCEDE SI FALTA EL ACTIVO? (IMPACTO)
4	Registro de actividad (Log)	Datos	Diego Peña	Diego Peña	Registro oficial de eventos que ocurren sobre un dispositivo en particular, durante un rango de tiempo en particular.	Servidores	Falta de registro de funciona - miento
5	Contraseñas de funcionarios	Datos	Diego Peña	Diego Peña	Credenciales de acceso de los funcionarios para ingresar al sistema	Servidor Betania2	Los usuarios no podrían ingresar a la red

Para el análisis en el Departamento Administrativo de las TIC de la Gobernación del Valle del Cauca se tuvo en cuenta 46 activos, los cuales se encuentra clasificados de la siguiente manera: Infraestructura 41%, Servicios 22%, Aplicaciones 15%, Datos 13% y Equipamiento Auxiliar 9%.

ACTIVOS SELECCIONADOS

CATEGORÍA ACTIVO	CANTIDAD
Datos	6
Servicios	10
Aplicaciones	7
Infraestructura	19
Equipamiento Auxiliar	4
TOTAL	46



Anexo C. Análisis de Riesgos

A continuación se presentan el registro parcial de la plantilla correspondiente al análisis de riesgos realizado:

FECHA:	22/02/2013
NOMBRE:	Diego Mauricio Peña Bolaños
CARGO:	Coordinador de Seguridad Informática

IDENTIFICADOR ACTIVO	ACTIVO	IDENTIFICADOR RIESGO	DESCRIPCION AMENAZA	CATEGORÍA AMENAZA	VALORACIÓN AMENAZA	DESCRIPCION VULNERABILIDAD	VALORACIÓN VULNERABILIDAD	RELEVANCIA DEL ACTIVO (IMPACTO)			RIESGO INHERENTE	DESCRIPCIÓN CONTROL	VALORACIÓN CONTROL	RIESGO RESIDUAL	PRIORIZACIÓN
								Confidencialidad	Disponibilidad	Integridad					
1	Base de datos	R1	Inserción/Alteración de información incorrecta	Fraude Interno/Externo	5	Falta de validación de datos	5	5	5	5	25	No tiene control asociado	1	25	25
		R2	Acceso no autorizado al sistema	Fraude Interno/Externo	5	Contraseñas del sistema débiles	5	5	5	5	25	No tiene control asociado	1	25	25
		R3	Perdida de información	Fraude Interno/Externo	5	Respaldos (backups) incompletos o inexistentes	5	5	5	5	25	No tiene control asociado	1	25	25

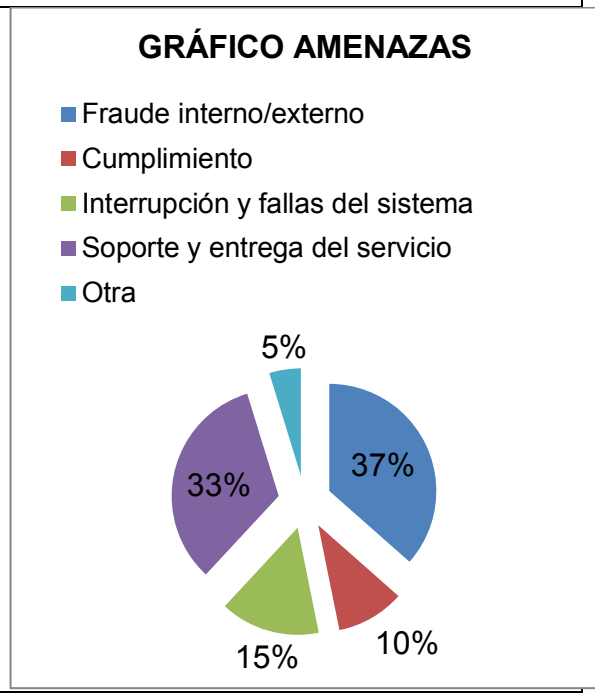
IDENTIFICADOR ACTIVO	ACTIVO	IDENTIFICADOR RIESGO	DESCRIPCION AMENAZA	CATEGORÍA AMENAZA	VALORACIÓN AMENAZA	DESCRIPCION VULNERABILIDAD	VALORACIÓN VULNERABILIDAD	Confidencialidad	Disponibilidad	Integridad	RIESGO INHERENTE	DESCRIPCIÓN CONTROL	VALORACIÓN CONTROL	RIESGO RESIDUAL	PRIORIZACIÒN
1	Base de datos	R4	Espionaje remoto	Fraude Interno/Externo	5	Falta de controles para denegar o aceptar transmisiones de una red a otra	5	5	5	5	25	No tiene control asociado	1	25	25
		R5	SQL Injection, Cross-site scripting, etc	Fraude Interno/Externo	5	Falta de validación de datos	5	5	5	5	25	No tiene control asociado	1	25	25
		R6	Desbordamientos de buffer para tomar control remoto del sistema	Fraude Interno/Externo	5	Falta de actualización de parches de la base de datos	5	5	5	5	25	No tiene control asociado	1	25	25
2	Codigo fuente	R7	Inserción de código mal intencionado	Fraude Interno/Externo	1	Falta de chequeos y/o auditorias sobre los códigos fuente	3	5	5	5	10	Revisiones y pruebas de los códigos fuente	4	2,5	2,5

