ESCUELA POLITÉCNICA NACIONAL

INGENIERÍA EN SISTEMAS INFORMÁTICOS Y DE COMPUTACIÓN

ANÁLISIS DE RIESGOS Y DISEÑO DE UN PLAN DE SEGURIDAD DE LA INFORMACIÓN PARA EL CONSEJO NACIONAL DE IGUALDAD DE DISCAPACIDADES "CONADIS".

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS INFORMÁTICOS Y DE COMPUTACIÓN

JHON ERIK GUANOLUISA HUERTAS
ejhon_nov88@hotmail.com

IVONNE FERNANDA MALDONADO SOLIZ
ennoviq_1040@hotmail.com

DIRECTORA: ING. GABRIELA LORENA SUNTAXI OÑA

Quito, Mayo 2015

DECLARACIÓN

Nosotros, Jhon Erik Guanoluisa Huertas, Ivonne Fernanda Maldonado Soliz, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Jhon Guanoluisa

Ivonne Maldonado

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Jhon Erik Guanoluisa Huertas e Ivonne Fernanda Maldonado Soliz, bajo mi supervisión.

Ing. Gabriela Suntaxi

DIRECTOR DE PROYECTO

AGRADECIMIENTOS

"Nunca es demasiado el agradecimiento, a quien nunca te abandonó en tus peores momentos." (Anónimo)

A Dios por haberme dado la vida.

Agradezco a cada uno de los ingenieros q fueron parte esencial en mi formación universitaria, no solo por ser grandes maestros sino por haberme brindado su amistad, en especial a mi tutora Ing. Gaby por todo el apoyo no solo a lo largo de la realización de este proyecto sino también cuando fue mi profesora.

A ti querido amigo, xq al igual q compartimos este trabajo, también compartimos esfuerzo, dedicación, cariño, amor y sobre todo paciencia, más tuya q mía, durante toda nuestra vida en la Poli, por estar a mi lado en cada momento dentro y fuera de las aulas, por seguir aquí pase lo q pase, por confiar incondicionalmente cuando todo parece estar perdido… si a ti mi "GORDITO" Jhon Erik por haber pasado de ser el compañero q no sabía q existía a ser mi apoyo, en ocasiones tarde pero mi apoyo al *fin*

A mis padres por darme la oportunidad de estudiar, a mis hermanos por estar a mi lado en el camino y a mis abuelit@s, mis ti@s y mis prim@s por cada día recibirme con una sonrisa y preguntar cómo me fue.

Y claro a ustedes AMIGOS(los q empezamos juntos, los q conocí durante el camino, los q acabo de conocer y los de otras facus) xq qué habría sido de mi vida estudiantil sin cada locura, cada chuma, cada ayuda, cada copia, cada juego… Me faltarían hojas para nombrarlos a todos pero agradezco en especial a ustedes mis CHUCUFUS por hacer de este camino algo más manejable, por haber olvidado la presión de la poli cuando estábamos en las canchas, simplemente con anotar un gol.

A todos quienes de una u otra manera me ayudaron no solo en este trabajo sino durante este tiempo en la Poli, pues cada persona ha puesto un granito de arena y me ha enseñado demasiado en este tiempo, en especial a ti COSITA por enseñarme a luchar aunque duela.

Amigos muchas gracias, lo logre!

ennoviQ #5

AGRADECIMIENTOS

Decir gracias es nada para demostrar eterna gratitud hacia todos quienes colaboraron para alcanzar este gran paso en mi vida.

Sin embargo debo decir GRACIAS madre, por todas las madrugadas, esfuerzos, veladas, enseñanzas, regaños y demás a lo largo de mi vida para llegar a estar en donde estoy.

Gracias padre, porque a pesar de todo has estado ahí apoyándome y brindándome tu apoyo incondicional.

Gracias a mis hermanas Verónica y Ximena, a mis hermanos Gonzalo y Byron por ser un apoyo en cada momento.

Gracias a ti Ivonne, por ser la persona que en estos últimos 5 años me ha soportado y por ser quien supo cambiarme la vida, ¡Lo logramos Gordita!.

Gracias a cada uno de mis amigos y compañeros con los que compartí aulas, porque con ustedes aprendí lo que es amistad y compañerismo.

Gracias a mis profesores por compartir sus conocimientos, estoy seguro que ustedes también aprenden cosas valiosas de nosotros como estudiantes y personas.

Por último y no menos importante, gracias DIOS por permitirme estar en la vida de cada una de las personas aquí nombradas porque sé que de cada una de ellas aprendí algo muy importante.

A todos ustedes, solo me queda decirles ¡LO LOGRE!

Jhon

DEDICATORIA

"Para triunfar en la vida, no es importante llegar primero. Para triunfar simplemente hay que llegar, levantándose cada vez que se cae en el camino." (Anónimo)

Madre a ti por ser la única q siempre ha estado a mi lado, la q sabe lo q tengo sin siquiera mirarme a los ojos, la q a pesar de sus enojos y regaños nunca dejo q me dé por vencida, la q ha secado mis lágrimas más de un centenar de veces, la q en algún momento estuvo dispuesta a cambiarme de universidad solo por hecho de no verme llorar más, a ti Jaqueline xq no me alcanzaran las palabras para decir todo lo q eres y todo lo q soy gracias a ti, por eso este gran logro te lo dedico a ti.

Pero, sería una malagradecida si no te mencionara a ti querido padre pues a pesar de tu mal humor y lo complicado q se te hace demostrarnos tus sentimientos, has sido el gran apoyo de mi madre en cada momento y sobre todo el pilar fundamental no solo de nuestro núcleo familiar sino de todos los q conformamos la familia Maldonado por eso este trabajo, junto con mis estudios te los dedico Iván y con ellos te demuestro q deje de ser una mediocre, como me lo dijiste en algún momento, q si aún me falta mucho por lograr pero q de a poco las cosas se consiguen, ahora entiendo lo q realmente quisiste decirme y por ello muchas gracias.

A ustedes hermanitos, Gabriela y Saúl, xq con sus diferencias han hecho de mi vida una experiencia loca, divertida, malhumorada pero sobre todo hermosa, este esfuerzo es por y para ustedes.

Esto también es para ustedes querida familia, abuelit@s, ti@s y prim@s, xq quizá nunca hayan entendido q es lo q realmente estudio pero eso no hizo q se alejen de mí.

Para quien mi mal humor, los gritos, malos tratos y el "así soy" no ha hecho q se aleje de mí, si Negrito Jhon Erik te dedico este logro, esta lucha, este sueño de llegar a ser ingenieros, xq a pesar de todo lo q nos ha pasado seguimos aquí.

Y a ti por ser todo lo contrario a lo q siempre tuve, por mirar la vida desde otro punto de vista, este esfuerzo también es para ti Edison, para q recuerdes q no debes rendirte y q cada caída solo sirve para darnos cuenta de lo fuertes q somos y de cuantas veces estamos dispuestos a levantarnos y continuar en la lucha.

ennoviQ #5

DEDICATORIA

“Ayer tu sonrisa se cortó para iluminar el cielo,

Ayer tu puesto en nuestra casa se quedó vacío.

Ayer tu esposa, tu hijo, tus padres, hermanos y demás

Familiares lloramos tu partida.

Ayer descansó tu alma; sentimos tu presencia…

Porque estás en nuestros corazones

Y la llama de nuestro amor perdurará por siempre”.

Anónimo

Donde sea que te encuentres todo este esfuerzo te lo dedico a ti flaco, mi mejor amigo, mi mejor compañero, mi mejor cómplice, mi mejor hermano. Te quiero hasta el infinito y más allá….!!!

Jhon

ÍNDICE DE CONTENIDOS

DECLARACIÓN 2

CERTIFICACIÓN 3

AGRADECIMIENTOS 4

AGRADECIMIENTOS 5

DEDICATORIA 6

DEDICATORIA 7

ÍNDICE DE CONTENIDOS 8

RESUMEN I

PRESENTACIÓN III

1. CAPÍTULO I – CARACTERIZACIÓN DE LA EMPRESA. 6

1.1. IDENTIFICACIÓN INSTITUCIONAL 6

1.1.1. ANTECEDENTES *6*

1.1.2. PLAN ESTRATÉGICO *9*

1.1.2.1. Misión 9

1.1.2.2. Visión 9

1.1.2.3. Objetivos 9

1.1.2.4. Funciones 10

1.1.2.5. Ejes para Políticas Públicas en Discapacidades 10

1.1.2.6. Estructura Organizacional 12

1.2. DESCRIPCIÓN DEL PROBLEMA 13

1.2.1. CENTRO DE INFORMACIÓN *13*

1.2.1.1. Funciones 13

1.2.1.2. Estructura Organizacional 14

1.2.1.3. Recursos Humanos 14

1.2.2. INFRAESTRUCTURA DE RED INFORMÁTICA *15*

1.2.2.1. Inventario de Hardware 15

1.2.2.2. Inventario de Software 16

1.2.2.3. Red 16

1.3. SELECCIÓN Y JUSTIFICACIÓN DE USO DEL ESTÁNDAR 18

1.3.1. ESTÁNDAR ISO/IEC 27001:2005 EN EL DIAGNÓSTICO DE LA SITUACIÓN ACTUAL Y DISEÑO DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN *19*

1.3.2. SELECCIÓN DE LA METODOLOGÍA PARA LA EVALUACIÓN Y ANÁLISIS DE RIESGOS *20*

1.3.2.1. MAGERIT - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. 21

1.3.2.2. OCTAVE - Operationally Critical Threat, asset and vulnerability evaluation. 21
1.3.2.3. ISO/IEC 27005 - Gestión de Riesgos de la Seguridad de la Información 22
1.4. DIAGNÓSTICO DE LA SITUACIÓN ACTUAL. 23
1.4.1. DIAGNÓSTICO BASADO EN EL ESTÁNDAR 24
1.5.1.1. Política de Seguridad 24
1.5.1.2. Organización de la Seguridad de Información 24
1.5.1.3. Gestión de Activos 25
1.5.1.4. Seguridad Ligada a los Recursos Humanos 25
1.5.1.5. Seguridad Física y del Entorno 26
1.5.1.6. Gestión de Comunicaciones y Operaciones 28
1.5.1.7. Control de Accesos 31
1.5.1.8. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información 33
1.5.1.9. Gestión de Incidentes de Seguridad de la Información 34
1.5.1.10. Gestión de Continuidad del Negocio 35
1.5.1.11. Conformidad 35
1.4.2. RESULTADO GENERAL DEL DIAGNÓSTICO 36
1.4.3. ESTADO DE CUMPLIMIENTO ACTUAL 38
1.4.3.1. Resultados del Estado de Cumplimiento Actual por Dominio. 40
2. CAPÍTULO II – EVALUACIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN. 44
2.1. ESTABLECIMIENTO DEL CONTEXTO. 44
2.1.1. ALCANCE Y LIMITES 45
2.1.2. METODOLOGÍA PARA EL ANÁLISIS DEL RIESGO 45
2.1.2.1. Metodología Cualitativa 46
2.1.2.2. Metodología Cuantitativa 46
2.1.3. CRITERIOS BÁSICOS 47
2.1.3.1. Criterios de valoración de activos 47
2.1.3.2. Criterios de probabilidad de ocurrencia de amenazas 49
2.1.3.3. Criterios de valoración de Impacto 49
2.1.3.4. Criterios de evaluación del riesgo 50
2.1.3.5. Criterios para el tratamiento del riesgo 51
2.1.3.6. Criterios de prioridad en la aplicación de controles 52
2.2. ANÁLISIS DE RIESGOS 53
2.2.1. IDENTIFICACIÓN DE RIESGOS 53
2.2.1.1. Identificación de Activos 53
2.2.1.2. Valoración de Activos 55
2.2.1.3. Identificación de Vulnerabilidades y Amenazas 56
2.2.1.4. Identificación de los Controles Existentes 60
2.2.2. ESTIMACIÓN DEL RIESGO 61
2.2.2.1. Valoración del Impacto 61

2.2.2.2. Valoración de Incidentes 62
2.3. EVALUACIÓN DE RIESGOS 63
2.3.1. OBSERVACIONES DE LA EVALUACIÓN DEL RIESGO 66
2.4. TRATAMIENTO DE RIESGOS 66
2.4.1. SELECCIÓN DE CONTROLES 67
2.4.2. OBSERVACIONES DEL TRATAMIENTO DEL RIESGO 68
3. CAPÍTULO III – DESARROLLO DE PLAN DE SEGURIDAD DE LA INFORMACIÓN 70
3.1. ALCANCE Y LÍMITES 71
3.2. ELABORACIÓN DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN 72
3.2.1. FASES Y ENTREGABLES 72
3.2.2. DESCRIPCIÓN DE ENTREGABLES 74
3.3. GUÍA DE IMPLEMENTACIÓN 98
3.4. ANÁLISIS DE IMPACTO DE LA PROPUESTA 100
3.4.1. APLICABILIDAD DE LA PROPUESTA 100
3.2.3.1. Aceptación de los funcionarios de la organización. 108
3.4.2. INVERSIÓN 110
3.2.4.1. Restricciones Económicas 110
3.2.4.2. Soluciones Económicas 111
3.2.4.3. Factibilidad Económica 111
4. CAPÍTULO IV – CONCLUSIONES Y RECOMENDACIONES 115
4.1. CONCLUSIONES 115
4.2. RECOMENDACIONES 118
REFERENCIAS BIBLIOGRÁFICAS 120
ANEXOS 123

ÍNDICE DE FIGURAS

Figura 1.1: Estructura Organizacional del CONADIS. 12
Figura 1.2: Estructura Organizacional del Centro de Información del CONADIS. 14
Figura 1.3: Topología de Red CONADIS 17
Figura 2.1: Proceso de Gestión del Riesgo. 46
Figura 3.1: Modelo PHVA de SGSI. 71
Figura 3.2: Porcentajes de Contestación por Pregunta. 109

ÍNDICE DE TABLAS

Tabla 1.1 Matriz de Ejes de Políticas. 11

Tabla 1.2: Recurso Humano del Centro de Información. 15

Tabla 1.3: Inventario de Hardware de Servidores. 15

Tabla 1.4: Comparación entre Magerit, Octave y la norma ISO/IEC 27005. 23

Tabla 1.5: Situación actual del CONADIS según la norma ISO/IEC 27001 para el dominio Seguridad Ligada a los Recursos Humanos. 37

Tabla 1.6: Lista de Cumplimiento Actual de Controles de la Norma ISO/IEC 27001 para Seguridad Física y del Entorno. 39

Tabla 1.7: Estado de Cumplimiento por Dominio. 40

Tabla 2.1: Criterios para la valoración de activos. 48

Tabla 2.2: Rango de valores para determinar el nivel de importancia de los activos. 49

Tabla 2.3: Criterios de probabilidad de ocurrencia de amenazas. 49

Tabla 2.4:Criterios de valoración de impacto. 50

Tabla 2.5: Criterios de evaluación del riesgo. 50

Tabla 2.6 Criterios de tratamiento del riesgo. 52

Tabla 2.7: Criterios de prioridad en la aplicación de controles. 52

Tabla 2.8: Activos Primarios 54

Tabla 2.9: Activos de Soporte y/o Apoyo 55

Tabla 2.10: Valoración de activos. 56

Tabla 2.11: Identificación de Vulnerabilidades según el tipo de amenaza. 58

Tabla 2.12: Identificación de Vulnerabilidades según las pruebas de penetración. 60

Tabla 2.13: Controles existentes. 61

Tabla 2.14:Ejemplo de Valoración de Impacto. 62

Tabla 2.15: Ejemplo de Valoración de Incidentes (Probabilidad de Ocurrencia). 62

Tabla 2.16: Evaluación del Riesgo. 65

Tabla 2.17: Ejemplo de Prioridad en la implementación de comtroles. 67

Tabla 2.18: Controles al activo crítico "Servidor Microsoft 2003 Server" 68

Tabla 3.1: Documentos del SGSI exigidos por la norma ISO/IEC 27001. 73

Tabla 3.2: Fases y entregables del Plan de Seguridad de la Información. 74

Tabla 3.3: Lista de Cumplimiento Esperado de Controles de la Norma ISO/IEC 27001 para Seguridad Física y del Entorno. 104

Tabla 3.4: Comparación de estado de cumplimiento actual con estado de cumplimiento esperado. 105

Tabla 3.5: Recursos económicos estimados para la implementacion del plan de seguridad de la información. 114

RESUMEN

El presente proyecto de titulación consta de cuatro capítulos, los mismos que abarcan; caracterización de la empresa, evaluación de riesgos de la seguridad de la información, desarrollo del plan de la seguridad de la información y finalmente las conclusiones y recomendaciones del proyecto.

El Capítulo I está dividido en cuatro secciones, en donde la primera muestra la identificación institucional que detalla los antecedentes para que la organización se establezca y su plan estratégico, la segunda muestra la situación actual en la que se encuentra el Consejo Nacional de Igualdad de Discapacidades y su Centro de Información tanto en estructura organizacional, recursos humanos e infraestructura de red. En la tercera sección se selecciona y justifica el uso de las normas y estándares para la realización del presente proyecto para finalmente en su última sección dar un diagnóstico de la situación actual de la organización basándose en los parámetros que dice la norma ISO/IEC 27001.

El Capítulo II evalúa los riesgos de la seguridad de la información, y para esto está dividido en cuatro secciones, la primera sección establece los criterios que se utilizan a lo largo de la evaluación del riesgo para la toma de decisiones, en la segunda sección se encuentra el análisis de riesgos como tal, en donde se identifican los activos críticos y los riesgos que afectarían a estos ante posibles amenazas y vulnerabilidades, en la tercera sección se desarrolla la evaluación de los riesgos lo que permite determinar qué hacer ante los riesgos encontrados, es decir, retenerlos (aceptarlos) o reducirlos, para finalmente en la cuarta sección enfocarse en el tratamiento de los riesgos en donde se proponen controles para los activos críticos, establecidos dentro de la norma ISO/IEC 27001 que ayudarán a mejorar la seguridad de la información.

El Capítulo III está constituido de cuatro secciones que se enfocan al desarrollo del plan de la seguridad de la información en donde la primera sección define el alcance y límites del plan, la segunda sección muestra la elaboración del plan como tal, en donde de acuerdo a la norma se debe cumplir con fases y determinar los respectivos entregables para cada una de estas, en la tercera sección se

realiza una guía de implementación que ayudará a que el Plan de Seguridad de la Información sea implementado en el caso de que las autoridades acepten su ejecución y finalmente se realiza un análisis de impacto, el mismo que determina las posibles mejoras que pudieran existir en la seguridad de la información ante la implementación de los controles propuestos.

El capítulo IV contiene las conclusiones y recomendaciones que se obtuvieron a lo largo de la elaboración del proyecto.

PRESENTACIÓN

Los avances de las Tecnologías de la Información y Comunicación (TIC) han ocasionado que los gobiernos otorguen mayor atención a la protección de sus activos de información con el fin de generar confianza en la ciudadanía, en sus propias instituciones y minimizar riesgos derivados de vulnerabilidades informáticas. [1]

La información es esencial dentro de cualquier organización y es por esta razón que es necesario que todas las instituciones realicen una apropiada gestión de riesgos, lo que les permitirá conocer las principales vulnerabilidades de los activos de información, es esta una de las razones por las que en el Ecuador la Secretaría Nacional de Administración Pública, considerando que las TIC son herramientas imprescindibles para el desempeño institucional e interinstitucional, y como respuesta a la necesidad de gestionar de forma eficiente y eficaz la seguridad de la información en las entidades públicas emitió el Acuerdo Ministerial 166, Registro Oficial Suplemento 88 de 25-sep-2013 con estado vigente, estableciendo la necesidad de aplicar normas y procedimientos que cumplan con estándares de seguridad que garanticen la confidencialidad, integridad y disponibilidad de la información [1] por lo que queda claro que todas las entidades públicas están obligadas a gestionar la seguridad de su información basándose en estándares.

El Consejo Nacional de Igualdad de Discapacidades al ser una entidad pública también debe cumplir con este acuerdo, y un Plan de Seguridad de la Información le ayudará a iniciar el cumplimiento del mismo, pues en este se define políticas para que la seguridad de la información sea gestionada de mejor manera basándose en la norma ISO/IEC 27001.

En el presente proyecto, con la ayuda de la norma ISO/IEC 27005 se realizó el análisis de riesgos del Consejo Nacional de Igualdad de Discapacidades con el fin de determinar las amenazas, vulnerabilidades y los riesgos que los activos críticos de información poseen, para poder proponer controles que se encuentran establecidos dentro de la norma ISO/IEC 27001 y así, diseñar un plan que

asegure una mejor gestión de la seguridad de la información, por tanto, la implementación, verificación, revisión y mejoras de este, quedará a criterio de la Organización y fuera del alcance de este proyecto.

1. CAPÍTULO I – CARACTERIZACIÓN DE LA EMPRESA.

El presente capitulo está enfocado en la caracterización del Consejo Nacional de Igualdad de Discapacidades, CONADIS, su estructura organizacional, la situación actual en la que se encuentra y el diagnóstico de la misma. Finalmente se justifica y selecciona las metodologías que se utilizarán en el transcurso de los siguientes capítulos.

1.1. IDENTIFICACIÓN INSTITUCIONAL.

Nombre: Consejo Nacional de Igualdad de Discapacidades CONADIS

Dirección: Avenida 10 de Agosto N37-193 entre Villalengua y Carondelet.

Teléfono: 593-2 2459243

Página web: http://www.consejodiscapacidades.gob.ec

El Consejo Nacional de Igualdad de Discapacidades, "…es una persona jurídica de derecho público, autónoma, con patrimonio y presupuesto propio…". [2]

El CONADIS tiene que cumplir y ejercer funciones y atribuciones que le asigna la ley vigente sobre discapacidades en el Ecuador dentro de un régimen administrativo y económicamente descentralizado.

1.1.1. ANTECEDENTES[1]

En el Ecuador, la población se encuentra en un valor ascendente aproximado de 14,5 millones de habitantes, por lo que la atención inicial a las personas con discapacidad se efectuó bajo criterios de caridad y beneficencia, para posteriormente irse tecnificando a partir de los años 50.

El gobierno tuve su primera intervención en temas de discapacidad en los años 40, y esto se evidenció con la creación de las primeras escuelas de educación

---

[1] Información tomada de la Agenda Nacional para La Igualdad en Discapacidades 2013-2017 y resumida por los autores.

especial, principalmente en las tres ciudades consideradas de mayor importancia, es decir, Quito, Guayaquil y Cuenca.

Para la década de los 70, existían favorables condiciones económicas lo que permitió que el sector público asumiera la responsabilidad dentro de la educación, salud y bienestar social lo que provocó la creación de organismos, como el Consejo Nacional de Rehabilitación Profesional, CONAREP, y la Unidad de Educación Especial, las cuales ayudaron y facilitaron el trabajo debido a que se emitieron normativas y reglamentaciones, entre las cuales estaba la Ley General de Educación.

En el año de 1980 se dio un paso muy importante, puesto que se creó la División Nacional de Rehabilitación del Ministerio de Salud Pública, la misma que fue la encargada de organizar e implementar servicios de medicina física y rehabilitación en las diferentes unidades médicas a lo largo de todo el Ecuador, servicio que se amplió ya que era exclusivamente para los afiliados.

Para el año de 1982 gracias a la Ley de Protección del Minusválido se creó la DINARIM (Dirección Nacional de Rehabilitación Integral del Minusválido), a la cual se le asignó la rectoría y coordinación nacional en todo el tema sobre discapacidades, reemplazando así a la antes encargada CONAREP, asignado personal suficiente y capacitado en las unidades operativas dependientes existentes hasta el momento, y así brindar toda la atención directa, necesaria y oportuna a las personas con discapacidades en diferentes aspectos, ya sea de: protección, educación especial, capacitación ocupacional e integración laboral. De igual manera se organizaron centros de rehabilitación y escuelas de educación especial dependientes del INNFA, y Organizaciones No Gubernamentales, ONG, como:

- Asociación de Niños con Retardo, ASENIR.
- Fundación de Asistencia Psicopedagógica para Niños Adolescentes y Adultos con Retardo Mental, FASINARM.
- Sociedad Ecuatoriana Pro-Rehabilitación de los Lisiados, SERLI.
- Asociación para el Desarrollo Integral del Niño Excepcional del Azuay, ADINEA.

- Fundación General Ecuatoriana, FGE.
- Fundación Hermano Miguel.
- Centro de Erradicación del Bocio Endémico y Capacitación de Minusválidos, CEBYCAM.
- Fundación Nacional de Parálisis Cerebral, FUNAPACE.
- Fundación Ecuatoriana de Olimpiadas Especiales, entre las más conocidas.

El INNFA, en 1991 con el respaldo de los Ministerios de Salud, Educación y Bienestar Social, publica el I Plan Nacional de Discapacidades.

La Ley 180 en el Registro Oficial Nº996 fue publicada el 10 de Agosto de 1992, ley que promueve la atención interinstitucional a personas con capacidades especiales enfocándose en sus derechos, y crea el Consejo Nacional de Discapacidades CONADIS, como entidad autónoma y rectora del tema en el país, con el mandato legal de dictar políticas, coordinar acciones públicas y privadas, e impulsar investigaciones sobre discapacidad.

En el 2001, las Naciones Unidas otorgó al Ecuador el premio internacional Franklin Delano Roosevelt, por haber cumplido un trabajo destacado, de carácter intersectorial e interinstitucional, siendo el primer país referente para algunos países de América Latina y el Caribe.

El CONADIS desde ese entonces ha venido cumpliendo sus funciones y siendo el ente rector de políticas en discapacidad en todos los sectores de la comunidad desarrollando acciones de prevención, atención e integración, con el fin de prevenir las discapacidades, y mejorar la calidad de vida de las personas con capacidades especiales basándose en la ejecución del I y II Plan Nacional de Discapacidades.

El 25 de septiembre de 2012, la Ley Orgánica de Discapacidad es publicada en el Registro Oficial Nº 796, el objetivo de esta ley es prevenir, detectar oportunamente, habilitar y rehabilitar cualquier tipo de discapacidad para así garantizar la plena vigencia, difusión y ejercicio de los derechos de las personas con capacidades especiales.

En la actual Constitución que fue aprobada el 2008, se planteó crear los Consejos Nacionales de Igualdad, es por esta razón que el Consejo Nacional de Discapacidades, pasó a llamarse Consejo Nacional de Igualdad de Discapacidades, CONADIS, el mismo que seguirá siendo el organismo que se encargue de velar y garantizar los derechos de las personas con capacidades especiales.

1.1.2. PLAN ESTRATÉGICO

El CONADIS, al ser un consejo, debe cumplir con la Ley de Creación de Consejos de Igualdad, razón por la cual se encuentra en un proceso de transición y al momento cuenta con un Plan Estratégico en reestructuración, es por esto que en esta sección se detalla el Plan Estratégico existente hasta el momento.

1.1.2.1. Misión[2]

"Es un organismo público y autónomo que genera políticas e información, planifica y coordina acciones con los sectores público y privado, en el ámbito de las discapacidades y canaliza recursos nacionales e internacionales en este campo." [3]

1.1.2.2. Visión[3]

"El Consejo Nacional de Discapacidades, será un organismo dinamizador y articulador de todos los sectores de la comunidad para desarrollar acciones de prevención, atención e integración, con el propósito de prevenir las discapacidades y elevar la calidad de vida de las personas con discapacidad." [3]

1.1.2.3. Objetivos[4] [4]

- Establecer las políticas, el Plan Nacional de Discapacidades y los Planes Operativos.

---

[2] Información proporcionada por el responsable del Centro de Información del CONADIS y tomada de http://www.conadis.gov.ec/mision.html
[3] Información proporcionada por el responsable del Centro de Información del CONADIS y tomada de http://www.conadis.gov.ec/vision.html
[4] Información tomada del Estatuto Orgánico- Registro Oficial. Enero 2008.

- Fortalecer y articular los subsistemas existentes involucrados en el área de las discapacidades.
- Coordinar acciones con los sectores público y privado en los ámbitos de prevención de la discapacidad; y, atención e integración de las personas con discapacidad.
- Defender jurídicamente los derechos de las personas con discapacidad.

