FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

DESARROLLO DE UNA GUÍA PARA PLANES DE CONTINUIDAD DE NEGOCIO DE TI ENFOCADO A LAS OPERADORAS MÓVILES DEL ECUADOR

AUTORA

Tamia Micaela Govea Robayo

AÑO

2018

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

DESARROLLO DE UNA GUÍA PARA PLANES DE CONTINUIDAD DE NEGOCIO DE TI ENFOCADO A LAS OPERADORAS MÓVILES DEL ECUADOR.

Trabajo de Titulación presentado en conformidad con los requisitos establecidos para optar por el título de Ingeniera en Electrónica y Redes de Información.

Profesor Guía

MSc. Luis Santiago Criollo Caizaguano

Autora

Tamia Micaela Govea Robayo

Año

2018

DECLARACIÓN DEL PROFESOR GUÍA

"Declaro haber dirigido el trabajo, Desarrollo de una guía para planes de continuidad de negocio de TI enfocado a las operadoras móviles del Ecuador, a través de reuniones periódicas con el estudiante Tamia Micaela Govea Robayo, en el semestre 2018-2, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación".

_____

Luis Santiago Criollo Caizaguano
Magister en Redes de Comunicaciones
C.I.: 1717112955

DECLARACIÓN DEL PROFESOR CORRECTOR

"Declaro haber revisado este trabajo, Desarrollo de una guía para planes de continuidad de negocio de TI enfocado a las operadoras móviles del Ecuador, de Tamia Micaela Govea Robayo, en el semestre 2018-2, dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación".

_____

Iván Patricio Ortiz Garcés
Magister en Redes de Comunicaciones
C.I.: 0602356776

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.”

_____

Tamia Micaela Govea Robayo

C.I.: 1727295857

AGRADECIMIENTOS

Agradezco principalmente a Dios por estar conmigo en cada paso que doy y a mis maestros por todo el apoyo, disponibilidad y asesoramiento brindado en todo momento.

DEDICATORIA

A mis padres y mis hermanos por haberme apoyado en todo momento, por sus sabios consejos, sus valores, por la motivación constante que me ha permitido ser una persona de bien, pero más que nada por su amor y confianza.

RESUMEN

Últimamente, las organizaciones han dado una gran importancia a la implementación de planes que garanticen la continuidad en los procesos críticos de su negocio en caso de que ocurriera alguna eventualidad o incidentes que no estuvieran planeados. Es por esto, que las leyes son cada vez más exigentes en lo relacionado con la fiabilidad y disponibilidad en la prestación de los servicios, lo que conlleva que, en la actualidad, estos tipos de planes sean muy comunes en las organizaciones. Cabe recalcar, que en Ecuador no existe ningún formato o ley que regule la presentación de estos planes para los prestadores de servicios.

En el segundo capítulo de este trabajo de titulación, se realiza una recopilación de los conceptos fundamentales que intervienen en la elaboración de un plan de continuidad del negocio (PCN). Además, se investigó todas las normas internacionales y nacionales que rigen los temas de continuidad del negocio, gestión de riesgos y seguridad de la información, sobre las cuales estará basada la guía.

Asimismo, en el tercer capítulo se hizo un análisis de la criticidad de las amenazas naturales en el Ecuador y el nivel de riesgo que causarían, dividido por zonas. Esta información será de mucha utilidad para las operadoras móviles, para el reconocimiento de los mejores lugares para ubicar sus instalaciones e infraestructura de suma importancia; además, ayudará en la toma de decisiones de los directivos de las organizaciones.

Finalmente, en el cuarto capítulo se propone una guía para el desarrollo de planes de continuidad del negocio enfocado a las operadoras móviles del Ecuador, y que estas puedan tener una base o un formato al cual regirse al momento de realizar sus propios planes. Esta guía estará basada en nomas y estándares nacionales e internacionales. De esta manera, los planes realizados cumplirán las leyes nacionales y evitaran algún tipo de sanción por parte de la ARCOTEL, que es la encargada de la revisión de los planes de contingencia de los prestadores de servicios en el Ecuador.

ABSTRACT

Lately, organizations have attached great importance to the implementation of plans that guarantee continuity in the critical processes of their business in the event of any eventuality or incidents that were not planned. This is why the laws are increasingly demanding in relation to reliability and availability in the provision of services, which means that currently, these types of plans are very common in organizations. It should be noted that in Ecuador there is no format or law that regulates the presentation of these plans for service providers.

In the second chapter of this titulación work, a compilation of the fundamental concepts that take part in the elaboration of a plan of continuity of the business (PCN) is made. In addition, all the international and national regulations that govern the business continuity, risk management and information security topics, on which the guide will be based, were investigated.

Likewise, in the third chapter an analysis was made of the critical nature of natural hazards in Ecuador and the level of risk they would cause, divided by zones. This information will be very useful for mobile operators, for the recognition of the best places to locate their facilities and infrastructure of utmost importance; In addition, it will help in the decision making of the managers of the organizations.

Finally, the fourth chapter proposes a guide for the development of business continuity plans focused on mobile operators in Ecuador, and that these may have a basis or format to be followed when making their own plans. This guide will be based on national and international standards and standards. In this way, the plans made will comply with national laws and avoid any type of sanction by ARCOTEL, which is in charge of reviewing the contingency plans of service providers in Ecuador.

ÍNDICE

1.INTRODUCCIÓN 1

1.1. Antecedentes 1

1.2. Alcance 1

1.3. Justificación 2

1.4. Objetivo general 3

1.5. Objetivos específicos 3

2.MARCO TEÓRICO Y LEGAL 3

2.1. MARCO TEÓRICO 3

2.1.1. Seguridad de la información 3

2.1.1.1.Objetivos de la seguridad de la información 4

2.1.1.2.Conceptos fundamentales de la seguridad de la información 5

2.1.2. Continuidad del negocio 7

2.1.2.1.Elementos principales de la continuidad del negocio 7

2.1.3. Plan de continuidad de negocio (PCN) 8

2.1.3.1.Alcance del plan 10

2.1.3.2.Premisas de partida 11

2.1.3.3.Funciones de la dirección 11

2.1.3.4.Etapas de implementación 12

2.1.4. Gestión de la continuidad del negocio (GCN) 15

2.1.4.1.Aspectos de seguridad de la información en la gestión de la continuidad del negocio 16

2.1.5. Plan de recuperación de desastres (PRD) 16

2.1.6. Análisis del impacto al negocio (BIA) 17

2.1.6.1.Características del análisis de impacto 18
2.1.7. Operador de Red Móvil 19
2.2. MARCO LEGAL 20
2.2.1. Normas y estándares internacionales 20
2.2.1.1.ISO 22301: Sistema de Gestión de Continuidad de Negocio 20
2.2.1.2.ISO 27031: Gestión de la Tecnología de Información y Comunicación y obtención de Continuidad de Negocio 21
2.2.1.3.ISO 27001: Tecnología de la información - Técnicas de seguridad - Gestión de la seguridad de la información sistemas – Requisitos 22
2.2.1.4.ISO 27005: Tecnología de la información - Técnicas de seguridad - Gestión del riesgo de seguridad de la información 22
2.2.2. Normas y Estándares Nacionales 23
2.2.2.1.Norma que regula la presentación de los planes de contingencia para la operación de las redes públicas de telecomunicaciones por parte de los prestadores de servicios del régimen general de telecomunicaciones 23
3.ANÁLISIS DE RIESGOS A NIVEL PAÍS POR ZONAS 24
3.1. Análisis de la criticidad de los riesgos a nivel país 24
3.1.1. Identificación de amenazas naturales en el Ecuador 24
3.1.1.1.Tsunamis 25
3.1.1.2.Sismos 26
3.1.1.3.Inundaciones 26
3.1.1.4.Incendios Forestales 26

3.1.1.5.Erupciones Volcánicas 27
3.1.1.6.Deslaves o deslizamientos 27
3.1.1.7.Sequia 27
3.1.1.8.Aguajes y oleajes..... 28
3.1.1.9.Cambios Climáticos..... 28
3.1.2. Análisis de amenazas por cantón en el Ecuador 29
3.1.2.1.Sismos..... 29
3.1.2.2.Tsunamis 30
3.1.2.3.Erupciones Volcánicas 31
3.1.2.4.Inundaciones 32
3.1.2.5.Incendios Forestales..... 33
3.1.2.6.Deslaves o deslizamientos 34
3.1.2.7.Sequía 35
3.1.2.8.Cambios Climáticos..... 36
3.1.3. Análisis del riesgo por amenaza de origen natural 36
3.1.3.1.Riesgo por amenaza sísmica 37
3.1.3.2.Riesgo por amenaza de tsunami 38
3.1.3.3.Riesgo por amenaza volcánica..... 40
3.1.3.4.Riesgo por amenaza de inundaciones..... 41
3.1.3.5.Riesgo por amenaza de deslaves o deslizamientos 43
3.1.3.6.Riesgo por amenaza de sequía..... 44
3.1.4. Cantones más vulnerables del Ecuador 45
3.1.5. Metodología de análisis del impacto y probabilidad..... 47
3.1.5.1.Determinación de la probabilidad 48
3.1.5.2.Determinación del impacto 49

3.1.6. Evaluación del riesgo y criticidad de las amenazas de origen natural en cada provincia 50
3.1.6.1. Riesgo sísmico 51
3.1.6.2. Riesgo tsunami 52
3.1.6.3. Riesgo volcánico 53
3.1.6.4. Riesgo inundaciones 55
3.1.6.5. Riesgo deslizamientos 56
3.1.6.6. Riesgo sequía 58
4. GUÍA GENERAL PARA ELABORACIÓN DE PLANES DE CONTINUIDAD DE NEGOCIOS PARA OPERADORAS MÓVILES 59
4.1. FASE 1: Análisis del negocio y riesgos 59
4.1.1. Análisis del negocio 60
4.1.1.1. Definición del contexto 60
4.1.1.2. Definición del alcance y límites 62
4.1.1.3. Criterios para la evaluación del riesgo 62
4.1.2. Identificación, análisis y evaluación de riesgos 63
4.1.2.1. Identificación del riesgo 65
4.1.2.2. Análisis del riesgo 81
4.1.2.3. Evaluación del riesgo 89
4.2. FASE 2: Análisis del impacto del negocio 92
4.2.1. Aspectos importantes 92
4.2.1.1. Preparar el equipo de trabajo 92
4.2.1.2. Identificar los participantes 93
4.2.1.3. Métodos para obtención de información 93
4.2.2. Evaluación de impacto financiero y operacional 94

4.2.2.1.Impacto financiero 94
4.2.2.2.Impacto operacional 94
4.2.3. Requerimientos de tiempo de recuperación 95
4.2.3.1.RTO 96
4.2.3.2.RPO 96
4.2.3.3.WRT 96
4.2.3.4.MTD 97
4.2.3.5.MTPoD 97
4.2.4. Metodología del análisis del impacto del negocio 97
4.2.4.1.Identificación de funciones y procesos 98
4.2.4.2.Evaluación de impactos operacionales 99
4.2.4.3.Identificación de procesos críticos 99
4.2.4.4.Establecimiento de tiempos de recuperación 100
4.2.4.5.Identificación de recursos críticos 100
4.2.4.6.Disposición de los RTO/RPO 101
4.2.4.7.Identificación de procesos alternos 101
4.2.4.8.Generación de informe de impacto del negocio 102
4.3. FASE 3: Selección de la estrategia 102
4.3.1. Centro alternativo 103
4.3.1.1.Localización dentro de la organización 104
4.3.1.2.Acuerdos recíprocos 104
4.3.1.3.Acuerdos con proveedores de equipos 105
4.3.1.4.Empresas de servicio 105
4.3.2. Comunicaciones alternativas o trabajo remoto 105
4.3.3. Procedimientos de backup 105
4.3.4. Centro de almacenamiento externo 105

4.4. FASE 4: Ejecución y desarrollo del plan 107
4.4.1. Organización y funciones de los equipos de recuperación 107
4.4.2. Plan de acción 113
4.4.2.1.Definición de desastres 113
4.4.2.2.Procedimientos para la continuidad del negocio 113
4.4.3. Plan de vuelta a la normalidad 115
4.5. FASE 5: Plan de evaluación y mantenimiento 115
4.5.1. Plan de evaluación 116
4.5.2. Mantenimiento 118
5.CONCLUSIONES Y RECOMENDACIONES 120
5.1. Conclusiones 120
5.2. Recomendaciones 122
REFERENCIAS 123
ANEXOS 126

ÍNDICE DE FIGURAS

Figura 1. Ciclo de vida del plan de continuidad del negocio. 10
Figura 2. RTO y RPO. 19
Figura 3. Mapa de nivel de amenaza sísmica por cantón en el Ecuador. 29
Figura 4. Mapa de nivel de amenaza por tsunami por cantón en el Ecuador. 30
Figura 5. Mapa de nivel de amenaza volcánica por cantón en el Ecuador. 31
Figura 6. Mapa de nivel de amenaza por inundación por cantón en el Ecuador. 32
Figura 7. Mapa de probabilidad de generación de incendios forestales y focos de calor. 33
Figura 8. Mapa de nivel de amenaza de deslizamientos por cantón en el Ecuador. 34
Figura 9. Mapa de nivel de amenaza de sequía por cantón en el Ecuador. 35
Figura 10. Mapa de los diferentes climas del Ecuador. 36
Figura 11. Riesgo por amenaza sísmica por cantón en el Ecuador. 37
Figura 12. Riesgo por amenaza por tsunami por cantón en el Ecuador. 38
Figura 13. Riesgo por amenaza volcánica por cantón en el Ecuador. 40
Figura 14. Riesgo de inundación por cantón en el Ecuador. 41
Figura 15. Riesgo por deslizamiento y deslaves por cantón en el Ecuador. 43
Figura 16. Riesgo por sequía por cantón en el Ecuador. 44
Figura 17. Nivel de amenaza de origen natural por cantón en el Ecuador. 47
Figura 18. Mapa de riesgo sísmico en el Ecuador 52
Figura 19. Mapa de riesgo de tsunami en el Ecuador 53
Figura 20. Mapa de riesgo volcánico en el Ecuador 55
Figura 21. Mapa de riesgo de inundaciones en el Ecuador 56
Figura 22. Mapa de riesgo de deslizamientos en el Ecuador 58

Figura 23. Mapa de riesgo de sequía en el Ecuador. 59
Figura 24. Proceso de gestión del riesgo. 65
Figura 25. Actividades de la identificación del riesgo. 66
Figura 26. Actividades de la identificación de los activos. 67
Figura 27. Clasificación general de los activos 68
Figura 28. Actividades de la identificación de las amenazas. 71
Figura 29. Identificación de los controles existentes. 74
Figura 30. Actividades de la identificación de las vulnerabilidades. 77
Figura 31. Actividades de las consecuencias. 80
Figura 32. Actividades del análisis del riesgo. 84
Figura 33. Actividades de la evaluación de las consecuencias. 85
Figura 34. Evaluación de la probabilidad de los incidentes. 87
Figura 35. Determinación del nivel del riesgo 88
Figura 36. Fase de evaluación del riesgo. 91
Figura 37. Metodología del análisis del impacto del negocio. 98
Figura 38. Funciones del equipo de gestión de incidentes. 108
Figura 39. Funciones del equipo de operaciones informáticas 109
Figura 40. Funciones del equipo de administración 110
Figura 41. Definición de desastres 113
Figura 42. Proceso de verificación del plan de continuidad de negocio 117

INDICE DE TABLAS

Tabla 1. Tabla de análisis del riesgo sísmico. 37
Tabla 2. Tabla de análisis de riesgo tsunami. 39
Tabla 3. Tabla de análisis de riesgo amenaza volcánica 40
Tabla 4. Tabla de análisis de riesgo inundación. 41
Tabla 5. Tabla de análisis de riesgos por deslizamiento y deslaves. 43
Tabla 6. Tabla de análisis del riesgo por sequía. 45
Tabla 7. Cantones clasificados según su grado de amenaza. 46
Tabla 8. Probabilidad de ocurrencia de un evento determinado 48
Tabla 9. Impacto de un determinado evento 49
Tabla 10. Matriz de evaluación de riesgos 50
Tabla 11. Riesgo sísmico por provincias en el Ecuador 51
Tabla 12. Riesgo de Tsunami por provincias en el Ecuador 52
Tabla 13. Riesgo volcánico por provincias en el Ecuador 53
Tabla 14. Riesgo inundaciones por provincias en el Ecuador 55
Tabla 15. Riesgo deslizamiento por provincias en el Ecuador 56
Tabla 16. Riesgo de sequía por provincia en el Ecuador 58
Tabla 17. Ítems para el análisis de la organización 60
Tabla 18. Ejemplo de criterio de nivel de impacto 63
Tabla 19. Ejemplo de criterio de nivel de probabilidad 63
Tabla 20. Ejemplo de criterio de nivel de riesgo 63
Tabla 21.Formato para la identificación de los activos 70
Tabla 22. Formato para identificación de las amenazas de los activos 73
Tabla 23. Ejemplos de tipos de control 75
Tabla 24. Formato identificación de vulnerabilidades 79
Tabla 25. Formato para identificación de consecuencias 81
Tabla 26. Ejemplo de evaluación del impacto 86
Tabla 27. Ejemplo de evaluación de probabilidad 87
Tabla 28. Matriz de calificación, evaluación y respuestas a riesgos 89
Tabla 29. Ejemplo de lista de evaluación de riesgos 91
Tabla 30. Costos considerados en el impacto financiero 94

Tabla 31. Formato para la identificación de funciones y procesos 98
Tabla 32. Formato para la evaluación de impactos operacionales..... 99
Tabla 33. Identificación de procesos críticos..... 99
Tabla 34. Formato de establecimiento de tiempos de recuperación. 100
Tabla 35. Formato para identificación de recursos críticos 101
Tabla 36. Formato para disposición de RTO, RPO y WRT 101
Tabla 37. Formato para identificación de procesos alternos 102
Tabla 38. Formato para miembros del equipo de gestión de incidentes 108
Tabla 39. Formato para miembros del equipo de operaciones informáticas..... 109
Tabla 40. Formato para miembros del equipo de administración..... 110
Tabla 41. Formato para miembros del equipo de atención a usuarios..... 111
Tabla 42. Formato para miembros del equipo de inmuebles 111
Tabla 43. Formato para miembros del equipo de inmuebles 112
Tabla 44. Formato para funciones de los equipos de recuperación..... 112
Tabla 45. Cantones del Ecuador clasificados según el grado de amenaza 127

1. INTRODUCCIÓN

1.1. Antecedentes

Anteriormente, se consideraba desastre a cualquier forma de calamidad que podría destruir recursos físicos como: archivos, libros, registros y máquinas de una empresa. Hoy en día, las empresas enfrentan nuevas formas de desastres, que afectan directamente a su principal activo que es la información.