IDENTIFICADOR ACTIVO	ACTIVO	IDENTIFICADOR RIESGO	DESCRIPCION AMENAZA	CATEGORÍA AMENAZA	VALORACIÓN AMENAZA	DESCRIPCION VULNERABILIDAD	VALORACIÓN VULNERABILIDAD	Confidencialidad	Disponibilidad	Integridad	RIESGO INHERENTE	DESCRIPCIÓN CONTROL	VALORACIÓN CONTROL	RIESGO RESIDUAL	PRIORIZACIÓN
2	Código fuente	R8	Errores de diseño (Programación insegura)	Otra	5	Falta de conocimientos para el desarrollo de aplicaciones seguras	4	4	1	5	15	Revisiones y pruebas de los códigos fuente	2	7,5	7,5
3	Datos de configuración	R9	Errores en los datos de configuración	Otra	4	Falta de chequeos de verificación	3	2	3	5	11	Revisiones y pruebas	3	3,8	3,8
4	Registro de actividad (Log)	R10	Saturación del sistema de información por almacenamiento de logs	Interrupción y Fallas del Sistema	5	Falta de capacidad de almacenamiento para Logs	5	1	5	1	11	Discos de almacenamiento	2	5,8	5,8

A partir de los 46 activos identificados anteriormente, se recopilaron 126 amenazas que pueden generar un impacto negativo para la organización, dichas amenazas se encuentra clasificadas de la siguiente manera: Fraude Interno/Externo 37%, Soporte y entrega del servicio 33%, Interrupción y fallas del sistema 15%, Cumplimiento 10% y Otra 5%.

AMENAZAS IDENTIFICADAS

CATEGORÍA AMENAZA	CANTIDAD
Fraude interno/externo	46
Cumplimiento	13
Interrupción y fallas del sistema	19
Soporte y entrega del servicio	42
Otra	6
TOTAL	126



Anexo D. Gestión de Riesgos

A continuación se presentan el registro parcial de la plantilla correspondiente a gestión de riesgos, donde se indican algunas medidas tomadas para los riesgos que generan mayor impacto a la organización.

IDENTIFICADOR RIESGO	RIESGO RESIDUAL	PRIORIZACIÒN	RESPONSABLE DEL TRATAMIENTO DEL RIESGO	TRATAMIENTO DEL RIESGO	ACCIONES TOMADAS	RESPONSABLE DEL MONITOREO DEL RIESGO	FECHA
R1	25	25	Diego Peña / It Security	MITIGAR	Imperva (Databases Firewall/ Web Application Firewall)	Juan Manuel Roncancio	--
R2	25	25	Diego Peña / It Security	MITIGAR	Check Point Firewall	Juan Manuel Roncancio	--
R3	25	25	Diego Peña / It Security	MITIGAR	Check Point Firewall	Juan Manuel Roncancio	--
R4	25	25	Diego Peña / It Security	MITIGAR	Check Point Firewall	Juan Manuel Roncancio	--
R5	25	25	Diego Peña / It Security	MITIGAR	Imperva (Databases Firewall/ Web Application Firewall)	Juan Manuel Roncancio	--
R6	25	25	Diego Peña / It Security	MITIGAR	Check Point Firewall	Juan Manuel Roncancio	--
R17	25	25	Diego Peña / It Security	MITIGAR	Politica de uso del servicio de internet / Firewall Check Point	Juan Manuel Roncancio	--
R32	21,6	21,6	Diego Peña / It Security	MITIGAR	Licenciamiento Comercial	Juan Manuel Roncancio	--
R43	18,3	18,3	Diego Peña / It Security	MITIGAR	Imperva (Databases Firewall/ Web Application Firewall)	Juan Manuel Roncancio	--
R44	18,3	18,3	Diego Peña / It Security	MITIGAR	Imperva (Databases Firewall/ Web Application Firewall)	Juan Manuel Roncancio	--
R60	18	18	Diego Peña	MITIGAR	Politica de software licenciado	Juan Manuel Roncancio	--