1.1.2.4. Funciones[5] [5]

- Formular políticas nacionales relacionadas con las discapacidades
- Establecer el Plan Nacional de Discapacidades
- Defender jurídicamente los derechos de las personas con discapacidad
- Coordinar, efectuar el seguimiento y evaluar las acciones que realizan en discapacidades las entidades del sector público y privado.
- Canalizar recursos nacionales e internacionales.
- Realizar o impulsar investigaciones en el área de las discapacidades
- Vigilar el cumplimiento de la Ley y la aplicación de sanciones o quienes la incumplan.

1.1.2.5. Ejes para Políticas Públicas en Discapacidades[6]

El CONADIS ha definido doce ejes, los cuales orientan la política pública en discapacidad. Estos ejes están relacionados con temas centrales tales como: la sensibilización a la población en general sobre la aceptación de la diversidad y los derechos humanos; el poder de participar en la vida pública y política; prevención de la discapacidad; acceso de las personas con discapacidad a la salud; educación y trabajo; accesibilidad al medio físico; transporte, tecnologías de la información y comunicación; participación en actividades culturales, artísticas, deportivas y de recreación, protección y seguridad social y lucha contra la discriminación. [6]

---

[5] Información proporcionada por el responsable del Centro de Información del CONADIS y tomada de http://www.conadis.gov.ec/legislacion/ley.html

[6] Información tomada de la Agenda Nacional para La Igualdad en Discapacidades 2013-2017.

EJES DE POLÍTICAS	
EJE	**POLÍTICA**
Sensibilización	Promover el reconocimiento de los derechos de las personas con capacidades especiales, el respecto a su dignidad y su debida valoración.
Participación	Fomentar el ejercicio de los derechos sociales, civiles y políticos, así como de las libertades fundamentales de las personas con capacidades especiales.
Prevención	Promover acciones de prevención de discapacidades, su diagnóstico y atención temprana.
Salud	Fomentar en las personas con capacidades especiales el ejercicio de su derecho a la salud.
Educación	Promover a las personas con capacidades especiales en una educación inclusiva y especializada de calidad y con calidez, y de oportunidades de aprendizaje a lo largo de la vida.
Trabajo	Defender y promover el derecho al trabajo de las personas con capacidades especiales, sin discriminación, en igualdad de derechos laborales y considerando las condiciones específicas de la persona.
Accesibilidad	Asegurar el acceso de las personas con capacidades especiales al medio físico, al transporte, a la comunicación, a la información, a los bienes y servicios básicos.
Turismo, cultura, arte, deporte y recreación.	Promover a las personas con capacidades especiales el acceso y disfrute del turismo, de la cultura, del arte, del deporte y de la recreación.
Protección y seguridad social	Promover a las personas con capacidades especiales el acceso a la protección y a la seguridad social.
Legislación y justicia	Promover en las personas con capacidades especiales el acceso a la justicia, sin discriminación y en igualdad de condiciones que las demás personas.
Vida sin violencia	Prevenir, sancionar y erradicar la violencia contra personas con capacidades especiales, sus familias y cuidadores.
Políticas públicas y rendición de cuentas	Promover, garantizar y desarrollar la institucionalidad, para personas con capacidades especiales, y su rendición de cuentas.

Tabla 1.1 Matriz de Ejes de Políticas[7]. **[6]**

[7] Tabla elaborada por los autores con información de la Agenda Nacional para La Igualdad en Discapacidades 2013-2017

1.1.2.6. Estructura Organizacional

El CONADIS se encuentra estructurado de acuerdo a tres niveles jerárquicos, tal como se muestra en la *Figura 1.1.*

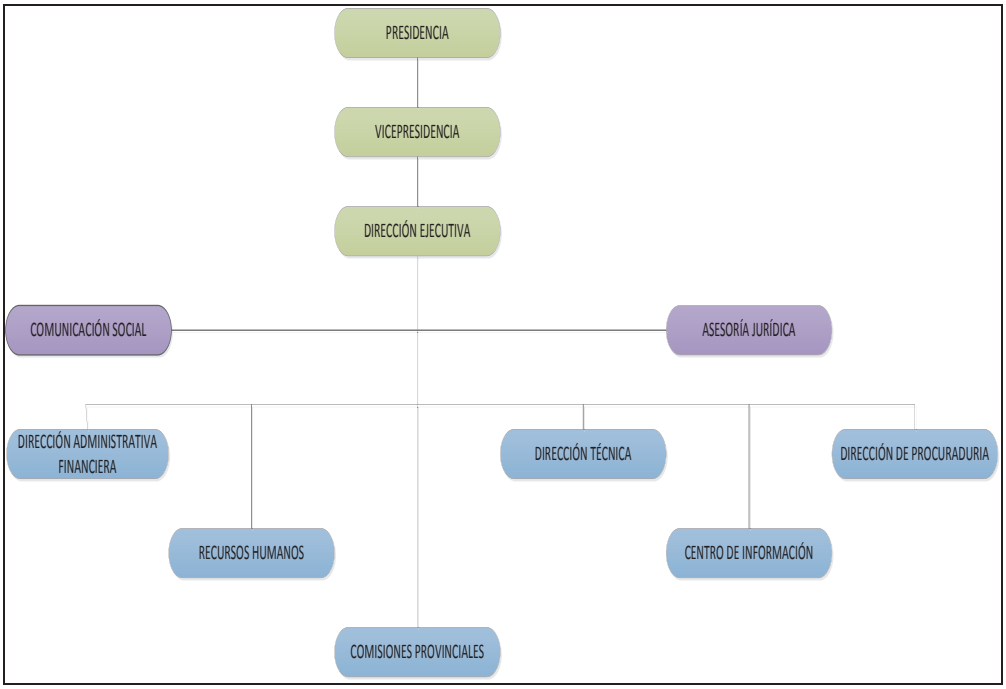

Figura 1.1: Estructura Organizacional del CONADIS[8].

Nivel Directivo: La Presidencia, Vicepresidencia y la Dirección Ejecutiva, se encuentran dentro de este nivel.

Nivel Asesor: Las área de Comunicación Social y Asesoría Jurídica, son parte de este nivel.

Nivel Operativo: En el último nivel se encuentran la Dirección Administrativa Financiera, Recursos Humanos, Dirección Técnica, Dirección de Procuraduría, Comisiones Provinciales y Centro de Información.

---

[8] Figura elaborada por los autores con información tomada del portal web del CONADIS http://www.consejodiscapacidades.gob.ec/organigrama/

1.2. DESCRIPCIÓN DEL PROBLEMA

Esta sección está dedicada a describir el problema de la seguridad de la información en el CONADIS en base a la descripción de la situación actual de la organización y de su Centro de Información, centrando el análisis en la seguridad de la información.

En los últimos años las instituciones púbicas del Ecuador han sido víctimas de una serie de incidentes de seguridad, lo que les ha conllevado no solo pérdidas económicas sino la desconfianza de los ciudadanos, esta es una de las razones por las que hoy en día estas instituciones están obligadas a cumplir con varias leyes y normativas nacionales en cuanto a seguridad de la información.

1.2.1. CENTRO DE INFORMACIÓN

Es el departamento encargado de gestionar de forma eficiente los activos de la organización de manera que administra, analiza, organiza, actualiza, alinea, gestiona e implementa todos los recursos necesarios para cumplir con este objetivo.

1.2.1.1. Funciones[9]

Las funciones que cumple el Centro de Información son:

- Regular el suministro de servicios, de tal manera que los datos y la información institucional sean procesados eficientemente.
- Emitir informes para la adquisición de nueva tecnología y presentarla para aceptación por parte de autoridades.
- Alinear y gestionar los recursos tecnológicos, brindando capacitación y apoyo técnico a usuarios y operadores de los sistemas informáticos.
- Implantar infraestructura de hardware y software con tecnología de punta logrando mayores beneficios para la organización.
- Implantar mecanismos de protección, salvaguardia y recuperación de

[9] Información proporcionada por el Responsable del Centro de Información y redactada por los autores.

información.

1.2.1.2. Estructura Organizacional

En la *Figura 1.2* se muestran los dos niveles por los cuales el Centro de información está constituido, el nivel administrativo, responsable del área, y el otro de los asistentes, administrativo y de sistemas, que conforman el nivel de soporte a usuario.

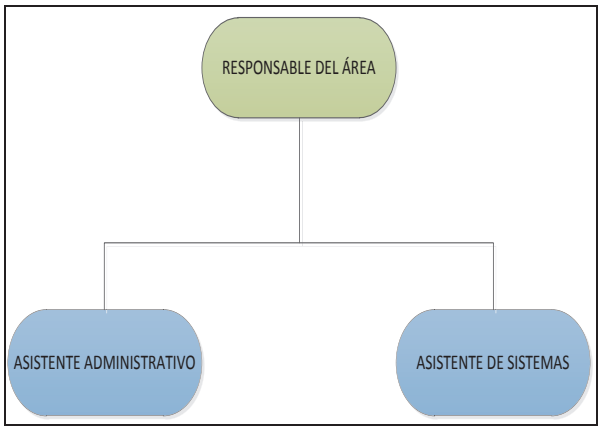

Figura 1.2: Estructura Organizacional del Centro de Información del CONADIS.[10]

1.2.1.3. Recursos Humanos

La *Tabla 1.2* muestra el personal con la que la institución cuenta actualmente.

NOMBRE	ÁREA DE TRABAJO	CARGO	FUNCIONES	PROFESIÓN
Fausto Villamarín	Responsable del Área	Analista de Sistemas	Administrar Hardware, Software, Aplicaciones, Bases de Datos, Red, y Seguridad Informática.	Ingeniero en Sistemas
Pablo Paredes	Soporte a Usuarios	Asistente Administrativo	Administrar y dar soporte a la Página Web de la organización. Elaborar guías para el adecuado uso de recursos informáticos y normas de seguridad. Organizar y Actualizar los Inventarios Informáticos.	Ingeniero en Sistemas

[10] Figura elaborada por los autores en base a información proporcionada por el Responsable del Área.

Hugo Lima	Soporte a Usuarios	Asistente de Sistemas	Proporcionar mantenimiento de Hardware y Asistencia Técnica de escritorio a los usuarios de la red. Dar soporte y mantenimiento a Aplicaciones, Base de Datos y Red de la organización.	Sin título de tercer nivel – Persona con Capacidades Especiales.

Tabla 1.2: Recurso Humano del Centro de Información.[11]

1.2.2. INFRAESTRUCTURA DE RED INFORMÁTICA

Esta sección describe la infraestructura de red del CONADIS a través del inventario de Hardware y Software así como también de su topología de red.

1.2.2.1. Inventario de Hardware[12]

Servidores

SERVIDORES			
N°	**Características**	**Función**	**Sistema Operativo**
1	Blade IBM, 1 chasis en S, 1 procesador Xeon 3.0 GHZ, memoria 4 GB, 4 Discos Duros de 136 GB.	Servidor de Aplicaciones Active Directory DNS	Microsoft 2003 Server
1	Blade IBM, 1 chasis en S, 1 procesador Xeon 3.0 GHZ, memoria 4 GB, 4 Discos Duros de 136 GB.	Firewall Proxy	Linux Red Hat Enterprise
1	HP Proliant, 1 procesador Xeon 3.0 GHZ, memoria 2 GB, 2 Discos Duros de 136 GB.	Web Mail JBoss PostgreSQL	Linux CentOS

Tabla 1.3: Inventario de Hardware de Servidores.[13]

Estaciones de Trabajo

El CONADIS cuenta con 50 estaciones de trabajo, con sistema operativo: Windows 7, Windows Vista, Windows XP y Ubuntu, distribuidas en sus diferentes departamentos.

---

[11] Tabla elaborada por los autores en base a información proporcionada por el Responsable del Área.
[12] Información proporcionada por el Responsable del Centro de Información y redactada por los autores.
[13] Tabla elaborada por los autores en base a información proporcionada por el Responsable del Área.

1.2.2.2. Inventario de Software[14]

Plataformas / Servicios

El CONADIS cuenta únicamente con JBoss dentro de lo que es la plataforma Java. Mientras que como plataforma para servicios tiene: Microsoft Windows 2003 Server, Linux CentOS y Linux Red Hat.

Además cuenta con servicio de Web Mail, correo y Active Directory.

Aplicaciones / Sistemas Utilizados

El CONADIS cuenta con: SQL Server, PostgreSQL y como software de escritorio Open Office 3.4 y Microsoft Office 2007.

Además de las aplicaciones; MEGAN como Sistema de Control de Bienes, BIOSYSTEM como Sistema de Control de Personal que incluye el sistema biométrico, LEXIS como Sistema Jurídico, todos estos cuentan con su respectiva licencia y aplicaciones del servicio público como QUIPUX, DIMM-SRI, etc.

Licencias

El CONADIS cuenta con equipos que poseen software Licenciado y Open Source, aunque ciertas estaciones de trabajo funcionan con sistema operativo con licencia no original. La mayor parte de licencias son adquiridas únicamente al momento de compra de equipos.

En el caso de requerir una nueva licencia ya sea por cambio de software o actualización se la gestiona por medio de solicitud a los directivos de la organización para su adquisición.

1.2.2.3. Red

Las instalaciones del CONADIS, sede Quito, están ubicadas en la Av. 10 de Agosto N37-193 entre Villalengua y Carondelet, divididas en dos edificaciones; la

---

[14] Información proporcionada por el Responsable del Centro de Información y redactada por los autores.

primera de una planta donde funciona la parte administrativa, mientras que la segunda de dos plantas las mismas que son utilizadas por los diferentes departamentos que componen el CONADIS.

La *Figura 1.3* describe la topología de red correspondiente al CONADIS.

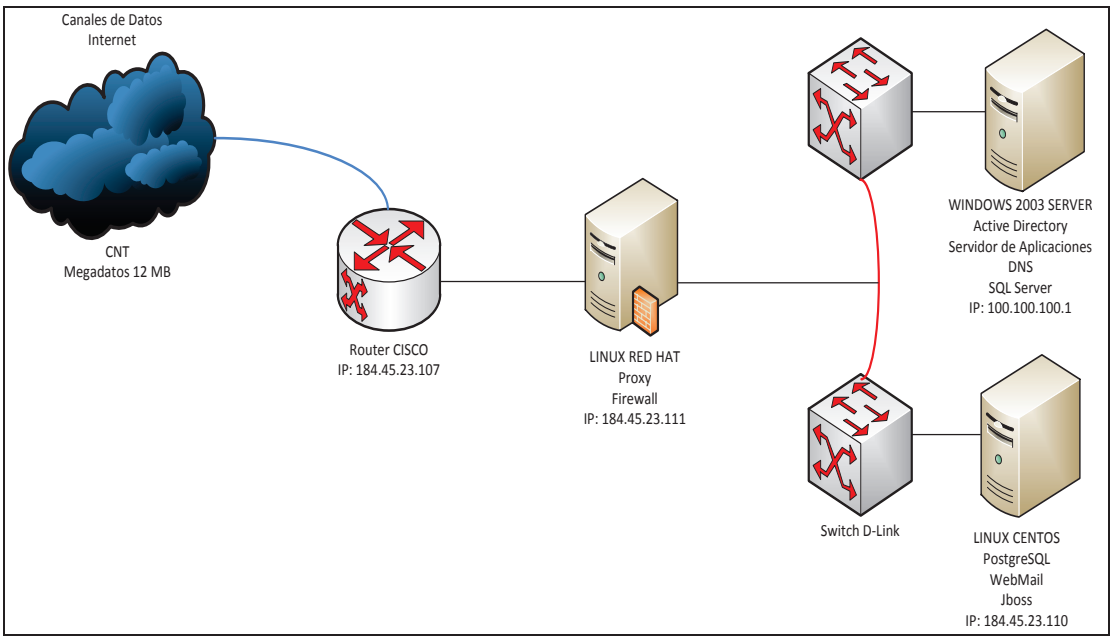

Figura 1.3: Topología de Red CONADIS[15]

Estructura de Red

La infraestructura de red del CONADIS es una red LAN tipo Ethernet, topología estrella, distribuida físicamente en 3 segmentos horizontales conectados a un segmento vertical principal mediante cableado estructurado de cable UTP categoría 6, que actualmente dispone de 50 estaciones de trabajo y 3 servidores.

Topología de Red

La red cuenta con Switches Cisco de 24 puertos de capa de red administrables conectados entre sí, de manera que se tiene redundancia en el trabajo y la carga de este es compartida.

---

[15] Figura elaborada por los autores en base a información proporcionada por el Responsable del Área.

El conmutador físicamente está ubicado en el cuarto de control del Centro de Información, el mismo permite la comunicación LAN tipo Ethernet con velocidad de 6Mbps, dicho dispositivo es el encargado de controlar el tráfico entre servidores y estaciones de trabajo utilizando la respectiva capa de enlace.

Conexión a Internet

El acceso a Internet por parte de los usuarios del CONADIS, es a través de un Router DLink ubicado en el Centro de Información, el cual está conectado con el proveedor de servicios de Internet, Corporación Nacional de Telecomunicaciones CNT. Esta conexión es por medio de fibra óptica a una velocidad de 12Mbps y la seguridad está garantizada por los equipos del proveedor.

Administración

La administración de la red de la organización garantiza el buen funcionamiento de la misma y esta está a cargo del responsable del Centro de Información.

1.3. SELECCIÓN Y JUSTIFICACIÓN DE USO DEL ESTÁNDAR.

Las tecnologías de la información son la base en las operaciones tanto administrativas como financieras, por ello deben existir formas de control que aseguren que la información es la real y que no ha sido cambiada o alterada en el transcurso de su transferencia. Por esto la información y su seguridad juegan un papel importante dentro de las organizaciones.

La seguridad de la información, va más allá de seguridades técnicas, pues son los riesgos del negocio y las vulnerabilidades a las que se está expuesto los que determinan cuan segura es nuestra información. Por ello la realización del análisis de los elementos; activos, vulnerabilidades y amenazas, que justos determinan los riesgos; que pueden ser físicos, operacionales, organizacionales y de TI, ayuda a entender cuán importante es la información y como hay que protegerla. Debido a esto en los siguientes apartados se justifica el uso de los estándares que permiten realizar el análisis de riesgos y diseñar el plan de seguridad de la información en el presente proyecto.

1.3.1. ESTÁNDAR ISO/IEC 27001:2005 EN EL DIAGNÓSTICO DE LA SITUACIÓN ACTUAL Y DISEÑO DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN

El Plan de Seguridad de la Información consiste en implantar un Sistema de Gestión de Seguridad de la Información, el estándar ISO 27001 “especifica los requerimientos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).” Además de que adopta el modelo del proceso Planear-Hacer-Chequear-Actuar (PDCA por sus siglas en inglés). [7]

El diseño del Plan de Seguridad de la Información para el CONADIS se encuentra enfocado en el uso del estándar ISO/IEC 27001:2005 ya que este proporciona los lineamientos para implementar la gestión de la seguridad de la información, además de que utiliza el modelo PDCA, del cual únicamente se cubre la parte de planificación, mientras que para la implementación, operación, monitorización, revisión, mantenimiento y mejora se dan recomendaciones para la ejecución.

La aplicación de este estándar a su vez implica la necesidad del uso del estándar ISO/IEC 27002 el mismo que diseña objetivos de control y controles “para ser implementados de manera que satisfaga los requerimientos identificados en una evaluación del riesgo.” [8]

Los dominios establecidos dentro del estándar ISO/IEC 27001 proporcionan una guía para diagnosticar la situación actual del CONADIS y de esta manera determinar el estado de cumplimiento actual de la norma dentro la organización.

Para lograr una buena gestión de seguridad de la información los conceptos, actividades y controles establecidos dentro de este estándar se encuentran directamente relacionados a la ISO 27002, lo que facilita y ayuda en el análisis de riesgos ya que establece los controles y los niveles de implementación con el fin de mitigar los riesgos dentro de la organización.

1.3.2. SELECCIÓN DE LA METODOLOGÍA PARA LA EVALUACIÓN Y ANÁLISIS DE RIESGOS

Hoy en día, hablar de Seguridad de la Información es hablar de una relación directamente proporcional con las amenazas y riesgos a los que una empresa u organización puede estar expuesta. Por este motivo, el proceso para establecer controles y medidas que ayuden a proteger la información puede resultar complicado pues dependerá del nivel de aplicación del mismo en la organización, y es en ese momento en donde un Análisis de Riesgos cumple un papel fundamental en la optimización de este proceso.

El objetivo de realizar un análisis de riesgos es, determinar cuáles serán los factores de riesgo que potencialmente tendrán un impacto significativo dentro de la organización. La implementación de este análisis conlleva a determinar todos los activos y en donde se note claramente el impacto provocado por los riesgos, calificándolos y evaluándolos con el objetivo de obtener información importante y de esta manera establecer el nivel de riesgo y los controles y/o acciones que se van a implementar dentro del Plan de Seguridad de la Información.

Cabe mencionar que este análisis y el diagnóstico tienen validez dentro del tiempo en el que se lo efectúa, esto se debe a que los controles y medidas que se puedan implantar dentro de la organización en algún momento podrían ser ineficientes a medida que el tiempo transcurra pues la existencia de nuevas amenazas, darán como resultado nueva ocurrencia de riesgos. Por esta razón, la organización debe replantear su diagnóstico para poder determinar nuevos síntomas o a su vez saber si los síntomas encontrados anteriormente ya fueron mitigados.

Existen diversas metodologías y/o guías para realizar el análisis de riesgos, la selección de esta dependerá de la información disponible y del detalle que se desea alcanzar en el análisis.

La palabra metodología tiene origen griego: metà que significa “más allá”, odòs con significado “camino” y logos que es el “estudio”. Entonces

metodología no es más que el conjunto de pasos a seguir que muestran qué hacer y cómo actuar en una determinada investigación de tipo científico. [9]

1.3.2.1. MAGERIT[16] - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

Esta metodología fue elaborada en España por el consejo superior de administración electrónica, y consiste en un método sistemático que permite analizar los riesgos que el uso de tecnologías de la información y comunicaciones pudieran provocar, de manera que se logre implementar medidas de control apropiadas que permitan mitigar dichos riesgos.

MAGERIT basa su análisis en el impacto que puede tener una organización ante la violación de la seguridad, buscando identificar las vulnerabilidades que son utilizadas por las amenazas, para así tener identificadas las posibles medidas preventivas y correctivas apropiadas.

1.3.2.2. OCTAVE[17] - Operationally Critical Threat, asset and vulnerability evaluation.

Es una técnica basada en el riesgo que permite planificar y tener una estrategia en seguridad. A diferencia de otras metodologías que enfocan su consultoría en la tecnología con objetivos de riesgos tecnológicos y temas operacionales, OCTAVE tiene como objetivo el riesgo organizacional enfocando su análisis a lo referente a la estrategia y a la práctica. La aplicación de OCTAVE, implica un trabajo en conjunto de toda la organización, desde un equipo de gente del sector operativo o de negocio hasta uno del departamento de tecnología de la información (IT) logrando así enfocarse en las necesidades de seguridad en tres aspectos: Riesgos Operativos, Prácticas de seguridad Y Tecnología.

---

[16] GUTIÉRREZ AMAYA CAMILO, MAGERIT: metodología práctica para gestionar riesgos, **14 MAY 2013,** http://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/

[17] DUQUE OCHOA BLANCA RUBIELA , Metodologías de Gestión de Riesgos http://auditoriauc20102mivi.wikispaces.com/file/view/Metodolog%C3%ACas+deGesti%C3%B2n+de+Riesgos.pdf

OCTAVE permite tener claro el manejo de recursos, identificación y evaluación de riesgos que afectan la seguridad en una organización. Además exige el apoyo de un patrocinador, interesado en seguridad, para la evaluación de la organización y del personal de la tecnología de información.

1.3.2.3. ISO/IEC 27005[18] - Gestión de Riesgos de la Seguridad de la Información

Esta norma proporciona las directrices para la gestión del riesgo en la seguridad de la información en una organización, particularmente dando soporte a los requisitos de un SGSI de acuerdo con la norma ISO/IEC 27001. Sin embargo, se debe tener claro que esta norma no especifica ninguna metodología para la gestión del riesgo en la seguridad de la información.

La ISO/IEC 27005 está basada en los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para facilitar la implementación satisfactoria de la seguridad de la información enfocando su análisis en la gestión del riesgo.

En otras palabras, la norma proporciona los elementos necesarios que se deben incluir en toda metodología de Análisis de Riesgos, por lo que, desde este punto de vista puede constituirse como una metodología en sí misma.

La *Tabla 1.4* muestra los resultados obtenidos al comparar la guía ISO/IEC 27005 con las metodologías Magerit y Octave.

	ISO/IEC 27005	OCTAVE	MAGERIT
DESCRIPCIÓN	Propone un enfoque de un proceso de gestión de riesgos de seguridad de la información basado en actividades.	Propone un enfoque en los problemas organizacionales y tecnológicos.	Propone un enfoque basado en los riesgos derivados del uso de tecnologías de la información.
EVALUACIÓN	Establecimiento del contexto. Valoración del riesgo: • Análisis del riesgo	Construir perfiles de amenaza basado en activos. Identificar	Modelo de valor. Mapa de riesgos. Declaración de aplicabilidad. Evaluación de salvaguardias.

[18] Información tomada de la Norma ISO/IEC 27005 y traducida por los autores.

	(Identificación y estimación del riesgo). • Evaluación del riesgo.	vulnerabilidades de infraestructura.	
TRATAMIENTO	Tratamiento del riesgo. Aceptación del riesgo.	Desarrollar planes y estrategias de seguridad.	Estado del riesgo. Informe de insuficiencias.
COMPONENTES ADICIONALES	Monitoreo y revisión del riesgo. Comunicación del riesgo.	Criterios de OCTAVE: Principios y atributos del enfoque OCTAVE.	Cumplimiento de normativa. Plan de seguridad.

Tabla 1.4: Comparación entre Magerit, Octave y la norma ISO/IEC 27005.[19]

En la *Tabla 1.4* se puede observar que los tres modelos cubren la evaluación y tratamiento del riesgo, sin embargo la norma ISO/IEC 27005, abarca adicionalmente el monitoreo y comunicación del riesgo además de que se alinea y apoya los conceptos de la norma ISO/IEC 27001, la misma que es utilizada para la elaboración del Plan de Seguridad de la Información.

De la comparación anterior, se puede determinar que la norma ISO/IEC 27005 es la que mejor se alinea con la ISO/IEC 27001, puesto que "proporciona directrices para la gestión de riesgos de seguridad de la información, apoyándose en los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar en la puesta en práctica satisfactoria del análisis y la gestión del riesgo, fase principal del diseño de todo buen SGSI." [10]

Cabe recalcar que la norma ISO/IEC 27005 no es una metodología, sino una guía que proporciona todos los elementos que debe incluir una metodología de análisis de riesgo, por lo que desde este punto de vista puede constituirse como una metodología en sí.

1.4. DIAGNÓSTICO DE LA SITUACIÓN ACTUAL.

En el transcurso de esta sección se muestra la información obtenida de las entrevistas efectuadas al Responsable del Centro de Información y a otros funcionarios del CONADIS. Con esta información se realiza un diagnóstico de la

[19] Tabla elaborada por los autores en base a información recolectada de sitios web.

situación actual, lo que nos permite evaluar el estado de cumplimiento de acuerdo al estándar ISO/IEC 27001, de manera que se identifiquen los problemas de la seguridad de la información y así definir posibles soluciones.

1.4.1. DIAGNÓSTICO BASADO EN EL ESTÁNDAR

1.5.1.1. Política de Seguridad

a) Política de seguridad de la información

El Centro de Información del CONADIS no dispone de un Plan de Seguridad de la Información definido, pero cuenta con varias políticas que las lleva a cabo dentro del Centro y de la organización.