Se puede considerar como desastre informático a la interrupción del servicio de forma momentánea o permanente que no haya sido planificada, y afecta a la infraestructura o servicios críticos de la organización.

Todo el tiempo, las organizaciones están expuestas a amenazas y riesgos informáticos, para lo cual se debe contar con un plan de contingencia o también llamado plan de continuidad de negocio que nos permita saber cómo reaccionar, restaurar y recuperar la información, manteniendo siempre la continuidad de los servicios.

En el 2017, en Ecuador la Agencia de Regulación y Control de las Telecomunicaciones, emitió la “norma que regula la presentación de los planes de contingencia para la operación de las redes públicas de telecomunicaciones por parte de los prestadores de servicios del régimen general de telecomunicaciones”. Esta norma tiene por objeto regular la presentación de planes de contingencia, por los prestadores de servicios de telecomunicaciones, para ejecutarlos en casos de desastres naturales o conmoción interna para garantizar la continuidad del servicio. (ARCOTEL, 2017).

1.2. Alcance

El alcance de este trabajo de titulación es elaborar una guía de plan de continuidad de negocio de TI, para que las operadoras móviles en el Ecuador

puedan tomar como referencia y así elaborar un plan que se ajuste a cada una; en caso de que ocurriera un desastre natural o en situaciones de emergencia. Esta guía estará basada en normas y estándares nacionales e internacionales como las ISO que nos permiten el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.

El resultado de todo este procedimiento será la obtención un documento guía que permitirá a cualquiera de las operadoras móviles del Ecuador, poder realizar su plan de continuidad de negocio.

1.3. Justificación

En la actualidad, más del 90% de todos los procesos en la industria están basados directa o indirectamente en la tecnología. Este es el caso de las operadoras móviles ya que una caída en sus servicios significaría un gran impacto sobre sus usuarios y esto a su vez daría como resultado la interrupción del servicio y por ende perdidas económicas.

Los resultados de estos desastres para las operadoras móviles, que no cuentan con un plan de continuidad de negocio, pueden significar la interrupción momentánea o permanente de sus servicios. Con la caída de su red dejarían incomunicados a numerosos usuarios; como sucedió durante el terremoto ocurrido el pasado 16 de abril de 2016, en la zona costera de Ecuador, donde se evidenció la caída de los servicios de las operadoras móviles del país.

Estos son los motivos que marcan la importancia de contar con un plan de continuidad de negocio, para proporcionar a las operadoras móviles la recuperación de sus procesos y restaurar sus servicios e infraestructura critica. Esta guía detectará el riesgo en la organización, permitiendo el normal funcionamiento de sus sistemas, y definirá la aplicación de los controles que sean necesarios para mitigarlos o eliminarlos; en la medida de lo posible.

1.4. Objetivo general

Generar una guía de plan de continuidad de negocio de TI para que las operadoras móviles del Ecuador la tomen como referencia al momento de realizar sus propios planes de contingencia.

1.5. Objetivos específicos

- Investigar las normas Internacionales que rigen el tema de planes de continuidad de negocios de las TI.
- Investigar las normativas y estándares sobre el riesgo país en el tema de catástrofes o desastres naturales que rigen en el Ecuador.
- Analizar la criticidad de los riesgos que existe en el Ecuador por zonas.
- Definir una guía de plan de contingencia de TI enfocado a las operadoras móviles del Ecuador.

2. MARCO TEÓRICO Y LEGAL

2.1. MARCO TEÓRICO

2.1.1. Seguridad de la información

La información es un activo que es esencial para las actividades de la organización y por lo tanto necesita una protección adecuada. Esto, es especialmente importante en el entorno de los negocios que cada vez se encuentran más interconectados. Como resultado de esta interconexión creciente, la información se expone a un gran número y variedad de amenazas y vulnerabilidades.

La seguridad de la información es la protección de la información contra una gran variedad de amenazas con el fin de asegurar la continuidad del negocio,

minimizar el riesgo y maximizar el retorno de inversiones y oportunidades del negocio (NTC-ISO/IEC 27002, 2007).

Según la ISO 27001, se puede definir como la preservación de la confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización (ISO 27001, 2013) .

2.1.1.1. Objetivos de la seguridad de la información

Los principales objetivos de la seguridad de la información son los siguientes:

- **Confidencialidad**

Es el requisito que intenta que la información privada o secreta no sea revelada a individuos no autorizados (Areitio Bertolin, 2008).

- **Integridad**

Se encarga de garantizar, que la información del sistema no haya sido alterada por usuarios no autorizados, evitando la perdida de consistencia, manteniendo la exactitud y completitud de la información (Areitio Bertolin, 2008).

- **Disponibilidad**

Acceso y utilización de la información y los sistemas de tratamiento de esta por parte de individuos, entidades o procesos autorizados cuando lo requieran (ISO 27001, 2013).

2.1.1.2. Conceptos fundamentales de la seguridad de la información

2.1.1.2.1. Incidente de seguridad

Corresponde a cualquier evento relacionado con la seguridad; por ejemplo, ataques de denegación de servicio, robo de información, fuga y la obtención de un acceso no autorizado a la información (Villamil, 2014).

2.1.1.2.2. Activo

Cualquier elemento que tenga valor para la organización y su negocio. Algunos ejemplos: bases de datos, software, equipos, servidores, dispositivos de red, personas, procesos y servicios (Villamil, 2014).

2.1.1.2.3. Amenaza

Cualquier evento que explote vulnerabilidades. Causa potencial de un incidente no deseado, que puede resultar en daños a un sistema u organización (Villamil, 2014).

2.1.1.2.4. Vulnerabilidad

Cualquier debilidad que puede ser explotada y ponga en peligro la seguridad de los sistemas y datos. Fragilidad de un activo o grupo de activos que pueden ser explotados por una o más amenazas. Las vulnerabilidades son fallas, que permiten la aparición de deficiencias en la seguridad general del equipo o de la red. Configuraciones incorrectas en el equipo o en la seguridad también permiten la creación de vulnerabilidades. A partir de esta falla, las vulnerabilidades son explotadas por amenazas que cuando se materializan, causan daños al computador, a la organización o a los datos personales (Villamil, 2014).

2.1.1.2.5. Riesgo

Combinación de la probabilidad (oportunidad de que la amenaza se materialice) de que ocurra un evento y sus consecuencias para la organización. Algo que puede ocurrir y sus efectos sobre los objetivos de la organización (Villamil, 2014).

2.1.1.2.6. Ataque

Cualquier acción que comprometa la seguridad de una organización (Villamil, 2014)**.**

2.1.1.2.7. Impacto

Resultado evaluado de evento particular (Villamil, 2014).

Por lo tanto, la seguridad de la información es un elemento muy importante cuando se habla de la continuidad del negocio de una empresa u organización. De manera que se debe tomar algunas consideraciones que están directamente relacionadas con el análisis de riesgos:

- La compresión de los riesgos para la organización en términos de probabilidades.
- Identificación de los procesos críticos de negocio y los activos directamente relacionados.
- La compresión de los impactos generados a los negocios por los incidentes de seguridad.
- Identificación de los contratos de seguro establecidos para los activos críticos de la organización.
- Identificación de las medidas preventivas, correctivas e ilustrativas aplicables.
- Identificación de los recursos financieros, de infraestructura, técnicos y ambientales necesarios para la recolección de los requisitos de seguridad.

- La consideración con respecto a las medidas para garantizar la protección de los recursos de procesamiento.
- La información detallada sobre los requisitos de seguridad de la información a ser incluidos.
- La formalización de las pruebas y del mantenimiento de los planes (de continuidad del negocio y de contingencias, por ejemplo) (Villamil, 2014).

2.1.2. Continuidad del negocio

Cada vez más, las organizaciones dependen casi completamente de todo lo que tenga que ver con tecnología y sistemas computacionales. Razón por la cual, la pérdida de la información o de los equipos con los que se cuentan, significaría una decaída en su negocio; llegando a causar grandes pérdidas financieras y en el peor de los casos hasta podría ser responsable del cierre de la organización.

Precisamente, para evitar este tipo de escenarios, se utiliza un concepto llamado continuidad del negocio, que se encarga de garantizar que el impacto de una interrupción en el negocio sea la mínima posible.

La continuidad del negocio se podría definir como la planificación que se debe tener en cuenta en una organización; para que en caso de que existiera algún desastre o incidente, esta pueda seguir operando y que además se pueda recuperar en caso de algún fallo. Incluye 3 elementos principales:

2.1.2.1. Elementos principales de la continuidad del negocio

- **Resistencia:** las funciones comerciales críticas y la infraestructura de soporte deben estar diseñadas de tal manera que no se vean afectadas por perturbaciones relevantes; por ejemplo, mediante el uso de redundancia y capacidad disponible.

- **Recuperación:** las organizaciones deben hacer arreglos para recuperar o restaurar funciones comerciales críticas y menos críticas que fallen por algún motivo.

- **Contingencia:** la organización establece una capacidad generalizada y la disposición para hacer frente de manera efectiva a los incidentes y catástrofes importantes que ocurran, incluidos los eventos que no estaban, y tal vez no pudieron haber sido, previstos. Los preparativos para contingencias constituyen una respuesta de último recurso si la resiliencia y los arreglos de recuperación resultan inadecuados en la práctica.

En resumen, la continuidad del negocio no es simplemente recuperación ante desastres, gestión de crisis, gestión de riesgos o recuperación tecnológica. No es simplemente una disciplina realizada por especialistas profesionales, sino un enfoque global de la actividad que integra un amplio espectro de actividades de gestión encaminadas al objetivo final de la organización.

Es decir, la continuidad del negocio crea el marco tanto estratégico como operativo para revisar y modificar la forma en que la organización proporciona sus productos y servicios. Por ende, aumentará su resistencia frente a interrupciones o pérdidas. (Martinez, 2010)

Para poder asegurar los puntos mencionados anteriormente, se recomienda que cada organización cuente con un plan de continuidad del negocio. Esto es totalmente responsabilidad de los líderes de cada organización.

2.1.3. Plan de continuidad de negocio (PCN)

Esta es una de las definiciones más importantes de este trabajo de investigación; puesto que, el principal objetivo del uso de esta guía para las operadoras móviles del Ecuador es que logren obtener un correcto y eficiente plan de continuidad del

negocio. Por lo tanto, es importante tener una idea bastante clara de lo que es y para qué sirve.

Según la ISO 27031, plan de continuidad de negocio, es un conjunto de procedimientos documentados que guían a las organizaciones a responder, recuperar, reanudar y restaurar a un nivel predefinido de operación después de la interrupción. Por lo general, esto cubre los recursos, los servicios y las actividades necesarias para garantizar la continuidad del negocio crítico (ISO/IEC 27031, 2011).

Hace algunos años, cuando se hablaba de planes de prevención o planes de contingencia, estos eran enfocados solamente a los sistemas informáticos que por lo general eran las áreas informáticas de cada organización, considerando que la información era almacenada de manera centralizada.

Pero actualmente, con la aparición del almacenamiento distribuido se ha tenido un cambio significativo en la orientación de estos planes, puesto que los PCN abarcan todo lo que sea considerado un activo en la organización, siendo la información el activo más importante.

En la figura 1, se muestra el ciclo de vida del plan de continuidad del negocio:

Figura 1. Ciclo de vida del plan de continuidad del negocio.

Tomado de (Bilait, s.f.)

2.1.3.1. Alcance del plan

El plan de continuidad de negocio debe ser diseñado para crear una situación de preparación que proporcione una respuesta inmediata diseñada en función de una serie de posibles escenarios previamente definidos.

En primer lugar, será preciso definir qué departamentos, dependencias, instalaciones, etc., van a ser incluidas en el plan. No es lo mismo abarcar solamente las instalaciones de un centro de procesamiento de datos centralizado que incorporar otras dependencias que puedan contener centros satélites. No es lo mismo desarrollar un plan de contingencia informático, que abarque solamente la recuperación y continuidad de las actividades informáticas que un PCN que considere todas las funciones críticas de la organización.

Después, será preciso elegir entre todo el catálogo de posibles amenazas, cuáles de ellas son más probables y descartar que las que, aun siendo posibles, su probabilidad de ocurrencia es mucho menor. Aquí juega un papel muy importante el presupuesto disponible para la implementación del PCN. La consideración de algunas amenazas puede entrañar la necesidad de implementación de medidas que supongan unos costes importantes. Es decir, a la hora de definir el alcance del plan se deben tener muy en cuenta las limitaciones presupuestarias y dimensionarlo de acuerdo con esas limitaciones. Cada uno de los supuestos elegidos pueden requerir soluciones muy diferentes en su diseño y coste. Por otra parte, como muchas otras que habrá que tomar a lo largo del desarrollo e implementación, la decisión del alcance del plan debe estar aprobada por la dirección (Martinez, 2010).

2.1.3.2. Premisas de partida

Aparte de la definición del alcance del plan, es importante definir y señalar una serie de supuestos sobre los cuales basar todas las actualizaciones en las que se fundamenta el plan. La posibilidad de aplicación de las medidas planificadas puede depender de múltiples factores externos. En la medida que esos factores se comporten de una u otra forma, las medidas previstas serán aplicables o no. Conviene pues, enumerar esos supuestos para, si la dirección considera que son excesivamente optimistas o pesimistas, corregir el plan a la baja o alza, ya que ello repercutirá, como siempre, no solo en el coste de las medidas a implantar, sino en un mayor o menor índice de cobertura (Martinez, 2010).

2.1.3.3. Funciones de la dirección

El proceso de elaboración e implementación del plan debe ser cuidadosamente realizado y previamente propuesto a la dirección para su aprobación, por consiguiente, para la mayor parte de incidentes, los procedimientos de respuesta y recuperación están previamente estudiados y aprobados. Las funciones de la dirección se limitan solamente a la revisión y aprobación de cualquier acción que

sobrepase de las estrategias de respuesta y recuperación planificadas y previamente aprobadas.

Únicamente para los casos en los que el incidente hubiera excedido las previsiones será requerida para la intervención directa de los órganos directivos.

En esos casos, el equipo de gestión de incidentes es total responsable de la preparación de informes para la dirección, con lo que ayudará a la gestión del día a día y a la toma de decisiones acerca de cuestiones no previstas en el PCN (Martinez, 2010).

2.1.3.4. Etapas de implementación

2.1.3.4.1. Estructura

La estructura de un PCN normalmente debe contener lo siguiente:

- Responsabilidades individuales necesarias para cada una de las actividades propuestas en el plan;
- Indicaciones de un gestor especifico;
- Las condiciones necesarias para la activación del plan.;
- Los procedimientos para garantizar la operación temporal de los procesos y sistemas de negocios, mientras se está ejecutando la recuperación;
- Los procedimientos de emergencia para situaciones en las que hay incidentes que afectan directamente a los negocios;
- Procedimientos de recuperación de procesos y operaciones de negocio en un rango de tiempo aceptable;
- Especificación del calendario de mantenimiento y pruebas a los planes;
- Promoción del entrenamiento en relación con la continuidad del negocio (Villamil, 2014).

2.1.3.4.2. Desarrollo e implementación

En la planificación de la continuidad del negocio se debe tomar en cuenta algunos elementos fundamentales que muestran el contenido que incluirá en el plan, los principales son los siguientes:

- Identificación de las responsabilidades y los procedimientos para la continuidad del negocio;
- Grado de identificación aceptable de pérdidas de información y servicios;
- La aplicación de los procedimientos de recuperación de las operaciones del negocio y la disponibilidad de información, teniendo en cuenta el marco de tiempo aceptable para restaurar el funcionamiento normal de las operaciones;
- La conciencia de las personas en función de sus responsabilidades y el conocimiento de los procedimientos involucrados;
- Pruebas;
- El mantenimiento regular del plan con el fin de reflejar los cambios significativos en el negocio de la organización.

Es importante tener en cuenta que todas las dependencias externas a la organización y los contratos existentes. Se recomienda también que se mantenga copias actualizadas y protegidas del PCN en los lugares remotos, como medida de contingencia para situaciones de desastre (Villamil, 2014).

2.1.3.4.3. Pruebas

El plan de continuidad del negocio debe probarse periódicamente para poder asegurar su actualización y eficiencia. Las pruebas también tienen como propósito asegurarse de que todos los miembros del equipo de recuperación y todo el personal de la organización tengan conocimiento del PCN.

Las pruebas deben indicar cómo y cuándo cada uno de sus componentes debe ser probada. Se recomienda probar los componentes individuales de los planes a menudo. Se pueden utilizar varias técnicas para asegurar la exactitud con la que operarán los planes en la vida real.

Entre ellos, se destacan:

- Pruebas de diferentes escenarios (discutiendo los acuerdos de recuperación, por ejemplo, usando interrupciones);
- Simulaciones (particularmente útiles para el entrenamiento del personal en sus puestos y funciones de gestión de la crisis);
- Pruebas de recuperación técnica (garantizando que los sistemas de información pueden ser efectivamente recuperados);
- Pruebas de recuperación en un sitio alternativo (ejecutando los procesos de negocio de forma paralela con las operaciones de recuperación fuera de la sede principal);
- Pruebas de las instalaciones de los proveedores de servicios (asegurando que los servicios y productos suministrados por fuentes externas cumplen con los requisitos contratados);
- Ensayo completo (probando la organización, el personal involucrado, los equipos, las instalaciones de procesamiento y los procesos para confirmar que pueden enfrentar y superar las interrupciones del entorno de operación) (Villamil, 2014).

2.1.3.4.4. Mantenimiento y reevaluación

El plan de continuidad del negocio debe someterse a mantenimiento en intervalos regulares de tiempo, y actualizarse para asegurar su efectividad. Además, existen varios factores, como cambios en el negocio o productos, que indicarían una necesidad de mejorar el PCN. Los cambios que se realicen deben ser documentados ya que servirán como fuente de datos para las próximas actualizaciones.

Los cambios relevantes que serán considerados en el mantenimiento del plan incluyen: la adquisición de nuevos equipos, nuevos sistemas, los cambios en las estrategias de negocio y los cambios en la legislación.

Se recomienda establecer responsabilidades para las revisiones regulares. La identificación de los cambios que han ocurrido en el negocio, pero aún no incluidas en el plan es una señal de que existe la necesidad de mantenimiento. El proceso de control de cambios debe garantizar que los planes actualizados serán distribuidos entre los sectores responsables (y para la sede remota, apropiadamente) (Villamil, 2014).