IDENTIFICADOR RIESGO	RIESGO RESIDUAL	PRIORIZACIÒN	RESPONSABLE DEL TRATAMIENTO DEL RIESGO	TRATAMIENTO DEL RIESGO	ACCIONES TOMADAS	RESPONSABLE DEL MONITOREO DEL RIESGO	FECHA
R66	15	15	Diego Peña	MITIGAR	Politicas y restricciones a Red WiFi	Juan Manuel Roncancio	--
R69	15	15	Diego Peña/ It Security	MITIGAR	DDoS Protector Appliance	Juan Manuel Roncancio	--
R79	15	15	Diego Peña/ It Security	MITIGAR	DDoS Protector Appliance	Juan Manuel Roncancio	--
R35	14,6	14,6	Diego Peña	MITIGAR	Controles de seguridad para la red WiFi	Juan Manuel Roncancio	--
R63	14	14	Diego Peña	MITIGAR	Terminación de Sesión	Juan Manuel Roncancio	--
R36	12,8	12,8	Diego Peña	MITIGAR	Controles de seguridad para la red WiFi	Juan Manuel Roncancio	--
R54	12,8	12,8	Diego Peña / It Security	MITIGAR	Acronis Backup	Juan Manuel Roncancio	--
R16	11,6	11,6	Diego Peña / EMCALI	MITIGAR	Canal Redundante del Servicio de Internet	Juan Manuel Roncancio	--
R18	11,6	11,6	Diego Peña / It Security	MITIGAR	DDoS Protector Appliance	Juan Manuel Roncancio	--
R37	11,6	11,6	Diego Peña / It Security	MITIGAR	DDoS Protector Appliance	Juan Manuel Roncancio	--
R74	11,6	11,6	Diego Peña/ It Security	MITIGAR	DDoS Protector Appliance Y SPAM(Check Point)	Juan Manuel Roncancio	--
R119	11,6	11,6	Diego Peña	MITIGAR	UPS APC	Juan Manuel Roncancio	--
R100	10,5	10,5	Diego Peña/ It Security	MITIGAR	DDoS Protector Appliance	Juan Manuel Roncancio	--
R20	9,3	9,3	----	ASUMIR	----	----	---- --

APROBACIÓN	
FECHA PRESENTACIÓN	
FECHA APROBACIÓN	
NOMBRE (Jefe de la organización)	
FIRMA	

Anexo E. Controles de la ISO 27002 seleccionados

A continuación se presentan un cuadro donde se indican algunos de los controles seleccionados de la ISO 27002, para obtener las recomendaciones y proceder a mitigar los riesgos que obtuvieron mayor impacto en su valoración:

IDENTIFICADOR ACTIVO	ACTIVO	IDENTIFICADOR RIESGO	DESCRIPCION AMENAZA	CATEGORÍA AMENAZA	DESCRIPCIÓN VULNERABILIDAD	NOMBRE DEL CONTROL – ISO 27002	NUMERO DEL CONTROL - ISO 27002	CONTROL – ISO 27002
1	Base de datos	R1	Inserción / Alteración de información incorrecta	Fraude Interno/Externo	Falta de validación de datos	Validación de datos de entrada	12.2.1	Se deberían validar los datos de entrada utilizados por las aplicaciones para garantizar que estos datos son correctos y apropiados.
		R2	Acceso no autorizado al sistema	Fraude Interno/Externo	Contraseñas del sistema débiles	Uso de Contraseñas	11.3.1	Se debería exigir a los usuarios el uso de las buenas prácticas de seguridad en la selección y uso de las contraseñas.

IDENTIFICADOR ACTIVO	ACTIVO	IDENTIFICADOR RIESGO	DESCRIPCION AMENAZA	CATEGORÍA AMENAZA	DESCRIPCIÓN VULNERABILIDAD	NOMBRE DEL CONTROL – ISO 27002	NUMERO DEL CONTROL - ISO 27002	CONTROL – ISO 27002
1	Base de datos	R3	Perdida de información	Fraude Interno/Externo	Respaldos (Backups) incompletos o inexistentes	Respaldo de la Información	10.5.1	Se deberían hacer regularmente copias de seguridad de toda la información esencial del negocio y del software, de acuerdo con la política acordada de recuperación.
						Fuga de Información	12.5.4	Se debería prevenir las posibilidades de fuga de información.
		R4	Espionaje remoto	Fraude Interno/Externo	Falta de controles para denegar o aceptar transmisiones de una red a otra	Autenticación de usuarios para conexiones externas	11.4.2	Se deberían utilizar métodos de autenticación adecuados para el control del acceso remoto de los usuarios.

IDENTIFICADOR ACTIVO	ACTIVO	IDENTIFICADOR RIESGO	DESCRIPCION AMENAZA	CATEGORÍA AMENAZA	DESCRIPCIÓN VULNERABILIDAD	NOMBRE DEL CONTROL – ISO 27002	NUMERO DEL CONTROL - ISO 27002	CONTROL – ISO 27002
1	Base de datos	R5	SQL Injection, Cross-site scripting, etc..	Fraude Interno/Externo	Falta de validación de datos	Validación de datos de entrada	12.2.1	Se deberían validar los datos de entrada utilizados por las aplicaciones para garantizar que estos datos son correctos y apropiados
		R6	Desbordamientos de buffer para tomar control remoto del sistema	Fraude Interno/Externo	Falta de actualización de parches de la base de datos	Administración de la Capacidad	10.3.1	Se debería monitorizar el uso de recursos, así como de las proyecciones de los requisitos de las capacidades adecuadas para el futuro con objeto de asegurar el funcionamiento requerido del sistema.