El CONADIS al ser una organización Estatal, debe someterse a la disposición transitoria Sexta de la constitución vigente, razón por la que se está adecuando su estructura y las funciones a la Constitución, es por esto que están obligados a desarrollar e implementar el Plan de Seguridad de la Información. La información que se maneja, se administrada dentro de los tres parámetros determinados para la seguridad de la información, los mismos que son:

- Confidencialidad
- Integridad
- Disponibilidad

Los parámetros antes mencionados permiten que la información sea clasificada y sea accesible solo para personas autorizadas, mediante controles y perfiles de usuario y bajo ningún motivo esta información puede ser accedida por quien no le corresponda. Cabe mencionar que la información, sus métodos y recursos deben ser exactos y estar siempre disponibles para cuando se los requiera.

1.5.1.2. Organización de la Seguridad de Información

a) Organización Interna.

La información para cada área se encuentra organizada y clasificada, lo que implica que se tiene acceso a la información de acuerdo a las funciones que se

desempeñan dentro del departamento, esta información es administrada por DNS, el mismo que establece las políticas de acceso a la información según el perfil de usuario.

El acceso a las bases de datos se lo realiza localmente por cada aplicación, esto debido a los privilegios de usuario que son asignados para desempeñar el trabajo en las aplicaciones y en cada área.

b) Terceros

Para poder acceder a la información institucional de manera externa, se lo realiza de manera remota, cabe mencionar que solo los miembros de tecnología tienen los permisos suficientes siempre y cuando ingresen con el perfil de administrador.

1.5.1.3. Gestión de Activos

a) Responsabilidad sobre los activos

Como responsabilidades hacia los activos, si se cumple con una gestión de estos, además de que cada funcionario perteneciente a la organización tiene la obligación de hacerse cargo de cada uno de los activos que se le han asignado, así como también posee un sistema de inventario.

El proceso de asignación de activos para cada uno de los funcionarios se lo realiza por medio de actas de entrega recepción, además de un acta de responsabilidad que evidencie la responsabilidad de cada funcionario con sus activos, también es necesario aclarar que ningún activo puede salir de la institución, en los casos que sea necesario el traslado de activos hacia lugares externos de la organización el procedimiento es mediante previa autorización.

b) Clasificación de la información

El CONADIS, clasifica la información de acuerdo al departamento o área en la cual la información es útil y de vital importancia.

1.5.1.4. Seguridad Ligada a los Recursos Humanos

a) Seguridad en la definición del trabajo y los recursos

Cuando existen vacantes disponibles, se las llena de acuerdo a las necesidades y requerimientos del departamento, para lo cual el procedimiento es de acuerdo a lo que dispone la Ley de Contratación Pública y rigiéndose a las disposiciones dictaminadas por el Ministerio de Relaciones Laborales.

Al ser una institución que se desenvuelve y cuenta con personas con capacidades especiales, y de acuerdo a la Ley, existe igualdad y equidad al momento de contratar personal con capacidad especial.

b) Seguridad en el desempeño de las funciones del empleo

Cuando las vacantes que existían han sido llenadas, se emite una solicitud, ya sea al Director del departamento en el cual va a desempeñar sus funciones o al departamento de Recursos Humanos con toda la información del nuevo funcionario, para proceder a realizar las siguientes actividades:

- Asignación de Correo Institucional
- Usuario de Red
- Activación de Perfiles de Usuario

De acuerdo a las responsabilidades y al rol que se le asigne dentro del área o departamento en el cual el funcionario se desempeñará se le brinda capacitación acerca de los procedimientos de seguridad y políticas de uso adecuado de todo medio que permita el proceso de información.

c) Finalización o cambio del puesto de trabajo

El proceso de finalización del puesto de trabajo es un proceso formal, esto es debido a que todo activo que se encuentra a su cargo es devuelto de acuerdo al inventario, así mismo el acceso a red, usuario y correo institucional son deshabilitados.

El proceso cuando es cambio de departamento o de funciones se realiza el mismo procedimiento que se sigue en la definición del puesto de trabajo, mediante la solicitud al Director de departamento o a Recursos Humanos.

1.5.1.5. Seguridad Física y del Entorno

a) Áreas seguras.

El acceso a las instalaciones del CONADIS se lo realiza mediante un registro, esta medida se la lleva acabo y se la gestiona por medio del servicio de guardianía existente en la entrada a la organización, cabe mencionar que en el mismo espacio se encuentra el sistema de CCTV[20] lo que permite que las áreas sean vigiladas.

El acceso al Centro de Información se lo realiza con previo aviso, sin embargo esto no siempre se cumple. Para acceder al Centro de Datos se lo hace únicamente mediante el personal autorizado, aquellas personas ajenas a esta área podrán ingresar con previa autorización y acompañados de una persona autorizada, para poder acceder a esta área existe la respectiva llave, que se encuentra a cargo del responsable del Centro de Información.

b) Seguridad de los Equipos.

El acceso al departamento como a la información no está permitido para el personal no autorizado.

Los reguladores de voltaje ayudan a la protección de las estaciones de trabajo, esto con el fin de evitar daños por cambios de voltaje, poseen también una regleta o cortapicos y de igual manera los cables de toda la red se encuentran canalizados y protegidos.

El CONADIS posee un generador eléctrico que le permite continuar de manera regular sus actividades cuando exista corte de energía.

Los medios de computación móvil se encuentran asegurados únicamente de manera interna, es decir, se encuentran protegidos contra daños y fallos dentro de la organización, en el caso de que se haya suscitado fuera de las instalaciones el responsable directo será el funcionario que se encuentra a cargo del activo. No existe una política formal, acerca de perdida de información en caso de existir algún percance en medios de computación móviles.

---

[20] CCTV, Circuito Cerrado de Televisión y Videovigilancia.

1.5.1.6. Gestión de Comunicaciones y Operaciones

a) Procedimientos y responsabilidades de operación.

Realizar el monitoreo, mantenimiento y administración de la infraestructura y de todas las actividades informáticas, es continuo debido a cuestiones de accesos a la red. Entre el monitoreo continuo se realiza:

- Monitoreo de Servicios y Aplicaciones.
- Monitoreo de Servidores.
- Monitoreo de red, con lo que tiene que ver a ataques.

Y para lo que es el mantenimiento y administración se lo realiza hacia:

- Portal web de la organización.
- Mail Server.
- Dominios.
- Accesos a recursos de red.

Estas operaciones y sus procedimientos son normales, pero no son documentados, se los realiza por medio de la experiencia en el cargo.

b) Supervisión de los servicios contratados a terceros.

Para los contratos con terceros se realiza un monitoreo regular y de esta manera se asegura que la prestación de los mismos se están cumpliendo según lo acordado en los SLA's (Acuerdos de Niveles de Servicio).

c) Planificación y aceptación del sistema.

Un sistema debe ser planificado y aceptado, para esto se debe seguir y basar de acuerdo a las necesidades de los usuarios, el procedimiento para realizar este proceso comienza con el levantamiento de requerimientos y de esta manera poder definir la automatización y/o mejoramiento del mismo, con lo cual vía solicitud y posterior aceptación realizar el levantamiento del proceso.

Una vez que se realiza el estudio y se levanta los requerimientos, se realiza el desarrollo o la adquisición del sistema a terceros, una vez que el sistema es

implementado se realizan las pruebas necesarias y de esta manera se determina si cumple son las necesidades.

d) Protección contra software malicioso y código móvil.

El CONADIS cuenta con herramientas que les permite controlar y monitorear los diferentes ataques que pudieran suscitarse, y que protegen la información sensible de la organización.

Estas herramientas son:

- Firewall.
- Plataforma de Antivirus.
- Plataforma de Antispam.

Estos procedimientos, los usuarios los llevan a cabo conjuntamente con actividades tales como:

- No abrir correos de remitentes desconocidos
- No descargar ficheros de sitios no confiables.

Los controles y medidas para detectar y evitar software no autorizado es responsabilidad del administrador, tanto para detectar como para evitar la introducción de software no autorizado, además de que cada uno de los usuarios conocen los peligros que puede causar un software malicioso, cabe mencionar que nada de esto se encuentra documentado.

e) Gestión interna de soportes y recuperación.

El CONADIS tiene definidos algunos procedimientos rutinarios, no documentados, que les permite mantener la integridad y la disponibilidad de la información y de la comunicación. Esto debido a que regularmente se efectúa copias de seguridad de la información especialmente de la denominada sensible.

El respaldo de este tipo de información y de acuerdo a su sensibilidad se lo realiza de la siguiente manera:

- Diaria

- Semanal
- Mensual
- Anual

Así, se tiene backups de servicios críticos de la organización, como son:

- Mail Server
- Proxy
- Tablas de Ruteo
- Active Directory
- Controlador de Dominio
- Portal Web Institucional
- Base de Datos

Toda esta información que se obtiene de los backups es probada en tiempos establecidos, de tal manera que se verifique que la información sea útil.

f) Gestión de redes.

Existe un constante y permanente monitoreo de la red de la organización de acuerdo a las políticas establecidas, que no necesariamente se encuentran documentadas adecuadamente, y que permiten observar todo el comportamiento y funcionamiento.

El bloqueo de puertos, así como de ciertas páginas es una de las formas de gestionar la red, por lo que así se asegura las funciones diarias de cada uno de los usuarios que se encuentran en la red y de esta manera optimizarla.

g) Utilización y seguridad de los soportes de información.

El procedimiento para la no divulgación de documentos no se encuentra formalmente establecido, por lo que no existe el control adecuado en los medios extraíbles en los cuales la información pudiera ser copiada o sustraída por los usuarios.

h) Intercambio de información y software.

El intercambio de información entre la sede Quito y las diferentes provincias es en tiempo real puesto que actualmente el CONADIS trabaja con sistema web.

Dentro de la organización el intercambio de información se lo realiza a través del mail institucional, que como gestor de correo electrónico tiene Microsoft Outlook.

i) Servicios de comercio electrónico.

El CONADIS no posee este servicio.

j) Monitorización.

Los sistemas son monitoreados y cada evento es registrado de tal manera que los registros de fallos puedan ser utilizados para identificar los posibles problemas del sistema. Este monitoreo permite verificar las políticas de acceso, con la utilización de logs de seguridad que son monitoreados, revisados y evaluados regularmente con el fin de tomar decisiones si así fuese necesario.

1.5.1.7. Control de Accesos

a) Requerimientos de negocio para el control de accesos.

La mayor parte de las políticas que posee el CONADIS no se encuentran ni documentadas adecuadamente, ni establecidas como política en sí, es decir están creadas más como reglas que se cumplen por parte de los propietarios de los activos de información que son los responsables de la protección de los activos que tienen a su cargo.

El acceso a la información depende tanto de la función como del departamento al que pertenece cada usuario, por ello se requiere permisos dependiendo del tipo o perfil de usuario dentro del sistema.

EL CONADIS cuenta con dos tipos de usuarios:

- **Administrador:** tipo de usuario asignado generalmente solo al personal técnico, quienes posee el manejo completo del computador, instalaciones, permisos, etc.
- **Usuario:** el acceso al computador es limitado, las aplicaciones a las

que se tiene acceso dependen de las funciones que cumple determinado usuario.

b) Gestión de acceso de usuarios.

El perfil de usuario que se le asigna a un funcionario depende del cargo que cumple en la organización, este procedimiento permite controlar los permisos de acceso al sistema y servicios de información.

La asignación de perfil de usuario es un procedimiento que inicia con la contratación de un nuevo funcionario, una vez que el departamento de Recursos Humanos da la notificación del nuevo contrato, es el Centro de Información el encargado de la creación de la cuenta, perfil que manejará, grupo al que pertenecerá así como los permisos, privilegios y asignación de clave para el acceso a la red. Cuando un funcionario deja de pertenecer a la organización el usuario es dado de baja y con ello todos los privilegios que estaban asignados son removidos.

La asignación de usuarios y el manejo de contraseñas es una actividad a cargo del Centro de Información, los técnicos de este departamento son los encargados de la creación de contraseñas, las mismas que son únicas y mantienen un formato establecido, dichas contraseñas no pueden ser cambiadas a menos que se pida formalmente el cambio.

c) Responsabilidades del usuario.

El uso correcto de contraseñas, cuentas y equipos asignados son responsabilidad de los usuarios a cargo.

Es el usuario el responsable de mantener la confidencialidad, asegurando la no divulgación, el acceso no autorizado y el uso responsable de contraseñas de usuario de red, con el objetivo de reducir el riesgo y mantener a salvo la información tanto personal como institucional a su cargo.

d) Control de acceso en red.

Los privilegios que cada usuario tiene son otorgados al momento de su creación, controlando el acceso a los servicios en la asignación de tipo y perfil de usuario, logrando acceso únicamente a los servicios para los que se le han asignado.

El acceso remoto es únicamente permitido para el usuario administrador y es autorizado dependiendo de las actividades que se vayan a realizar.

e) Control de acceso al sistema operativo.

Los privilegios de acceso, a los diferentes sistemas operativos, para un usuario son otorgados en el momento de asignación de tipo de usuario, ya que en ese momento se otorga el grupo al cual pertenece.

Las sesiones de trabajo se desconectan después de un periodo de inactividad, este tiempo depende del tipo de perfil del usuario.

No existe gestión del uso de contraseñas ya que estas son únicas e indefinidas, únicamente se realiza cambio por medio de petición formal al Centro de Información.

f) Control de acceso a las aplicaciones.

Los permisos de acceso a las diferentes aplicaciones dependen del perfil asignado y del departamento al que pertenece el usuario.

Las tareas asignadas por el departamento y cargo que posee un funcionario determinan el nivel de permisos de acceso a la información. Control que se lo realiza al momento de ingreso en las aplicaciones a las que posee permisos y con cuenta de usuario y contraseña.

g) Informática móvil y tele trabajo.

La organización no cuenta con un procedimiento que involucre la informática móvil y tele trabajo.

1.5.1.8. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

a) Requisitos de seguridad de los sistemas.

Al ser una institución pública que no desarrolla sistemas de información, la seguridad de los sistemas con los que cuenta es determinada y establecida en el momento de la adquisición, lo que permite el control de acceso a la información en cada uno de los usuarios y departamentos.

b) Seguridad de las aplicaciones del sistema.

El monitoreo a las aplicaciones es diario, controlando así el correcto, buen uso y no perdida de información.

c) Controles criptográficos.

El CONADIS no cuenta con políticas de controles criptográficos.

d) Seguridad de los ficheros del sistema.

La asignación de perfil dentro del grupo de trabajo, determinan las acciones que se pueden realizar en un determinado archivo o fichero, siendo así únicamente el usuario Administrador el que posee todos los privilegios.

e) Seguridad en los procesos de desarrollo y soporte.

El CONADIS no realiza procesos de desarrollo de sistemas, sin embargo controla y exige que el desarrollo y soporte se cumpla de acuerdo a lo establecido en los acuerdos de niveles de servicio o contratos.

f) Gestión de las vulnerabilidades técnicas.

No se tiene establecidas políticas de gestión de vulnerabilidades técnicas, por lo que la obtención de información sobre vulnerabilidades existentes no es oportuna, lo que da como resultado el no tener claro os riesgos a los que se está expuesto.

1.5.1.9. Gestión de Incidentes de Seguridad de la Información

a) Comunicación de eventos y debilidades en la seguridad de la información.

No existe una política debidamente establecida para la comunicación de eventos y debilidades como tampoco para la solución de los mismos. En los casos de los

eventos que pueden ser controlados inmediatamente, no existe informe ni documentación alguna de las actividades que se realizaron, solo en los casos en el que el evento es de mayor relevancia, se emite informes de daños y reparaciones efectuadas.

b) Gestión de incidentes y mejoras en la seguridad de la información.

Debido a que los eventos de incidencia no son documentados, a excepción de los de mayor importancia, no se tiene un registro de los eventos comunes que permitan establecer políticas de solución, y disminución, o en el mejor de los casos eliminación de estos eventos.

1.5.1.10. Gestión de Continuidad del Negocio

a) Aspectos de la gestión de continuidad del negocio

El CONADIS cuenta con varias políticas de seguridad, no documentadas adecuadamente pero que son utilizadas al momento de garantizar el funcionamiento de las actividades y procesos, frente a la ocurrencia de desastres o fallos de los sistemas de información.

La seguridad de la información es parte importante de la Gestión de la Continuidad del Negocio, por ello el Centro de Datos al contener toda la información cuenta con políticas de backups y otras medidas de seguridad, tales como:

- Acceso de personal autorizado
- Sistema contra incendios
- Sistema de Alimentación Ininterrumpida

1.5.1.11. Conformidad

a) Conformidad con los requisitos legales

El Centro de Información del CONADIS es el encargado de hacer cumplir los requisitos legales de licenciamiento y de actualización de software, así como también de sus plataformas.

b) Revisiones de la política de seguridad y de la conformidad técnica

Las políticas y estándares de seguridad que se siguen dentro de la institución, aunque no se encuentran documentadas adecuadamente, en su gran mayoría se cumplen de acuerdo a las guías y/o costumbres del puesto de trabajo en el que el funcionario se desempeña.

c) Consideraciones sobre la auditoría de sistemas

En el CONADIS se realizan auditorías internas de manera regular, con el fin de evaluar constantemente las políticas y procesos, con el objetivo de encontrar evidencias que permitan mejorar la eficiencia y eficacia de la organización.

Hasta el momento no se han efectuado auditorías externas, únicamente han sido sometidos a las evaluaciones y controles que realiza la Contraloría General del Estado de forma rutinaria a todas las instituciones públicas.

1.4.2. RESULTADO GENERAL DEL DIAGNÓSTICO

En conclusión, después del diagnóstico realizado al Centro de Información, se puede observar que no se encuentra en el nivel jerárquico en el que debería estar dentro de la organización, es decir, a un nivel Asesor y de esta manera trabajar conjuntamente con los Directivos. Por otra parte no existe una adecuada gestión de la seguridad de la información, esto se debe principalmente a que ninguna política que se llevan a cabo dentro de la organización se encuentra documentada adecuadamente. Sin embargo, existen actividades, métodos y procedimientos definidos como “políticas” por la organización, que son realizados de manera rutinaria por los funcionarios, que sin ser parte de una norma o estándar ayudan a que la gestión se realice. Finalmente, el Centro de Información no tiene una adecuada seguridad física, puesto que los controles para el ingreso al Data Center son mínimos.

La *Tabla 1.5* muestra el resultado del diagnóstico de la situación actual según la norma ISO/IEC 27001 para el dominio A.8. Seguridad Ligada a los Recurso Humanos. El resultado completo del análisis e encuentra en el Anexo I.

A.8. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	A.8.1. Seguridad en la definición del trabajo y los recursos.	A.8.1.1. Inclusión de la seguridad en las responsabilidades laborales.	Contrato Laboral	El contrato que el funcionario firma al momento del ingreso a la institución describe roles y funciones que desempeñará.
		A.8.1.2. Selección y política de personal.	Ley de Contratación Pública	El CONADIS se rige a esta ley para poder contratar personal.
		A.8.1.3. Términos y condiciones de la relación laboral.	Contrato Laboral	Todos los funcionarios deben firmar el contrato laboral.
	A.8.2. Seguridad en el desempeño de las funciones del empleo.	A.8.2.1. Supervisión de las obligaciones.	Supervisión de actividades	Las actividades que realizan los funcionarios son supervisadas constantemente, en especial a las personas con capacidades especiales.
		A.8.2.2. Formación y capacitación en seguridad de la información.	Inducción al nuevo personal	La organización brinda la respectiva capacitación al momento que ingresa el funcionario.
		A.8.2.3. Procedimiento disciplinario.		
	A.8.3. Finalización o cambio del puesto de trabajo.	A.8.3.1. Cese de responsabilidades.	Documento de Cese de Responsabilidades	Cuando un funcionario deja de pertenecer a la organización o existe cambio en sus funciones, el proceso de finalización del puesto de trabajo es un proceso formal.
		A.8.3.2. Restitución de activos.	Devolución de activos.	Todo activo que se encuentra a su cargo es devuelto e inventariado.
		A.8.3.3. Cancelación de permisos de acceso.	Deshabilitación de recursos tecnológicos	El acceso a la red, usuario y correo institucional son deshabilitados.

Tabla 1.5: Situación actual del CONADIS según la norma ISO/IEC 27001 para el dominio Seguridad Ligada a los Recursos Humanos.[21]

[21] Tabla elaborada por los autores.

1.4.3. ESTADO DE CUMPLIMIENTO ACTUAL

Realizado el diagnóstico del estado actual del CONADIS por medio de entrevistas y utilizando la norma ISO/IEC 27001, ver Sección 1.4, se elaboró una matriz en la que se presenta cada dominio, su objetivo de control y los controles que la norma ISO/IEC 27001 propone, y con ello los controles existentes actualmente en la organización correspondientes a cada control en la norma, el valor de “1” se asigna cuando cumpla un control mientras que el valor de “0” cuando no lo cumpla, lo que nos da como resultado el porcentaje de cumplimiento de la Norma ISO/IEC 27001 en el CONADIS.

La *Tabla 1.6* muestra el estado de cumplimiento actual en el dominio A.8 Seguridad Ligada a los Recursos Humanos que presenta tres objetivos de control con 9 controles de los cuales la organización cumple con ocho, lo que en términos porcentuales representa el 88,89% de cumplimiento en este dominio. El estado de cumplimiento actual de la organización frente a toda la norma ISO/IEC 27001 se puede observar en el ANEXO I.

A.8 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	A.8.1 Seguridad en la definición del trabajo y los recursos.	Contrato Laboral	El contrato que el funcionario firma al momento del ingreso a la institución describe roles y funciones que desempeñará.	A.8.1.1 Inclusión de la seguridad en las responsabilidades laborales.	1	88,89%
		Ley de Contratación Pública	El CONADIS se rige a esta ley para poder contratar personal.	A.8.1.2 Selección y política de personal.	1	
		Contrato Laboral	Todos los funcionarios deben firmar el contrato laboral.	A.8.1.3 Términos y condiciones de la relación laboral.	1	
	A.8.2 Seguridad en el desempeño de las funciones del empleo.	Supervisión de actividades	Las actividades que realizan los funcionarios son supervisadas constantemente, en especial a las personas con capacidades especiales.	A.8.2.1 Supervisión de las obligaciones.	1	
		Inducción al nuevo personal	La organización brinda la respectiva capacitación al momento que ingresa el funcionario.	A.8.2.2 Formación y capacitación en seguridad de la información.	1	
				A.8.2.3 Procedimiento disciplinario.	0	
	A.8.3 Finalización o cambio del puesto de trabajo.	Documento de Cese de Responsabilidades	Cuando un funcionario deja de pertenecer a la organización o existe cambio en sus funciones, el proceso de finalización del puesto de trabajo es un proceso formal.	A.8.3.1 Cese de responsabilidades.	1	
		Devolución de activos.	Todo activo que se encuentra a su cargo es devuelto e inventariado.	A.8.3.2 Restitución de activos.	1	
		Deshabilitación de recursos tecnológicos	El acceso a la red, usuario y correo institucional son deshabilitados.	A.8.3.3 Cancelación de permisos de acceso.	1	

Tabla 1.6: Lista de Cumplimiento Actual de Controles de la Norma ISO/IEC 27001 para Seguridad Física y del Entorno.[22]

[22] Tabla elaborada por los autores en base a información obtenida del diagnóstico de la situación actual de la organización y la norma ISO/IEC 27001.

1.4.3.1. Resultados del Estado de Cumplimiento Actual por Dominio.

A continuación la *Tabla 1.7* muestra el resumen del estado de cumplimiento por cada dominio de la norma, que es el resultado del análisis de la información obtenida de las entrevistas en la organización, la norma ISO27001 y la matriz de cumplimiento mostrada en la sección 1.4.3.

A.5. Política de Seguridad.	0,00%
A.6. Organización de la Seguridad de la Información.	36,36%
A.7. Gestión de Activos.	80,00%
A.8. Seguridad Ligada a los Recursos Humanos.	88,89%
A.9. Seguridad Física y del Entorno.	61,54%
A.10. Gestión de Comunicaciones y Operaciones.	53,13%
A.11. Control de Accesos.	40,00%
A.12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.	12,50%
A.13. Gestión de Incidentes de la Seguridad de la Información.	0,00%
A.14. Gestión de Continuidad del Negocio.	20,00%
A.15. Conformidad.	20,00%

Tabla 1.7: Estado de Cumplimiento por Dominio.[23]

Como se mencionó en secciones anteriores, el hecho de que el CONADIS no cuente con la adecuada documentación no es razón suficiente para que no cuente con medidas o procesos que de una u otra forma ayudan a mantener la seguridad de la información dentro de la organización, esto se puede observar en la tabla anterior, sin embargo también se puede ver que existen dominios que poseen menos de la mitad del cumplimiento o en el peor de los casos su cumplimiento es cero, lo que significa que aun cuando cuenta con determinados controles, no son los suficientes para que la seguridad de la información sea la apropiada.

A continuación se presenta los problemas encontrados dentro del CONADIS por cada dominio de la norma ISO/IEC 27001:

- **Política de Seguridad:** porcentaje de cumplimiento 0%, lo que evidencia la falta total de documentación y de políticas que garanticen la seguridad de

[23] Tabla elaborada por los autores en base a la matriz de estado de cumplimiento actual, Anexo XI.

la información. Por lo que se recomienda poner en práctica un proceso de mejora, el cual permita definir de manera formal una política de seguridad de la información en la que se presenten claramente los objetivos, el alcance y como mantener la seguridad de la información en la organización, así también se debería elaborar un plan de revisiones continuas, para garantizar la efectividad y el cumplimiento de dichas políticas, además de comprometer, de manera formal, a los directivos, gerentes y toda la institución con la seguridad de la información.

- **Organización de la Seguridad de la Información**: porcentaje de cumplimiento 36,36%, este porcentaje se debe a que si existen definidas ciertas responsabilidades, mediante perfiles de usuario, y acuerdos para mantener la seguridad de la información, al realizarse revisión de procedimientos de manera informal, por lo que se recomienda la creación de un comité de seguridad para que coordine las actividades que ayuden a identificar y tratar los riesgos que pueden producirse y de esta manera afectar la seguridad de la información.
- **Gestión de Activos:** porcentaje de cumplimiento 80%, este dominio dentro de la norma posee cinco controles, el porcentaje evidencia que existe un único control que no se cumple dentro de la organización este es el de "Marcado y tratamiento de la información" por lo que se recomienda definir procedimientos adecuados para el etiquetado y el tratamiento de la información.
- **Seguridad Ligada a los Recursos Humanos:** porcentaje de cumplimiento 88,89%, este dominio dentro de la norma posee nueve controles, el porcentaje evidencia que existe un único control que no se cumple dentro de la organización este es el de "Procedimiento disciplinario" por lo que se recomienda definir un proceso formal disciplinario para actuar frente a los funcionarios que produzcan brechas en la seguridad de la información.
- **Seguridad Física y del Entorno:** porcentaje de cumplimiento 61,54%, este porcentaje evidencia el cumplimiento de seguridades físicas puesto que si existen controles de registro al momento de ingreso a la organización además de contar con diferentes sistemas; CCTV, contra incendios, de enfriamiento e ininterrumpido de energía, que garantizan una adecuada

seguridad, además de contar con controles al momento de asegurar el cableado y los equipos tanto en las instalaciones de la organización como fuera de ella. Al existir un considerable tratamiento de la seguridad en el aspecto de la seguridad física y del entorno, se recomienda documentar los procesos y de igual manera implementar mayor seguridad en oficinas y/o despachos y de esta manera tener un control y registro de quien accede a la información y a determinada área.