2.1.4. Gestión de la continuidad del negocio (GCN)

La gestión de la continuidad del negocio cuenta con dos elementos muy importantes que son la prevención y la recuperación, todo esto para garantizar la disponibilidad del servicio y la continuidad del negocio. Uno de sus principales propósitos claramente es proteger los procesos críticos que pueden ser desatados por algún riesgo o falla y en caso de que ocurriera una pérdida de información. Esta gestión nos proporcionaría los pasos para la recuperación de todos los activos críticos y así poder restablecer todos los servicios y poder brindan todas las funciones normales a la organización. Es muy importante el tiempo que tomaría esta recuperación de las funciones ya que debe ser el mínimo posible.

Lo anterior se lo puede confirmar con la siguiente definición; La GCN es el “proceso de gestión holística que identifica amenazas potenciales para una organización y los impactos que causarían en las operaciones si dichas amenazas llegan a realizarse. Además, proporciona un marco de trabajo para la construcción de resistencia con la capacidad de una respuesta efectiva que proteja los intereses de sus grupos de interés, reputación, marcas y actividades creadoras de valor” (ISO/IEC 27031, 2011).

2.1.4.1. Aspectos de seguridad de la información en la gestión de la continuidad del negocio

Como lo define la ISO 27002 el principal objetivo es contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres, y asegurar su recuperación oportuna.

Se debería implementar un proceso de gestión de la continuidad del negocio para minimizar el impacto y la recuperación por la pérdida de activos de información en la organización (la cual puede ser el resultado de, por ejemplo, desastres naturales, accidentes, fallas del equipo y acciones deliberadas) hasta un nivel aceptable mediante la combinación de controles preventivos y de recuperación. (ISO27002, 2007)

En el caso de que ocurra un desastre, perdidas del servicio o algún tipo de fallas en la seguridad de la información, las consecuencias de estas deben pasar por un proceso de análisis de impacto que tendría en la organización.

2.1.5. Plan de recuperación de desastres (PRD)

El plan de recuperación de desastres es un documento en el cual se especifica el proceso que la organización debe realizar para proteger toda la infraestructura tecnológica ya sean estos datos, hardware o software. Como lo define la ISO 27031; es un plan claramente definido y documentado que recupera las capacidades de las TIC cuando ocurre una interrupción. (ISO/IEC 27031, 2011)

Existe una gran confusión cuando se habla de plan de recuperación de desastres y plan de continuidad del negocio, aunque los dos contribuyen con la estabilidad de los sistemas críticos de las organizaciones, su principal diferencia está en su alcance.

La principal característica del PRD es que su alcance se limita a los procesos e infraestructura de las tecnologías de información, y este se encuentra dentro del PCN. En pocas palabras se podría decir que el PCN es un plan de planes, como por ejemplo plan de recuperación de desastres, plan de contingencia, etc.

2.1.6. Análisis del impacto al negocio (BIA)

El BIA, es otro elemento muy importante que permitirá conocer que afectación tendrá la empresa en caso de algún desastre, en esta fase se deben identificar tanto los recursos como los procesos críticos y después clasificarlos según el impacto que estos tengan en la organización. Para lograr todo esto se recomienda realizar entrevistas con los líderes y gerentes de cada área de la empresa ya que son ellos los que saben cuánto afectará en su sector específicamente en caso de algún fallo. Y así las autoridades puedan tomar decisiones con respecto a las inversiones que la empresa destinará para asegurar la continuidad del negocio.

Existen muchos autores que definen al BIA como el estudio de las consecuencias que tendría en el negocio en una parada de sus procesos vitales por un determinado tiempo: qué hay que recuperar, cuánto cuesta hacerlo, y cómo hay que recuperarlo. (Giménez Albacete, 2015)

A diferencia de una evaluación de riesgos, que se enfoca en cómo podría verse afectada una organización a través de la identificación, análisis y valoración de amenazas de seguridad con base en su impacto sobre los activos críticos y la probabilidad de ocurrencia. El BIA, es un proceso más especializado en la identificación de los tipos de impacto, orientado en conocer qué podría verse afectado y las consecuencias sobre los procesos de negocio (Mendoza, 2018).

2.1.6.1. Características del análisis de impacto

El *Business Impact Analysis* tiene dos objetivos principales; el primero de ellos consiste en proveer una base para identificar los procesos críticos para la operación de una organización. Una vez generado ese punto de partida, el segundo se refiere a la priorización de ese conjunto de procesos, siguiendo el criterio de cuanto mayor sea el impacto, mayor será la prioridad.

El BIA está directamente relacionado con aquellos procesos que poseen un tiempo crítico para su operación, porque si bien todos los procesos sujetos a un tiempo crítico son de misión crítica, no todos los procesos de misión crítica están relacionados con un tiempo crítico para su ejecución.

De manera adicional, el desarrollo de este análisis permite estimar los recursos necesarios para los procesos identificados, de manera especial para aquellos que representan mayor sensibilidad con relación al tiempo y el impacto.

Para ello se define el tiempo objetivo de recuperación (RTO por sus siglas en inglés), que es el período permitido para la recuperación de una función o recurso de negocio a un nivel aceptable luego de una interrupción o desastre. Asimismo, el punto objetivo de recuperación (RPO por sus siglas en inglés) que describe la antigüedad máxima de los datos para su restauración, es decir, la tolerancia que el negocio puede permitir para operar con datos de respaldo, por lo que el RPO estará en función de las actividades primordiales de una organización (Mendoza, 2018).

En la figura 2, se puede apreciar de mejor manera cómo funcionan estos dos conceptos.

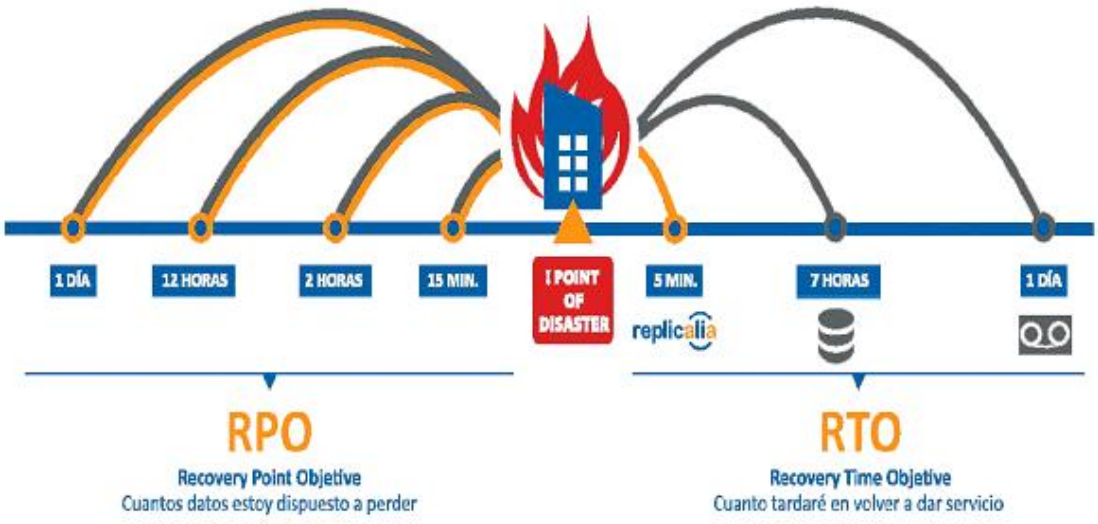

Figura 2. RTO y RPO.

Tomado de (Fluidsignal Group, s.f.)

2.1.7. Operador de Red Móvil

Un operador de red móvil, también conocido como proveedor de servicios de comunicaciones inalámbricas es el que tiene y controla todos los elementos que sean necesarios para entregar servicios a sus suscriptores. Estos elementos pueden ser: infraestructura de red inalámbrica, asignación de espectro radioeléctrico, infraestructura de *backhaul*, facturación, atención al cliente, etc. (Machi, 2018).

Un operador móvil debe contar con una licencia para el uso del espectro radioeléctrico, emitida por una entidad reguladora o gubernamental. En Ecuador, quien otorga los títulos habilitantes es la Agencia de Regulación y Control de las Telecomunicaciones más conocida como ARCOTEL.

Los operadores de telefonía móvil que operan en el Ecuador son:

- Conecel S.A (Claro).
- Otecel S.A (Movistar).
- Corporación Nacional de Telecomunicaciones (CNT).

2.2. MARCO LEGAL

2.2.1. Normas y estándares internacionales

2.2.1.1. ISO 22301: Sistema de Gestión de Continuidad de Negocio

ISO 22301 es una norma internacional de gestión de continuidad de negocio. Esta ha sido creada en respuesta a la fuerte demanda internacional que obtuvo la norma británica original, BS 25999-2 y otras normas.

ISO 22301 identifica los fundamentos de un Sistema de Gestión de la Continuidad de negocio, estableciendo el proceso, los principios y la terminología de gestión de continuidad de negocio. Además, proporciona una base de entendimiento, desarrollo e implantación de continuidad de negocio dentro de la organización. Se usa para asegurar a las partes interesadas clave que su empresa está totalmente preparada y que puede cumplir con los requisitos internos, regulatorios y del cliente.

La norma proporciona a las organizaciones un marco que asegura que ellos pueden continuar trabajando durante las circunstancias más difíciles e inesperadas, siempre protegiendo a sus empleados, manteniendo su reputación y proporcionando la capacidad de continuar trabajando y comercializando. (ISO 22301, 2012)

La norma ISO 22301 puede ser aplicada a todo tipo y tamaño de organizaciones que quieran:

- Establecer, implantar, mantener y mejorar un SGCN.
- Demostrar conformidad con la política establecida de la continuidad de negocio de la organización.
- Dar a las partes interesadas confianza en su conformidad y compromiso con las buenas prácticas reconocidas internacionalmente.

2.2.1.2. ISO 27031: Gestión de la Tecnología de Información y Comunicación y obtención de Continuidad de Negocio

Esta Norma Internacional describe los conceptos y principios de información y comunicación preparación tecnológica (TIC) para la continuidad del negocio, y proporciona un marco de métodos y procesos para identificar y especificar todos los aspectos (como los criterios de rendimiento, diseño e implementación) para mejorar una preparación de TIC de la organización para garantizar la continuidad del negocio.

Se aplica a cualquier organización (privada, gubernamentales, y no gubernamentales, independientemente de su tamaño) desarrollando su disponibilidad de TIC para los negocios programa de continuidad (IRBC, por sus siglas en inglés) y exige que sus servicios / infraestructuras de TIC estén listos para respaldar el negocio operaciones en caso de incidentes e incidentes emergentes, e interrupciones relacionadas, que podrían afectar la continuidad (incluida la seguridad) de funciones comerciales críticas.

También permite a una organización medir el rendimiento parámetros que se correlacionan con su IRBC de una manera consistente y reconocida.

El alcance de esta norma internacional abarca todos los eventos e incidentes (incluidos los relacionados con la seguridad) que podría tener un impacto en la infraestructura y los sistemas de TIC. Incluye y extiende las prácticas de gestión de la información y gestión de incidentes de seguridad. Además, la planificación y servicios de preparación de TIC. (ISO/IEC 27031, 2011)

2.2.1.3. ISO 27001: Tecnología de la información - Técnicas de seguridad - Gestión de la seguridad de la información sistemas – Requisitos

ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013.

La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2. Puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande.

Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001. (Kosutic, 2018)

2.2.1.4. ISO 27005: Tecnología de la información - Técnicas de seguridad - Gestión del riesgo de seguridad de la información

ISO 27005 es el estándar internacional que se ocupa de la gestión de riesgos de seguridad de información. La norma suministra las directrices para la gestión de riesgos de seguridad de la información en una empresa, apoyando particularmente los requisitos del sistema de gestión de seguridad de la información definidos en ISO 27001.

ISO-27005 es aplicable a todo tipo de organizaciones que tengan la intención de gestionar los riesgos que puedan complicar la seguridad de la información de su organización. No recomienda una metodología concreta, dependerá de una serie

de factores, como el alcance real del Sistema de Gestión de Seguridad de la Información (SGSI), o el sector comercial de la propia industria. (SGCI, 2018)

2.2.2. Normas y Estándares Nacionales

En el Ecuador no existe ninguna norma o estándar que regule los planes de continuidad de negocio. Lo que existe es una norma para regular la presentación de los planes de contingencia ya que, en la Ley Orgánica de Telecomunicaciones, publicada en el Tercer Suplemento del Registro Oficial No. 439 de 18 de febrero de 2015, en el artículo 24, numeral 24 establece la obligación para que los prestadores de servicios del régimen general de telecomunicaciones el contar con planes de contingencia, para ejecutarlos en casos de desastres naturales o conmoción interna para garantizar la continuidad del servicio de acuerdo con las regulaciones respectivas.

2.2.2.1. Norma que regula la presentación de los planes de contingencia para la operación de las redes públicas de telecomunicaciones por parte de los prestadores de servicios del régimen general de telecomunicaciones

El 21 de diciembre del 2016 se publicó el informe de presentación de proyecto de regulación N.º CRDS-IT-2016-007. Esta norma tiene por objeto regular la presentación de planes de contingencia, por parte de los prestadores de servicios del régimen general de telecomunicaciones, para ejecutarlos en casos de desastres naturales o conmoción interna y garantizar la continuidad del servicio.

Esta norma fue aprobada mediante la Resolución No. ARCOTEL-2017-0858 el 13 de septiembre de 2017, por lo que los formatos establecidos ya se encuentran en la página oficial de la Agencia de Regulación y Control de las Telecomunicaciones como archivos descargables (ARCOTEL, 2018).

3. ANÁLISIS DE RIESGOS A NIVEL PAÍS POR ZONAS

3.1. Análisis de la criticidad de los riesgos a nivel país

En este capítulo se realizará un análisis de los desastres naturales que representan un riesgo para las operadoras móviles en el país, para un mejor manejo de la información se lo dividirá por cantones.

“El Ecuador se encuentra situado en una de las zonas de más alta complejidad tectónica del mundo, en el punto de encuentro de las placas de Nazca y Sudamérica. Es parte del denominado “cinturón de fuego del Pacífico”, con una larga serie de volcanes en su mayoría activos que provoca una permanente actividad sísmica y volcánica y determinan una elevada vulnerabilidad” (FAO, 2008)

“El Ecuador está ubicado dentro del cinturón de bajas presiones que rodea el globo terrestre, en la zona de convergencia intertropical, un área sujeta a amenazas hidrometeorológicas como inundaciones, sequías, heladas o efectos del fenómeno El Niño” (FAO, 2008).

Para poder realizar el análisis de vulnerabilidades y riesgos lo primero que se debe saber, son los fenómenos naturales o peligros a los cuales se pueden enfrentar.

3.1.1. Identificación de amenazas naturales en el Ecuador

Un desastre natural se puede definir como cualquier evento catastrófico causado por fenómenos naturales o procesos naturales de la tierra, como terremotos, inundaciones, deslizamientos de tierra, etc. (Roble, s.f.).

Se los pueden clasificar en:

- **Hidrológicos**: “son todos aquello que se originan en el agua. Ocurren como consecuencia de la acción de los mares y océanos estos son el tsunami o maremotos, inundaciones u oleajes tempestuosos” (Roble, s.f.).
- **Meteorológicos**: “son aquellos que pueden darse en muchas variaciones y todas ellas relacionadas con el clima. Estos pueden predecirse con cierta anticipación gracias a tecnologías que definen el comportamiento del clima y analizan la posibilidad de que lleguen a afectar un lugar determinado. Por ejemplos los tifones, frentes fríos y cálidos, el niño y la niña, tornados, tormentas tropicales, huracanes, nevadas, granizo, sequia e inundaciones por lluvia” (Roble, s.f.).
- **Geofísicos**: “son todos aquellos que se forman o surgen de la superficie terrestre. Dentro de este grupo se puede encontrar las avalanchas, derrumbes, tormentas solares, terremotos, erupciones volcánicas, incendios y hundimientos de la tierra, entre otros” (Roble, s.f.).

Ahora bien, una vez identificados los diferentes fenómenos naturales que pueden convertirse en desastres, se debe evaluar la amenaza que representa. Se realizará una evaluación sobre la ubicación, severidad y posibilidad de que ocurra un evento natural dentro de un periodo de tiempo determinado (OEA, 1991).

En Ecuador, la secretaria de Gestión de riesgos señala las siguientes amenazas naturales a nivel país:

3.1.1.1. Tsunamis

“Es un término de origen japonés: Tsu (puerto) nami (ola). Tsunami quiere decir “grandes olas en el puerto”. Un tsunami no causa daños en alta mar; pero es destructivo en las playas” (Secretaría de Gestión de Riesgos, s.f.).

Para que se produzca este fenómeno, lo que ocurre es que en la plataforma submarina ubicada en el fondo del océano pueden ocurrir sismos, erupciones

volcánicas o derrumbes, que generan una cantidad enorme de energía la cual se esparcida en todas direcciones. Esta energía da como resultado la formación de varias olas que van aumentando en altura, volumen y velocidad a medida que se acercan a la playa. Asimismo, cuando ocurre un terremoto de grado mayor o igual que 7 en la escala de Richter podría generar un tsunami.

Aquí en el Ecuador es muy probable que ocurra este evento, ya que la mayoría de estos fenómenos han ocurrido en el océano Pacifico a lo largo de la historia mundial. Por lo tanto, toda la zona costera de Ecuador es una zona de riesgos para este tipo de amenaza (INAMHI, s.f.).

3.1.1.2. Sismos

Se denominan terremotos, movimientos sísmicos o sismos a los movimientos bruscos y repentinos del suelo, de intensidad sumamente variable, que oscilan entre las sacudidas leves que solo registran los aparatos más sensibles, y las fuertes que devastan las ciudades (IGEPN, s.f.).

3.1.1.3. Inundaciones

Se pueden distinguir dos tipos de inundaciones, las originadas por desbordamiento de ríos causadas por la excesiva escorrentía como consecuencia de fuertes precipitaciones, y la segunda son inundaciones originadas en el mar, o inundaciones costeras, causadas por olas ciclónicas exacerbadas por la escorrentía de las cuencas superiores. Los tsunamis son un tipo especial de inundación costera (OEA, 1991).

3.1.1.4. Incendios Forestales

Se llama incendio forestal al fuego que se propaga sin control, especialmente en zonas rurales, afectando la vegetación como árboles, matorrales, pastos y cultivos (Secretaría de Gestión de Riesgos, s.f.).