IDENTIFICADOR ACTIVO	ACTIVO	IDENTIFICADOR RIESGO	DESCRIPCION AMENAZA	CATEGORÍA AMENAZA	DESCRIPCIÓN VULNERABILIDAD	NOMBRE DEL CONTROL – ISO 27002	NUMERO DEL CONTROL - ISO 27002	CONTROL – ISO 27002
7	Internet	R16	Interrupción de la red	Interrupción y Fallas del Sistema	Falta del servicio de Internet por parte del proveedor	Entrega de Servicios	10.2.1	Se debería garantizar que los controles de seguridad, definiciones de servicio y niveles de entrega incluidos en el acuerdo de entrega de servicio externo sean implementados, operados y mantenidos por la parte externa.
		R17	Descargas de software con Malware	Cumplimiento	Falta de medidas para evitar descargas de software por Internet	Controles contra el código descargado en el cliente	10.4.2	La configuración debería asegurar que dicho código móvil opera de acuerdo a una política de seguridad definida y se debería evitar la ejecución de los códigos móviles no autorizados.

IDENTIFICADOR ACTIVO	ACTIVO	IDENTIFICADOR RIESGO	DESCRIPCION AMENAZA	CATEGORÍA AMENAZA	DESCRIPCIÓN VULNERABILIDAD	NOMBRE DEL CONTROL – ISO 27002	NUMERO DEL CONTROL - ISO 27002	CONTROL – ISO 27002
7	Internet	R18	Denegación de servicio	Interrupción y Fallas del Sistema	Falta de análisis y filtrado del tráfico	Seguridad en los servicios de red	10.6.2	Se deberían identificar e incluir, en cualquier acuerdo sobre servicios de red, las características de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, independientemente de que estos servicios sean provistos desde la propia organización o se contratan desde el exterior.
12	Acceso a red privada virtual (VPN)	R32	Interrupción del servicio	Interrupción y Fallas del Sistema	Falta de licenciamiento comercial	Autenticación de usuarios para conexiones externas	11.4.2	Se deberían utilizar métodos de autenticación adecuados para el control del acceso remoto de los usuarios.

IDENTIFICADOR ACTIVO	ACTIVO	IDENTIFICADOR RIESGO	DESCRIPCION AMENAZA	CATEGORÍA AMENAZA	DESCRIPCIÓN VULNERABILIDAD	NOMBRE DEL CONTROL – ISO 27002	NUMERO DEL CONTROL - ISO 27002	CONTROL – ISO 27002
12	Acceso a red privada virtual (VPN)	R32	Interrupción del servicio	Interrupción y Fallas del Sistema	Falta de licenciamiento comercial	Diagnóstico remoto y protección del puerto de configuración	11.4.4	Se debería controlar la configuración y el acceso físico y lógico a los puertos de diagnóstico.
		R32	Interrupción del servicio	Interrupción y Fallas del Sistema	Falta de licenciamiento comercial	Diagnóstico remoto y protección del puerto de configuración	11.4.4	Se debería controlar la configuración y el acceso físico y lógico a los puertos de diagnóstico. .
14	Servicios inalámbricos (Wi-Fi)	R35	Acceso a la red inalámbrica de la organización por entes externos	Cumplimiento	Conexiones de red WiFi sin protección /o sin restricción de acceso	Computación y comunicaciones móviles	11.7.1	Establecer una política formal y se deberían adoptar las medidas de seguridad adecuadas para la protección contra los riesgos derivados del uso de los recursos de informática móvil y las telecomunicaciones

IDENTIFICADOR ACTIVO	ACTIVO	IDENTIFICADOR RIESGO	DESCRIPCION AMENAZA	CATEGORÍA AMENAZA	DESCRIPCIÓN VULNERABILIDAD	NOMBRE DEL CONTROL – ISO 27002	NUMERO DEL CONTROL - ISO 27002	CONTROL – ISO 27002
14	Servicios inalámbricos (Wi-Fi)	R36	Interceptación de datos	Fraude Interno/Externo	Uso de protocolos de transmisión en texto plano (HTTP, FTP, TELNET)	Controles de Red	10.6.1	Se deberían mantener y controlar adecuadamente las redes para protegerlas de amenazas y mantener la seguridad en los sistemas y aplicaciones que utilizan las redes, incluyendo la información en tránsito