- **Gestión de Comunicaciones y Operaciones:** porcentaje de cumplimiento 53,13%, al ser el dominio más extenso y cumplir con más del 50%, evidencia que la organización posee procedimientos que de una u otra forman garantizan el funcionamiento seguro de las plataformas tecnológicas dentro de la red del CONADIS, sin embargo, al igual que en los otros dominios ningún procedimiento esta formalmente documentado. Se recomienda como primer paso, documentar formalmente todos los procesos existentes, definir una política para el intercambio de información así como también establecer procedimientos para evitar la divulgación, modificación, retirada o destrucción de activos no autorizada dentro de la organización.
- **Control de Accesos:** porcentaje de cumplimiento 40%, esto se debe a que la organización no cuenta con políticas de control de acceso formalmente establecidas, sin embargo cuenta con una serie de controles que permiten asegurar el control de acceso de los usuarios, el principal problema radica en que no se cuenta con una buena gestión de contraseñas y los usuarios no poseen la debida concientización ante la seguridad de la información. Se recomienda elaborar formalmente la política de control de acceso, en la que se especifique detalladamente la gestión del acceso a usuarios, gestión de acceso a la red, gestión de acceso a los sistemas operativos y gestión de acceso a las aplicaciones, así como planes de concientización a los usuarios de la red.
- **Adquisición, Desarrollo y Mantenimiento de Sistemas de Información:** porcentaje de cumplimiento 12,5%, esto se debe a que únicamente la organización adquiere sistemas de información, el desarrollo y mantenimiento de los mismos se controla en los Acuerdos de Nivel de

Servicio o Contratos en los que se especifican los requisitos de seguridad para los sistemas de información a adquirir.

- **Gestión de Incidentes de la Seguridad de la Información:** porcentaje de cumplimiento 0%, lo que evidencia que la organización no tiene definido ni los procedimientos ni los responsables de la notificación, registro y tratamiento de las incidencias en la seguridad de la información. Se recomienda documentar los incidentes de seguridad y sus soluciones para tener registro de los mismos, con el fin analizarlos y proponer la forma de evitarlos en el futuro, así también para que dichos registros puedan ser utilizados como respaldo para posibles auditorias.
- **Gestión de Continuidad del Negocio:** porcentaje de cumplimiento 20%, este resultado evidencia que existen procedimientos que garantizan el funcionamiento de las actividades y procesos frente a la ocurrencia de desastres o fallos de los sistemas de información, los cuales no son formales ni se encuentran documentados como parte de un plan de continuidad de negocio. Se recomienda definir de manera formal una política que incluya planes de continuidad del negocio que contengan a la seguridad de la información, con el fin de identificar y evaluar los riesgos a los que está expuesta la organización, para proponer mejoras y re-evaluar estos planes de continuidad del negocio de manera continua.
- **Conformidad:** porcentaje de cumplimiento 20%, lo que evidencia que no existe la adecuada conformidad respecto a la seguridad de la información. Se recomienda ejecutar formalmente las guías y costumbres existentes tanto en el puesto de trabajo como dentro de la organización para evitar el mal uso de dispositivos, además de tener claro conocimiento e identificar las leyes a las que se rigen para evitar violaciones al derecho de propiedad intelectual.

2. CAPÍTULO II – EVALUACIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN.

La evaluación de riesgos puede realizarse de diversas formas y con diferentes grados de detalle, dependiendo por un lado de la metodología y por otro de los activos involucrados y el valor que tiene cada uno.

Este capítulo está dedicado a la evaluación de riesgos y para ello se reconoce los controles existentes en la organización además se identifican, estiman y evalúan los activos, las amenazas y las vulnerabilidades existentes dentro del CONADIS, para finalmente determinar el nivel de importancia con que se debe implementar controles con el fin de minimizar los riesgos por medio de la propuesta de tratamiento a los mismos.

La norma ISO/IEC 27005 es una guía para la Gestión de la Seguridad de la Información en una organización, apoyando los requisitos de un SGSI según la ISO/IEC 27001. Sin embargo, esta norma no proporciona ninguna metodología específica para la gestión de riesgos de seguridad de la información[24] [11], por lo que es necesario definir una metodología la misma que se explica en la sección 2.1.2 “Metodologías para la Estimación del Riesgo”.

2.1. ESTABLECIMIENTO DEL CONTEXTO.

Una vez que se ha realizado el diagnóstico de la situación actual de la organización y con la información relevante que se obtuvo se puede establecer los criterios que se utilizan a lo largo de la evaluación del riesgo para la toma de decisiones, basándose principalmente en el criterio para el tratamiento del riesgo y en la importancia de la implementación de los controles, los mismos que únicamente se propondrán debido a que la implementación de estos depende de la aprobación de la alta gerencia.

---

[24] Información tomada de la Norma ISO/IEC 27005 y traducida por los autores.

2.1.1. ALCANCE Y LIMITES

El análisis de riesgos que se presenta a continuación comprende a los activos de soporte y/o apoyo del CONADIS, que dentro de su red de datos maneja y administra información importante de las personas con capacidades especiales, por lo que es transcendental que funcione correctamente y de esta manera actuar ante un evento que se suscite logrando así mitigarlo.

El objetivo del análisis es identificar los activos críticos de la organización, así como las vulnerabilidades y amenazas a las que se encuentran expuestos dichos activos, y así evaluar los riesgos y poder presentar recomendaciones que permitan mitigar los incidentes en la organización y que puedan afectar los servicios que brinda la misma.

2.1.2. METODOLOGÍA PARA EL ANÁLISIS DEL RIESGO

La ISO/IEC 27005 proporciona una guía para realizar el análisis de riesgos de la seguridad de la información especificando parámetros que se debe cumplir en las diferentes fases del proceso, sin embargo se debe apoyar en una metodología, la misma que facilita la estimación del riesgo. Esta metodología puede ser cualitativa, cuantitativa o una combinación de las dos, esto dependerá del nivel de detalle con que se desee analizar así como también de la información que se tenga.

La *Figura 2.1* muestra el proceso de gestión de riesgos de la seguridad de la información que la norma ISO/IEC 27005 propone como guía y la cual se encuentra apoyada en la metodología que se expone en la siguiente sección.

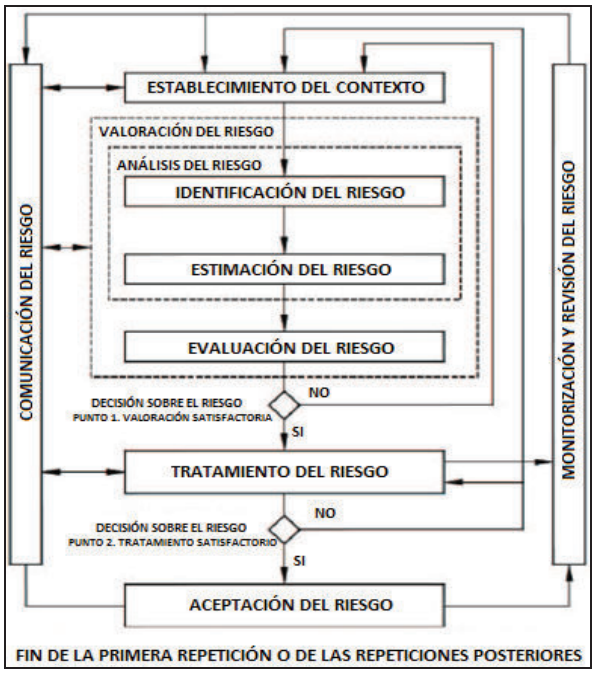

Figura 2.1: Proceso de Gestión del Riesgo.[25]

2.1.2.1. Metodología Cualitativa

Cuando se habla de estimación de riesgos, esta metodología es la más aplicada para la toma de decisiones, ya que es apoyada en su experiencia, dinamismo e intuición, además que está basada en escalar los atributos calificativos describiendo la magnitud del impacto potencial de estos, por ejemplo: Bajo, Moderado, Alto y Crítico.

En esta metodología interactúan cuatro elementos; las amenazas, las vulnerabilidades, el impacto ante la ocurrencia de una amenaza y los controles que se apliquen ya sean preventivos o correctivos. La ventaja que posee esta metodología es su facilidad de comprensión hacia lo que se está realizando.

2.1.2.2. Metodología Cuantitativa

Esta metodología es menos utilizada pues consiste en recolectar datos, realizar cálculos y usar técnicas de modelamiento, etc., que pueden dar como resultado información difícil de estimar. Usa escalas de valoración numérica ya sea para la

---

[25] Figura tomada de la norma ISO/IEC 27005 y traducida por los autores.

evaluación de probabilidades de ocurrencia como para el impacto de estas en base a varios datos lo que permite calcular el nivel de riesgo. La complejidad y exactitud de los valores numéricos, así como la validez del modelo utilizado determina el éxito del uso de esta metodología.

2.1.3. CRITERIOS BÁSICOS

De acuerdo a lo expuesto en las dos metodologías anteriores para llevar a cabo el análisis de riesgos en el CONADIS se constituyen los criterios básicos en base a la combinación de estas, ya que por un lado se califica los atributos como define la metodología cualitativa y junto con ello se da una valoración numérica, que no representa exactamente el uso de la metodología cuantitativa pues no se realizan cálculos matemáticos complejos, sin embargo ayuda a que la estimación del riesgo tenga mayor exactitud.

A continuación se definen los parámetros a tomar en cuenta para la valoración cualitativa de cada atributo de los diferentes criterios que se utilizan para el análisis de riesgo.

Estos criterios se basan en la información recopilada de visitas efectuadas dentro de la organización, además de los criterios puestos en práctica en diferentes proyectos de titulación[26],[27] y a juicio de los autores.

2.1.3.1. Criterios de valoración de activos

Los criterios de valoración de activos se dan de acuerdo a la importancia, funciones dentro de la red y dependencia de estos hacia otros activos. La evaluación de los activos utilizará los criterios de cualificación y valoraciones numéricas que se muestra en la *Tabla 2.1.*

---

[26] Chicaiza P, Díaz A, “Diseño de un Plan de Gestión de Seguridades de la Información para Instituciones Públicas Ecuatorianas”, Proyecto de Titulación EPN, 2014

[27] González A, Tenemaza D, “Análisis de Riesgos y Vulnerabilidades de la Red de Datos de la Empresa Plywood Ecuatoriana S.A utilizando el estándar ISO/IEC 27005:2008”, Proyecto de Titulación EPN, 2012

1	BAJO	Ningún otro activo depende de este para entregar servicios a usuarios.	Activo con capacidades tecnológicas muy limitadas.	La divulgación, modificación y no disponibilidad del activo puede afectar de forma insignificante la entrega de servicios a usuarios.
2	MODERADO	Pocos activos dependen de este para entregar servicios a usuarios.	Activo con capacidades tecnológicas limitadas.	La divulgación, modificación y no disponibilidad del activo puede afectar en parte la entrega de servicios a usuarios.
3	ALTO	Una gran cantidad de activos dependen de este para entregar servicios a usuarios.	Activo con capacidades tecnológicas avanzadas.	La divulgación, modificación y no disponibilidad del activo puede afectar significativamente la entrega de servicios a usuarios.
4	CRÍTICO	Todos los activos dependen de este para entregar servicios a usuarios.	Activo con capacidades tecnológicas de última generación.	La divulgación, modificación y no disponibilidad del activo puede afectar totalmente la entrega de servicios a usuarios.

Tabla 2.1: Criterios para la valoración de activos.[28]

El producto de los valores obtenidos de cada parámetro identificado en la tabla anterior determinará el valor de cada activo, que a su vez pertenecerá a un nivel de importancia, el cual será evaluado de acuerdo a la *Tabla 2.2* que se muestra a continuación.

1 – 8	1	POCO IMPORTANTE	El activo tiene poca importancia para la entrega de servicios a través de la red de datos, de acuerdo a los criterios de dependencia, funcionalidad y confidencialidad, integridad y disponibilidad.
9 – 26	2	IMPORTANTE	El activo es importante para la entrega de servicios a través de la red de datos, de acuerdo a los criterios de dependencia, funcionalidad y confidencialidad, integridad y disponibilidad.

[28] Tabla elaborada por los autores en base a criterios puestos en práctica en diferentes proyectos de titulación.

27 - 64	3	CRÍTICO	El activo es vital para la entrega de servicios a través de la red de datos, de acuerdo a los criterios de dependencia, funcionalidad y confidencialidad, integridad y disponibilidad.
VALOR DEL ACTIVO = DEPENDENCIA * FUNCIONALIDAD * (CONFIDENCIALIDAD, INTEGRIDAD, DISPONIBILIDAD)			

Tabla 2.2: Rango de valores para determinar el nivel de importancia de los activos.[29]

2.1.3.2. Criterios de probabilidad de ocurrencia de amenazas

En la *Tabla 2.3* se muestran los criterios calificativos y los valores numéricos a ser utilizados para la valoración de la probabilidad de amenazas que podrían explotar alguna vulnerabilidad existente.

1 (0 – 25)%	POCO PROBABLE	Probabilidad muy baja de que una amenaza explote una vulnerabilidad.
2 (26 – 50)%	MEDIANAMENTE PROBABLE	Probabilidad baja de que una amenaza explote una vulnerabilidad.
3 (51 – 75)%	PROBABLE	Probabilidad alta de que una amenaza explote una vulnerabilidad.
4 (76 – 100)%	MUY PROBABLE	Probabilidad muy alta de que una amenaza explote una vulnerabilidad.

Tabla 2.3: Criterios de probabilidad de ocurrencia de amenazas.[30]

2.1.3.3. Criterios de valoración de Impacto

El impacto es medir la consecuencia de la materialización de un riesgo, además de ser el valor promedio entre los impactos de integridad, confidencialidad y disponibilidad, siendo así un punto importante al momento de la toma de decisiones para la puesta en marcha de los controles.

---

[29] Tabla elaborada por los autores en base a criterios puestos en práctica en diferentes proyectos de titulación.
[30] Tabla elaborada por los autores en base a criterios puestos en práctica en diferentes proyectos de titulación.

Para valorar el impacto, se debe definir criterios de valoración para la confidencialidad, integridad y disponibilidad, siendo estos “1” para el valor mínimo, “2” para el valor medio y “3” para el valor alto.

La *Tabla 2.4* muestra los criterios de valoración de impacto, estos valores están dados por el promedio entre la confidencialidad, integridad y disponibilidad.

1	BAJO	El impacto entre la confidencialidad, integridad y disponibilidad es mínimo.
2	MEDIO	El impacto entre la confidencialidad, integridad y disponibilidad es medio.
3	ALTO	El impacto entre la confidencialidad, integridad y disponibilidad es alto.

Tabla 2.4:Criterios de valoración de impacto.[31]

2.1.3.4. Criterios de evaluación del riesgo

El producto entre la probabilidad de ocurrencia de una amenaza y el impacto que esta pudiese ocasionar da como resultado el nivel de riesgo de cada activo, los valores para esta evaluación se pueden observar en la *Tabla 2.5.*

1 – 2	BAJO	El riesgo del activo es bajo
3 – 4	MODERADO	El riesgo del activo es moderado
5 – 8	ALTO	El riesgo del activo es alto.
9 – 12	CRÍTICO	El riesgo del activo es crítico.
NIVEL DE RIESGO = PROBABILIDAD * IMPACTO		

Tabla 2.5: Criterios de evaluación del riesgo.[32]

[31] Tabla elaborada por los autores en base a criterios puestos en práctica en diferentes proyectos de titulación.

2.1.3.5. Criterios para el tratamiento del riesgo

El tratamiento de riesgos es tomar decisiones frente a los diferentes riesgos existentes de acuerdo a la estrategia de la organización. Las posibles acciones de tratamiento de riesgo son:

- **Reducir:** consiste en elegir controles de corrección, eliminación, prevención, mitigación del impacto, detección, recuperación, monitoreo y concienciación con el fin de reducir el nivel del riesgo.
- **Aceptar:** no es necesario implementar controles adicionales, estos riesgos podrán ser aceptados teniendo en cuenta que la organización asume los daños provocados por la materialización del riesgo.
- **Evitar:** o eliminar el riesgo, que no suele ser la mejor opción ya que resulta difícil o demasiado costoso, pues muchas de las veces se basa en eliminación de procesos o incluso del activo involucrado.
- **Transferir:** a un tercero de forma que se asegure el activo, o subcontratando el servicio.

De acuerdo a la política de tratamiento de riesgos que maneja el CONADIS, la cual está aprobada y en vigencia, las acciones para tratar los riesgos son: “Aceptar” y “Reducir”.

“Cuando los daños provocados por la materialización de un riesgo no han afectado mayormente las actividades regulares de los funcionarios de la organización, el CONADIS toma la decisión de aceptar dicho riesgo.” [12]

“Cuando los daños provocados por la materialización de un riesgo han afectado las actividades regulares de los funcionarios de la organización, el CONADIS toma la decisión de reducir dicho riesgo. El Centro de Información tiene la obligación de reducir el riego por medio de implementación de controles que mitiguen el impacto que provocaría la materialización del mismo.” [12]

---

[32] Tabla elaborada por los autores en base a criterios puestos en práctica en diferentes proyectos de titulación.

Dado que esta política ha sido aprobada por la dirección, se encuentra vigente y ha sido validada por la organización en base a las necesidades de la misma, en el presente proyecto se utilizarán los mismos criterios de tratamiento de riesgo según la *Tabla 2.6* que se muestra a continuación.

BAJO	ACEPTAR EL RIESGO
MODERADO	
ALTO	REDUCIR EL RIESGO
CRÍTICO	

Tabla 2.6 Criterios de tratamiento del riesgo.[33]

2.1.3.6. Criterios de prioridad en la aplicación de controles

Para la aplicación de los controles se debe tomar en cuenta la prioridad en que deben ser implementados dichos controles. El cálculo de dicha prioridad está basado tanto en el nivel del riesgo como en el nivel de importancia del mismo. La *Tabla 2.7* muestra los criterios de prioridad en la aplicación de controles.

1 – 13	BAJA	Los controles a los activos pueden esperar para ser implementados hasta después de que los controles de media y alta prioridad se hayan efectuado.
14 – 23	MEDIA	Los controles a los activos pueden esperar para ser implementados hasta después de que los controles de alta prioridad se hayan efectuado.
24 – 36	ALTA	Los controles a los activos deben ser implementados de forma inmediata.
PRIORIDAD EN LA APLICACIÓN DEL CONTROL = NIVEL DE IMPORTANCIA * NIVEL DEL RIESGO		

Tabla 2.7: Criterios de prioridad en la aplicación de controles.[34]

---

[33] Tabla elaborada por los autores de acuerdo a las estrategias de tratamiento de riesgo de la organización.
[34] Tabla elaborada por los autores en base a criterios puestos en práctica en diferentes proyectos de titulación.

2.2. ANÁLISIS DE RIESGOS

El objetivo del análisis de riesgos es identificar los activos que aportan valor a la organización, las amenazas que podrían afectar el funcionamiento normal de las actividades de la organización además del impacto que podrían causar estas de llegar a darse, y las medidas que se deben llevar a cabo para minimizar o eliminar el impacto de los riesgos existentes.

2.2.1. IDENTIFICACIÓN DE RIESGOS

El objetivo principal dentro de la identificación de riesgos, es determinar los activos que proveen servicios a través de la red de datos del CONADIS hacia todos sus usuarios, ya sean internos y/o externos, así como las amenazas a los que se encuentran expuestos estos activos, las vulnerabilidades que podrían ser explotadas por las amenazas y el impacto que podrían ocasionar si no se cuenta con controles apropiados.

2.2.1.1. Identificación de Activos

Identificar los activos de la organización es un punto clave para poder validar los mismos para lo cual se ha dividido en Activos Primarios y Activos de Soporte y/o Apoyo.

Activos Primarios

En esta categoría están servicios, procesos y actividades que son esenciales para el correcto funcionamiento de la organización además de que estos activos dependen de los activos de soporte o apoyo y están divididos en de procesos y actividades del negocio y de información.

La *Tabla 2.8* que se muestra a continuación presenta una lista de Activos Primarios del CONADIS.

Procesos y Actividades del Negocio	Gestión y Manejo de políticas e información del sector público y privado en el ámbito de discapacidades.
	Canalizar recursos nacionales e internacionales en el campo de discapacidades.
	Gestión de actividades para la prevención, atención e integración de personas con capacidades especiales.

	Internet Corporativo (Incluye Correo y Web Hosting).
	Telefonía Interna.
Información	Base de Datos del Sistema Centralizado del CONADIS.
	Base de Datos de Correo Electrónico.
	Base de Datos Nómina Personal.
	Manuales y Documentación Base del CONADIS.
	Archivos de trabajo de empleados.
	Respaldos información de CONADIS.
	Respaldos personales realizados por empleados.

Tabla 2.8: Activos Primarios[35]

Activos de Soporte y/o Apoyo

En esta categoría están aquellos activos de los cuales dependen los activos primarios y están divididos en de soporte físico[36] y de soporte humano[37].

La *Tabla 2.9* que se muestra a continuación presenta una lista de Activos de Soporte y/o Apoyo del CONADIS.

Activos de Soporte Físico – Hardware	Servidor Microsoft 2003 Server
	Servidor Linux Red Hat
	Servidor Linux CentOS
	UPS
	PCs
	Laptops
	Impresoras
Activos de Soporte Físico – Software Base Empresarial	Sistema Operativo Windows 2003 Server
	Sistema Operativo Linux Red Hat
	Sistema Operativo Linux CentOS
	Sistema Operativo Windows 2008 Server
	Sistema Operativo Windows 7 (PCs)
	Sistema Operativo Windows XP (PCs)
	Sistema Operativo Windows Vista (PCs)
	Sistema Operativo Linux Ubuntu (PCs)
	Sistema de Control de Bienes MEGAN
	Sistema de Control de Personal BIOSYSTEM
	Sistema Jurídico LEXIS
	Gestor de Respaldos
	Microsoft Office
	Open Office
	Antivirus
	Gestor de Base de Datos
	Sistema Documental Quipux

[35] Tabla elaborada por los autores en base a información proporcionada por el responsable del Centro de información y la norma ISO/IEC 27005.
[36] Soporte tanto de hardware, de software y de red.
[37] Tanto personal del centro de información como personal administrativo que requiera acceso a la red de la organización.

	Sistema Declaración de Información en Medio Magnético
Activos de Soporte Físico – Red	Switch/Hub Principal
	Switch Edificio Administrativo
	Switch Edificio 2
	Access Point 1
	Access Point 2
Activos de Soporte Humano	Director General
	Director Administrativo Financiero
	Director Técnico
	Director de Procuraduría
	Director de Recursos Humanos
	Responsable Centro de Información

Tabla 2.9: Activos de Soporte y/o Apoyo[38]

2.2.1.2. Valoración de Activos

La *Tabla 2.10* muestra la valoración de los activos utilizando los criterios definidos según la escala mostrada en la sección 2.1.3.1 "Criterios de valoración de activos".

	DEPENDENCIA	**FUNCIONALIDAD**	**CONFIDENCIALIDAD INTEGRIDAD Y DISPONIBILIDAD**	
Servidor Microsoft 2003 Server	4	3	4	48
Servidor Linux Red Hat	4	3	3	36
Servidor Linux CentOS	4	3	3	36
UPS	4	3	2	24
PCs	2	3	2	12
Laptops	2	3	2	12
Impresoras	2	2	2	8
Sistema Operativo Windows 2003 Server	1	3	4	12
Sistema Operativo Linux Red Hat	1	3	4	12
Sistema Operativo Linux CentOS	1	3	4	12
Sistema Operativo Windows 2008 Server	1	2	2	4

[38] Tabla elaborada por los autores en base a información proporcionada por el responsable del Centro de información y la norma ISO/IEC 27005.

Sistema Operativo Windows 7 (PCs)	3	3	2	18
Sistema Operativo Windows XP (PCs)	2	3	2	12
Sistema Operativo Windows Vista (PCs)	1	2	2	4
Sistema Operativo Linux Ubuntu (PCs)	3	3	2	18
Sistema de Control de Bienes MEGAN	4	3	1	12
Sistema de Control de Personal BIOSYSTEM	2	4	1	8
Sistema Jurídico LEXIS	2	3	1	6
Gestor de Respaldos	3	3	2	18
Microsoft Office	2	3	2	12
Open Office	2	3	2	12
Antivirus	4	3	2	24
Gestor de Base de Datos	3	3	2	18
Sistema Documental Quipux	2	3	2	12
Sistema Declaración de Información en Medio Magnético	2	3	2	12
Switch/Hub Principal	3	3	3	27
Switch Edificio Administrativo	3	2	3	18
Switch Edificio 2	3	2	3	18
Access Point 1	2	3	3	18
Access Point 2	2	3	3	18

Tabla 2.10: Valoración de activos.[39]

De acuerdo a los resultados obtenidos en la tabla anterior, los activos críticos de la organización y que serán sometidos al análisis son; Servidor Microsoft 2003 Server, Servidor Linux Red Hat, Servidor Linux CentOS y el Switch/Hub Principal.

2.2.1.3. Identificación de Vulnerabilidades y Amenazas

[39] Tabla elaborada por los autores.

“Una vulnerabilidad o fallo de seguridad, es todo aquello que hace que nuestros sistemas de información funcionen de forma diferente para lo que estaban pensados, afectando a la seguridad de los mismos, pudiendo llegar a provocar entre otras cosas la pérdida y robo de información sensible” [13].

Las vulnerabilidades se relacionan directamente con las amenazas[40] ya que si no existe amenaza tampoco existe vulnerabilidad o la importancia de esta es nula ya que no hay forma de que cause daño dicha amenaza. La lista completa de amenazas de acuerdo a la norma se encuentra detallada en el Anexo II.

La identificación de vulnerabilidades a consecuencia de las amenazas naturales, físicas o ambientales, humanas o accidentales y organizacionales se realizó en base a visitas y entrevistas en el CONADIS. La *Tabla 2.11* muestra las vulnerabilidades encontradas en estos grupos y de acuerdo a las amenazas existentes dentro de la organización.

VULNERABILIDAD	FUENTE DE AMENAZA
No posee un Plan de Contingencia de Recuperación de desastres.	Fenómenos Sísmicos
Falla de la planta de energía propia o generadores de energía eléctrica de respaldo.	Tormenta Eléctricas
Los equipos que tienen una vida de uso alta, no se encuentran asegurados contra daño.	
Falla en los reguladores de voltaje para los equipos de computación.	Falla eléctrica
Falla de la planta de energía propia o generadores de energía eléctrica de respaldo.	
No existen sistemas de ventilación o aire acondicionado adecuados.	Sobrecalentamiento de equipos
No existen sistemas de ventilación o aire acondicionado adecuados.	Condiciones de trabajo inadecuadas
El puesto de trabajo del personal en algunos casos se encuentra fuera del área correspondiente.	

[40] Amenaza: posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema, http://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/

VULNERABILIDAD	FUENTE DE AMENAZA
Falta de conocimiento ante ausencia de un empleado.	Pérdida de personal
No existe la política de cambio de clave cada determinado tiempo.	Crimen Computacional
Falta de identificación emisor – receptor.	
No existe control sobre Ingeniería Social.	
Falla en las políticas de seguridad establecidas.	
Falta de continua capacitación al personal con respecto a la Seguridad Informática.	Personal y Usuarios internos descontentos, negligentes, deshonestos, cesados, etc.
Falta de concientización con respecto a la Seguridad Informática.	
Trabajo no supervisado de personal externo.	
VULNERABILIDAD	**FUENTE DE AMENAZA**
No posee Plan de Contingencias.	Falta/Insuficiencia de normas
No existe política que exija documentar toda actividad realizada.	Falta e inadecuada documentación
Falta de uso de estándares para la documentación.	
Incumplimiento de las políticas de seguridad informática.	Falta o Insuficiente gestión de la seguridad de la información
Falta de asignación adecuada de responsabilidades en la seguridad de la información.	
Falta de bitácoras.	
Falta de licencias	Falta de licencias de software propietario o violaciones de derecho de autor

Tabla 2.11: Identificación de Vulnerabilidades según el tipo de amenaza.[41]

Por otra parte la identificación de vulnerabilidades que se relacionan con las amenazas técnicas fueron realizadas con la técnica de Pruebas de Penetración o también conocido como Hacking Ético, (para mayor información sobre Hacking Ético ver Anexo III), que permiten evaluar las medidas de seguridad en una red. La herramienta para ello fue Nessus, (para mayor información sobre Nessus ver Anexo IV).

La *Tabla 2.12* muestra las vulnerabilidades técnicas que se identificaron en la red, después de haber realizado las pruebas de penetración, (para mayor detalle sobre las pruebas realizadas ver Anexos V, VI y VII), las mismas que harían que

[41] Tabla elaborada por los autores en base a ejemplos especificados en la norma ISO/IEC 27005.

una amenaza se concrete.