3.1.1.5. Erupciones Volcánicas

Es la expulsión de roca fundida a temperaturas muy altas (MAGMA) desde el interior de la tierra hacia la superficie. Es un fenómeno que se puede predecir.

El Ecuador está ubicado en una región con volcanes activos y, por lo mismo, es un país de alto riesgo a las erupciones (Secretaría de Gestión de Riesgos, s.f.).

3.1.1.6. Deslaves o deslizamientos

Se podría definir como la caída de rocas o tierra desde una ladera, en forma lenta o rápida, que se produce en épocas de lluvia o a causa de un sismo. Dependiendo de la magnitud, destruye todo lo que se encuentra a su paso.

En la costa, sierra y en la región oriental ocurren deslizamientos porque Ecuador es un país montañoso. La mayoría se presenta durante las estaciones lluviosas. Cuando el suelo recibe una gran cantidad de agua, la tierra se ablanda y se desprende formando flujos de lodo, que se precipitan pendiente a bajo (Secretaría de Gestión de Riesgos, s.f.).

Algunas personas aportan para que ocurran deslizamientos, al construir con materiales muy pesados en terrenos muy débiles, o también cuando ejecutan excavaciones que desmoronan las laderas. Otra de las causas es la deforestación, ya que el suelo queda demasiado desprotegido (Secretaría de Gestión de Riesgos, s.f.).

3.1.1.7. Sequia

Es un fenómeno natural de desarrollo lento, originado por la ausencia total o parcial de lluvias.

La sequía es uno de los peores enemigos de la humanidad, porque afecta gravemente y a los seres vivos, por la falta de agua (Secretaría de Gestión de Riesgos, s.f.).

3.1.1.8. Aguajes y oleajes

Se conoce como aguaje, a las mareas que ocurren cada 14 días, durante las fases de luna nueva y luna llena y que se caracterizan porque las pleamares son de mayor amplitud, y las bajamares son menores que el promedio, ocasionando incremento en el nivel del mar y mayores corrientes.

Por otro lado, los oleajes son eventos que se presentan por la acción de vientos lejanos o locales sobre la superficie del mar, causando olas de gran energía que se desplazan hacia la zona costera provocando destrucción por la energía que acarrean.

Estos oleajes fuertes pueden producir las denominadas corrientes de resaca que son corrientes que se dirigen mar adentro, con velocidades que pueden superar a las del mejor nadador (INAMHI, s.f.).

3.1.1.9. Cambios Climáticos

El clima del planeta Tierra se está alterando significativamente, como resultado del aumento de concentraciones de gases invernadero.

Las variaciones climáticas han existido en el pasado y existirán siempre a consecuencia de diferentes fenómenos naturales. Sin embargo, durante las últimas décadas se han producido variaciones anormales causadas por la actividad humana, que alteran la composición global atmosférica (Secretaría de Gestión de Riesgos, s.f.).

3.1.2. Análisis de amenazas por cantón en el Ecuador

El presente análisis estará basado en la información recopilada por (D'Ercole & Trujillo, 2003) en su libro. Para lo cual se han escogido ocho tipos de amenazas que son las más recurrentes en el Ecuador como las amenazas geofísicas (sismos, terremotos, erupciones volcánicas) y amenazas hidrológicas y meteorológicas (inundaciones, deslizamientos, sequias, aguajes y cambios climáticos).

Desde la figura 3 hasta la figura 10, se mostrarán mapas por cada tipo de amenaza mostrando el nivel de amenaza diferenciado por cantones en el país:

3.1.2.1. Sismos

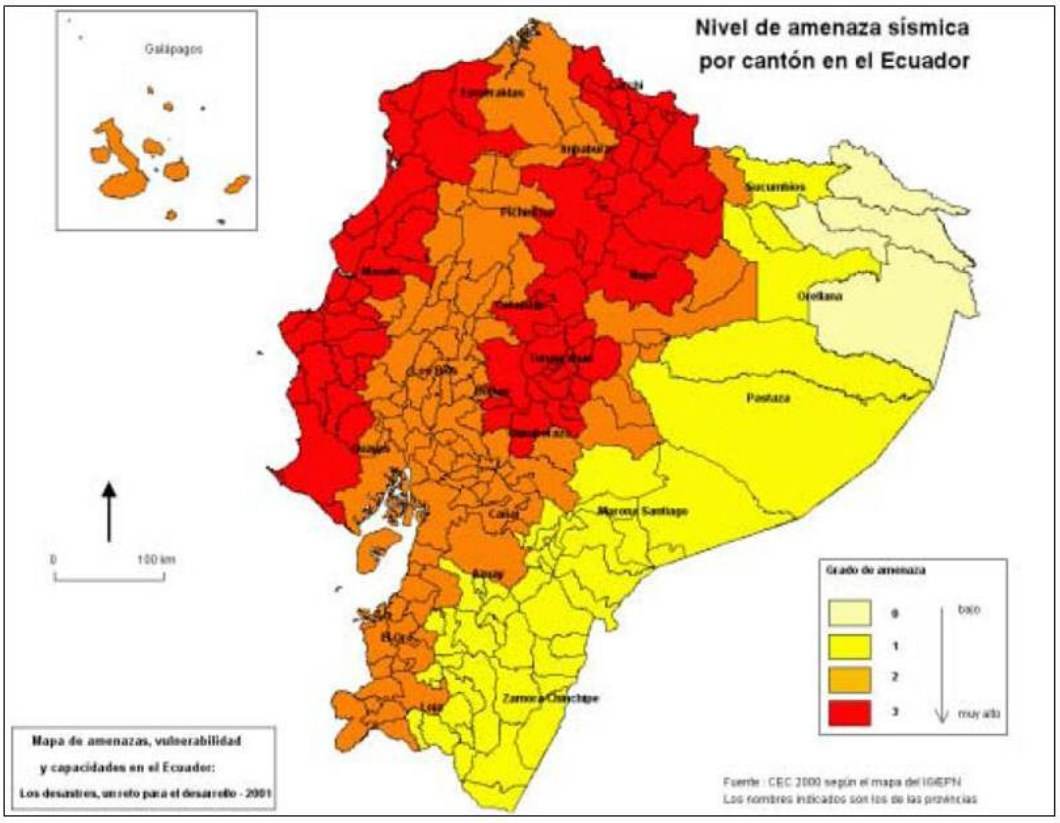

Figura 3. Mapa de nivel de amenaza sísmica por cantón en el Ecuador. Tomado de (OPS, s.f.)

Como se puede observar en la figura 3, los cantones con mayor grado de amenaza sísmica se encuentran en la región Costa y Sierra del país.

3.1.2.2. Tsunamis

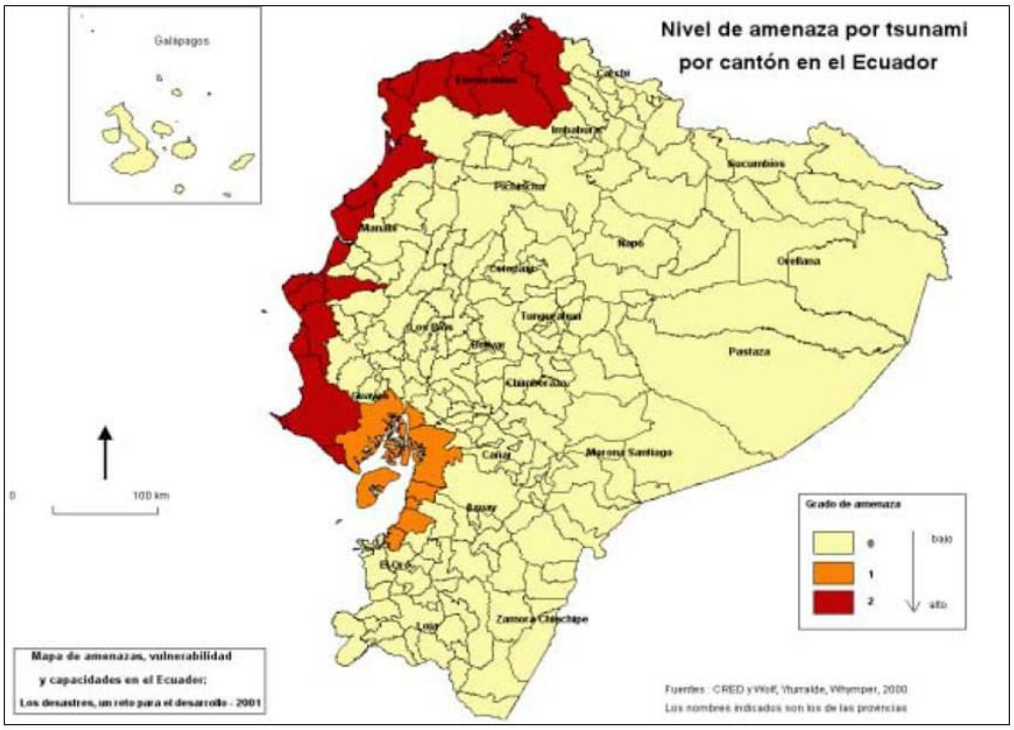

Figura 4. Mapa de nivel de amenaza por tsunami por cantón en el Ecuador. Tomado de (OPS, s.f.)

Como se puede observar en la figura 4, la mayoría de los cantones con alto grado de amenaza de tsunami, se encuentran en todo el borde costero del Ecuador que delimita el país con el océano pacifico.

3.1.2.3. Erupciones Volcánicas

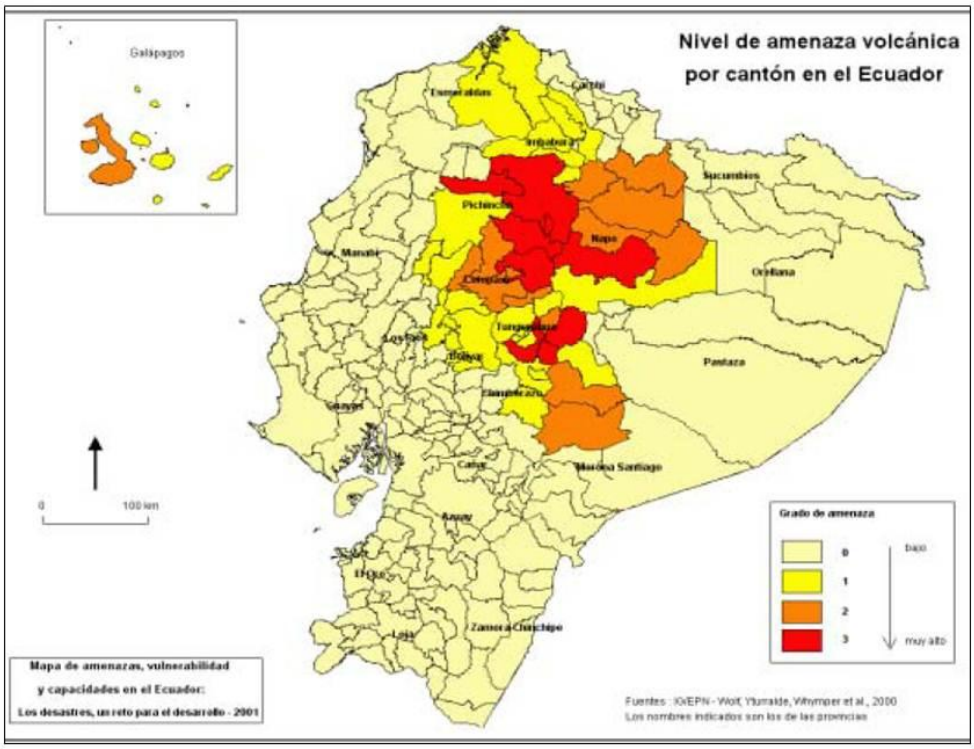

Figura 5. Mapa de nivel de amenaza volcánica por cantón en el Ecuador. Tomado de (OPS, s.f.)

La figura 5 nos muestra que el mayor grado de amenaza volcánica se concentra en el centro norte del país, ya que la mayoría de los volcanes activos del Ecuador como el Cotopaxi, Tungurahua y Reventador se encuentran rodeando esta zona.

3.1.2.4. Inundaciones

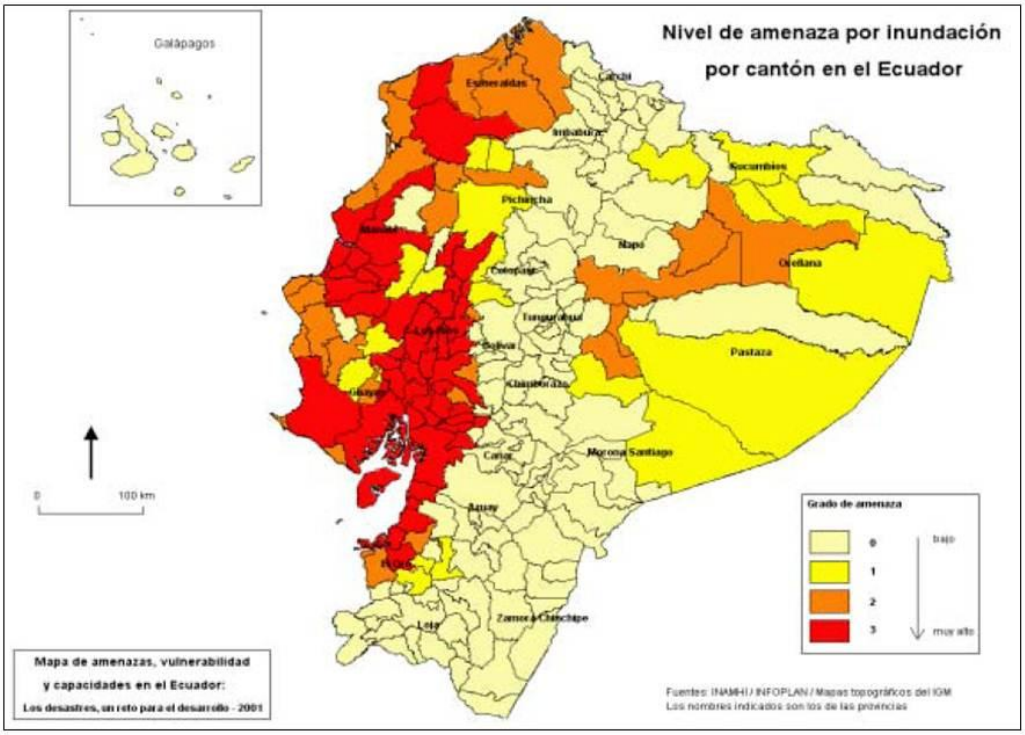

Figura 6. Mapa de nivel de amenaza por inundación por cantón en el Ecuador. Tomado de (OPS, s.f.)

La mayoría de los cantones con mayor nivel de amenaza por inundación se encuentran en la región costa del país, sobre todo en las provincias del Guayas, Manabí, Santa Elena y Los Ríos tal como lo muestra la figura 6.

3.1.2.5. Incendios Forestales

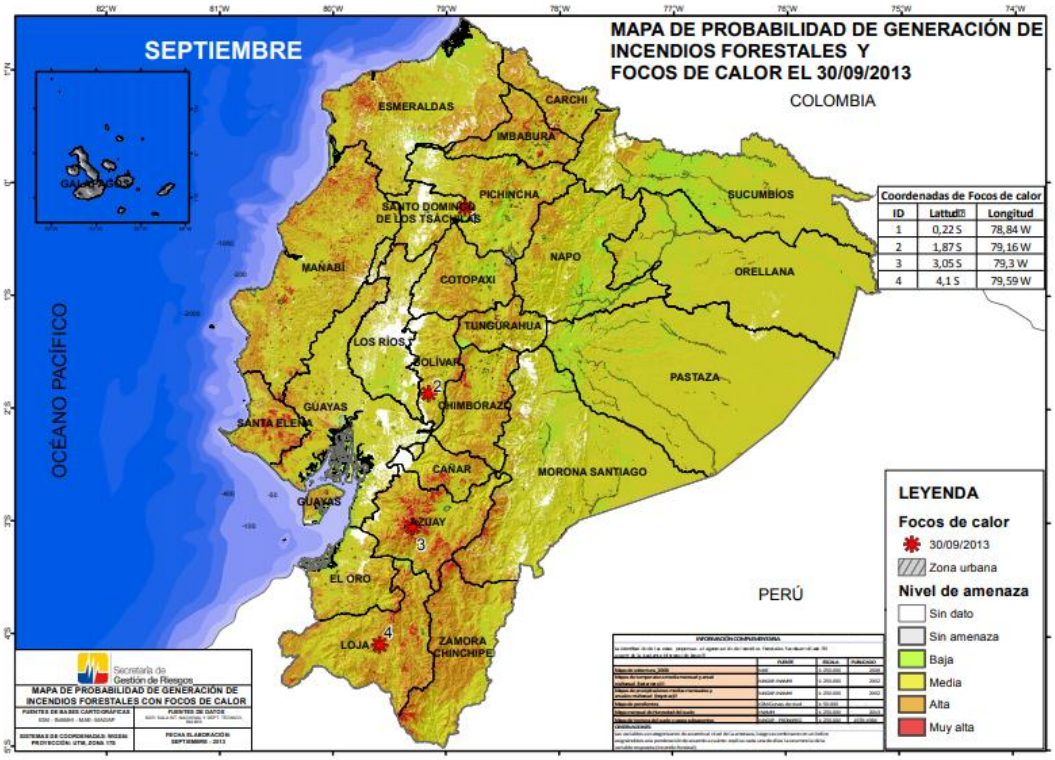

Figura 7. Mapa de probabilidad de generación de incendios forestales y focos de calor.

Tomado de (Secretaría de Gestión de Riesgos, s.f.)

En la figura 7 se puede apreciar que en el Ecuador existen focos de calor en las provincias de Loja, Azuay, bolívar y Santo Domingo de los Tsáchilas, que hacen que sean zonas más vulnerables para incendios forestales. Este tipo de amenaza no se lo puede predecir con exactitud ya que varía mucho por cambios climáticos o épocas del año.