Los controles son efectuados por la experiencia más que por una política o un procedimiento.	Operación incorrecta de Controles existentes
Controles obsoletos, que muchas de las veces no brindan la suficiente seguridad a los activos de información.	
Falta de monitorización que verifique que los controles se están realizando y que están cumpliendo el propósito para el cual fueron implementados.	
Software y/o aplicaciones nuevas (implementación de nuevas aplicaciones a nivel entidades públicas y poca capacitación en el uso de las mismas.)	Falla de Software/Aplicaciones
Falta de documentación y manuales de uso.	
Defectos del nuevo software y/o aplicación.	
Uso de software no licenciado	
Deficiente diseño de red.	Saturación de red
Puntos de red con fallas.	
Acceso a red a invitados poco segura, vulnerable a ataques informáticos.	
Puertos con poca seguridad(puertos abiertos)	Ataques informáticos (Nivel de gravedad informativo)
Obtención de información de host (SO, red)	
Servicios compartidos de archivos o impresoras en estado de escucha.	
Habilitación de Windows Terminal Services[42]	
Servicio RPC corriendo[43].	
Posibilidad de inicio de sesión en el host remoto mediante cuentas: Sesión NULL, cuenta de invitado y Credenciales dadas.	
Cliente RDP no hace ningún esfuerzo para validar la identidad del servidor al configurar el cifrado[44]	Ataques informáticos (Nivel de gravedad
Servidor RDP almacena una clave privada RSA no modificable[45].	

[42] Cuando se encuentra habilitado Windows Terminal Services, un usuario podría registrarse remotamente y gráficamente en el host, pudiendo actuar como un usuario local.
[43] Cuando el Servicio RPC está corriendo posibilita la conexión y enlace con cada servicio mediante una solicitud RPC al puerto.
[44] El cliente RDP no hace ningún esfuerzo para validar la identidad del servidor al configurar el cifrado lo que provoca que el Terminal Service sea vulnerable a un ataque “man-in-the-middle”(un ataque de esta naturaleza permitiría al atacante obtener información sensible transmitida, incluyendo las credenciales de autenticación, https://www.owasp.org/index.php/Man-in-the-middle_attack)
[45] Cuando el servidor RDP almacena una clave privada RSA no modificable por lo que cualquier usuario local con acceso al archivo puede recuperar la clave y utilizarla para el ataque.

	Riesgo Medio)
Falta de esquema de remplazo periódico de equipos.	Falla de equipos
Sobrecalentamiento de equipos.	
Equipos sobrecargados de funciones.	
Falta de capacitación de uso de equipos a usuarios finales.	

Tabla 2.12: Identificación de Vulnerabilidades según las pruebas de penetración.[46]

2.2.1.4. Identificación de los Controles Existentes

Como se mencionó en el primer capítulo el CONADIS posee muy poca información documentada, esto implica que no posee adecuada documentación sobre controles y menos de planes de implementación de tratamiento de riesgos. A pesar de esto el Centro de Información aun cuando no posee documento formal de políticas de administración de red realiza actividades de controles que de una u otra forma logran minimizar la probabilidad de que una amenaza pueda ocurrir.

La *Tabla 2.13* muestra los controles que se encuentran implementados en la organización.

AMENAZAS NATURALES, FÍSICAS O AMBIENTALES	Sistemas contra Incendios	Toda la organización posee detectores de humo, extintores y la respectiva señalética en caso de una emergencia.
	Sistemas de enfriamiento (ventiladores, aire acondicionado)	Existe este tipo de control, sin embargo los ventiladores con los que se cuenta no son suficientes, a excepción del área de servidores.
	Backups	Dependiendo del tipo de información, los backups se realizan de acuerdo a la política establecida dentro de la organización. Los servicios más sensibles también cuentan con sus respectivos backups, además de que todos estos backups son probados cada cierto tiempo para asegurar su funcionamiento.
	Sistema Ininterrumpible de Energía (UPS)	El funcionamiento continuo de los servidores está garantizado debido a este control.
	Planta de Energía	Permite continuar de manera regular sus actividades cuando exista corte de energía.
	Seguridad Física	Existe un control de registro al momento de ingreso a la organización, mas no así para el ingreso a sus diferentes áreas. Además de que cuenta con un sistema CCTV.

[46] Tabla elaborada por los autores en base a ejemplos especificados en la norma ISO/IEC 27005.

	Seguridad en el Cableado	Existen canaletas que protegen todo el cableado de la organización.
AMENAZAS HUMANAS O ACCIDENTALES	Antivirus	Al ser una entidad pública cuenta con antivirus corporativo que ayuda a que este control se cumpla.
	Capacitación al personal de la organización	Cuando existe contratación de personal, este es capacitado para cumplir las funciones que se le serán asignadas. Además todo el personal se encuentra en constante capacitación tanto técnica como social, esta última corresponde a que interactúan con personas con capacidades especiales.
	Auditorías Internas	Existe este control, debido a que la Contraloría General del Estado las efectúa de manera rutinaria como en todas las instituciones públicas
	Firewall	Control implementado ante acceso no autorizado a la red.
	Uso de recursos de red	El control se encuentra establecido, debido a que la red se encuentra monitoreada constantemente además de que existen bloqueos de acceso a ciertos sitios web.
	Usuario y contraseña	El control esta implementado, pero el usuario y contraseña con únicos y por ningún motivo el usuario puede cambiarlo sin petición formal al Centro de Información.
AMENAZAS TÉCNICAS	Personal capacitado para brindar soporte (mesa de servicios)	Hasta el momento, el personal que brinda soporte a la organización está totalmente capacitado para dar solución a un inconveniente.
AMENAZAS ORGANIZACIONALES	Garantías	Los equipos cuentan con garantía de fábrica.
	Licencias	Las estaciones de trabajo cuentan con software licenciado y open source.
	Seguros	El personal y los equipos se encuentran debidamente asegurados. En el caso de los equipos el seguro cubre daños y robos suscitados dentro de la organización

Tabla 2.13: Controles existentes.[47]

2.2.2. ESTIMACIÓN DEL RIESGO

La estimación del riesgo es la “Actividad para asignar valores a la posibilidad y las consecuencias de un riesgo” [7]

2.2.2.1. Valoración del Impacto

[47] Tabla elaborada por los autores en base a ejemplos especificados en la norma ISO/IEC 27005.

Para la valoración del impacto que producen las amenazas a cada activo, se utiliza los criterios de impacto definidos en la *Tabla 2.4,* en el ejemplo de la *Tabla 2.14* el promedio de valoraciones entre confidencialidad, integridad y disponibilidad es de 1.67 lo que en números enteros será 2 de impacto en el activo crítico Servidor de Aplicaciones cuando la vulnerabilidad de No poseer un Plan de Contingencia de Recuperación de desastres frente a la amenaza Fenómeno Sísmico llegase a materializarse.

SERVIDOR DE APLICACIONES						
TIPO DE AMENAZA	**VULNERABILIDAD**	**FUENTE DE AMENAZA**	**CONFIDENCIALIDAD**	**INTEGRIDAD**	**DISPONIBILIDAD**	**IMPACTO**
AMENAZAS NATURALES, FÍSICAS O AMBIENTALES	No posee un Plan de Contingencia de Recuperación de desastres.	Fenómenos Sísmicos	1	1	3	2

Tabla 2.14:Ejemplo de Valoración de Impacto.[48]

2.2.2.2. Valoración de Incidentes

Para la valoración de los incidentes para cada activo, se utiliza los criterios de probabilidad de ocurrencia de amenazas que se muestra en la *Tabla 2.3*, en el ejemplo de la *Tabla 2.15* la probabilidad de ocurrencia de la amenaza Fenómenos Sísmicos es baja por lo que su valoración es 1.

TIPO DE AMENAZA	**VULNERABILIDAD**	**FUENTE DE AMENAZA**	**PROBABILIDAD**
AMENAZAS NATURALES, FÍSICAS O AMBIENTALES	No posee un Plan de Contingencia de Recuperación de desastres.	Fenómenos Sísmicos	1

Tabla 2.15: Ejemplo de Valoración de Incidentes (Probabilidad de Ocurrencia).[49]

[48] Tabla elaborada por los autores.
[49] Tabla elaborada por los autores.

2.3. EVALUACIÓN DE RIESGOS

Esta sección está dedicada a la evaluación del riesgo, para lo cual se identificó los activos críticos, así como también sus respectivas vulnerabilidades y el impacto que provoca si la amenaza ocurre.

La T*abla 2.16* muestra los resultados obtenidos de la evaluación del riesgo al activo crítico “Servidor Microsoft 2003 Server”, de acuerdo a los criterios de evaluación del riesgo, definidos en la sección 2.1.3.4, así mismo los resultados obtenidos de los demás activos críticos se encuentran en el Anexo VIII.

SERVIDOR DE APLICACIONES									
TIPO DE AMENAZA	**VULNERABILIDAD**	**FUENTE DE AMENAZA**	**CONFIDENCIALIDAD**	**INTEGRIDAD**	**DISPONIBILIDAD**	**IMPACTO**	**PROBABILIDAD**	**NIVEL DE RIESGO**	**PT[50]**
AMENAZAS NATURALES, FÍSICAS O AMBIENTALES	No posee un Plan de Contingencia de Recuperación de desastres.	Fenómenos Sísmicos	1	1	3	2	1	2	ACEPTAR
	Falla de la planta de energía propia o generadores de energía eléctrica de respaldo.	Tormenta Eléctricas	1	1	3	2	2	4	ACEPTAR
	Los equipos que tienen una vida de uso alta, no se encuentran asegurados contra daño.								
	Falla de la planta de energía propia o generadores de energía eléctrica de respaldo.	Falla eléctrica	1	2	3	2	3	6	REDUCIR
AMENAZAS HUMANAS O ACCIDENTALES	Falta de continua capacitación al personal con respecto a la Seguridad Informática.	Personal y Usuarios internos descontentos, negligentes, deshonestos, cesados, etc.	2	2	1	2	1	2	ACEPTAR
	Falta de concientización con respecto a la Seguridad Informática.								
AMENAZAS ORGANIZACIONALES	No posee Plan de Contingencias.	Falta/Insuficiencia de normas	1	2	1	1	3	3	ACEPTAR
	No existe política que exija documentar toda actividad realizada.	Falta e inadecuada documentación	2	1	3	2	2	4	ACEPTAR
	Falta de uso de estándares para la documentación.								
	Falta de bitácoras.	Falta o Insuficiente gestión de la seguridad de la Información.	3	3	2	3	4	12	REDUCIR
AMENAZAS TÉCNICAS	Los controles son efectuados por la experiencia más que por	Operación incorrecta de Controles existentes	2	3	3	3	3	9	REDUCIR

[50] Plan de Tratamiento del Riesgo

	una política o un procedimiento.								
	Falta de monitorización que verifique que los controles se están realizando y que están cumpliendo el propósito para el cual fueron implementados.								
	Falta de documentación y manuales de uso.	Falla de Software/Aplicaciones	1	2	3	2	3	6	REDUCIR
	Puertos con poca seguridad(puertos abiertos)	Ataques informáticos (Nivel de gravedad informativo)	2	3	1	2	3	6	REDUCIR
	Obtención de información de host (SO, red)								
	Servicios compartidos de archivos o impresoras en estado de escucha.								
	Habilitación de Windows Terminal Services								
	Servicio RPC corriendo								
	Equipos sobrecargados de funciones.	Falla de equipos	1	2	3	2	3	6	REDUCIR

Tabla 2.16: Evaluación del Riesgo.[51]

[51] Tabla elaborada por los autores en base a la norma ISO/IEC 27005 y los criterios de evaluación propuestos en el presente proyecto.

2.3.1. OBSERVACIONES DE LA EVALUACIÓN DEL RIESGO

Una vez que se determinaron los activos críticos dentro del Consejo Nacional de Igualdad de Discapacidades y se los evaluaron se determinaron las siguientes observaciones:

- Los riesgos representados en color rojo determinan el valor de riesgo más alto y son estos los que se debe tener muy en cuenta al momento de establecer los controles establecidos dentro de la norma.
- Una de las amenazas evaluadas con mayor nivel de riesgo es; Falta o Insuficiente gestión de la seguridad de la información, esto se debe a que la probabilidad de que ocurra esta amenaza es crítica y el impacto respecto a la integridad, confidencialidad y disponibilidad es alto.
- Los servidores y el Switch/Hub Principal detectados como activos críticos deben tener mejores medidas de seguridad evitando así daños y accesos físicos no deseados. El continuo funcionamiento de estos es de gran prioridad para la organización debido a que son los más importantes para brindar servicios.
- El nivel de riesgo determinado por las amenazas técnicas, se determina como alto en los activos analizados, esto debido a que el impacto y la probabilidad de ocurrencia son altos, razón por la que se debe concientizar en las políticas y en los métodos de aplicación de un control.

2.4. TRATAMIENTO DE RIESGOS

En esta sección se determina los controles que la norma establece para tratar los riesgos antes identificados. Para identificar la prioridad con que se debe implementar los controles, a cada uno de los activos críticos, se realiza lo siguiente:

Para la amenaza Falla eléctrica en la *Tabla 2.17,* el valor que se determinó para el Nivel de Riesgo (NR) fue 6 lo que indica que se encuentra en el nivel cualificado como “Alto”. De la misma manera, se toma la valoración del activo crítico para este caso el “Servidor Microsoft 2003 Server”, que fue de 48 lo que indica que se encuentra en un nivel cualificado como “Crítico” es decir el Nivel de Importancia

(NI) es de 3. Con estos valores se determina la Prioridad, mediante el producto de estos, en la que los controles deben ser implementados sobre los activos críticos, es decir, (NR = 6) x (NI = 3) = 18, que de acuerdo a la *Tabla 2.7* este valor se encuentra dentro de una Prioridad "Media".

ACTIVO	NI	AMENAZA	VULNERABILIDAD	CONTROL	NR	PRIORIDAD
Servidor Microsoft 2003 Server	3	Falla Eléctrica	Falla de la planta de energía propia o generadores de energía eléctrica de respaldo.	A.9.2.2 Suministro eléctrico.	6	18

Tabla 2.17: Ejemplo de Prioridad en la implementación de comtroles.[52]

La prioridad en la implementación de los controles seleccionados se encuentra en el Anexo IX.

2.4.1. SELECCIÓN DE CONTROLES

Identificados los activos de información críticos, las vulnerabilidades y amenazas, y evaluado el nivel del riesgo, se seleccionan controles de seguridad de acuerdo a la norma ISO/IEC 27001 para mitigar dichos riesgos. La *Tabla 2.18* muestra los controles a implementar en el activo crítico "Servidor Microsoft 2003 Server". Todos los controles que fueron seleccionados se encuentran en el Anexo X y los controle seleccionados por activo crítico en el Anexo IX.

ACTIVO	AMENAZA	VULNERABILIDAD	Nivel de Riesgo	CONTROLES SELECIONADOS
Servidor Microsoft 2003 Server	Falla Eléctrica	Falla de la planta de energía propia o generadores de energía eléctrica de respaldo.	6	A.9.2.2 Suministro eléctrico.
	Falta o Insuficiente gestión de la seguridad de la información	Falta de bitácoras.	12	A.13.2.1 Identificación de responsabilidades y procedimientos. A.13.2.3 Recogida de pruebas.

[52] Tabla elaborada por los autores.

	Operación incorrecta de Controles existentes	Los controles son efectuados por la experiencia más que por una política o un procedimiento.	6	A.5.1.2 Revisión de la política de seguridad de la información. A.6.1.8. Revisión Independiente de la Seguridad de la Información. A.10.1.2. Control de cambios operacionales.
		Falta de monitorización que verifique que los controles se están realizando y que están cumpliendo el propósito para el cual fueron implementados.		
	Ataques Informáticos (Nivel de gravedad informativo)	Puertos con poca seguridad (puertos abiertos).	6	A.10.4.1 Medidas y controles contra software malicioso. A10.6.1 Controles de red. A10.6.2 Seguridad en los servicios de red. A.10.10.2 Supervisión del uso de los sistemas. A.11.4.1 Política de uso de los servicios de red. A.11.4.2 Autenticación de usuario para conexiones externas. A.11.4.3 Autenticación de nodos de la red. A.11.4.7 Control de encaminamiento en la red.
		Obtención de información de host.		
		Servicios compartidos de archivos o impresoras en estado de escucha.		
		Habilitación de Windows Terminal Services.		
		Servicio RPC corriendo.		
	Falla de equipos	Equipos sobrecargados de funciones.	6	A.9.2.1 Instalación y protección de equipos. A.9.2.4 Mantenimiento de equipos.
	Falla de Software/ Aplicaciones	Falta de documentación y manuales de uso.	6	A. 7.1.3 Acuerdos sobre el uso adecuado de los activos. A.10.1.1. Documentación de procedimientos operativos.

Tabla 2.18: Controles al activo crítico "Servidor Microsoft 2003 Server"[53]

2.4.2. OBSERVACIONES DEL TRATAMIENTO DEL RIESGO

Los controles que se sugiere sean implementados se encuentra en el Anexo X, el cual muestra todos los controles de la norma y especifica los que aplican a los activos críticos. Cabe mencionar que sin la autorización, apoyo y compromiso de

[53] Tabla elaborada por los autores en base a la norma ISO/IEC 27002, la norma ISO/IEC 27005 y los criterios de evaluación propuestos en el presente proyecto.

la Dirección, la implementación no podría efectuarse, por tal motivo todos los controles relacionados con esto serán incluidos como aplicables.

Los controles a estas amenazas existentes en estos activos, propuestos por la norma, se sugiere que sean implementados según los criterios de prioridad de implementación mostrados en la *Tabla 2.7*, para ver la prioridad en la implementación de controles ver Anexo IX, sin embargo no todos pueden ser puestos en marcha al mismo tiempo, por lo que se deben ir implementando según las posibilidades y necesidades de priorización que el Centro de Información les dé a los mismos y sobre todo después de la aprobación de las autoridades de la organización.

3. CAPÍTULO III – DESARROLLO DE PLAN DE SEGURIDAD DE LA INFORMACIÓN.

Para el desarrollo de un plan de seguridad de la información se debe tener claro lo que es un SGSI, para lo cual se empezará diciendo que es un conjunto de políticas de administración de la información que permiten reducir los riesgos por medio de la incorporación y seguimiento de controles para así reducir las amenazas hasta que estas sean asumibles por la organización, de tal manera que si llegase a ocurrir un incidente los daños se minimizarían y la continuidad del negocio estaría asegurada.

"Como concepto clave de un SGSI se tiene que es el diseño, implantación y mantenimiento de un conjunto de procesos que permiten la gestión eficientemente de la accesibilidad de la información, logrando asegurar la confidencialidad, integridad y disponibilidad de los activos de información y minimizando al mismo tiempo los riesgos de seguridad de la información." [14]

Algunos de los beneficios de un SGSI son[54]:

- Permitir el análisis de riesgos, por medio de la identificación de amenazas, vulnerabilidades, mostrando el impacto en la actividad del negocio.
- Mejorar la continuidad en la gestión de la seguridad.
- Garantizar la continuidad y disponibilidad del negocio.
- Reducir los costos que provocan los incidentes.

La familia de normas ISO/IEC 27000 adopta un modelo para la implementación y mejora de un SGSI denominado PHVA (planear-hacer-verificar-actuar), dicho modelo se basa en la mejora continua.

---

[54] Información tomada de http://www.ceeisec.com/nuevaweb/doc/informacionSGSI.pdf

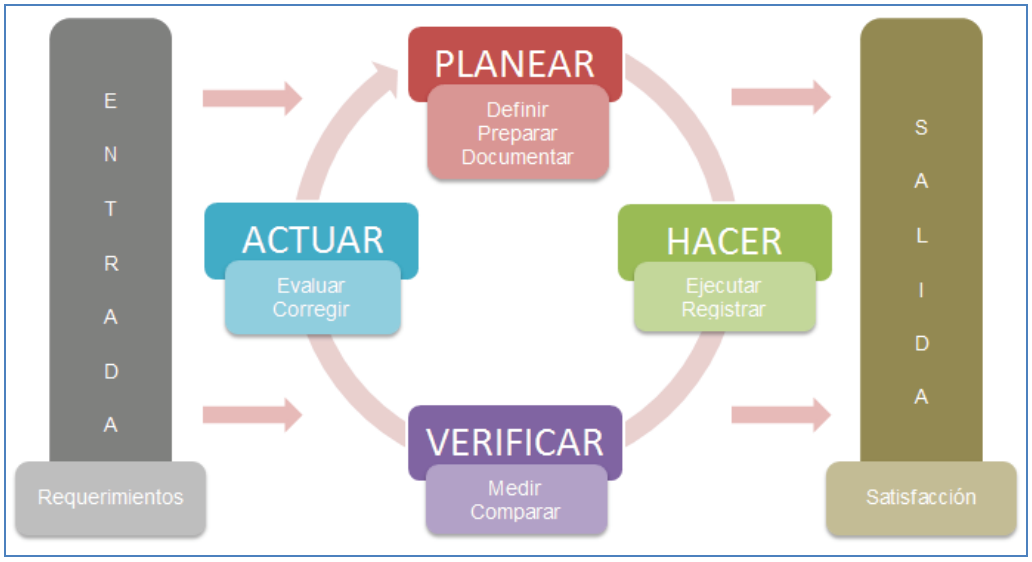

Figura 3.1: Modelo PHVA de SGSI.[55]

3.1. ALCANCE Y LÍMITES.

El plan de seguridad de la información se enfoca a reducir los riesgos encontrados en las diferentes áreas, procesos y activos dentro de una organización y dependiendo cual sea el caso se define el alcance y límite al que se encuentra ligado. Para el caso del CONADIS, el plan de seguridad de la información está orientado a tratar los riesgos de los activos críticos obtenidos del análisis realizado anteriormente, y de esta manera gestionar adecuadamente la información, además de dar pautas para mitigar los riesgos de seguridad de la información.

Se debe tomar en cuenta que la implementación de un plan de seguridad de la información requiere de recursos, por lo que la organización debe estar consciente de las razones del porque implementarlo, estás razones conllevan a determinar costos, aprobación de Dirección o Alta Gerencia y beneficios los mismos que deben estar documentados.

El plan de seguridad de la información que se presenta a continuación está enfocado a proteger a los activos críticos, sin embargo la implementación no se

[55] Figura elaborada por los autores en base al material proporcionado del Curso: Seguridad de la Información – SGSI basado en ISO 27001, CEC-EPN, Noviembre 2014.

encuentra dentro del alcance de este proyecto de titulación pero se proporciona una guía para poder implementarlo cuando la Dirección lo desee.

3.2. ELABORACIÓN DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN.

El plan de seguridad de la información proporciona directrices necesarias para gestionar de manera correcta la seguridad de la información basándose principalmente en la gestión actual de la misma y proponiendo ideas para mejorarla en el momento de su implementación.

Es por esta razón que el diseño del plan de seguridad de la información para el CONADIS servirá como guía para gestionar adecuadamente la información asociada a los activos críticos, así como también proporcionará una serie de pautas para priorizar el manejo de los riesgos de la seguridad de la información.

Cabe recalcar que el presente proyecto de titulación está centrado en la fase de planificación, es decir que la implementación, verificación y mejoramiento del plan queda a total criterio de los directivos del CONADIS. Esta fase consiste en definir políticas, objetivos, procesos y procedimientos del SGSI para la gestión del riesgo y la mejora de la seguridad de la información.[56]

3.2.1. FASES Y ENTREGABLES

El SGSI según la norma ISO/IEC 27001 incluye diferentes documentos entregables, la *Tabla 3.1* muestra la aplicabilidad de los documentos para el presente proyecto:

Procedimiento para Control de Documentos y Registros	SI	Documento generado en la primera fase del SGSI
Política del SGSI, que incluya los objetivos de seguridad	SI	Define los objetivos de seguridad de la información.
Metodología de Evaluación de Riesgos	SI	Se define la metodología para la evaluación de riesgos.

[56] Información tomada de la norma ISO/IEC 27001 y resumida por los autores.

Informe de Evaluación de Riesgos	SI	Muestra los riesgos encontrados con sus niveles de criticidad.
Plan de Tratamiento de Riesgos	SI	Muestra los controles seleccionados para la mitigación de los riesgos encontrados.
Procedimientos documentados acerca de controles implementados y sus métricas de eficacia	NO	El proyecto no abarca la implementación del SGSI.
Declaración de Aplicabilidad	SI	Muestra la Declaración de aplicabilidad de los controles seleccionados para los riegos encontrados.
Incidentes de Seguridad	SI	Muestra Incidentes y Mejoras en la Seguridad de la Información
Concientización y Capacitación en el SGSI	NO	El proyecto no abarca la implementación del SGSI.
Ejecución de Auditorías Internas	NO	El proyecto no abarca la implementación del SGSI.
Revisiones del SGSI	NO	El proyecto no abarca la implementación del SGSI.
Acciones Correctivas Implementadas	NO	El proyecto no abarca la implementación del SGSI.
Acciones Preventivas Implementadas	NO	El proyecto no abarca la implementación del SGSI.

Tabla 3.1: Documentos del SGSI exigidos por la norma ISO/IEC 27001. [57]

Un plan de seguridad de la información comprende cinco fases y cada uno con sus respectivos entregables, los cuales se muestran en la *Tabla 3.1*, además también se puede observar el mapeo entre los entregables que la norma establece con los entregables generados en este proyecto de titulación.

FASE	**DESCRIPCIÓN**	**ENTREGABLES ESTABLECIDOS EN LA NORMA**	**ENTREGABLES GENERADOS EN EL PROYECTO DE TITULACIÓN**
Aprobación de la dirección para la iniciación del proyecto	Busca obtener la aprobación y el compromiso por parte de la Dirección de la institución para iniciar el proyecto SGSI.	• Caso de negocio • Borrador del proyecto de SGSI.	• Solicitud de permiso para ejecución de proyecto en la organización. • Solicitud de permiso para realizar actividades de Hackeo Ético No Intrusivo.

[57] Tabla elaborada por los autores.

Definir el alcance del SGSI, límites y políticas del SGSI	Definir el alcance y límites organizacionales, tanto de las TIC's como físicos que consideren los activos de información críticos.	• Descripción del alcance y límites. • Política del SGSI.	• Plan de Proyecto de Titulación. • Política de Seguridad de la Información.
Realizar el análisis de los requerimientos de seguridad de la información	Analizar la situación actual de la organización para identificar los requerimientos de seguridad de la información y los activos de información críticos a ser considerados en el SGSI.	• Requerimientos de seguridad de la información. • Activos críticos de información. • Resultado de la evaluación de la seguridad de la información.	• Anexo V - Vulnerabilidades con Nessus. • Anexo IV – Análisis de vulnerabilidades. • Anexo VI – Lista de vulnerabilidades con Nessus. • Anexo VII – Resumen de vulnerabilidades técnicas. • Sección 2.2 - Análisis de Riesgos y Anexo VII – Evaluación de riesgos en activos críticos. • Sección 2.3 - Evaluación del Riesgo y Anexo XIII – Declaración de aplicabilidad.
Realizar la evaluación del riesgo y la planificación del tratamiento del riesgo	Definir la metodología de evaluación del riesgo en base a la cual se seleccionarán los controles pertinentes para su mitigación.	• Aprobación de la dirección para la implementación del SGSI. • Plan de tratamiento del riesgo. • Declaración de aplicabilidad de los controles seleccionados.	• El presente proyecto no contempla la implementación del Plan. • Sección 2.4 – Tratamiento del Riesgo. • Anexo XIII – Declaración de aplicabilidad.
Diseño del SGSI	Fase "Hacer" del modelo PHVA, consiste en el diseño de la seguridad organizacional, basándose en las opciones de tratamiento del riesgo, los requerimientos de registro y documentación y el diseño de controles.	• Plan de implementación del proyecto de SGSI	• Guía de Implementación. • Análisis de Impacto de la propuesta.