3.1.2.6. Deslaves o deslizamientos

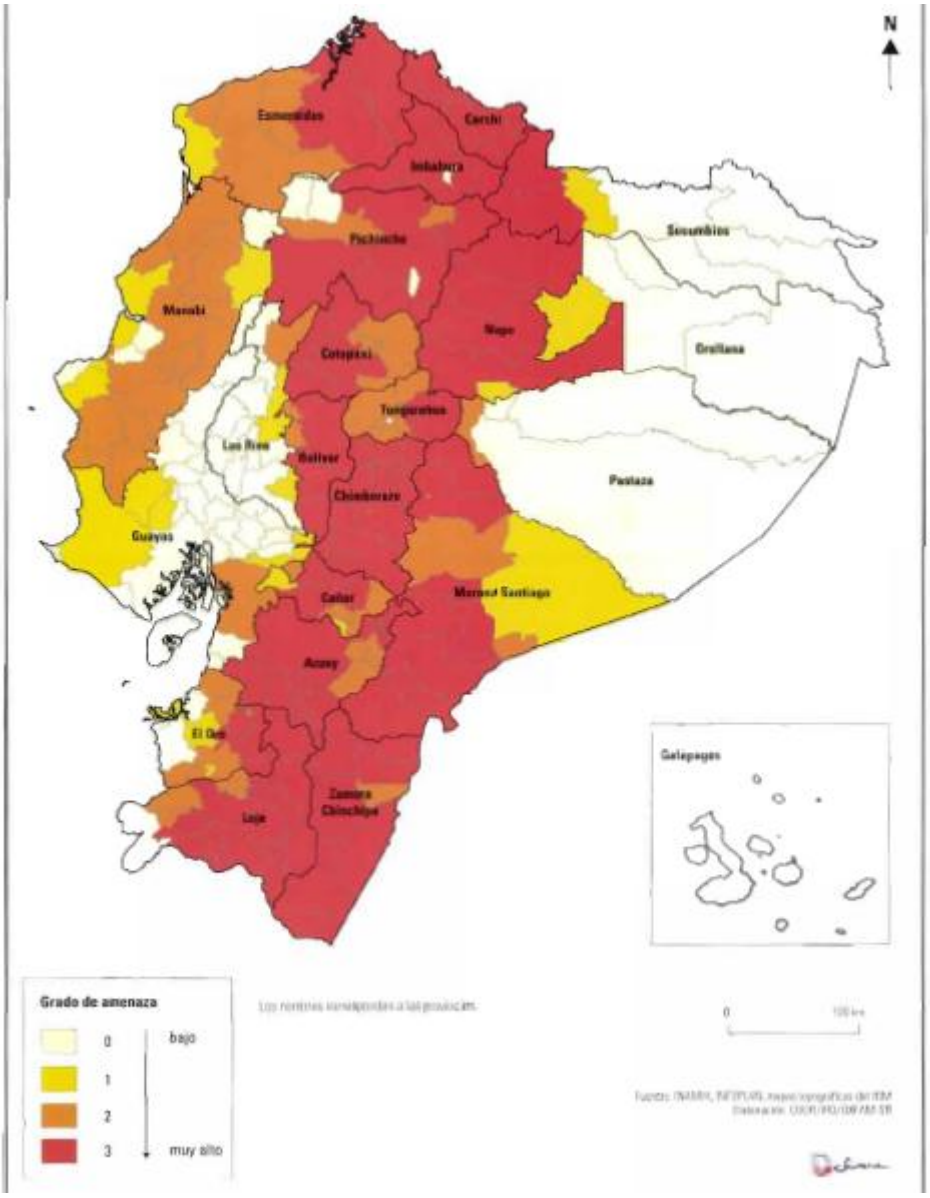

Figura 8. Mapa de nivel de amenaza de deslizamientos por cantón en el Ecuador. Tomado de (D'Ercole & Trujillo, 2003)

Tal como lo muestra la figura 8, la mayor cantidad de los cantones con grado de amenaza muy alta de deslizamientos o deslaves, se encuentran a lo largo de toda la región Sierra del país con otras pequeñas partes de la amazonia y costa del país.

3.1.2.7. Sequía

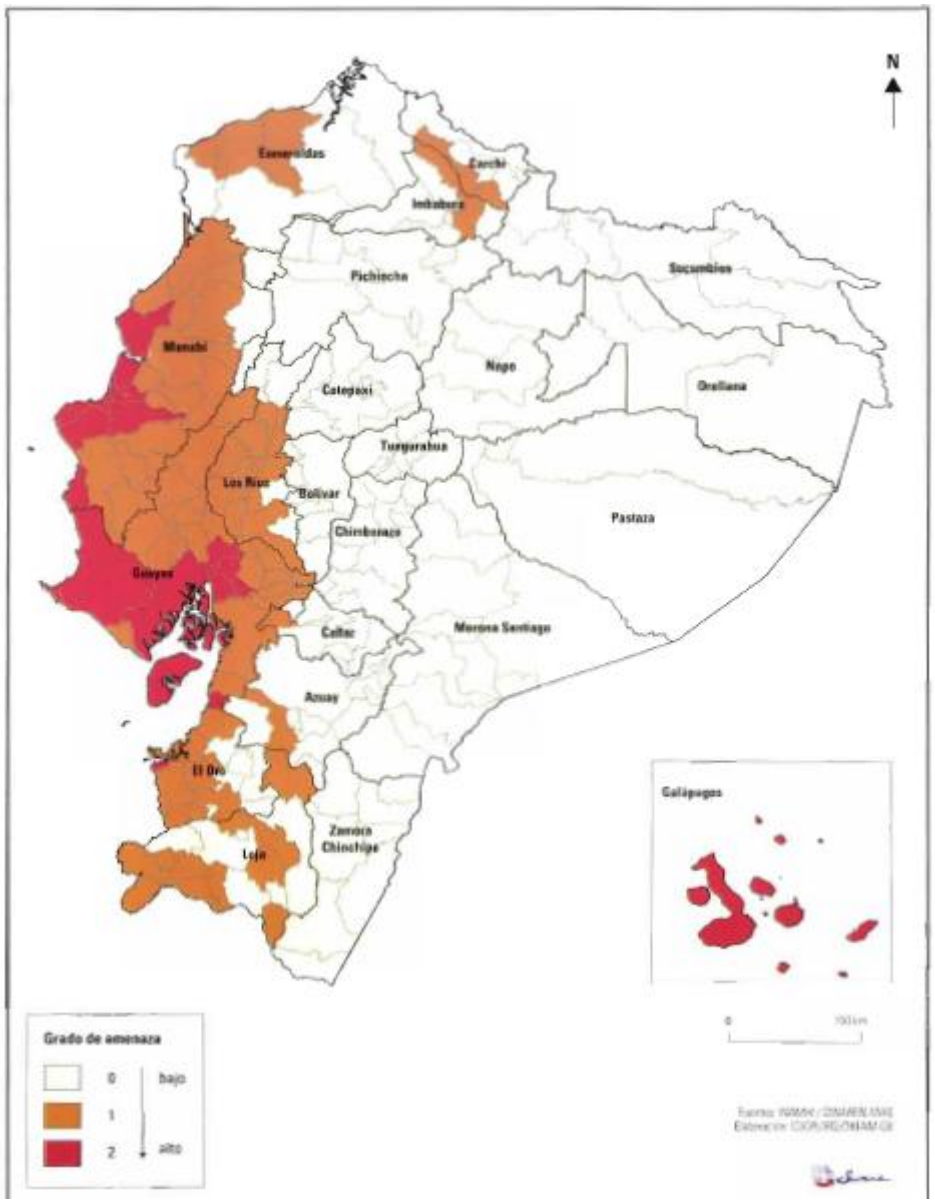

Figura 9. Mapa de nivel de amenaza de sequía por cantón en el Ecuador. Tomado de (D'Ercole & Trujillo, 2003)

Se puede notar claramente en la figura 9 que el nivel de amenaza por sequía está concentrado mayor mente en la provincia del Guayas y en la región insular (Galápagos) y en menor proporción en la provincia de Manabí.

3.1.2.8. Cambios Climáticos

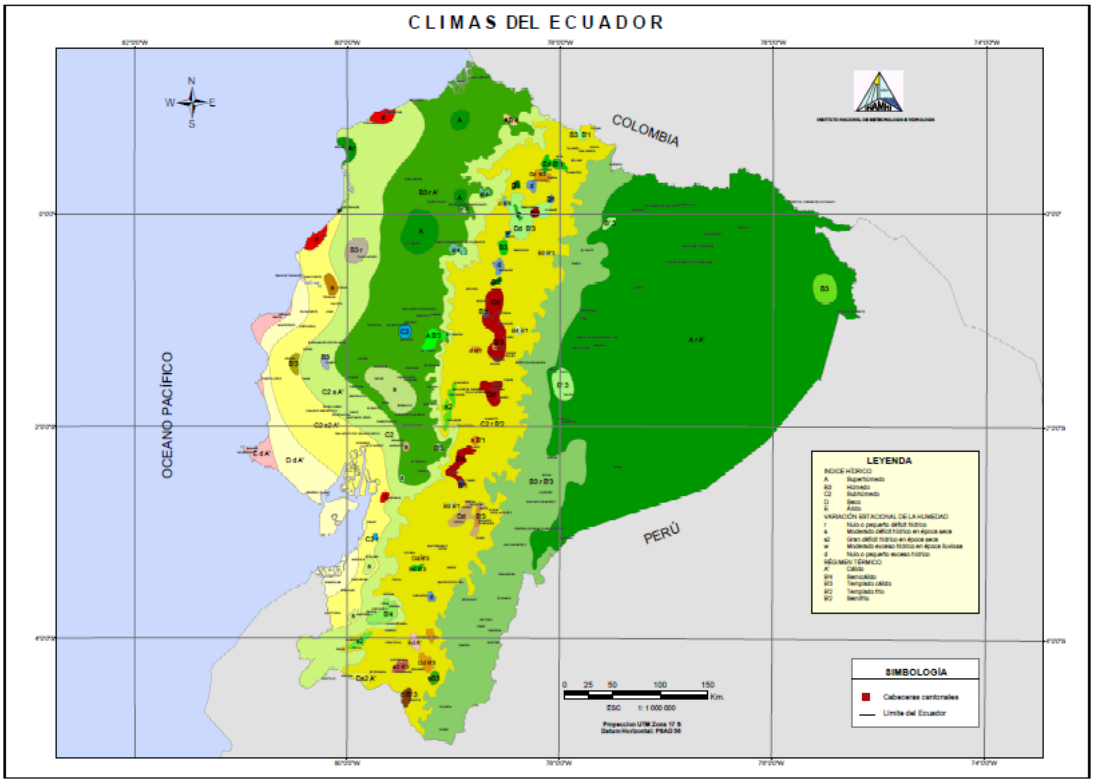

Figura 10. Mapa de los diferentes climas del Ecuador.

Tomado de (INAMHI, s.f.)

En la figura 10 lo que se puede observar son los diferentes climas que tiene el Ecuador. Se podría decir que el país tiene un clima tropical que varía dependiendo la altitud y las regiones. Esto de sebe a que Ecuador está ubicado en la línea Ecuatorial.

3.1.3. Análisis del riesgo por amenaza de origen natural

En esta sección se propone un análisis del riesgo según el tipo de amenaza de origen natural. Se presentarán mapas que nos proporcionarán una visión global de los sectores de alto riesgo y además se puede conocer el grado de amenaza para los cantones.

3.1.3.1. Riesgo por amenaza sísmica

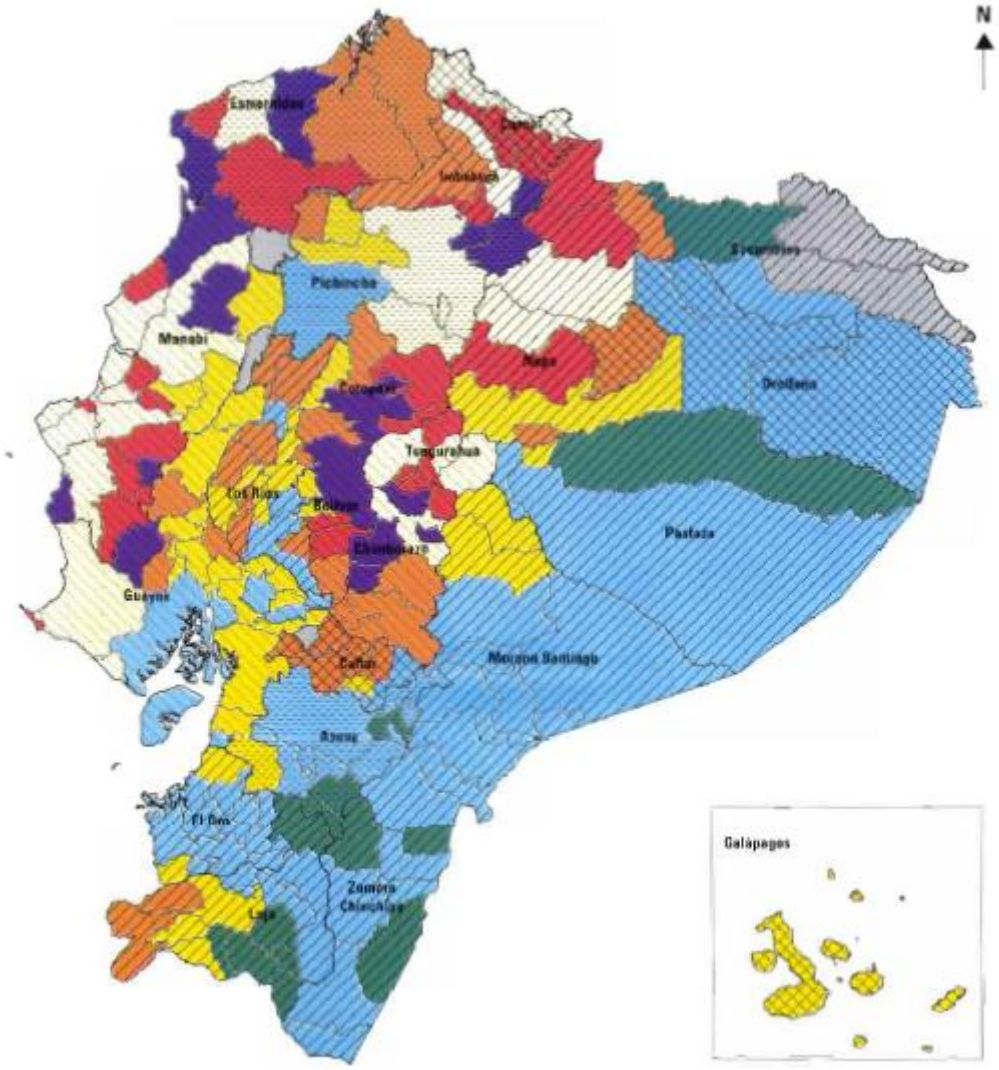

Figura 11. Riesgo por amenaza sísmica por cantón en el Ecuador. Tomado de (D'Ercole & Trujillo, 2003)

Tabla 1.

Tabla de análisis del riesgo sísmico.

		Grado de vulnerabilidad		
		Muy alto a Alto	Relativamente alto	Relativamente bajo a Bajo
Grado de	Muy alto a Alto	**Alto riesgo**		

	Relativamente alto		**Medio riesgo**	
	Relativamente bajo a Bajo			**Bajo riesgo**

Adaptado de (D'Ercole & Trujillo, 2003)

De manera general se puede observar en la figura 11 que existen dos zonas en donde el riesgo por sismos es mayor. La primera es la parte norte y noroccidente del Ecuador y la segunda se encuentra en la región cierra en la parte central.

3.1.3.2. Riesgo por amenaza de tsunami

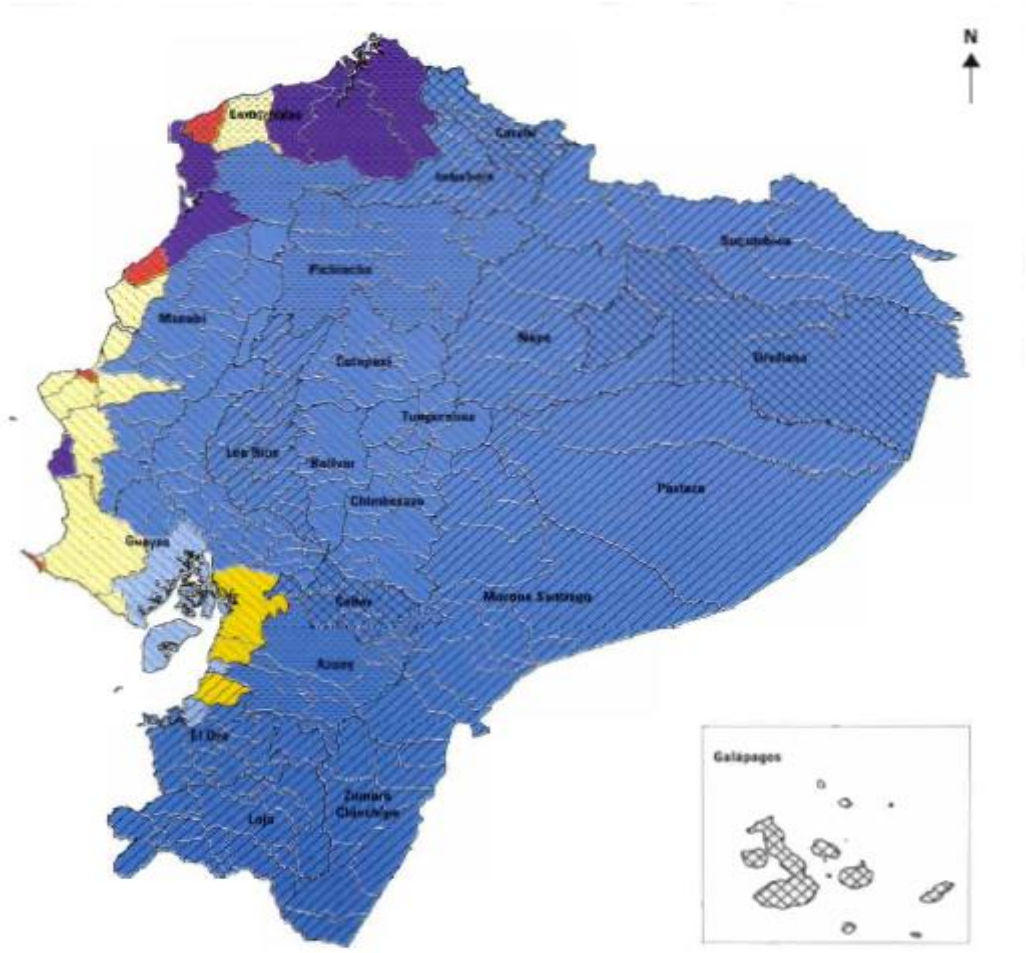

Figura 12. Riesgo por amenaza por tsunami por cantón en el Ecuador.

Tomado de (D'Ercole & Trujillo, 2003)

Tabla 2.