Tabla 3.2: Fases y entregables del Plan de Seguridad de la Información.[58]

3.2.2. DESCRIPCIÓN DE ENTREGABLES

Cuando se han seleccionado los controles a implementarse en cada uno de los activos críticos, ver sección 2.4, que ayudarán a reducir los riesgos en los mismos, se procede a elaborar las políticas de seguridad que forman parte del plan de seguridad de la información, estas políticas de seguridad contienen

[58] Tabla elaborada por los autores en base a información tomada de la norma ISO/IEC 27003:2012

diferentes controles por lo cual no es necesario elaborar un documento formal para cada control.

Los entregables que se determinaron para este proyecto son las que se listan a continuación:

- Procedimiento para Control de Documentos y Registros.
- Política de Seguridad de la Información.
- Declaración de Aplicabilidad
- Política para el manejo de información clasificada
- Registro de Compromiso de la Dirección con la Seguridad de la Información.
- Asignación de Responsabilidades.
- Seguridad de los Equipos.
- Uso Adecuado de Activos.
- Gestión de Redes.
- Gestión de Incidentes y Mejoras en la Seguridad de la Información.

3.2.2.1. Procedimiento para Control de Documentos y Registros.

PROCEDIMIENTO PARA CONTROL DE DOCUMENTOS Y REGISTROS				Consejo Nacional de Igualdad de Discapacidades
Código:	**Versión:**		**Número de páginas:**	
Elaborado por:		**Fecha de elaboración:**		
No. De Versión del Documento:	**Revisado por:**	**Fecha de Revisión:**	**Cambio Realizado:**	
Aprobado por:				

Objetivo:

- Definir tanto el manejo de documentos internos y externos del CONADIS como el control de los registros.

Alcance:

- El presente documento muestra la forma en que deben ser elaborados los documentos del CONADIS.

Usuarios de la Política:

Dirigida a todos los funcionarios de la organización.

Documentos de Apoyo:

- Norma ISO/IEC 27001 (Sección 4.3. Requisitos de la Documentación)

POLÍTICAS

El procedimiento establecido a continuación permite que la documentación del CONADIS sea elaborada, aprobada y de forma ágil y eficiente, de manera que se todos los funcionarios de la organización contribuyan a la correcta preservación de la documentación.

ELABORACIÓN DE DOCUMENTOS

Todos los documentos deben ser elaborados de la siguiente manera:

FORMATO

Todos los documentos; manuales, instructivos, guías, informes, protocolos, etc. del CONADIS se deben elaborar cumpliendo:

- ✓ Tamaño A4
- ✓ Márgenes:
  - Superior 2,5 cm

- Izquierda 3 cm
- Inferior 2,5 cm
- Derecha 3 cm

✓ Letra Arial 10

✓ Interlineado 1,5

ESTILO

Todos los documento deben empezar con un encabezado como el que se presenta a continuación:

NOMBRE DEL DOCUMENTO		Consejo Nacional de Igualdad de Discapacidades
Código:	Versión:	Número de páginas:

✓ Primer cuadro, dividido en dos partes:

- Parte izquierda: Nombre del Documento. Todo en mayúsculas, letra Arial 12 y Netrita.
- Parte derecha: Logo de la institución.

✓ Segundo cuadro, dividido en tres partes:

  - Parte izquierda: código del documento, es independiente de la versión.

- Parte central: número de versión del documento.
- Parte derecha: número de páginas del documento.

Seguido del cuadro de historial del documento:

Elaborado por:		Fecha de elaboración:	
No. De Versión del Documento:	Revisado por:	Fecha de Revisión:	Cambio Realizado:
Aprobado por:			

✓ Elaborado por: nombre del funcionario que realizó el documento.

✓ Fecha de elaboración: fecha en la que fue elaborado el documento.

✓ No. de versión del documento: la versión del documento que se está presentando.

✓ Realizado por: nombre del funcionario que revisa el documento.

- ✓ Fecha de revisión: fecha en que el documento fue revisado.
- ✓ Cambio realizado: cambio realizados en el documento.
- ✓ Aprobado por: funcionario que aprueba el documento.

En el caso de que el documento posea varias versiones, todas estas deben incluirse en esta parte del documento, como se muestra a continuación:

No. De Versión del Documento:	Revisado por:	Fecha de Revisión:	Cambio Realizado:
V1.0	Nombre del funcionario	Fecha	.....
V1.2	Nombre del funcionario	Fecha	.....
V2.0	Nombre del funcionario	Fecha	.....
V2.1	Nombre del funcionario	Fecha	.....
Aprobado por:			

Además todos los documentos deben tener el objetivo, alcance, usuarios y documentos de apoyo.

Objetivo:
Alcance:
Usuarios de la Política:
Documentos de Apoyo:

- ✓ Objetivo: se debe definir el objetivo del documento.
- ✓ Alcance: se debe especificar cuál será el alcance del documento.
- ✓ Usuarios: a que usuarios estará dirigido el documento.
- ✓ Documentos de apoyo: listar los documentos en los cuales se apoyó para poder realizar el presente documento.

Finalmente todos los documentos deben tener fecha de caducidad y periodicidad de revisión del mismo al final de cada uno.

Fecha de caducidad:	Periodicidad de revisión:

CONTROL DE REGISTROS

Las actividades necesarias para la identificación, el almacenamiento, la conservación, la recuperación, y disposición de los registros deben tener un control y para esto se debe tener en cuenta:

LEGIBILIDAD

- ✓ Pueden llenarse a mano o a computadora

- ✓ Escribir con letra clara y legible
- ✓ Usar tinta durable.
- ✓ Utilizar el formato de documentación.
- ✓ Evitar tachones y enmendaduras.

TIEMPO DE RETENCIÓN

Todos los Registros se conservaran por 1 año salvo que correspondan a contabilidad los cuales se guardaran por 5 años.

ALMACENAMIENTO

- ✓ Los registros en medios electrónicos serán guardados en los computadores de cada jefe de departamento.
- ✓ Los documentos impresos serán guardados dependiendo del nivel de clasificación de la información y debidamente etiquetada.

PROTECCIÓN

Los funcionarios de cada departamento son responsables de la integridad y seguridad de los registros generados a su cargo.

REVISIÓN

Los responsables y/o dueños de procedimientos depuran archivos de registros para dar disposición final a aquellos que hayan cumplido su tiempo de retención.

DIFUSIÓN

El funcionario líder de proceso deberá asegurarse de que todos los funcionarios involucrados sepan los cambios realizados en un lapso no mayor a una semana después de la publicación del mismo.

RESPONSABILIDAD

Todos los documentos y registros deben tener el responsable del mismo. Para lo cual al final de cada documento se debe incluir firma de responsabilidad, nombre, cargo y fecha, que debe ser llevado con esferográfico y sellado.

NOMBRE:_____ CARGO:_____ FECHA:_____	_____ FIRMA DE RESPONSABILIDAD (SELLO DEL DEPARTAMENTO)

_____

FIRMA DE RESPONSABILIDAD

(SELLO DE LA ORGANIZACIÖN)

NOMBRE:_____

CARGO:_____

FECHA:_____	
Fecha de caducidad:	**Periodicidad de revisión:**

3.2.2.2. Política de Seguridad de la Información.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN			Consejo Nacional de Igualdad de Discapacidades
Código:	**Versión:**		**Número de páginas:**
Elaborado por:		**Fecha de elaboración:**	
No. De Versión del Documento:	**Revisado por:**	**Fecha de Revisión:**	**Cambio Realizado:**
Aprobado por:			

Objetivo:

- Definir el objetivo y proporcionar directrices y reglas necesarias para una correcta gestión de la seguridad de la información.

Alcance:

- El presente documento muestra las políticas que deberán ser aplicadas al Centro de Información del CONADIS, debido a que esta área es la responsable de los activos críticos determinados.

Usuarios de la Política:

Dirigida a todos los funcionarios y usuarios involucrados en las actividades y procesos de la organización.

Documentos de Apoyo:

- Norma ISO/IEC 27001 (A.5.1.1. Documento de política de seguridad de la información, A. 10.1.1. Documentación de los procedimientos operativos, A.10.10.2. Supervisión del uso de los sistemas.)
- Norma ISO/IEC 27002
- Norma ISO/IEC 27003
- ANEXO XI - Instructivo para Revisión de Políticas. (A.5.1.2. Revisión de la política de seguridad de la información)
- ANEXO XII - Registro de Seguimiento de Políticas. (A.5.1.2. Revisión de la política de seguridad de la información)

POLÍTICAS

Las políticas de seguridad de la información que se contemplan en el presente documento, están orientadas

dentro de 4 niveles: Gerencial, Coordinador, Administrador de red y Técnico, las mismas que se detallan a continuación:

LA GERENCIA ESTA OBLIGADA A:

1. Aprobar el Plan de Seguridad de la Información.
2. Establecer un documento con las políticas de seguridad informática para ser aplicadas a los activos críticos.
3. Revisar el documento de las políticas de seguridad informática cada 6 meses o cuando existan circunstancias que lo ameriten (cambios tecnológicos, jurídicos, etc.), ver Anexo XI - Instructivo para Revisión de Políticas.
4. Crear registros de las revisiones incluyendo fechas de revisión, novedades encontradas, personas involucradas en la revisión, etc. ver Anexo XII – Registro de Seguimiento de Políticas.
5. Aprobar el documento de compromiso de la dirección con la seguridad de la información.
6. Designar una persona encargada de coordinar, (Coordinador), las actividades de seguridad de la información.
7. Realizar una auditoría interna exclusiva del Plan de Seguridad de la Información, para verificar el estado y cumplimiento del mismo. La auditoría estará a cargo de una persona ajena al área de la seguridad de la información de la organización.
8. Aprobar la documentación que el Coordinador realice como parte de la mejora en la seguridad de la información.

EL COORDINADOR ESTA OBLIGADO A:

1. Crear el Plan de Seguridad de la Información.
2. Establecer tareas y responsabilidades explícitas a sus subordinados, para evitar confusión o malos entendidos.
3. Mantener un conocimiento actualizado sobre seguridad de la información, para de esta forma capacitar continuamente al personal.
4. Apoyar activamente las auditorías internas que realice la gerencia.
5. Establecer procedimientos para el monitoreo de las actividades de procesamiento de información y revisar regularmente los resultados.
6. Crear documentos de: asignación de responsabilidades, seguridad de los equipos, gestión de activos, gestión de redes y gestión de incidentes y mejoras en la seguridad de la información, además de las sanciones correspondientes en caso de que se incumplan.
7. Establecer criterios para priorizar la asignación de controles a los activos críticos en términos de su valor, sensibilidad e importancia.
8. Comunicar, a Gerencia, de manera formal todas las novedades que puedan alterar la seguridad de la información.
9. Elaborar una propuesta para compra de servidores de tal manera que los nuevos y los existentes cumplan una sola función, es decir que sean dedicados.

EL ADMINISTRADOR DE RED ESTA OBLIGADO A:

1. Determinar las especificaciones tanto de hardware como de software, que se adapten de acuerdo a las necesidades de la organización, cuando exista la necesidad de adquirir nuevos equipos o software para estos.
2. Verificar, controlar y monitorear el ingreso de un equipo externo a la red de la organización y las tareas que se realizan durante la conexión.
3. Monitorear el servidor de antivirus para detectar posibles infecciones en la red y tomar acciones ante

cualquier eventualidad.

4. Elaborar un cronograma de mantenimiento de todos los equipos, priorizando esta actividad a los activos críticos determinados.
5. Elaborar un documento en el que se especifique el diagrama de infraestructura y puntos de red, los mismos que deben estar etiquetados físicamente.
6. Monitorear periódicamente los elementos principales de conmutación de la red (Switch, Access Point, etc.).
7. Generar los respectivos documentos de los monitoreos que se realicen.
8. Documentar y mantener los procedimientos de operación que estén a su cargo.

EL TÉCNICO ESTA OBLIGADO A:

1. Participar de eventos relacionados a la seguridad de la información y de esta manera conocer cómo actuar ante nuevas amenazas y vulnerabilidad que se puedan presentar.
2. Realizar respaldos de los equipos, especialmente de los servidores, estos respaldos serán diarios, semanales, mensuales o anuales dependiendo del tipo de información.
3. Revisar periódicamente las configuraciones de los elementos del firewall.
4. Revisar el tráfico de la red dos veces al mes o cuando sea necesario para determinar si existen comportamientos anómalos y así poder analizarlos, documentarlos y reportarlos sea el caso.
5. Revisar las políticas del Active Directory para otorgar o quitar permisos a los diferentes usuarios
6. Documentar y mantener los procedimientos de operación que estén a su cargo.

Todos los documentos de los procedimientos de operación deben estar disponibles para los usuarios que lo necesiten. Además de las políticas anteriores; cada usuario es responsable de mantener la confidencialidad e integridad de la información que maneja.

Cada usuario está en la obligación de salvaguardar todos y cada uno de los activos que le pertenecen cumpliendo; obligaciones, responsabilidades y uso adecuado para no comprometerlos, de no ser así serán sancionados.

Los usuarios están en la obligación de utilizar los recursos de red netamente necesarios para cumplir con las funciones que les fueron asignadas.

_____

FIRMA DE RESPONSABILIDAD

(SELLO DE LA ORGANIZACIÒN)

NOMBRE:_____

CARGO:_____

FECHA:_____

Fecha de caducidad:	**Periodicidad de revisión:**

3.2.2.3. Declaración de Aplicabilidad

DECLARACIÓN DE APLICABILIDAD			Consejo Nacional de Igualdad de Discapacidades
Código:	**Versión:**		**Número de páginas:**
Elaborado por:		**Fecha de elaboración:**	
No. De Versión del Documento:	**Revisado por:**	**Fecha de Revisión:**	**Cambio Realizado:**
Aprobado por:			
Objetivo: • Definir los controles adecuados para implementar en el Consejo Nacional de Igualdad de Discapacidades CONADIS, así también determinar cuáles son los objetivos de estos controles.			
Alcance: • Este documento involucra a los controles seleccionados.			
Usuarios de la Política: Los usuarios de este documento son todos los funcionarios del Consejo Nacional de Igualdad de Discapacidades que cumplen una función dentro del SGSI.			
Documentos de Referencia: • Norma ISO/IEC 27001, sección 4.2.1 j) Elaborar una Declaración de Aplicabilidad. • Política de Seguridad de la Información. • Anexo X – Selección de Controles			
Para Declaración de Aplicabilidad completa ver Anexo XIII.			

3.2.2.4. Políticas para el Manejo de Información Clasificada

POLÍTICA PARA EL MANEJO DE INFORMACIÓN CLASIFICADA			Consejo Nacional de Igualdad de Discapacidades
Código:	**Versión:**		**Número de páginas:**
Elaborado por:		**Fecha de elaboración:**	
No. De Versión del Documento:	**Revisado por:**	**Fecha de Revisión:**	**Cambio Realizado:**
Aprobado por:			

Objetivo:

- Garantizar la protección de la información según el nivel de la misma.

Alcance:

- El presente documento muestra los tipos de información, ya sea en papel o medios electrónicos, aplicaciones o bases de datos.

Usuarios de la Política:

Dirigida a todos los funcionarios de la organización.

Documentos de Apoyo:

- Norma ISO/IEC 27001 (A.7.2. Clasificación de la Información, A.10.7.3. Procedimientos de manejo de Información y A.11.6.1. Restricción al acceso de la información.)
- Política de Seguridad de la Información.
- Declaración de Aplicabilidad.

POLÍTICAS

El manejo de la información es responsabilidad del funcionario dueño de la misma, sin embargo dicha información debe estar clasificada por el nivel de confidencialidad que posee, este nivel de clasificación puede ser:

Pública	PUBLICO	Información de acceso público, no puede dañar a la organización de ninguna forma.	La información está disponible para todos.
Uso interno	USO INTERNO	El acceso no autorizado a la información podría ocasionar daños y/o inconvenientes menores a la organización.	La información está disponible para los funcionarios de la organización.
Restringida	RESTRINGIDO	El acceso no autorizado a la información podría dañar considerablemente el negocio y/o la reputación de la organización	La información está disponible solo para un grupo específico de funcionarios.
Confidencial	CONFIDENCIAL	El acceso no autorizado a la información podría dañar de forma irreparable el negocio y/o la reputación de la organización	La información está disponible solamente para determinados funcionarios (por ejemplo gerentes)

ETIQUETADO DE LA INFORMACIÓN

- **Documentos en papel**: Indicar el nivel de confidencialidad en la esquina superior derecha de cada página del documento; la carpeta que contiene el documento debe estar también etiquetada.
  Documentos electrónicos: Indicar el nivel de confidencialidad en la esquina superior derecha de cada página del documento.
- **Correo electrónico:** Indicar el nivel de confidencialidad en la primera línea del cuerpo del correo electrónico.

- **Soporte de almacenamiento electrónico (discos, tarjetas de memoria, etc.):** Indicare el nivel de confidencialidad sobre la superficie de cada soporte.

MANEJO DE INFORMACIÓN CLASIFICADA

Los funcionarios que tienen acceso a información clasificada deben cumplir con:

Documentos en papel	• Sólo las personas autorizadas pueden tener acceso. • Para enviarlo fuera de la organización, el documento debe ser enviado por correo certificado. • Los documentos deben ser retirados constantemente de impresoras y máquinas de fax.	• El documento debe ser almacenado en un gabinete con llave. • Los documentos pueden ser transferidos dentro y fuera de la organización solamente en un sobre cerrado. • Los documentos deben ser retirados inmediatamente de impresoras y máquinas de fax. • Solamente el propietario del documento puede copiarlo. • Solamente el propietario del documento puede destruirlo.	• El documento debe ser almacenado en una caja fuerte. • El documento puede ser transferido dentro y fuera de la organización solamente por una persona confiable y en un sobre sellado. • No está permitido enviar el documento por fax. • Es posible imprimir el documento sólo si la persona autorizada está al lado de la impresora.
Documentos electrónicos	• Las personas de la organización pueden tener acceso a este documento. • El acceso a los sistemas de información que almacenen estos documentos debe estar protegido por una clave segura.	• Sólo las personas autorizadas pueden tener acceso a este documento. • Proteger el documento con encriptación. • Solamente el propietario del documento puede borrarlo.	• El documento debe ser almacenado en un formato encriptado. • El documento solamente puede ser archivado en servidores controlados por la organización.
Correo electrónico	• Sólo las personas autorizadas pueden tener acceso. • El remitente debe verificar cuidadosamente el destinatario. • Aplican todas las reglas mencionadas para "Sistemas de información".	• El correo electrónico debe estar encriptado si se envía fuera de la organización.	• Todos los correos electrónicos deben ser encriptados.
Soportes de almacenamiento electrónico	• Sólo las personas autorizadas pueden tener acceso.	• Los soportes y archivos deben estar encriptados.	• El soporte debe ser almacenado en una caja fuerte.

	• Los soportes o archivos deben estar protegidos con clave. • El soporte solamente puede ser guardado en habitaciones con acceso físico controlado.	• El soporte debe ser almacenado en un gabinete con llave. • Sólo el propietario del soporte puede borrar sus datos o destruirlo.	• El soporte puede ser transferido dentro y fuera de la organización solamente por una persona confiable y en un sobre cerrado y sellado.

_____

FIRMA DE RESPONSABILIDAD

(SELLO DE LA ORGANIZACIÒN)

NOMBRE:_____

CARGO:_____

FECHA:_____

Fecha de caducidad:	**Periodicidad de revisión:**

3.2.2.5. Registro de Compromiso de la Dirección con la Seguridad de la Información.

REGISTRO DE COMPROMISO DE LA DIRECCIÓN CON LA SEGURIDAD DE LA INFORMACIÓN			Consejo Nacional de **Igualdad de Discapacidades**
Código:	**Versión:**		**Número de páginas:**
Elaborado por:		**Fecha de elaboración:**	
No. De Versión del Documento:	**Revisado por:**	**Fecha de Revisión:**	**Cambio Realizado:**
Aprobado por:			
Objetivo: ▪ Registrar el compromiso de la dirección con el Plan de Seguridad de la Información.			
Alcance: ▪ Este documento muestra el compromiso de aceptación de la dirección de la organización, aplica y deberá ser firmado por todos quienes la conforman, puesto que son los encargados de la toma de decisiones.			
Usuarios de la Política: Dirigida a todos los funcionarios que conforman la dirección de la organización.			

Documentos de Apoyo:

- Norma ISO/IEC 27001. (A.6.1.1. Compromiso de la Dirección con la seguridad de la información, A.6.1.2. Coordinación de la seguridad de la información, A.15.2.1. Conformidad con la política de seguridad.)
- Plan de Seguridad de la Información.
- Política de Seguridad de la Información.

COMPROMISO DE LA DIRECCIÓN CON EL PLAN DE SEGURIDAD DE LA INFORMÁCIÓN

La Dirección del Consejo Nacional de Igualdad de Discapacidades, CONADIS, ha leído el Plan de Seguridad de la Información y esta consiente cuán importante es el establecimiento de políticas de seguridad de información dentro de la organización y en especial dentro del Centro de Información, los mismos que son los encargados del manejo de los activos críticos. Por esta razón la Dirección manifiesta el total compromiso y apoyo para su implementación, asegurando que todos los procedimientos de la seguridad de la información se realicen correctamente y cumplan con los estándares y políticas de seguridad.

Las actividades para la seguridad de la información serán coordinadas por los responsables asignados por el Coordinador.

Cabe recalcar que la Dirección puede intervenir durante el proceso de desarrollo e implementación de políticas, además de tener la potestad de dar por terminado el proceso en caso de considerarlo necesario.

PRESIDENTE	VICEPRESIDENTE	DIRECTOR EJECUTIVO

Fecha de caducidad:	Periodicidad de revisión:

3.2.2.6. Registro de Asignación de responsabilidades.

REGISTRO DE ASIGNACIÓN DE RESPONSABILIDADES	Consejo Nacional de Igualdad de Discapacidades

Código:	Versión:	Número de páginas:

Elaborado por:	Fecha de elaboración:

No. De Versión del Documento:	Revisado por:	Fecha de Revisión:	Cambio Realizado:

Aprobado por:

Objetivo:

- Relacionar y asignar responsabilidades a los miembros y equipos de trabajo involucrados en la seguridad de la información dentro de la organización.

Alcance:

- Este documento especifica las actividades y sus respectivos responsables involucrados con la seguridad de la información en la organización.

Usuarios de la Política:

Dirigida a todos los responsables de la seguridad de la información de la organización.

Documentos de Apoyo:

- Norma ISO/IEC 27001. (A.6.1.3. Asignación de responsabilidades)
- Plan de Seguridad de la Información.
- Política de seguridad de la información.
- Contratos laborales.

ASIGNACIÓN DE RESPONSABILIDADES

Las responsabilidades de acuerdo a las actividades que se deberán realizar para salvaguardar los activos críticos y con ello mantener la seguridad de la información dentro de la organización estarán distribuidas de la siguiente manera:

Implementación de servidores dedicados.	Administrador de red
Coordinar las actividades de seguridad.	Coordinador
Monitoreo de equipos.	Administrador de red
Mantenimiento de equipos.	Técnico
Realizar el inventario de activos	Administrador de red
Etiquetar cableado	Técnico
Depuración de equipos de la red	Administrador de red
Asignación de responsabilidades y obligaciones	Coordinador
Respaldo de información	Técnico
Controlar cumplimiento de políticas	Coordinador

_____

FIRMA DE RESPONSABILIDAD

(SELLO DE LA ORGANIZACIÒN)

NOMBRE:_____

CARGO:_____

FECHA:_____

Fecha de caducidad:	**Periodicidad de revisión:**

3.2.2.7. Seguridad de los Equipos.

POLÍTICA DE SEGURIDAD DE LOS EQUIPOS.			Consejo Nacional de Igualdad de Discapacidades
Código:	**Versión:**		**Número de páginas:**
Elaborado por:		**Fecha de elaboración:**	
No. De Versión del Documento:	**Revisado por:**	**Fecha de Revisión:**	**Cambio Realizado:**
Aprobado por:			

Objetivo:

- Establecer lineamientos que deberán seguirse para la seguridad y protección de los equipos que manejan información y proporcionan servicios dentro de la organización.

Alcance:

- El presente documento específica prácticas fundamentales para la seguridad de la información, que deberán ser aplicadas para asegurar los activos críticos de la organización.

Usuarios de la Política:

Dirigida a los miembros del Centro de Información.

Documentos de Apoyo:

- Norma ISO/IEC 27001. (A.9.2.1. Instalación y protección de equipos, A.9.2.2. Suministro eléctrico, A.9.2.3. Seguridad del cableado, A.9.2.4. Mantenimiento de los equipos, A.9.2.6. Seguridad en la reutilización o eliminación de equipos, A.10.4.1. Medidas y controles contra software malicioso.)
- Plan de seguridad de la información.
- Política de seguridad de la información.
- Manuales de uso de equipo.

POLÍTICA DE SEGURIDAD DE LOS EQUIPOS.

El presente documento muestra políticas que pretenden evitar pérdida, daño y /o robo de los activos críticos así como de la interrupción de las actividades en la organización. Estas políticas estarán divididas de acuerdo a los controles que deberán ser implementados de acuerdo a lo establecido.

INSTALACIÓN Y PROTECCIÓN DE EQUIPOS.

Los equipos deben estar ubicados y protegidos con el objetivo de reducir el riesgo ante una amenaza y/o acceso no autorizado.

1. Impedir la salida de equipos de la organización sin previa autorización escrita.
2. Ubicar los equipos de tal manera que se evite accesos innecesarios a áreas restringidas.
3. Mantener aislados los servicios de procesamiento de información con datos sensibles, para reducir riesgos de acceso a información por parte de personas no autorizadas.
4. Mantener protegidas las instalaciones ante posibles descargas eléctricas, especialmente las líneas

de comunicación.

5. Establecer directrices que eviten actividades; tales como ingeniería social, comer, fumar y beber, etc., en las cercanías de los equipos y puestos de trabajo.
6. Implantar controles de detección, prevención y recuperación contra software malicioso.

SUMINISTRO ELÉCTRICO.

Los equipos deben estar protegidos contra fallos de energía eléctrica.

1. Verificar regularmente los sistemas de suministro eléctrico.
2. Ubicar múltiples tomacorrientes o líneas de suministro para evitar un único punto de falla en el suministro de energía.
3. El sistema de energía ininterrumpible (UPS) deberá asegurar el apagado regulado y sistemático, o la ejecución continua del equipamiento que sustenta las operaciones críticas de la organización.
4. Definir componentes necesarios para el abastecimiento de energía alternativa ante posibles interrupciones prolongadas de energía.

SEGURIDAD DEL CABLEADO.

Las líneas de comunicación deben estar protegidas para que los datos y servicios que soportan no se vean afectados ante posibles interceptaciones o daños.

1. Disponer de líneas de energía y de telecomunicaciones subterráneas protegidas.
2. Separar los cables de energía de los cables de comunicaciones para evitar confusiones y/o interferencias.
3. Identificar y etiquetar el cableado para evitar errores en el manejo.
4. Documentar, diseños, planos y la distribución de conexiones.
5. Controlar el acceso al patch panel y cuartos de cableado.

MANTENIMIENTO DE LOS EQUIPOS.

Garantizar mediante el mantenimiento la continua disponibilidad e integridad de los equipos.

1. Realizar mantenimientos periódicos a los equipos y dispositivos con personal calificado, especificando tiempos y responsables.
2. Registrar el detalle de los mantenimientos efectuados, ya sean preventivos o correctivos. Estos registros deben mantenerse actualizados.
3. Registrar que un equipo fue retirado por motivos de mantenimiento.
4. Respaldar y proteger la información confidencial del equipo que será sometido a mantenimiento.

SEGURIDAD EN LA REUTILIZACIÓN O ELIMINACIÓN DE EQUIPOS.

Revisar todo dispositivo de almacenamiento dentro del equipo, para garantizar que los datos sensibles se hayan eliminado o sobrescrito con seguridad.

1. Utilizar técnicas de no recuperación de la información al momento de eliminar, borrar o sobrescribir los dispositivos que contienen información sensible.
2. Evaluar los dispositivos afectados que contengan información sensible antes de enviar a reparación, borrar la información o determinar si se debería eliminar físicamente el dispositivo.