Tabla de análisis de riesgo tsunami.

		Grado de vulnerabilidad		
		Muy alto a Alto	Relativamente alto	Relativamente bajo a Bajo
Grado de amenaza	Muy alto a Alto	**Alto riesgo**		
	Relativamente alto		**Medio riesgo**	
	Relativamente bajo a Bajo			**Bajo riesgo**

Adaptado de (D'Ercole & Trujillo, 2003)

En la figura 12, se muestra de manera muy clara que los cantones en donde existe mayor riesgo de tsunamis son los que están ubicados por la línea costera, mayormente en la zona norte en la provincia de Esmeraldas, ya que son los más expuestos a este tipo de amenazas.

3.1.3.3. Riesgo por amenaza volcánica

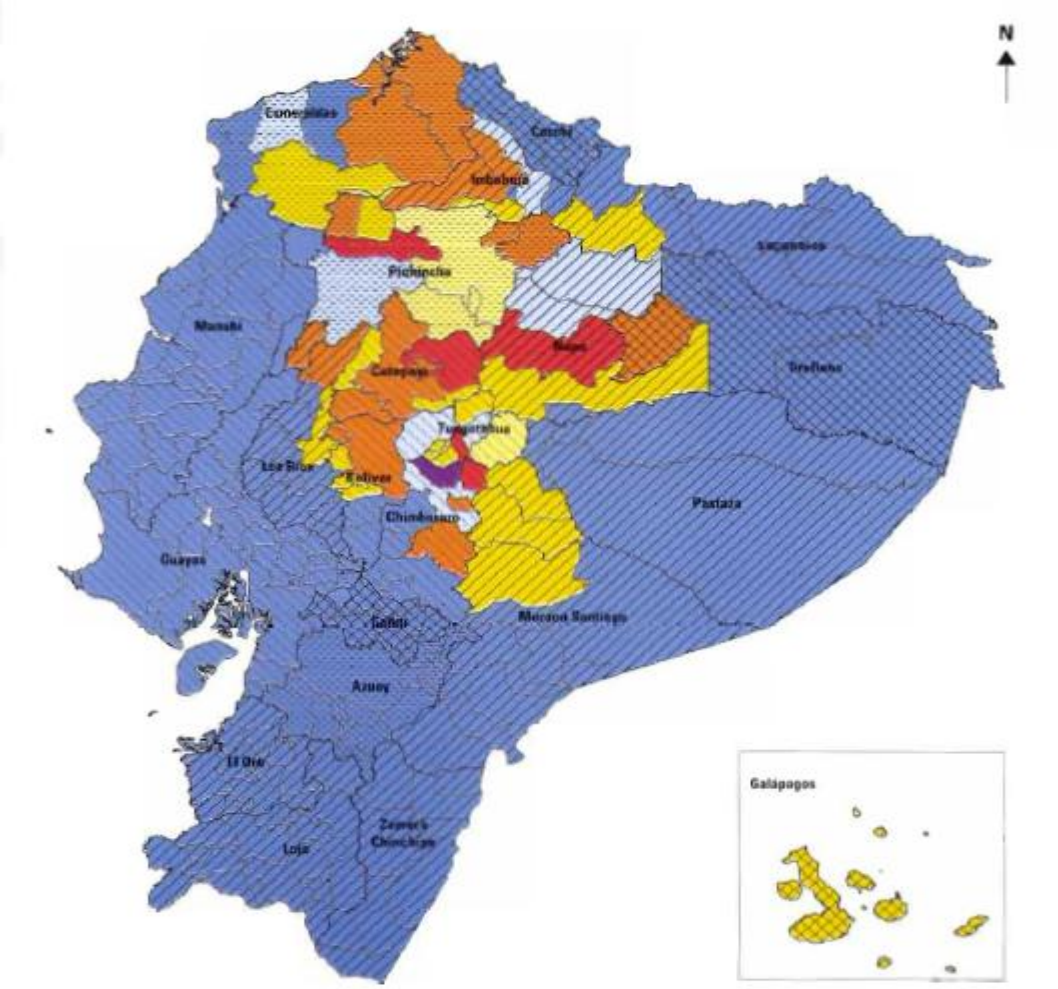

Figura 13. Riesgo por amenaza volcánica por cantón en el Ecuador. Tomado de (D'Ercole & Trujillo, 2003)

Tabla 3.

Tabla de análisis de riesgo amenaza volcánica

		Grado de vulnerabilidad		
		Muy alto a Alto	Relativamente alto	Relativamente bajo a Bajo
Grado de amenaza	Muy alto a Alto	**Alto riesgo**		
	Relativamente alto		**Medio riesgo**	
	Relativamente bajo a Bajo			**Bajo riesgo**

Adaptado de (D'Ercole & Trujillo, 2003)

Tal y como muestra la figura 13, la zona con mayor riesgo por amenaza volcánica está concentrado en la región Sierra central y centro norte. Como ya se mencionó anteriormente, esto se debe a la ubicación de los volcanes activos del Ecuador.

3.1.3.4. Riesgo por amenaza de inundaciones

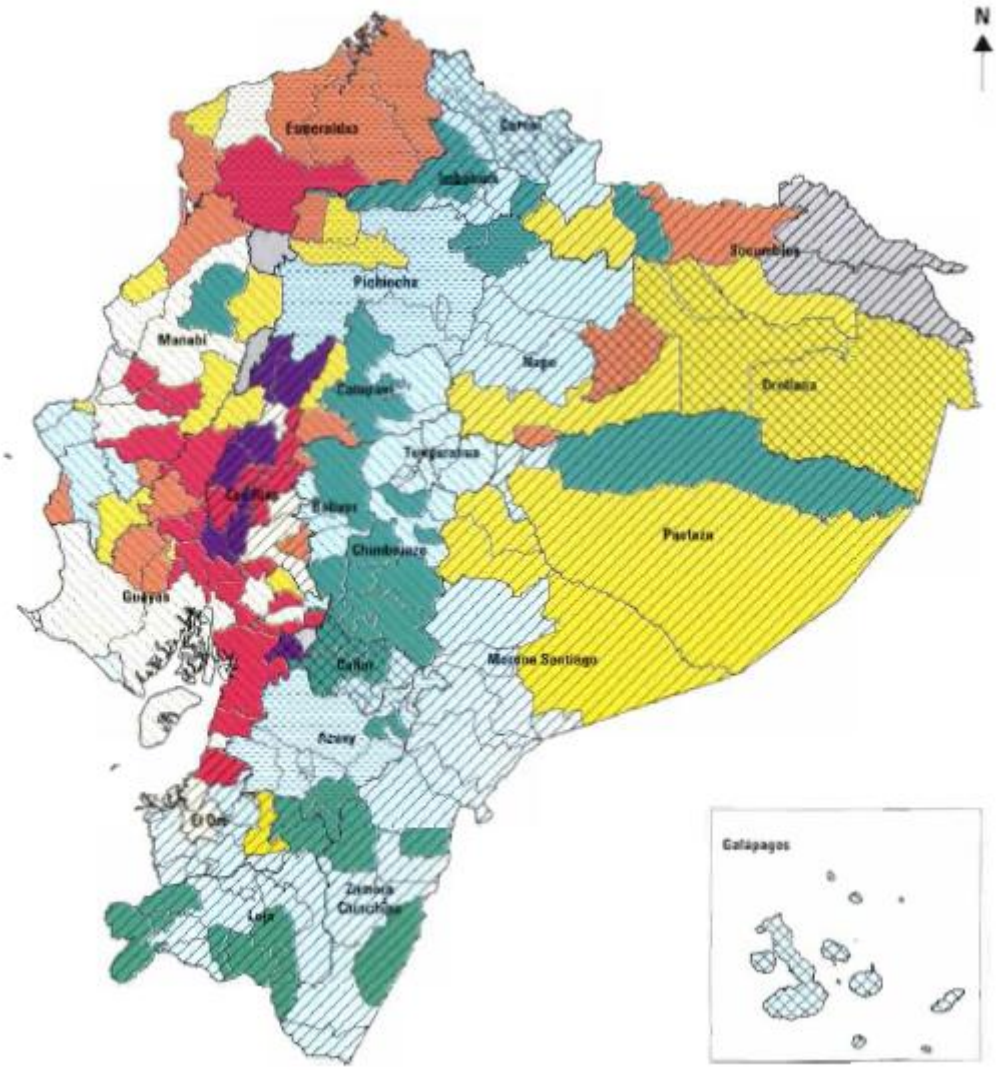

Figura 14. Riesgo de inundación por cantón en el Ecuador.

Tomado de (D'Ercole & Trujillo, 2003)

Tabla 4.

Tabla de análisis de riesgo inundación.

Grado de vulnerabilidad

		Muy alto a Alto	Relativamente alto	Relativamente bajo a Bajo
Grado de amenaza	Muy alto a Alto	**Alto riesgo**		
	Relativamente alto		**Medio riesgo**	
	Relativamente bajo a Bajo			**Bajo riesgo**

Adaptado de (D'Ercole & Trujillo, 2003)

Se puede observar en la figura 14 que los cantones con más riesgo por inundaciones se encuentran en la región Costa y Oriente. En la Costa esto se debe a su cercanía con el rio Guayas y en la región Amazónica se debe al fenómeno de El Niño lo que ocasiona el desbordamiento de varios ríos (D'Ercole & Trujillo, 2003).

3.1.3.5. Riesgo por amenaza de deslaves o deslizamientos

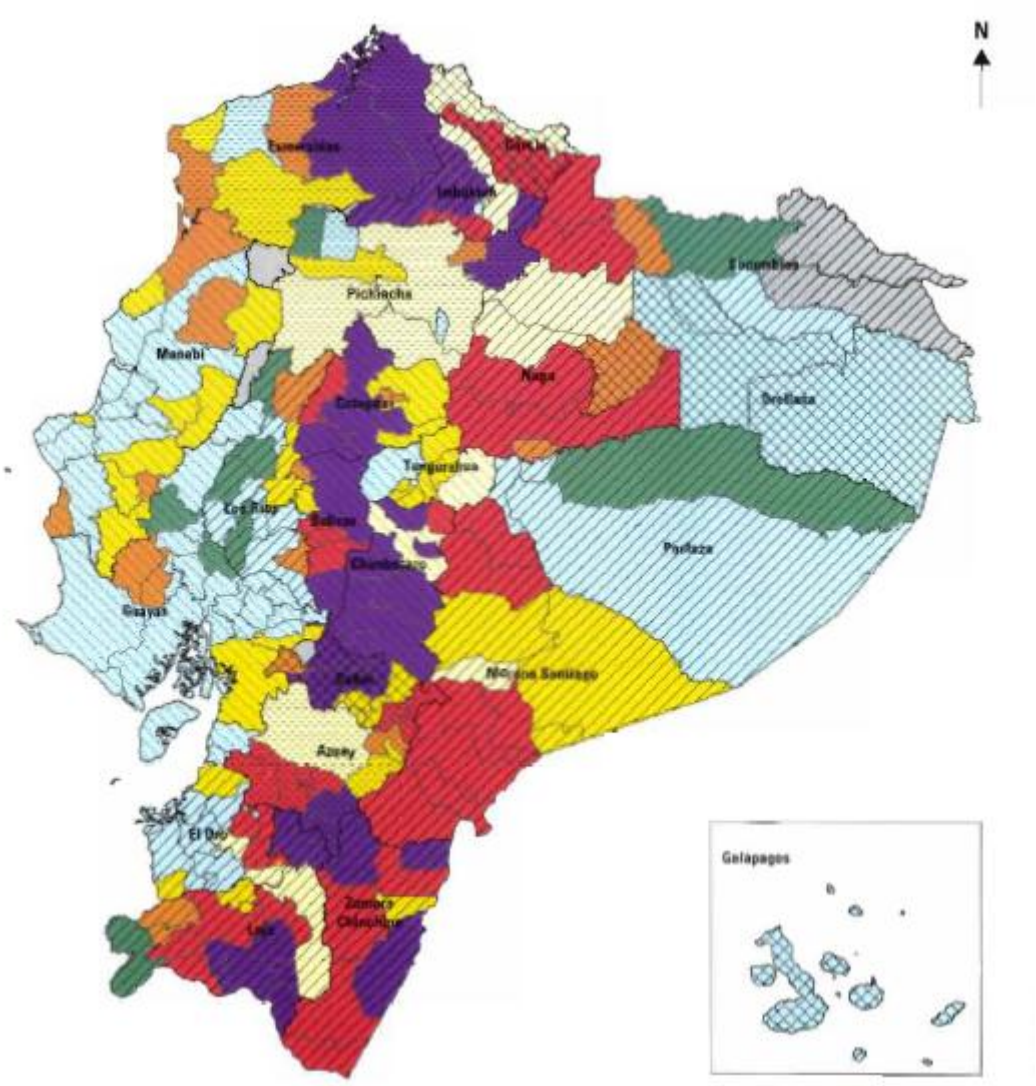

Figura 15. Riesgo por deslizamiento y deslaves por cantón en el Ecuador. Tomado de (D'Ercole & Trujillo, 2003)

Tabla 5.

Tabla de análisis de riesgos por deslizamiento y deslaves.

		Grado de vulnerabilidad		
		Muy alto a Alto	Relativamente alto	Relativamente bajo a Bajo
Grado de amenaza	Muy alto a Alto	**Alto riesgo**		
	Relativamente alto		**Medio riesgo**	

	Relativamente bajo a Bajo			**Bajo riesgo**

Adaptado de (D'Ercole & Trujillo, 2003)

La figura 15 nos muestra las zonas en donde existe mayor riesgo por deslizamientos o deslaves, específicamente son la parte norte y centro sur de la región Sierra. Además, de las estribaciones entre la Sierra y Amazonia.

3.1.3.6. Riesgo por amenaza de sequía

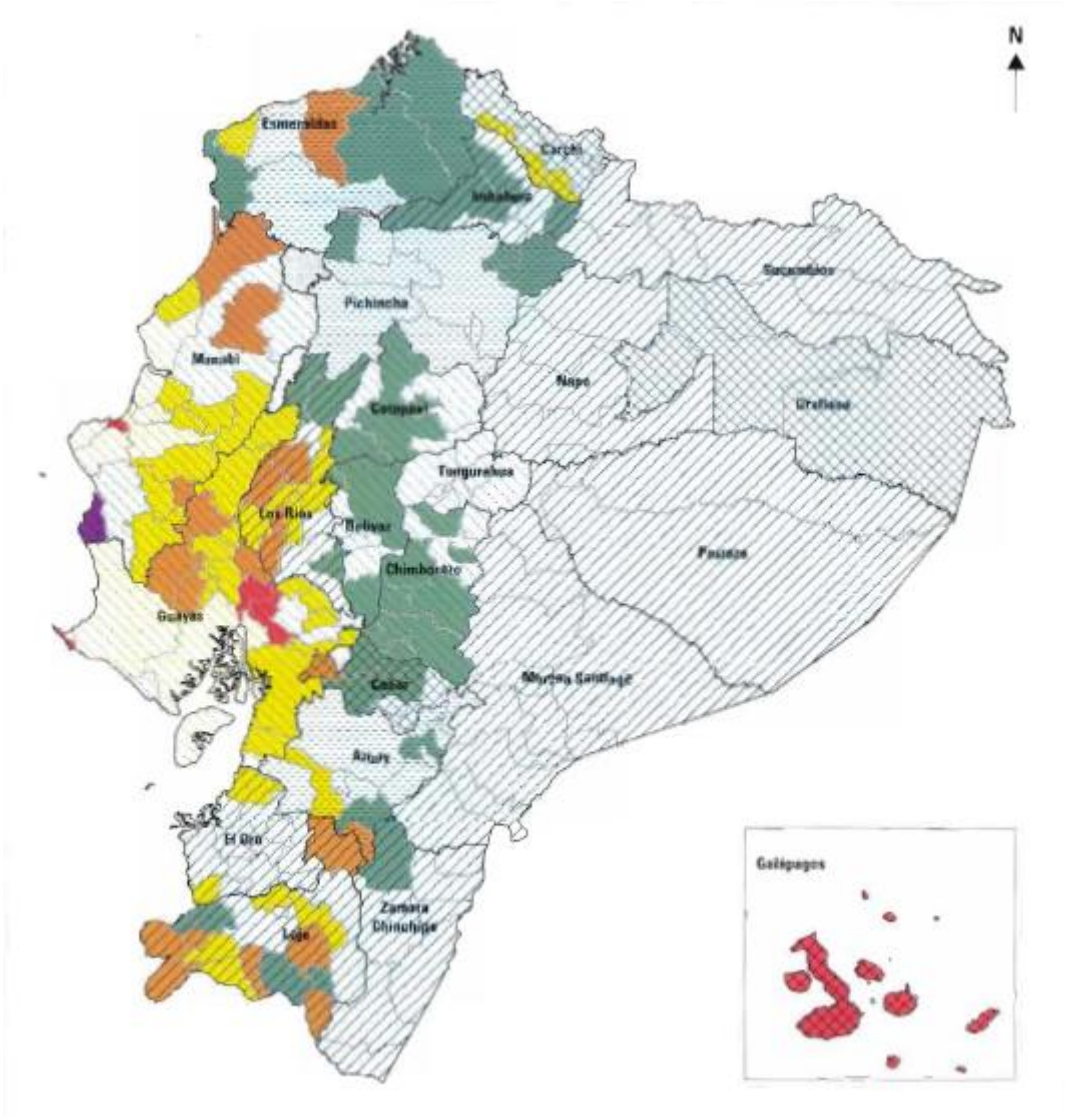

Figura 16. Riesgo por sequía por cantón en el Ecuador.

Tomado de (D'Ercole & Trujillo, 2003)

Tabla 6.

Tabla de análisis del riesgo por sequía.

		Grado de vulnerabilidad		
		Muy alto a Alto	Relativamente alto	Relativamente bajo a Bajo
Grado de amenaza	Muy alto a Alto	**Alto riesgo**		
	Relativamente alto		**Medio riesgo**	
	Relativamente bajo a Bajo			**Bajo riesgo**

Adaptado de (D'Ercole & Trujillo, 2003)

De manera general, se puede observar en la figura 16 que el mayor riesgo por sequía en el Ecuador se encuentra en la región Insular seguida de la región Costa.

3.1.4. Cantones más vulnerables del Ecuador

En esta sección se mostrará los cantones que se ven más afectados por los diferentes tipos de amenazas de origen natural. Se debe recordar que la escala nacional impide hacer un análisis muy preciso. No obstante, lo que se pretende es dar una idea general de los territorios más expuestos.

Se tomaron en cuenta las seis principales amenazas (sísmicas, volcánicas, inundaciones, deslizamientos y sequías), no se consideraron los aguajes ni los cambios climáticos ya que no se puede hacer un análisis cuantitativo de estos, porque son amenazas no medibles ni predecibles.

Tabla 7.

Cantones clasificados según su grado de amenaza.

Cantón	Provincia	Valor amenaza global	Grado amenaza global
Portoviejo	Manabí	12	muy alto
Esmeraldas	Esmeraldas	12	muy alto
Santa Elena	Santa Elena	11	muy alto
Sucre	Manabí	11	muy alto
Puerto López	Manabí	11	muy alto
Eloy Alfaro	Esmeraldas	11	muy alto
San Lorenzo	Esmeraldas	11	muy alto
Atacames	Esmeraldas	10	muy alto
Rio Verde	Esmeraldas	10	muy alto
Jipijapa	Manabí	10	muy alto
Montecristi	Manabí	10	muy alto
Pedernales	Manabí	10	muy alto
Jama	Manabí	10	muy alto
Jaramijó	Manabí	10	muy alto

Adaptado de (D'Ercole & Trujillo, 2003)

Véase en el anexo 1 la lista de los cantones clasificados según su grado de amenaza global y tipo de amenaza.

En la figura 17, se muestra un mapa sintetizado del análisis cuantitativo de las amenazas, en donde se refleja los cantones con grado muy alto de amenaza global con color rojo obscuro.

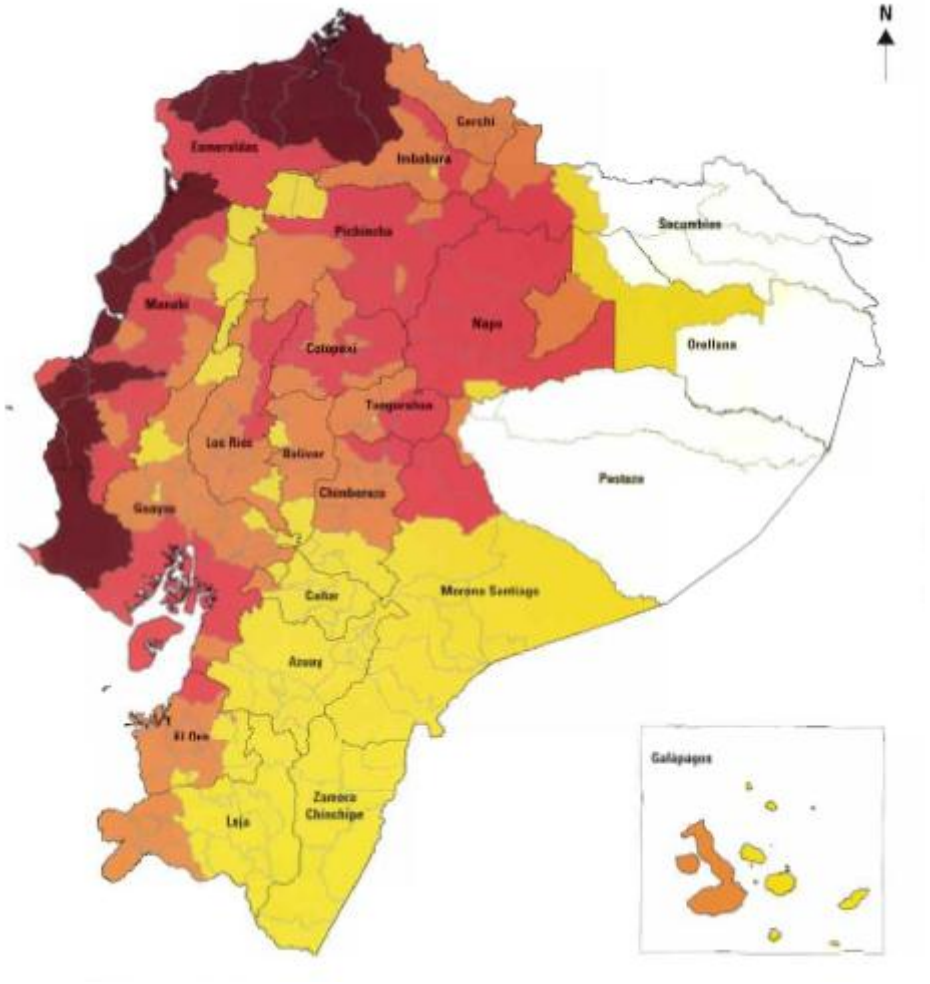

Figura 17. Nivel de amenaza de origen natural por cantón en el Ecuador. Adaptado de (D'Ercole & Trujillo, 2003)

Con la figura 17 se puede facilitar el entendimiento de los sectores más vulnerables de todas las amenazas mencionadas anteriormente. De manera general se puede decir que la provincia más afectada es Esmeraldas, seguida de Guayas, Manabí y Santa Elena.

3.1.5. Metodología de análisis del impacto y probabilidad

Para poder realizar una correcta evaluación de riesgos se deben identificar las amenazas, vulnerabilidades y riesgos centrándonos en la información, que es el activo principal que se desea proteger en las organizaciones. De esta manera, asegurar un ambiente informativo seguro, que cumplan los cuatro criterios

fundamentales que son la disponibilidad, confidencialidad e integridad de la información (SISTESEG, 2007).

Existen dos puntos fundamentales que se debe tener en cuenta:

- Probabilidad de una amenaza
- La magnitud del impacto sobre el sistema

3.1.5.1. Determinación de la probabilidad

SISTESEG (2007) señala que existen dos factores muy importantes que deben ser tomados en cuenta para poder establecer una estimación o probabilidad de la ocurrencia de una amenaza, que son los siguientes:

- Fuente de la amenaza y su capacidad
- Naturaleza de la vulnerabilidad.

La probabilidad de que una vulnerabilidad pueda ser explotada por una amenaza se la puede clasificarla como se muestra en la tabla 8:

Tabla 8.

Probabilidad de ocurrencia de un evento determinado

NIVEL	VALOR
Altamente probable	5
Probable	4
Ocasional	3
Remota	2
Improbable	1

Para poder determinar de una manera más exacta la ocurrencia de las amenazas o eventos, se define una escala en donde la probabilidad alta se le asigna el valor de P=5, la probabilidad mediana se le asigna el valor de P=3 y a la probabilidad baja se le asigna el valor de P=1. Esta asignación de valores es una relación directa con el número de veces que ocurre el evento en el periodo de un

año, siendo P=5 cuando el evento ocurriera al menos dos veces al año (SISTESEG, 2007).

3.1.5.2. Determinación del impacto

Para poder realizar la determinación del impacto que tendría un evento para la organización, en el caso de que ocurriera la explotación por parte de una amenaza de una determinada vulnerabilidad, según el autor SISTESEG (2007) se debe considerar los siguientes aspectos:

- Consecuencias de tipo financiero, es decir pérdidas causadas sobre un activo.
- La importancia crítica de los datos y el sistema.
- Sensibilidad de los datos y el sistema.

Tabla 9.

Impacto de un determinado evento

NIVEL	VALOR
Catastrófico	5
Mayor	4
Moderado	3
Menor	2
Despreciable	1

Una vez que se tiene definidos los valores del impacto y de la probabilidad, se debe realizar la matriz de calificación del riesgo que servirá para identificar el riesgo de la amenaza, para realizar este procedimiento se utilizará la siguiente ecuación:

$$Riesgo = Probabilidad \times Impacto \qquad \text{(Ecuación 1)}$$

Tabla 10.

Matriz de evaluación de riesgos

			IMPACTO				
			1	2	3	4	5
			Despreciable	Menor	Moderado	Mayor	Catastrófico
PROBABILIDAD	5	Altamente probable	5	10	15	20	25
	4	Probable	4	8	12	16	20
	3	Ocasional	3	6	9	12	15
	2	Remota	2	4	6	8	10
	1	Improbable	1	2	3	4	5

MUY ALTO
ALTO
MEDIO
BAJO

3.1.6. Evaluación del riesgo y criticidad de las amenazas de origen natural en cada provincia

Para un mejor entendimiento, en esta sección se mostrará los resultados de la evaluación del riesgo y la criticidad separados por el tipo de amenazas y estas a su vez mostrarán los resultados obtenidos por provincias.

De esta manera, se puede dar una información a las operadoras móviles del país, que será de mucha ayuda al momento de realizar sus planes de continuidad de negocio. Además, pueden tener en cuenta esta información como guía para validar la ubicación de su infraestructura y equipos, asegurándose de que estén en los lugares menos probables de ocurrencias de estos eventos.

3.1.6.1. Riesgo sísmico

Tabla 11.

Riesgo sísmico por provincias en el Ecuador

RIESGO SÍSMICO				
PROVINCIAS	**IMPACTO**	**PROBABILIDAD**	**RIESGO**	**CRITICIDAD**
AZUAY	4	3	12	ALTO
BOLÍVAR	4	4	16	MUY ALTO
CAÑAR	4	3	12	ALTO
CARCHI	4	5	20	MUY ALTO
CHIMBORAZO	4	4	16	MUY ALTO
COTOPAXI	4	4	16	MUY ALTO
EL ORO	4	3	12	ALTO
ESMERALDAS	4	4	16	MUY ALTO
GALÁPAGOS	4	3	12	ALTO
GUAYAS	4	3	12	ALTO
IMBABURA	4	4	16	MUY ALTO
LOJA	4	3	12	ALTO
LOS RIOS	4	3	12	ALTO
MANABÍ	4	5	20	MUY ALTO
MORONA SANTIAGO	4	2	8	ALTO
NAPO	4	4	16	MUY ALTO
ORELLANA	4	2	8	ALTO
PASTAZA	4	2	8	ALTO
PICHINCHA	4	4	16	MUY ALTO
SANTA ELENA	4	4	16	MUY ALTO
STO. DOMINGO DE LOS TSÁCHILAS	4	3	12	ALTO
SUCUMBÍOS	4	2	8	ALTO
TUNGURAHUA	4	5	20	MUY ALTO
ZAMORA CHINCHIPE	4	2	8	ALTO

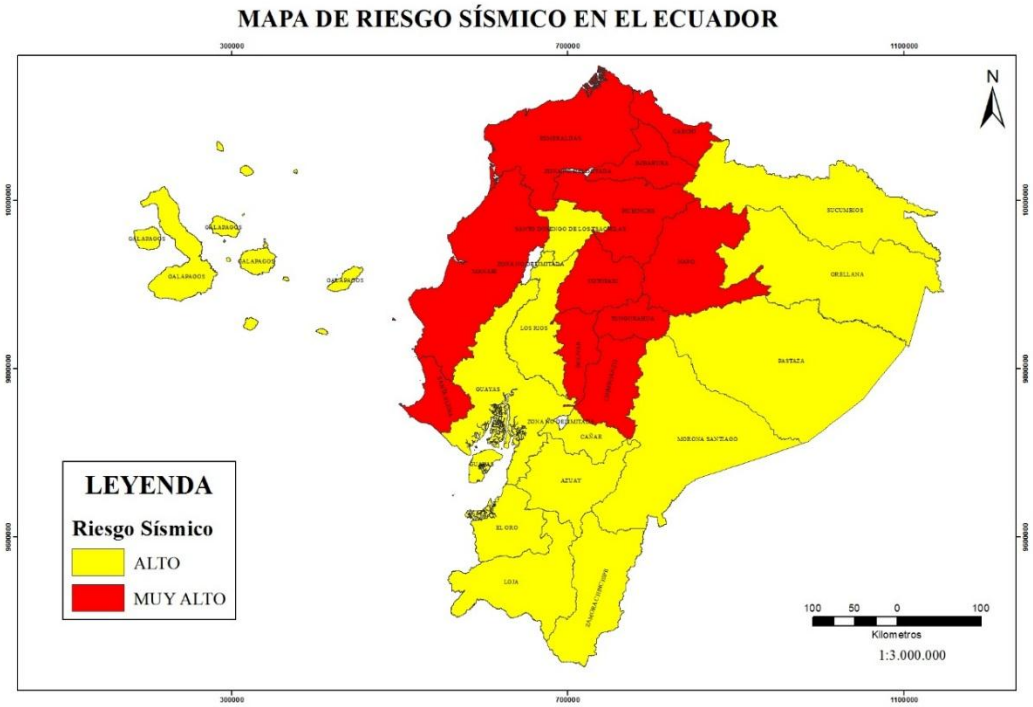

Figura 18. Mapa de riesgo sísmico en el Ecuador

3.1.6.2. Riesgo tsunami

Tabla 12.

Riesgo de Tsunami por provincias en el Ecuador.

RIESGO TSUNAMI				
PROVINCIAS	**IMPACTO**	**PROBABILIDAD**	**RIESGO**	**CRITICIDAD**
AZUAY	5	1	5	MEDIO
BOLÍVAR	5	1	5	MEDIO
CAÑAR	5	1	5	MEDIO
CARCHI	5	1	5	MEDIO
CHIMBORAZO	5	1	5	MEDIO
COTOPAXI	5	1	5	MEDIO
EL ORO	5	4	20	MUY ALTO
ESMERALDAS	5	5	25	MUY ALTO
GALÁPAGOS	5	1	5	MEDIO
GUAYAS	5	5	25	MUY ALTO
IMBABURA	5	1	5	MEDIO
LOJA	5	1	5	MEDIO
LOS RIOS	5	1	5	MEDIO

MANABÍ	5	5	25	MUY ALTO
MORONA SANTIAGO	5	1	5	MEDIO
NAPO	5	1	5	MEDIO
ORELLANA	5	1	5	MEDIO
PASTAZA	5	1	5	MEDIO
PICHINCHA	5	1	5	MEDIO
SANTA ELENA	5	5	25	MUY ALTO
STO. DOMINGO DE LOS TSÁCHILAS	5	1	5	MEDIO
SUCUMBÍOS	5	1	5	MEDIO
TUNGURAHUA	5	1	5	MEDIO
ZAMORA CHINCHIPE	5	1	5	MEDIO

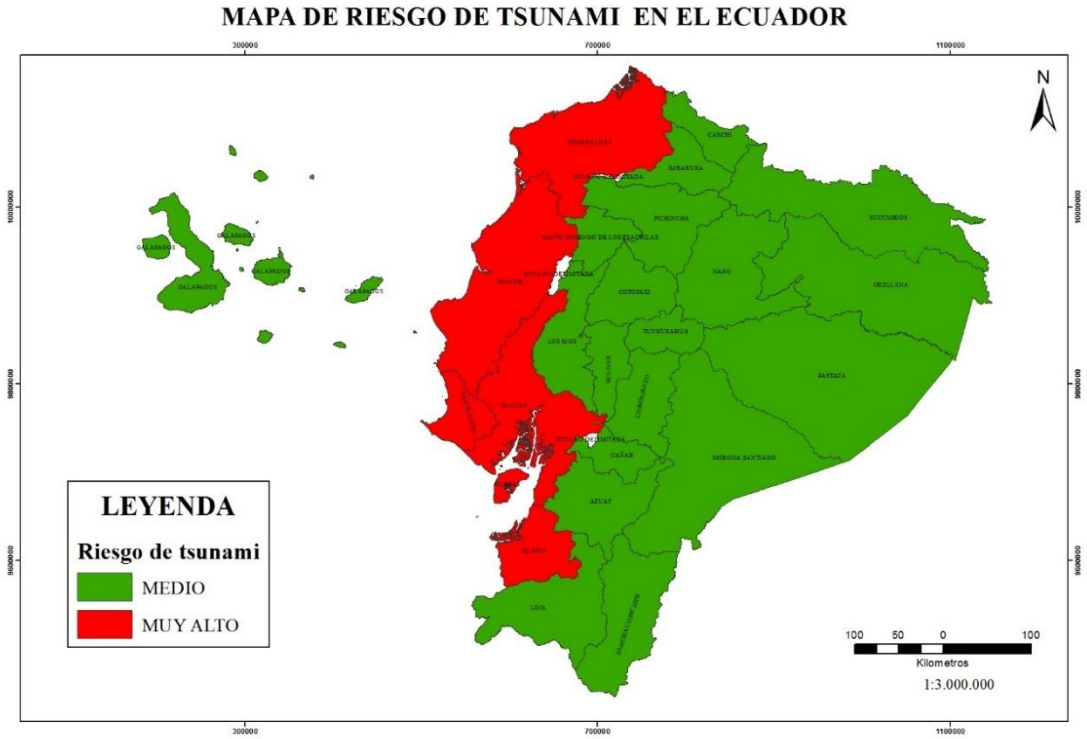

Figura 19. Mapa de riesgo de tsunami en el Ecuador

3.1.6.3. Riesgo volcánico

Tabla 13.