_____

FIRMA DE RESPONSABILIDAD

(SELLO DE LA ORGANIZACIÒN)

NOMBRE:_____

CARGO:_____ **FECHA:**_____	
Fecha de caducidad:	**Periodicidad de revisión:**

3.2.2.8. Uso Adecuado de Activos.

ACUERDO SOBRE USO ADECUADO DE ACTIVOS		Consejo Nacional de **Igualdad de Discapacidades**	
Código:	**Versión:**	**Número de páginas:**	
Elaborado por:		**Fecha de elaboración:**	
No. De Versión del Documento:	**Revisado por:**	**Fecha de Revisión:**	**Cambio Realizado:**
Aprobado por:			
Objetivo: ▪ Establecer acuerdos para el cumplimiento de actividades y prácticas que permitan garantizar que los activos de información reciban un apropiado nivel de protección durante todo su ciclo de vida.			
Alcance: ▪ El presente documento establece actividades y prácticas para el uso adecuado de activos de información dentro de la organización.			
Usuarios de la Política: Dirigida a todos quienes conforman la organización.			
Documentos de Apoyo: ▪ Norma ISO/IEC 27001. (A.7.1.3. Acuerdo sobre el uso adecuado de los activos.) ▪ Plan de seguridad de la información. ▪ Política de seguridad de la información. ▪ ANEXO XI - Instructivo para Revisión de Políticas. (A.5.1.2. Revisión de la política de seguridad de la información) ▪ ANEXO XII - Registro de Seguimiento de Políticas. (A.5.1.2. Revisión de la política de seguridad de la información)			
ACUERDO SOBRE EL USO ADECUADO DE ACTIVOS Identificar, documentar e implantar reglas para el uso adecuado de la información y los activos asociados a recursos de tratamiento de la información. Cualquier funcionario que tenga a cargo uno o varios activos, está en la obligación de mantener el uso adecuado de los mismos de acuerdo a las siguientes prácticas:			

1. El Coordinador es el encargado de asegurar de que los lineamientos para utilización de recursos de TI cumplan con los requisitos de seguridad establecidos, teniendo en cuenta el nivel de criticidad de la información.
2. Los documentos y la información generada en y por la organización son propiedad de la misma, ya sea utilizada y/o enviada por cualquier medio, ya sea correo electrónico, etc.
3. Reglamentar el uso de correo electrónico institucional:
   - 3.1 Este servicio debe ser de uso exclusivo para tareas propias de la organización.
   - 3.2 El contenido del mensaje y toda información adjunta es responsabilidad de la persona que lo envía.
   - 3.3 La organización puede monitorear y conservar todos los mensajes, esta última se efectuará en carpetas personales.
   - 3.4 Una única cuenta de usuario debe estar asociada a una cuenta de correo electrónico.
   - 3.5 La información que se utilice debe ser gestionada de forma centralizada y no de las estaciones de trabajo.
   - 3.6 Deben utilizarse herramientas que permitan identificar la presencia de virus tanto de los mensajes como de la información adjunta.
   - 3.7 La destrucción de los mensajes con origen desconocido y las consecuencias que puede producir es responsabilidad de la persona que lo recibe.
   - 3.8 Debe existir cifrado de los datos que permitan conservar la integridad de la información cuando se la envíe por un determinado medio.
   - 3.9 Debe existir un control de envío no autorizado de correos masivos.
4. Reglamentar el acceso y uso de Internet además de sus aplicaciones y/o servicios:
   - 4.1 El servicio debe ser de uso exclusivo para tareas propias de las funciones que se cumplen dentro de la organización.
   - 4.2 La información y el contenido a los que el usuario accede y guarda dentro de un medio de almacenamiento o de un equipo de la organización es responsabilidad del mismo.
   - 4.3 Debe limitarse a los usuarios el acceso a portales, aplicaciones o servicios de Internet y la Web que pudieren perjudicar los intereses y la reputación de la institución, tanto a equipos fijos como a equipos móviles.
   - 4.4 El Coordinador debe verificar que se cumplan los procedimientos de acceso y uso de Internet, sin excepción alguna, especificados en este documento además de implementar otros que la organización crea necesarios.
   - 4.5 Los accesos pueden ser sujetos de monitoreo y conservación por parte de la organización.
   - 4.6 El acceso y uso de Internet, mediante conexión alámbrica o inalámbrica, a los funcionarios o terceros puede ser bloqueado o limitado con el fin de garantizar un adecuado uso de recursos de red.

_____

FIRMA DE RESPONSABILIDAD

(SELLO DE LA ORGANIZACIÒN)

NOMBRE:_____

CARGO:_____

FECHA:_____	
Fecha de caducidad:	**Periodicidad de revisión:**

3.2.2.9. Política de Gestión de Redes.

POLÍTICA DE GESTIÓN DE REDES			Consejo Nacional de **Igualdad de Discapacidades**
Código:	**Versión:**		**Número de páginas:**
Elaborado por:		**Fecha de elaboración:**	
No. De Versión del Documento:	**Revisado por:**	**Fecha de Revisión:**	**Cambio Realizado:**
Aprobado por:			

Objetivo:

- Monitorear y controlar los recursos y elementos de comunicaciones para garantizar un nivel de servicio adecuado.

Alcance:

- El presente documento muestra procedimientos y actividades para brindar seguridad a la red de la organización y a la información de la misma.

Usuarios de la Política:

Dirigida a todos los usuario de la red de la organización.

Documentos de Apoyo:

- Norma ISO/IEC 27001. (A.10.6.1. Controles de red, A.10.6.2. Seguridad en los servicios de red, A.11.4.1. Política de uso de los servicios de red, A.11.4.2. Autenticación de usuario para conexiones externas, A.11.4.3. Autenticación de nodos de la red, A.11.4.7. Control de encaminamiento en la red.)
- Plan de seguridad de la información.
- Política de la seguridad de la información.
- ANEXO XI - Instructivo para Revisión de Políticas. (A.5.1.2. Revisión de la política de seguridad de la información)
- ANEXO XII - Registro de Seguimiento de Políticas. (A.5.1.2. Revisión de la política de seguridad de la información)

POLÍTICA DE GESTIÓN DE REDES

El presente documento muestra políticas que pretenden asegurar la protección de la información en las redes así como también impedir el acceso no autorizado a los servicios que presta la red de la organización. Estas

políticas estarán divididas de acuerdo a los controles que deberán ser implementados de acuerdo a lo establecido.

CONTROLES DE RED.

Definir controles que garanticen la seguridad de los datos y servicios de la red ante posibles accesos no autorizados de manera que se mantenga y controle adecuadamente la red para protegerla de amenazas y mantener la seguridad en la misma.

1. Establecer un responsable dedicado al área de redes, el cual cumpla con la responsabilidad de mantener la seguridad de la red.
2. El Responsable asignado deberá establecer controles de confidencialidad e integridad de los datos y su procesamiento, así como la disponibilidad de los servicios de la red.
3. El Responsable identificará la red y servicios de red a los cuales se permite el acceso a cada grupo de usuarios.
4. Supervisar el cumplimiento de los controles establecidos.
5. Elaborar el esquema de red de la organización que contenga los enlaces de datos, Internet y/o subredes.

SEGURIDAD EN LOS SERVICIOS DE RED.

Se deben 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 contraten desde el exterior.

1. Instalar y habilitar únicamente los servicios necesarios para las actividades netamente laborales de los usuarios.
2. Controlar el acceso lógico, por parte de los usuarios, a los servicios que brinda la red de la organización.
3. Configurar adecuadamente los servicios de la red, incorporando tecnología de seguridad como autenticación, encriptación y controles de conexión de red, manteniéndola segura y evitando cualquier vulnerabilidad que pueda presentarse.
4. Actualizar periódicamente los sistemas de seguridad.
5. Definir procedimientos para la utilización y restricción de los servicios de red.

POLÍTICA DE USO DE LOS SERVICIOS DE RED.

Autorizar el acceso a los usuarios únicamente a los servicios necesarios para cumplir sus actividades laborales.

1. Autorizar del acceso a los servicios y recursos de red, únicamente de acuerdo al pedido formal de ingreso de usuario a red.
2. Tener documentado cada servicio de red y los usuarios que acceden a cada uno de estos.
3. Definir perfiles y roles para cada usuario de la red.
4. Definir mecanismos de control y bloqueos para proteger el acceso a las conexiones y servicios de red.

AUTENTICACIÓN DE USUARIO PARA CONEXIONES EXTERNAS.

Utilizar técnicas de autenticación que brinden un mayor nivel de protección al momento del acceso remoto de los usuarios.

1. Utilizar técnicas de encriptación, implementación de redes privadas virtuales o Servicios de Acceso Remoto de tal manera que se asegure la información transmitida por los canales de conexión remota.

2. Llevar control de registros (logs) así como también realizar limitaciones de accesos en los segmentos de red a los usuarios que requerían conexiones remotas con el objetivo de diferenciar la autenticación de dichos usuario.
3. Utilizar líneas dedicadas privadas o una herramienta de verificación de dirección del usuario de red para conocer el origen de la conexión.

AUTENTICACIÓN DE NODOS DE LA RED.

Identificar automáticamente los equipos como medio de autenticación de conexiones en la red de la organización.

1. Documentar e identificar todos los equipos que se encuentran en la red, especificando cuales están activos y cuáles no.
2. Controlar que la comunicación solo sea permitida desde un equipo o lugar específico.
3. Documentar la identificación tanto de los equipos permitidos como de los no permitidos para acceso a cierta información.
4. Utilizar métodos para que la identificación del equipo esté en relación a la autenticación del usuario.

CONTROL DE ENCAMINAMIENTO EN LA RED.

Establecer controles de enrutamiento en las rede, asegurando que tanto las conexiones de los equipos como los flujos de información no incumplen la política de control de accesos a las aplicaciones.

1. Configurar políticas de control de acceso para el enrutamiento en la red, según los requerimientos de la organización.
2. Validar la dirección fuente/destino en los puntos de control de la red utilizando puertas de enlace de la seguridad (gateway) para filtrar el tráfico entre dominios y bloquear el acceso no autorizado.
3. Dividir la red en dominios lógicos de red, dominios de red interna, dominios de red externa y red inalámbrica.
4. Documentar la segregación de red, identificando las direcciones IP que se encuentran en cada segmento de red.

_____

FIRMA DE RESPONSABILIDAD

(SELLO DE LA ORGANIZACIÒN)

NOMBRE:_____

CARGO:_____

FECHA:_____

Fecha de caducidad:	**Periodicidad de revisión:**

3.2.2.10. Política de Gestión de Incidentes y Mejoras en la Seguridad de la Información.

POLÍTICA DE GESTIÓN DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN.			Consejo Nacional de Igualdad de Discapacidades
Código:	**Versión:**	**Número de páginas:**	
Elaborado por:		**Fecha de elaboración:**	
No. De Versión del Documento:	**Revisado por:**	**Fecha de Revisión:**	**Cambio Realizado:**
Aprobado por:			

Objetivo:

- Establecer medidas apropiadas que garanticen la comunicación de incidentes de seguridad de la información, permitiendo que todos los usuarios reporten las debilidades para prevenir y limitar el impacto que pudiese darse de ocurrir algún incidente.

Alcance:

- El presente documento muestra actividades y procedimientos para gestionar de manera efectiva los incidentes en la seguridad de la información.

Usuarios de la Política:

Dirigida a los miembros del Centro de Información

Documentos de Apoyo:

- Norma ISO/IEC 27001. (A.13.2.1. Identificación de responsabilidades y procedimientos, A.13.2.2. Evaluación de incidentes en seguridad, A.13.2.3. Recogida de pruebas.)
- Plan de seguridad de la información.
- Política de la seguridad de la información.

POLÍTICA DE GESTIÓN DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN

El presente documento muestra políticas que pretenden asegurar la respuesta eficaz y de forma adecuada ante la ocurrencia de un incidente en la seguridad de la información que pueda o afecte potencialmente la misma. Estas políticas estarán divididas de acuerdo a los controles que deberán ser implementados de acuerdo a lo establecido.

IDENTIFICACIÓN DE RESPONSABILIDADES Y PROCEDIMIENTOS.

Establecer responsabilidades y procedimientos para asegurar una respuesta rápida, efectiva y ordenada ante la ocurrencia de un incidente en la seguridad de información una vez que han sido comunicados.

1. Asignar un responsable para la gestión de incidentes dentro de la organización.
2. Implementar una bitácora de registro de incidentes y el reporte de vulnerabilidades de la seguridad de la información, así como también el monitoreo y gestión de la misma.
3. Identificar y clasificar por tipo de incidentes de seguridad de la información, con el objetivo de priorizar el tratamiento de los mismos.
4. Identificar y analizar las posibles causas de un incidente ocurrido, con el fin de evitar que vuelva a

suceder.

5. Planificar e implementar acciones correctivas para evitar la recurrencia del incidente
6. Notificar a todos los funcionarios afectados que el incidente ha sido resuelto satisfactoriamente.
7. Realizar el reporte de incidente, donde se explique detalladamente por qué y las áreas afectadas por el mismo, que deberá ser entregado a la dirección.
8. Recolectar toda la evidencia relacionada con el incidente.

EVALUACIÓN DE INCIDENTES EN SEGURIDAD.

Definir un mecanismo que permitan cuantificar y monitorear los tipos, volúmenes y costes de incidentes en la seguridad de información.

1. Determinar el número de incidentes por tipo, el número de incidentes graves, el tiempo medio de resolución de incidentes, etc.
2. Determinar el costo promedio por incidente.
3. Determinar el número de incidentes recurrentes.
4. Determinar la frecuencia de un incidente recurrente.

RECOGIDA DE PRUEBAS.

Recolectar, retener y presentar evidencia cuando debido a un incidente en la seguridad de información, se presenta una acción legal de seguimiento contra un funcionario o la organización.

1. Desarrollar y cumplir procedimientos internos y de forma disciplinaria cuando se recolecta y se presenta evidencia.
2. Asegurar que los sistemas de información cumplan con las normas legales para la producción de evidencia.
3. Demostrar la calidad de los controles empleados para proteger correcta y consistentemente la evidencia, logrando así peso necesario de la evidencia, para ello se debe realizar lo siguiente:
   3.1. Tomar duplicados o copias de todos los medios removibles, la información en los discos duros o la memoria, garantizando la disponibilidad, sin olvidar registrar todas las acciones durante el proceso de copiado y teniendo testigos del procedimiento; y, el medio y el registro originales se deberán conservar intactos y de forma segura.
   3.2. Proteger la integridad de todo el material de evidencia. El proceso de copia del material de evidencia debe estar supervisado y se debe registrar la información sobre cuándo y cómo se realizó dicho proceso, quién ejecutó las actividades de copiado y qué herramientas o programas se utilizaron en esto.

_____

FIRMA DE RESPONSABILIDAD

(SELLO DE LA ORGANIZACIÒN)

NOMBRE:_____

CARGO:_____

FECHA:_____

Fecha de caducidad:	Periodicidad de revisión:

3.3. GUÍA DE IMPLEMENTACIÓN.

Para poder implementar el plan, existe una secuencia de actividades que se deben realizar y seguir, se puede añadir otras actividades siempre y cuando las necesidades de la organización lo requieran. Las personas o funcionarios encargados de la ejecución de estas actividades son: el Coordinador[59] y el Responsable del Centro de Información.

[59] Persona designada por un Comité o la Presidencia, diferente del Responsable del Centro de Información debido a que también se encuentra involucrado en la ejecución de las actividades.

1. Identificación de marco legal: Investigación sobre todas las normas, leyes y reglamentos vigentes en el Ecuador y a las que se rige la organización. (ver Anexos/Marco Legal)
2. Diagnóstico de la situación actual de la seguridad de la información dentro del CONADIS, en este caso con ayuda de la norma ISO 27002 (ver Sección 1.4)
3. Aprobación del plan de seguridad.
4. Definir una metodología para análisis de riesgos (ver Sección 1.3.3).
5. Definir los criterios básicos para la evaluación de riesgos de la seguridad de la información (ver Sección 2.1).
6. Realizar el análisis de riesgos para lograr identificar los activos que aportan valor a la organización, las amenazas y el impacto que podrían afectar el funcionamiento normal de las actividades y las medidas para minimizar o eliminar el impacto de los riesgos existentes.
   6.1. Identificar activos con el objetivo de encontrar cuales de estos son críticos en relación a la información (ver Sección 2.2.1.2 y Sección 2.2.1.2).
   6.2. Identificar las vulnerabilidades y sus amenazas asociadas (ver Sección 2.2.1.3).
   6.3. Identificar los controles existentes (ver Sección 2.2.1.4).
7. Evaluar el riesgo en base a la estimación del mismo con la valoración del impacto y la valoración de incidentes (ver Sección 2.3).
8. Propuesta para el tratamiento del riesgo seleccionando controles de seguridad, definidos en la norma ISO/IEC 27002 (ver Sección 2.4).
   8.1. Los controles deben ser implementados según los criterios de prioridad. (ver Sección 2.1.3.6), en el orden siguiente:
      8.1.1. Implementar los controles que tengan prioridad “Alta”. (ver Anexo IX).
      8.1.2. Implementar los controles que tengan prioridad “Media”. (ver Anexo IX).
      8.1.3. Implementar los controles que tengan prioridad “Baja”. (ver Anexo IX).
9. Elaboración de Procedimiento para Control de Documentos y Registros (ver Sección 3.2.2.1).

10. Elaboración de la Política de Seguridad de la Información (ver Sección 3.2.2.2).
11. Elaborar la Declaración de Aplicabilidad (ver Sección 3.2.2.3).
12. Elaborar la Política para el manejo de información clasificada (ver Sección 3.2.2.4).
13. Elaboración del Registro de Compromiso de la Gerencia con la Seguridad de la Información (ver Sección 3.2.2.5).
14. Elaboración del Registro de Asignación de Responsabilidades (ver Sección 3.2.2.6).
15. Elaboración de la Política de Seguridad de los Equipos (ver Sección 3.2.2.7).
16. Elaboración de Acuerdo sobre Uso Adecuado de Activos (ver Sección 3.2.2.8).
17. Elaboración de Política de Gestión de Redes (ver Sección 3.2.2.9).
18. Elaboración de Política de Gestión de Incidentes y Mejoras en la Seguridad de la Información (ver Sección 3.2.2.10).
19. Elaboración de otras políticas; si los controles establecidos dentro de este plan no son los suficientes y es necesario que se añadan otros, estos deben ser parte de estas nuevas políticas.
20. Capacitación al personal.
21. Implementación de las políticas de seguridad establecidas.

La fecha de implementación de las políticas y sus respectivos controles dependerá de la aprobación por parte de la gerencia.

3.4. ANÁLISIS DE IMPACTO DE LA PROPUESTA

En esta sección se realiza la comparación del estado de cumplimiento actual, ver sección 1.4.3, con el estado de cumplimiento esperado una vez que se implementen los controles recomendados en la Sección 2.4, para de esta manera finalizar con el detalle del análisis y resultado de la encuesta de aceptación realizada a los usuarios de la red de la organización.

3.4.1. APLICABILIDAD DE LA PROPUESTA

Luego de haber evaluado los riesgos y determinado los activos críticos, ver Sección 2.3, se proponen los respectivos controles dados por la norma ISO/IEC

27001, ver ANEXO X – Selección de Controles, que ayudarán a mejorar la seguridad de la información a estos activos.

Con estos controles propuestos se elaboró la matriz de cumplimiento esperado, para mayor detalle ver ANEXO XIV, la cual muestra el nuevo porcentaje de cumplimiento de los controles en el caso de la implementarlos, tal como se muestra en la *Tabla 3.4* en la que se puede observar el estado de cumplimiento esperado en el dominio A.10 Gestión de Comunicaciones y Operaciones que presenta diez objetivos de control con 32 controles de los cuales la organización cumple con 17, de estos, cuatro de los propuestos se encuentran dentro de la selección de controles los mismos que están representados en color morado, y al momento de establecer un estado de cumplimiento esperado no afecta en el porcentaje final.

Por otra parte, el porcentaje final en el estado de cumplimiento esperado varía del 53.13% al 56.25% a causa del quinto control propuesto A. 10.1.1 Documentación de los procesos operativos, el mismo que se encuentra representado en color verde.

A.10. GESTIÓN DE COMUNICACIONES Y OPERACIONES.	A.10.1 Procedimientos y responsabilidades de operación.			A.10.1.1 Documentación de los procedimientos operativos.	1	56,25%
		Monitoreo de operaciones	Monitoreo constante de las operaciones aunque estas no sean documentadas adecuadamente.	A.10.1.2 Control de cambios operacionales.	1	
				A.10.1.3 Segregación de tareas.	0	
				A.10.1.4 Separación de los recursos para desarrollo y producción.	0	
	A.10.2 Supervisión de los servicios contratados a terceros.	Acuerdo de Nivel de Servicio	Se controla que los acuerdos de servicio se cumplan.	A.10.2.1 Prestación de servicios.	1	
		Monitoreo de servicios contratados	Se monitorea constantemente que los servicios prestados sean los acordados.	A.10.2.2 Monitorización y revisión de los servicios contratados.	1	
		Acuerdo de Nivel de Servicio	Se controla que los acuerdos de servicio se cumplan.	A.10.2.3 Gestión de los cambios en los servicios contratados.	1	
	A.10.3 Planificación y aceptación del sistema.	Levantamiento de información	Se realiza un análisis de requerimientos para determinar el sistema adecuado.	A.10.3.1 Planificación de capacidades.	1	
		Pruebas del sistema	Cuando el Sistema es aceptado se realizan las pruebas necesarias para determinar si satisface todos los requerimientos.	A.10.3.2 Aceptación del sistema.	1	
	A.10.4 Protección contra software malicioso y código móvil.	Herramientas de control	Firewall, Plataforma de antivirus, plataforma de antispam junto con procedimientos que los usuarios cumplen.	A.10.4.1 Medidas y controles contra software malicioso.	1	
		Herramientas de control	Análisis automático de dispositivos extraíbles.	A.10.4.2 Medidas y controles contra código móvil.	1	

	A.10.5 Gestión interna de soportes y recuperación.	Backups	Se realizan copias de seguridad constantemente de acuerdo a la sensibilidad de la información.	A.10.5.1 Recuperación de la información.	1	
	A.10.6 Gestión de redes.	Monitoreo de red	Observación de la actividad de la red, tráfico y su funcionamiento.	A.10.6.1 Controles de red.	1	
		Protección de puertos	Existen puertos inhabilitados y bloqueo de páginas.	A.10.6.2 Seguridad en los servicios de red.	1	
	A.10.7 Utilización y seguridad de los soportes de información.			A.10.7.1 Gestión de soportes extraíbles.	0	
				A.10.7.2 Eliminación de soportes.	0	
				A.10.7.3 Procedimientos de utilización de la información.	0	
				A.10.7.4 Seguridad de la documentación de sistemas.	0	
	A.10.8 Intercambio de información y software.			A.10.8.1 Políticas y procedimientos de intercambio de información.	0	
				A.10.8.2 Acuerdos de intercambio.	0	
				A.10.8.3 Soportes físicos en tránsito.	0	
		Monitoreo del correo electrónico	Se monitorea constantemente la mensajería electrónica.	A.10.8.4 Mensajería electrónica.	1	
		Interconexión de sistemas	Cada departamento de la organización posee su respectivo sistema de acuerdo a las funciones que tienen a su cargo y estos se interconectan de forma segura.	A.10.8.5 Sistemas de información empresarial.	1	

	A.10.9 Servicios de comercio electrónico.			A.10.9.1 Seguridad en comercio electrónico.	0	
				A.10.9.2 Seguridad en transacciones en línea.	0	
				A.10.9.3 Seguridad en información pública.	0	
	A.10.10 Monitorización.	Auditorías internas	Los registros de las auditorías internas permanecen guardados durante el tiempo necesario y puedan ser utilizados para identificar posibles problemas.	A.10.10.1 Registros de incidencias.	1	
		Herramientas de monitoreo	Se utilizan logs de seguridad.	A.10.10.2 Supervisión del uso de los sistemas.	1	
		Herramientas de monitoreo	Detectan el procesamiento no autorizado de la información.	A.10.10.3 Protección de los registros de incidencias.	1	
				A.10.10.4 Diarios de operación del administrador y operador.	0	
		Herramientas de monitoreo	Registro de fallos para determinar posibles problemas.	A.10.10.5 Registro de fallos.	1	
				A.10.10.6 Sincronización del reloj.	0	

Tabla 3.3: Lista de Cumplimiento Esperado de Controles de la Norma ISO/IEC 27001 para Seguridad Física y del Entorno.[60]

[60] Tabla elaborada por los autores en base a información obtenida del diagnóstico de la situación actual de la organización y la norma ISO/IEC 27001.
.

Una vez realizado el estado de cumplimiento actual y el estado de cumplimiento esperado (este último, ver Anexo XIV) la *Tabla 3.4* muestra la comparación entre estos, en el caso de que se implementen los controles recomendados y seleccionados en la sección 2.4. "Tratamiento del Riesgo".

A.5. Política de Seguridad.	0,00%	100,00%
A.6. Organización de la Seguridad de la Información.	36,36%	54,55%
A.7. Gestión de Activos.	80,00%	80,00%
A.8. Seguridad Ligada a los Recursos Humanos.	88,89%	88,89%
A.9. Seguridad Física y del Entorno.	61,54%	76,92%
A.10. Gestión de Comunicaciones y Operaciones.	53,13%	56,25%
A.11. Control de Accesos.	40,00%	44,00%
A.12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.	12,50%	12,50%
A.13. Gestión de Incidentes de la Seguridad de la Información.	0,00%	60,00%
A.14. Gestión de Continuidad del Negocio.	20,00%	20,00%
A.15. Conformidad.	20,00%	20,00%

Tabla 3.4: Comparación de estado de cumplimiento actual con estado de cumplimiento esperado.[61]

En la tabla anterior se aprecia un aumento significativo en los dominios de Política de Seguridad (del 0% al 100%) y Gestión de Incidentes de la Seguridad de la Información (del 0% al 60%), cabe recalcar que los controles recomendados para la implementación son solo para los activos críticos, por lo que si se establece un mayor alcance al Plan en donde se tome en cuenta más activos de la organización, los resultados dentro de cada dominio sería un porcentaje mayor al 50%.

Se puede apreciar que los dominios que aumentan el porcentaje de cumplimiento son los de tipo técnico, mientras que los dominios de tipo administrativo no han

[61] Tabla elaborada por los autores en base a la matriz de estado de cumplimiento esperado, Anexo XII.

tenido un aumento, excepto el de Política de Seguridad y Organización de Seguridad de la Información, la razón para esto es que el presente proyecto de titulación tiene como función ser una guía con lo que tiene que ver con la seguridad de la información, en donde las decisiones las tienen única y exclusivamente la alta Gerencia de la organización.

El dominio A.5 Política de Seguridad es el que sufre el mayor aumento pasando del 0% al 100%, esto se debe a que si existe la aprobación e implementación del Plan por parte de las autoridades pertinentes, ayudaría a que se implementen controles tanto de tipo técnicos como de tipo administrativos que ayuden a mejorar la seguridad de la información. Por lo que permitirá cumplir con los controles A.5.1.1 Documento de política de seguridad de la información y A.5.1.2 Revisión de la política de seguridad de la información.

El dominio A.6 Organización de la Seguridad de la Información sufre un aumento de 18.19 puntos porcentuales, pasando del 36,36% al 54,55%. Dentro de este dominio se seleccionó los controles A.6.1.1 Compromiso de la Dirección con la seguridad de la información, A.6.1.2 Coordinación de la seguridad de la información y A.6.1.3 Asignación de responsabilidades, mismos que permitirán mejorar la seguridad de la información.

El dominio A.7 Gestión de Activos, no tiene variación en el porcentaje de cumplimiento y se mantiene en 80% puesto que el control que se propone en este dominio y que se relaciona directamente con los activos críticos es el A.7.1.3 Acuerdo sobre el uso adecuado de los activos que ya se encuentra implementado.

El dominio A.8 Seguridad ligada a los recursos humanos, también se mantiene con un porcentaje de 88,89% debido a que los controles que no se cumplen no están involucrados directamente con los activos críticos.

El dominio A.9 Seguridad Física y del Entorno aumenta en 15,38 puntos porcentuales, pasando del 61,54% al 76,92%. Esto se debe a que dentro de este dominio se seleccionaron los controles A.9.2.4 Mantenimiento de los equipos y A.9.2.6 Seguridad en la reutilización o eliminación de equipos, además de los que

ya se encuentran implementados y se relacionan directamente con los activos críticos, mismos que ayudarán a mejorar la seguridad de la información.

El dominio A.10 Gestión de Comunicaciones y Operaciones aumenta en 3,12 puntos porcentuales, pasando de 53,13% al 56,25%. Esto se debe a que a pesar de que existen los controles necesarios dentro de la organización en este dominio no se los documenta, razón por la cual se seleccionó el control A.10.1.1 Documentación de los procedimientos operativos, que ayudará a mejorar la seguridad de la información.

El dominio A.11 Control de Accesos también aumenta, en 4 puntos porcentuales pasando de 40% al 44%, esto debido a que el control seleccionado que ayudará a mejorar la seguridad de la información es el A.11.4.1 Política de uso de los servicios de red, además de los que se proponen que ya están implementados e involucran a los activos críticos.

El dominio A.12 Adquisición, Desarrollo y Mantenimiento de Sistemas de Información no sufre cambios en el porcentaje de cumplimiento manteniéndose en 12,50%, esto se debe a que los controles especificados dentro de este dominio respecto a los que se encuentran ya implementados no se involucran directamente con la seguridad de la información de los activos críticos.

El dominio A.13 Gestión de Incidentes de la Seguridad de la Información, tiene un aumento significativo de 0% al 60%, esto se debe a que se seleccionaron los controles A.13.2.1 Identificación de responsabilidades y procedimientos, A.13.2.2 Evaluación de incidentes en seguridad y A.13.2.3 Recogida de pruebas, que ayudarán a mejorar la seguridad de la información.

El dominio A.14 Gestión de Continuidad del Negocio, no tiene variación en el porcentaje de cumplimiento y se mantiene en 20% debido a que estos controles no se involucran directamente con los activos críticos.

El dominio A.15 Conformidad, no tiene variación en el porcentaje de cumplimiento y se mantiene en 20% puesto que el control que se propone en este dominio y que se relaciona directamente con los activos críticos es el A.15.2.1 Conformidad con la política de seguridad que ya se encuentra implementado.

3.2.3.1. Aceptación de los funcionarios de la organización.

Para poder implementar un Sistema de Gestión de Seguridad de la Información dentro de una organización, uno de los requisitos para garantizar el éxito es la aceptación y compromiso de todos los funcionarios pertenecientes a la misma, para que de esta forma se involucren en el cumplimiento de la seguridad de la información.

Es por esta razón que se aplicó una encuesta (para ver la encuesta, ver Anexo XV) a cinco miembros de la organización, de los cuales tres pertenecen al Centro de Información, la misma que ayudó a determinar una postura ante una posible implementación de un SGSI. La *Figura* 3.2 muestra los resultados obtenidos de la encuesta realizada.

Las preguntas cuentan con cuatro opciones de respuesta, los porcentajes que se muestran corresponden a cada una de las contestaciones obtenidas por parte de los encuestados, es decir, cada respuesta en una misma pregunta tiene un valor del 20%.

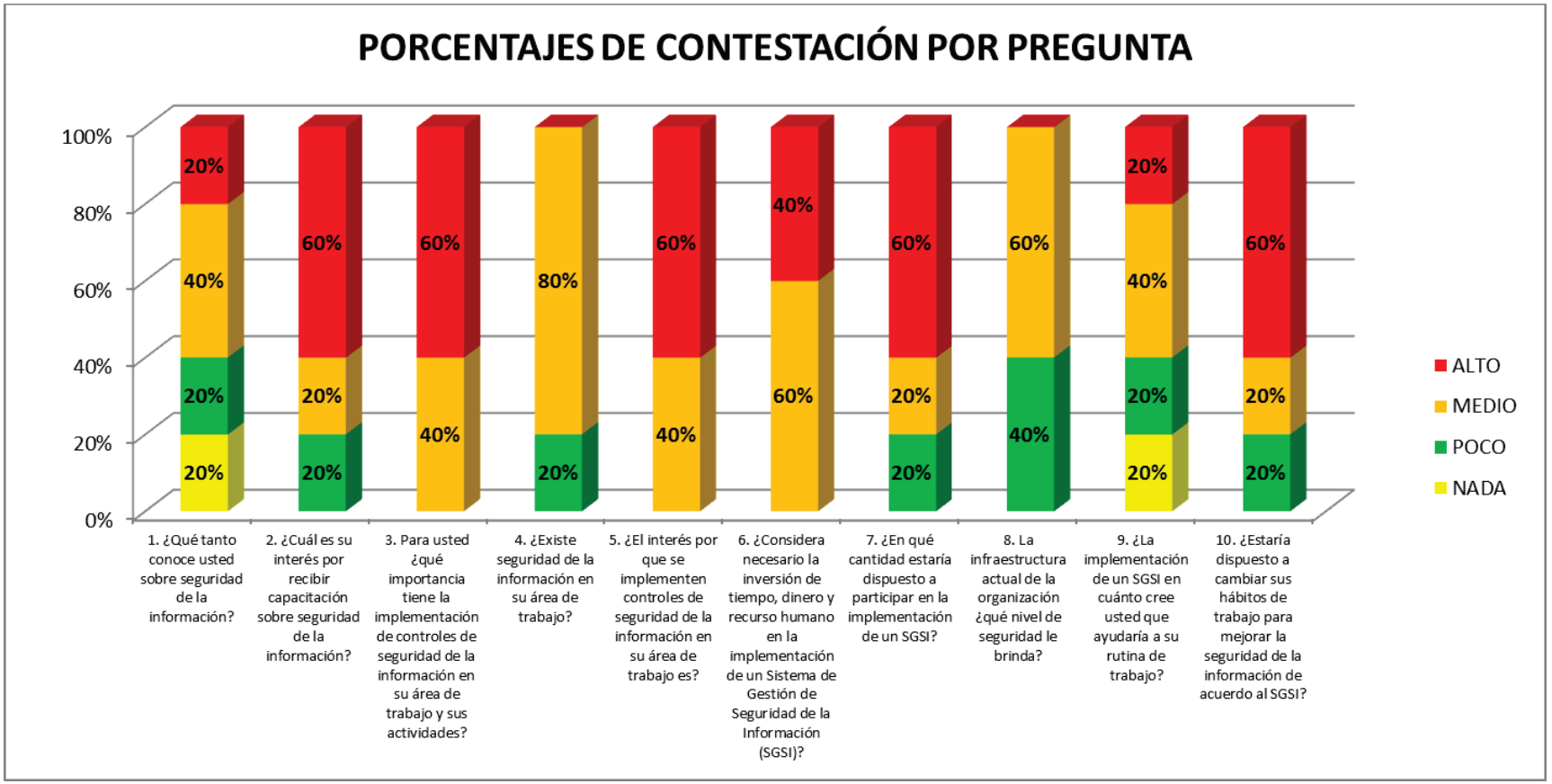

Figura 3.2: Porcentajes de Contestación por Pregunta.[62]

---

[62] Figura elaborada por los autores en base a los resultados obtenidos de la Encuesta de Aceptación.

Como resultado de la encuesta realizada, se puede resaltar que existe un nivel alto de lo siguientes puntos:

- Interés de los usuarios por capacitarse en seguridad de la información.
- Los usuarios están conscientes de lo importante que es implementar controles de seguridad de la información en sus áreas de trabajo y actividades, así como también muestran el respectivo interés en que estos controles se implementen.
- Los usuarios están dispuestos a participar activamente en la implementación de un SGSI, además de cambiar sus hábitos de trabajo para mejorar la seguridad de la información.

Además los usuarios en la encuesta, evidencian que la infraestructura de la seguridad de la información en las áreas de trabajo se encuentra en un nivel medio.

3.4.2. INVERSIÓN

Para poder implementar un plan de seguridad de la información se requiere de un análisis de impacto de la propuesta, tomando en cuenta condiciones como tiempo, presupuesto y personal necesario para el logro de los objetivos establecidos.

Al ser el caso de estudio una entidad pública el mayor punto a tomar en cuenta es el aspecto económico pues depende de que el Estado asigne este recurso, por esta razón en esta sección se presenta las restricciones, soluciones y un estimado de los recursos que deberán estar disponibles para la implementación del plan y si el Centro de Información cuenta con ellos.

3.2.4.1. Restricciones Económicas

El presupuesto designado para la implementación del plan depende del Estado, es por este motivo que un presupuesto reducido sea la mayor restricción en el proceso de implementación.

El tiempo y el personal que se asignen dentro de la implementación del plan son factores que afecta directamente el aspecto económico por lo cual también dependen directamente del presupuesto asignado a la entidad.

Por estas razones los beneficios que se pudieran obtener en la implementación del plan pueden no llegar a ser los esperados.

3.2.4.2. Soluciones Económicas

El análisis de factibilidad económica garantiza que el presupuesto necesario sea lo más exacto posible, es decir que se minimice el desperdicio de recursos económicos.

Cabe mencionar al CONADIS, que la implementación del plan no representa beneficios netamente económicos, sino que está enfocado en garantizar un ahorro a la organización en caso de que un ataque afecte a la seguridad de la información al implementarse los controles tomados en cuenta dentro del plan.

3.2.4.3. Factibilidad Económica

Como una de las soluciones ante las restricciones económicas en esta sección se presenta el análisis de factibilidad, en el cual los encargados de la seguridad de la información dentro del CONADIS podrán conocer el estimado de recursos que deberán estar disponibles para la implementación del Plan de Seguridad de la Información.

Como se mencionó en la sección 3.4.3.2 Soluciones Económicas, el beneficio que se obtiene del plan representa un ahorro debido a que evita gastos de recuperación ante un ataque y no de ingresos económicos para la institución, es por esto que un factor a considerar durante el análisis son los costos de implementación y mantenimiento de los controles seleccionados dentro del plan ya que el grado de factibilidad en la implementación depende de estos costos.

La *Tabla 3.6* que se muestra a continuación presenta un estimado de recursos económicos a considerar, necesarios para la implementación del plan.

Servidor de archivos	$3200,00	$3200,00	La organización no cuenta con la infraestructura necesaria para virtualizar un servidor de archivos, por lo que es importante su adquisición.
Recurso Humano	$30000,00	$18000,00	Se requiere designar un técnico, un administrador de red, un coordinador y un responsable para la gestión de incidentes, estos dos últimos deberán ser contratados debido a que en la organización no existen. Los valores corresponden a un salario mensual durante 6 meses aproximadamente.
Firewall	$7000,00	$0.00	La organización cuenta con un firewall, el mismo que protege a toda la organización a nivel de red.
Cámaras de seguridad	$3000,00	$0.00	La organización cuenta con un circuito cerrado de cámaras de seguridad que monitorea el ingreso a la sala de servidores así como a las áreas restringidas.
Sistema biométrico	$289,99	$0,00	La organización cuenta con sistema biométrico sin embargo es necesario reforzar el control para tener un registro de acceso a la sala de servidores.
Sistema contra incendios	$750,00	$0.00	Todos los espacios dentro de la organización se encuentran protegidos con un sistema contra incendios.
Sistemas de suministro eléctrico	$8000,00	$0.00	La organización cuenta con un sistema de suministro eléctrico y UPS que permite el continuo funcionamiento de los equipos eléctricos.
Antivirus	$1200,00	$0.00	La organización cuenta con la licencia de antivirus corporativo.
Capacitación	$1557,00	$1557,00	Es necesario que el personal del área de tecnología sea capacitado en seguridad de la información, de esta

			manera serán ellos los encargados de transmitir el conocimiento adquirido al personal restante en el caso de que sea necesario.
Norma ISO/IEC 27000[63]	$168,38	$168,38	Es necesario adquirir la norma debido a que proporciona una visión general de las normas que componen la serie 27000, introducción a los sistemas de gestión de seguridad de la información y una descripción del proceso PDCA.
Norma ISO/IEC 27001[63]	$144,04	$144,04	Es necesario adquirir la norma debido a que es la principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información.
Norma ISO/IEC 27002[63]	$217,07	$217,07	Es necesario adquirir la norma debido a que es la guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a la seguridad de la información.
Norma ISO/IEC 27003[63]	$180,56	$180,56	Es necesario adquirir la norma que aunque no es certificable, es la guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para la eficacia de un SGSI y de los controles o grupo de controles implementados según la ISO/IEC 27001.
Norma ISO/IEC 27005[63]	$180,56	$180,56	Es necesario adquirir la norma que de igual manera no es certificable pero proporciona las directrices para la gestión del riesgo en la seguridad de la información, además de apoyar los conceptos especificados en la norma ISO/IEC 27001.
Seguridad en el cableado	$1000	$0.00	El cableado se encuentra debidamente canalizado, etiquetado

[63] Documento de respaldo que debe ser alojado en el servidor de archivos, y disponible para el personal de la organización.

			y protegido.
TOTAL	$56887,60	$23647,61	

Tabla 3.5: Recursos económicos estimados para la implementacion del plan de seguridad de la información[64].

El costo estimado para la implementación del plan de seguridad de la información propuesto en el presente proyecto es de $56.887,60, donde se toma en cuenta los recursos iniciales necesarios, sim embargo el CONADIS cuenta actualmente con algunos de estos recursos por lo que el valor real de estimación de costos para la implementación del plan, tomando en cuenta lo dicho, es de $23.647,61.

[64] Tabla elaborada por los autores.

4. CAPÍTULO IV – CONCLUSIONES Y RECOMENDACIONES.

En este capítulo se muestran las conclusiones y recomendaciones que se obtuvieron a lo largo de la elaboración del proyecto.

4.1. CONCLUSIONES.

- El Consejo Nacional de Igualdad de Discapacidades cuenta con controles de seguridad que se encuentran implementados, pero no existe una evidencia formal de los mismos debido a que no se encuentran debidamente documentados, a pesar de ello estos controles fueron tomados en cuenta durante el análisis de estado de cumplimiento actual respecto a la norma ISO/IEC 27001, teniendo en cuenta que para el estado de cumplimiento esperado todos deben estar formalmente documentados.
- La red del Consejo Nacional de Igualdad de Discapacidades se encuentra soportada en base a tres servidores, los mismos que se encargan de brindar los servicios y recursos necesarios a las subredes y cada uno de los funcionarios de la organización, sin embargo solo uno de estos está dedicado a la subred interna del CONADIS.
- Los riesgos de la seguridad de la información determinados dentro del proyecto son a causa de varias amenazas y vulnerabilidades presentes en cada uno de los activos críticos, lo que conlleva no solo a identificarlos si no que también involucra la realización de determinadas actividades para una correcta gestión de los mismos, es por este motivo que la norma ISO/IEC 27005:2008 ayudó a realizar un correcto estudio de riesgos de seguridad de la información, ya que esta norma va desde definir un alcance para el proceso de gestión, pasando por el tratamiento, valoración y aceptación, hasta el monitoreo y revisión de los mismos, este último es responsabilidad de la organización en el caso de implementación de los controles propuestos.
- El tratamiento de riesgos de la seguridad de la información se lo puede realizar de cuatro maneras, las mismas que son:

- Reducción del riesgo, en el cual se debe elegir e implementar controles.
- Aceptación del riesgo, en la cual no es necesaria la implementación de controles.
- Transferencia del riesgo, en donde se lo traslada a terceros.
- Evitar el riesgo, en el cual se elimina el riesgo de tal manera que se llega al punto de eliminar el proceso o el activo.

De las cuales, en el proyecto se hace referencia a las dos primeras ya que estas dos forman parte de las estrategias y políticas con las que el CONADIS trata un riesgo, pero solamente la reducción del riesgo fue la que se adoptó para el tratamiento de los mismos, esto debido a que se busca demostrar el aporte que los controles propuestos de la norma ISO/IEC 27001 tienen en el mejoramiento del estado actual de la seguridad de la información dentro de la organización.

- En el Ecuador por medio de la secretaria de la Administración Pública se emitió en el 2013 el Acuerdo Ministerial 166, en el cual se establece como obligación que las entidades públicas gestionen la seguridad de su información por medio de estándares basados en la familia de Normas Técnicas Ecuatorianas NTE INEN ISO/IEC 27000, lo que muestra que las leyes nacionales obligan a la implementación de controles de seguridad en los organismos públicos. La norma NTE INEN-ISO/IEC 27001 es una adaptación de la ISO/IEC 27001 motivo por el cual el diseño del plan de seguridad de la información basado en esta última permitirá al CONADIS cumplir con los requisitos de seguridad establecidos por las leyes nacionales.
- El diseño del plan de seguridad de la información basado en la norma ISO/IEC 27001 establece los controles que de ser implementados garantiza al CONADIS la solución de problemas de seguridad mediante el análisis de riesgos, asegurando adecuadamente la gestión de la seguridad en la organización, en función del tratamiento de los riesgos hacia los activos críticos determinados.
- La gestión de seguridad de la información basada en la norma ISO/IEC 27001 plantea la implementación de un sistema de gestión de mejora

continua basada en el ciclo Deming: PHVA. El plan de seguridad de la información del CONADIS conforma la fase de planeación, ya que define el alcance y las Políticas de Seguridad, basadas en el análisis de riesgos actual de la organización, definiendo el plan de tratamiento de estos y proponiendo los controles de seguridad que deberán ser implementados para mitigar dichos riesgos. Las tres fases restantes, no son parte del alcance de este proyecto y quedarán a criterio de los directivos de la organización puesto que estas dependen de la aprobación que se le dé al plan.

- Durante la elaboración de la declaración de aplicabilidad se identificaron controles que no tiene que ver directamente con los activos críticos pero que son importantes al momento de definir los controles que ayudarán a mitigar los riesgos de la organización, dichos controles son todos aquellos que tienen que ver con la toma de decisiones o involucran a la dirección en la seguridad de la información.
- La elaboración de las políticas de seguridad que forman parte del plan de seguridad de la información contienen los diferentes controles que fueron seleccionados dentro de la declaración de aplicabilidad en el tratamiento del riesgo y en base al análisis de los activos críticos, por lo cual no es necesario elaborar un documento formal para cada control, sin embargo el conjunto de entregables contienen todos los que fueron seleccionados para asegurar dichos activos basándose en el alcance del plan, es decir la organización podrá crear nuevas políticas o modificar las que este plan propone, de ampliarse el alcance del plan.
- Se determinó que el nivel de riesgo más alto está directamente relacionado a la falta de documentación, esto se debe a la falta de gestión al momento de documentar cualquier proceso o actividad que se realiza dentro de la organización lo que provoca que exista mayor vulnerabilidad en este aspecto.

4.2. RECOMENDACIONES.

- Al encontrarse vigente el Acuerdo Ministerial 166, la implementación de Sistema de Gestión de Seguridad de la Información puede ser una actividad de alto compromiso por lo que necesita de una buena gestión de recursos, es por ese motivo que se recomienda seguir los lineamientos de la norma NTE INEN-ISO/IEC 27001, que es una adaptación de la norma general definida por la ISO que permite a las empresas y/u organizaciones ecuatorianas, públicas o privadas, a conseguir la implementación de un sistema de seguridad de la información adaptándose a las necesidades del entorno en el que se envuelven, lo que permite además obtener una certificación a nivel nacional puesto a que es reconocida a nivel internacional.
- La necesidad de una metodología apropiada y que se adapte a lo que se busca asegurar al momento de realizar el análisis de riesgo de la seguridad de la información es de suma importancia por lo que utilizar la norma de la familia ISO/IEC 27000 es un gran aporte a la realización de este tipo de actividades ya que contempla un marco completo para el análisis de riesgos.
- Las pruebas de penetración y las actividades que involucren la ejecución del Hackeo Ético deben ser llevadas en conjunto con encargados de la organización que se encuentren debidamente capacitados, para de esta manera evitar errores o posibles diagnósticos erróneos en la detección de vulnerabilidades. Además se deben planificar cronogramas para que este tipo de actividades se las realicen en circunstancias en las que se obtenga resultado pero que a la vez no afecte a las actividades normales de los usuarios de la organización.
- Los niveles de riesgo más altos determinados en este proyecto deben ser tratados con mayor prioridad debido a que si estos riesgos llegan a materializarse las consecuencias pueden provocar perjuicios a la organización. Los riesgos de menor nivel reciben un trato diferente, la organización definirá el tratamiento de los mismos, es decir, los elimina, los transfiere, los acepta o los reduce, como se ha mencionado a lo largo del

proyecto las autoridades de la organización son los que deciden. Por ello se recomienda que la organización revise la política de Tratamiento de Riesgos con el objeto de analizar la posibilidad de agregar otras formas de tratamiento, por ejemplo transferir el riesgo a una parte externa a la organización, de forma que se asegure el activo o se subcontrate un servicio.

- El análisis de riesgos de la seguridad de la información involucra diversas actividades y tareas que se deben realizar, para eso existen varios marcos de trabajo que pueden ser utilizados y que ayudan a la selección de controles, es por eso que al tener una metodología definida la mejor opción para el análisis de los riesgos es la propuesta por la norma ISO/IEC 27005, la misma que pertenece a la familia de normas utilizada y que facilita el trabajo.
- El cambio constante de las tecnologías o la integración de nuevos activos de información generaría nuevas amenazas y con ello los riesgos de la organización cambiarían, haciendo que el plan actual quede obsoleto y sin mucha ayuda en la seguridad de la información, por tal razón es necesario realizar revisiones periódicas al presente plan.
- El que los usuarios de la organización conozcan la importancia de la seguridad de la información y se involucren en la misma asegura el manejo de la información que cada funcionario posee, por esto el programar capacitaciones y difundir el trabajo realizado en este proyecto es de vital importancia.
- Las campañas de concientización hacia el personal es fundamental, esto con el fin de asegurar el buen uso de los activos que manejan y de los cuales son responsables, de la misma manera una buena práctica es difundir las políticas actuales, de tal manera que todos conozcan y las perciban como obligatorias, llegando a un punto en el que todos se adapten puesto que tienen que saber que se está trabajando en nuevas políticas que ayudarán a mejorar la seguridad de la información y que deberán ser parte del cumplimiento diario en sus actividades.

REFERENCIAS BIBLIOGRÁFICAS

[1] S. N. d. I. A. Pública, «ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACION EGSI,» 25 Septiembre 2013. [En línea]. Available: http://www.planificacion.gob.ec/wp-content/uploads/downloads/2013/12/Esquema-Gubernamental-de-Seguridades-de-la-Informaci%C3%B3n.pdf. [Último acceso: 10 Enero 2015].

[2] C. NACIONAL, *Ley sobre Discapacidades del Ecuador,* Quito, Pichincha, 2001.

[3] CONADIS, «Consejo Nacional de Discapacidades,» [En línea]. Available: http://www.conadis.gov.ec.

[4] O. d. G. d. Ecuador, *Suplemento Registro Oficial N° 252,* Quito, 2008.

[5] C. N. d. Discapacidades, «Consejo Nacional de Discapacidades - Legislación,» [En línea]. Available: http://www.conadis.gov.ec/legislacion/ley.html. [Último acceso: Junio 2014].

[6] CONADIS, «Ejes para políticas públicas en discapacidades,» de *Agenda Nacional para La Igualdad en Discapacidades 2013-2017*, Quito, 2013, pp. 100-113.

[7] I. O. f. Standardization, «Estándar Internacional ISO/IEC 27001 Tecnologías de la Información- Técnicas de Seguridad-Sistemas de Gestión de Seguridad de la Información- Requerimientos,» 2005.

[8] I. O. f. Standarization, «Estandar Internacional ISO/IEC 17799 - Teccología de la Información - Técnicas de seguridad - Código para la práctica de la gestión de la seguridad de la información,» 2005.

[9] definiciones.de, «definiciones.de,» 2008. [En línea]. Available: http://definicion.de/metodologia/. [Último acceso: 07 marzo 2015].

[10] J. C. Avellaneda, «Sistemas de Gestión Seguridad de la Información,» 10 Junio 2008. [En línea]. Available: http://sgsi-iso27001.blogspot.com/2008/06/publicada-la-iso-270052008-sobre-gestin.html. [Último acceso: 29 Septiembre 2014].

[11] I. O. f. Standardization, «ISO/IEC 27005 Information technology - Security techniques - Information security risk management,» Primera Edición, 15-06-2008.

[12] C. N. d. I. d. Discapacidades, «Intranet de la Organización,» [En línea].

[13] R. C. R. E. Crespo Crespo María Augusta, «UPS,» 2012. [En línea]. Available: http://dspace.ups.edu.ec/bitstream/123456789/3223/1/UPS-GT000334.pdf. [Último acceso: Noviembre 2014].

[14] B. firma-e, «¿Qué es un SGSI - Sistema de Gestión de Seguridad de la Información?,» Blog firma-e, 19 Febrero 2013. [En línea]. Available: http://blog.firma-e.com/que-es-un-sgsi-sistema-de-gestion-de-seguridad-de-la-informacion/. [Último acceso: 01 Diciembre 2014].

[15] ISO, «The ISO 27000 Directory,» ISO 27000, 2013. [En línea]. Available: http://www.27000.org/iso-27002.htm. [Último acceso: 16 Julio 2014].

[16] I. N. d. T. d. I. Comunicación, «Introducción a las Vulnerabilidades,» INTECO, [En línea]. Available: http://www.inteco.es/Formacion/Amenazas/Vulnerabilidades/. [Último acceso: 1 Septiembre 2014].

[17] Consejo Nacional de Igualdad de Discapacidades, «Agenda Nacional para la Igualdad en Discapacidades 2013-2017, » CONADIS, 2013.

[18] Consejo Nacional de Discapacidades, «Plan Estratégico», CONADIS, [En línea]. Not available: http://www.conadis.gov.ec

[19] Consejo Nacional de Igualdad de Discapacidades, «Organigrama», CONADIS, [En línea]. Available: http://www.consejodiscapacidades.gob.ec

[20] Instituto Ecuatoriano de Normalización, «NTE INEN-ISO/IEC 27003:2012 Tecnologías de la Información - Técnicas de Seguridad - Guía de Implementación del Sistema de Gestión de Seguridad de la Información,» Primera Edición, Fases y Entregables.

[21] International Organitation for Standardization, «Information technology - Security techniques - Information security risk management,» Primera Edición, 15-06-2008.

[22] Markus Erb, «Gestión de Riesgo en la Seguridad Informática,» 6. Amenazas y Vulnerabilidades, [En línea]. Available: https://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/

[23] Centro de Servicios para la Estandarización de Seguridad Informática, «informacionSGSI.pdf,» UN SGSI, ¿QUÉ BENEFICIOS APORTA?, [En línea]. Available: http://www.ceeisec.com/nuevaweb/doc/informacionSGSI.pdf

[24] Centro de Educación Continua de la Escuela Politécnica Nacional, «Curso: Seguridad de la Información - SGSI basado en la ISO 27001,» noviembre 2014, Introducción a ISO 27001.

ANEXOS

Anexos / Marco Legal

Anexos / Normas y Estándares

Anexo I – Matriz de Cumplimiento Actual

Anexo II – Identificación de Amenazas

Anexo III – Hackeo Ético

Anexo IV – Vulnerabilidades con Nessus

Anexo V – Análisis de Vulnerabilidades

Anexo VI – Lista de Vulnerabilidades con Nessus

Anexo VII – Resumen de Vulnerabilidades Técnicas

Anexo VIII – Evaluación de Riesgos en Activos Críticos

Anexo IX – Prioridad en la Implementación de Controles

Anexo X – Selección de Controles

Anexo XI – Instructivo para Revisión de Políticas

Anexo XII – Registro de Seguimiento de Políticas

Anexo XIII – Declaración de Aplicabilidad

Anexo XIV – Matriz de Cumplimiento Esperado

Anexo XV – Encuesta de Aceptación

Anexo XVI – Resultados de la Encuesta de Aceptación