Riesgo volcánico por provincias en el Ecuador

RIESGO VOLCÁNICO				
PROVINCIAS	**IMPACTO**	**PROBABILIDAD**	**RIESGO**	**CRITICIDAD**

AZUAY	4	1	4	MEDIO
BOLÍVAR	4	3	12	ALTO
CAÑAR	4	1	4	MEDIO
CARCHI	4	1	4	MEDIO
CHIMBORAZO	4	2	8	ALTO
COTOPAXI	4	4	16	MUY ALTO
EL ORO	4	1	4	MEDIO
ESMERALDAS	4	3	12	ALTO
GALÁPAGOS	4	4	16	MUY ALTO
GUAYAS	4	1	4	MEDIO
IMBABURA	4	3	12	ALTO
LOJA	4	1	4	MEDIO
LOS RIOS	4	2	8	ALTO
MANABÍ	4	1	4	MEDIO
MORONA SANTIAGO	4	3	12	ALTO
NAPO	4	5	20	MUY ALTO
ORELLANA	4	3	12	ALTO
PASTAZA	4	1	4	MEDIO
PICHINCHA	4	5	20	MUY ALTO
SANTA ELENA	4	1	4	MEDIO
STO. DOMINGO DE LOS TSÁCHILAS	4	3	12	ALTO
SUCUMBÍOS	4	3	12	ALTO
TUNGURAHUA	4	5	20	MUY ALTO
ZAMORA CHINCHIPE	4	1	4	MEDIO

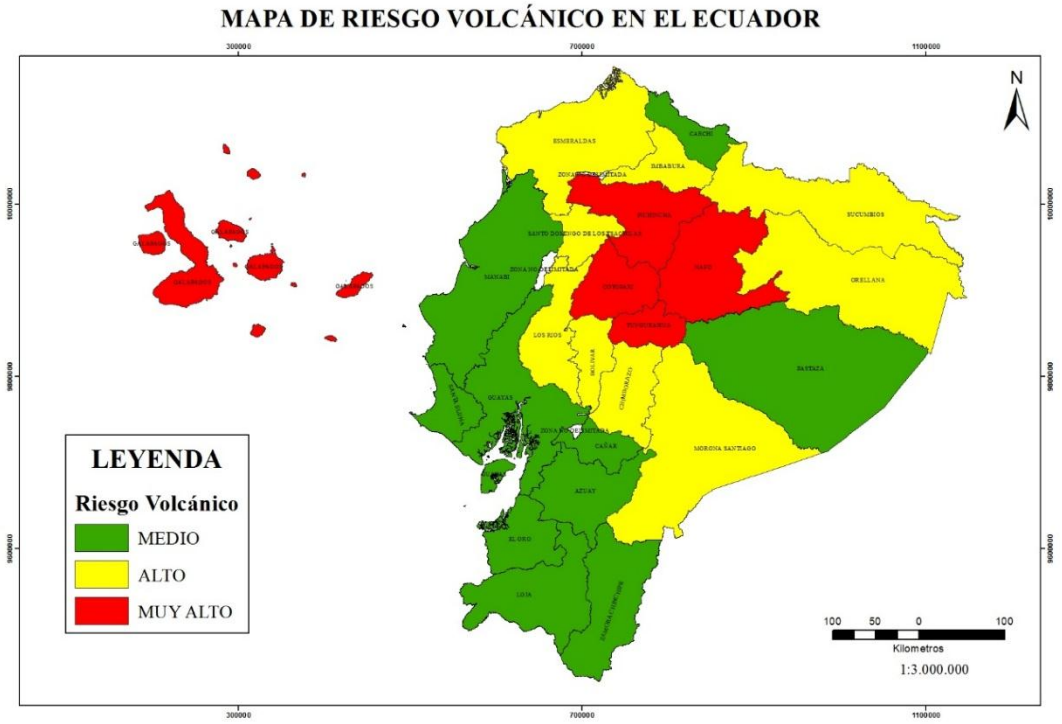

Figura 20. Mapa de riesgo volcánico en el Ecuador

3.1.6.4. Riesgo inundaciones

Tabla 14.

Riesgo inundaciones por provincias en el Ecuador.

RIESGO INUNDACIONES				
PROVINCIAS	**IMPACTO**	**PROBABILIDAD**	**RIESGO**	**CRITICIDAD**
AZUAY	3	1	3	BAJO
BOLÍVAR	3	1	3	BAJO
CAÑAR	3	1	3	BAJO
CARCHI	3	1	3	BAJO
CHIMBORAZO	3	1	3	BAJO
COTOPAXI	3	3	9	ALTO
EL ORO	3	5	15	MUY ALTO
ESMERALDAS	3	5	15	MUY ALTO
GALÁPAGOS	3	1	3	BAJO
GUAYAS	3	5	15	MUY ALTO
IMBABURA	3	1	3	BAJO
LOJA	3	1	3	BAJO
LOS RIOS	3	5	15	MUY ALTO

MANABÍ	3	5	15	MUY ALTO
MORONA SANTIAGO	3	3	9	ALTO
NAPO	3	4	12	ALTO
ORELLANA	3	4	12	ALTO
PASTAZA	3	3	9	ALTO
PICHINCHA	3	4	12	ALTO
SANTA ELENA	3	5	15	MUY ALTO
STO. DOMINGO DE LOS TSÁCHILAS	3	3	9	ALTO
SUCUMBÍOS	3	3	9	ALTO
TUNGURAHUA	3	1	3	BAJO
ZAMORA CHINCHIPE	3	1	3	BAJO

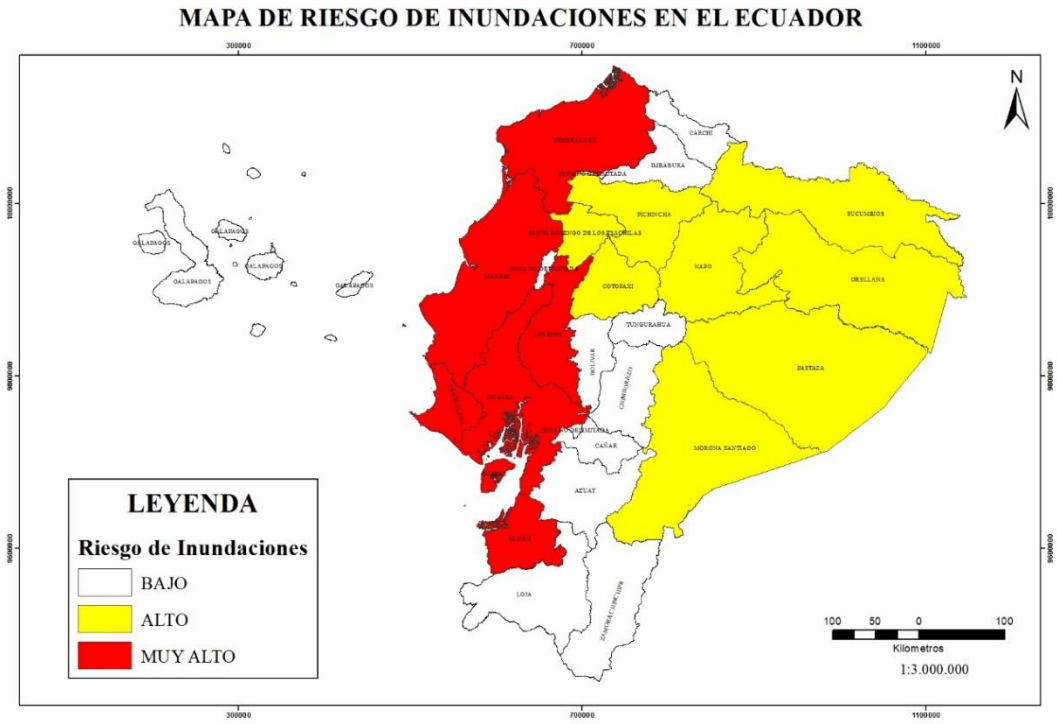

Figura 21. Mapa de riesgo de inundaciones en el Ecuador

3.1.6.5. Riesgo deslizamientos

Tabla 15.

Riesgo deslizamiento por provincias en el Ecuador.

RIESGO DESLIZAMIENTOS				
PROVINCIAS	**IMPACTO**	**PROBABILIDAD**	**RIESGO**	**CRITICIDAD**

AZUAY	1	5	5	MEDIO
BOLÍVAR	1	5	5	MEDIO
CAÑAR	1	5	5	MEDIO
CARCHI	1	5	5	MEDIO
CHIMBORAZO	1	5	5	MEDIO
COTOPAXI	1	5	5	MEDIO
EL ORO	1	4	4	MEDIO
ESMERALDAS	1	5	5	MEDIO
GALÁPAGOS	1	1	1	BAJO
GUAYAS	1	2	2	BAJO
IMBABURA	1	5	5	MEDIO
LOJA	1	5	5	MEDIO
LOS RIOS	1	2	2	BAJO
MANABÍ	1	4	4	MEDIO
MORONA SANTIAGO	1	5	5	MEDIO
NAPO	1	5	5	MEDIO
ORELLANA	1	2	2	BAJO
PASTAZA	1	1	1	BAJO
PICHINCHA	1	5	5	MEDIO
SANTA ELENA	1	3	3	BAJO
STO. DOMINGO DE LOS TSÁCHILAS	1	5	5	MEDIO
SUCUMBÍOS	1	1	1	BAJO
TUNGURAHUA	1	5	5	MEDIO
ZAMORA CHINCHIPE	1	5	5	MEDIO

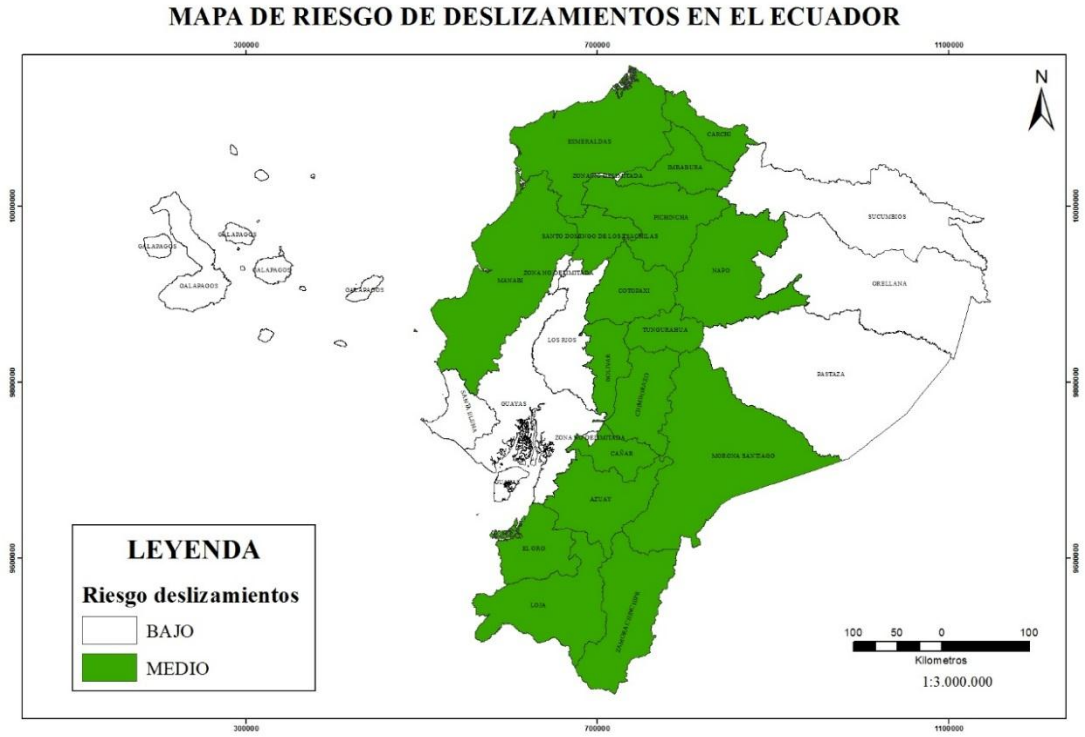

Figura 22. Mapa de riesgo de deslizamientos en el Ecuador

3.1.6.6. Riesgo sequía

Tabla 16.

Riesgo de sequía por provincia en el Ecuador

RIESGO SEQUÍA				
PROVINCIAS	**IMPACTO**	**PROBABILIDAD**	**RIESGO**	**CRITICIDAD**
AZUAY	1	1	1	BAJO
BOLÍVAR	1	1	1	BAJO
CAÑAR	1	1	1	BAJO
CARCHI	1	3	3	BAJO
CHIMBORAZO	1	1	1	BAJO
COTOPAXI	1	1	1	BAJO
EL ORO	1	4	4	MEDIO
ESMERALDAS	1	4	4	MEDIO
GALÁPAGOS	1	5	5	MEDIO
GUAYAS	1	5	5	MEDIO
IMBABURA	1	3	3	BAJO
LOJA	1	3	3	BAJO
LOS RIOS	1	4	4	MEDIO

MANABÍ	1	5	5	MEDIO
MORONA SANTIAGO	1	1	1	BAJO
NAPO	1	1	1	BAJO
ORELLANA	1	1	1	BAJO
PASTAZA	1	1	1	BAJO
PICHINCHA	1	1	1	BAJO
SANTA ELENA	1	5	5	MEDIO
STO. DOMINGO DE LOS TSÁCHILAS	1	1	1	BAJO
SUCUMBÍOS	1	1	1	BAJO
TUNGURAHUA	1	1	1	BAJO
ZAMORA CHINCHIPE	1	1	1	BAJO

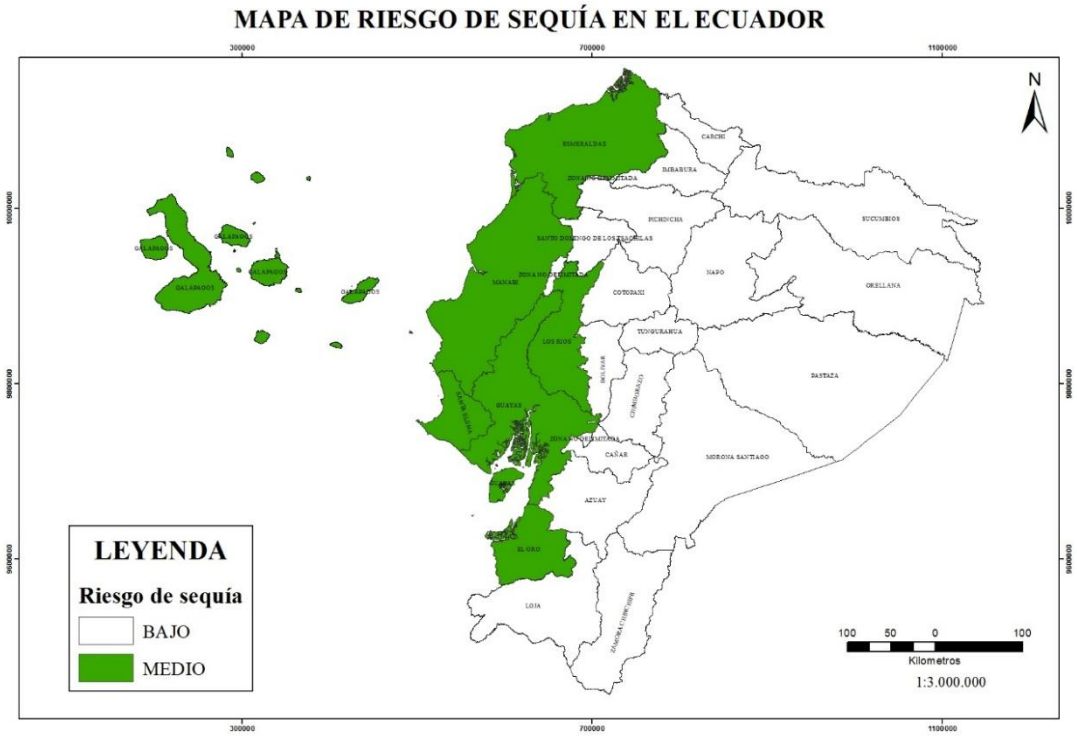

Figura 23. Mapa de riesgo de sequía en el Ecuador.

4. GUÍA GENERAL PARA ELABORACIÓN DE PLANES DE CONTINUIDAD DE NEGOCIOS PARA OPERADORAS MÓVILES

4.1. FASE 1: Análisis del negocio y riesgos

4.1.1. Análisis del negocio

En esta fase se debe definir el contexto en el cual se va a desarrollar el plan, en este punto se debe definir el ambiente, el alcance, criterios de evaluación, entre otros ajustes. Para poder realizar este apartado es esencial que el equipo encargado para la realización del plan tenga total acceso y pleno conocimiento de toda la información de la organización, tales como: datos técnicos, negocios, legislación y procesos.

4.1.1.1. Definición del contexto

Como primer paso se debe hacer un levantamiento de toda la información relevante de la organización, es decir, los elementos que caracterizan y contribuyen al desarrollo de la organización. El objetivo de esta sección es identificar los procesos críticos y sus interdependencias con otros procesos, además de los recursos mínimos con los cuales la organización puede prestar sus servicios.

El análisis de la organización debe contener al menos los siguientes ítems que se muestran en la tabla 17.

Tabla 17.

Ítems para el análisis de la organización

Ítems para identificación	Ejemplos de preguntas
Objetivo principal de la organización	¿Cuál es el propósito de la organización? ¿Cuáles son sus objetivos?
Organización empresarial	
Negocio	¿Cuál es su negocio? ¿Cuál es el propósito de lo que se produce/desarrollado?
Misión	¿Cuál es su misión? ¿Para que existe? ¿Lo que ella se propone a hacer? ¿Para quién?
Visión	¿Cuál es su visión del futuro? ¿Qué se espera de ella en el tiempo?

Valores	¿Cuáles son sus valores? ¿Cómo se muestran?
Estructura organizacional	¿Cómo está organizada y estructurada? ¿Y la seguridad de la información? ¿Y las responsabilidades por la seguridad?
Organigrama	¿Cuál es su organigrama? ¿Quién es quién en el sector que trabaja? ¿Hay zona de seguridad de la información?
Estrategias	¿Cuáles son sus principales estrategias de negocios? ¿Y de seguridad de la información?
Productos	¿Cuáles son sus productos? ¿Cuál es el principal producto de apalancamiento de los negocios?
Socios	¿Quiénes son sus socios? ¿Cómo se eligen? ¿Cómo colaboran? ¿Cómo es la relación de la seguridad de la información a ellos? ¿Cuáles son las obligaciones de seguridad de información?
Terceros	¿Quiénes son los terceros? ¿Cómo se eligen? ¿Cómo colaboran? ¿Cómo es la relación de la seguridad de la información a ellos? ¿Cuáles son las obligaciones de seguridad de información?
Instalaciones	¿Cómo se divide el personal de la organización? ¿Dónde están los servidores? ¿Existe algún mecanismo para prevenir un incendio? ¿Cómo es hecha la protección física? ¿Cómo son los accesos?
Funcionarios	¿Cómo son contratados? ¿Hay capacitación en seguridad?
Procesos	¿Cuáles son los procesos de negocio de la organización?
Proveedores	¿Cuáles son sus principales proveedores?
Políticas internas	¿Cuáles son los requisitos de las políticas internas de la organización?
Reglamentos	¿Cuáles son los requisitos legales o reglamentarios?

Adaptado de (Páez Parra, 2014)

4.1.1.2. Definición del alcance y límites

Es muy impórtate que la organización defina su alcance y los límites que tendrá el plan de continuidad del negocio, ya que de esta manera se evitarán malas interpretaciones por parte del equipo de trabajo. Por lo tanto, el alcance debe ser muy claro y estar bien definido.

Dentro del alcance debe constar como mínimo los límites, su cobertura, los resultados y los entregables que tendrá el plan de continuidad del negocio de la operadora móvil.

Al definir el alcance, deben ser considerados aspectos de la organización como los siguientes:

- Objetivos y políticas;
- Estructura y funciones;
- Procesos de negocios;
- Activos;
- Expectativas;
- Restricciones.

4.1.1.3. Criterios para la evaluación del riesgo

Para poder realizar los siguientes puntos del plan de continuidad del negocio, se necesita definir los criterios para la evaluación del riego. Es decir, establecer un patrón o formato del que se regirá la organización.

Los criterios son adaptados y dependen de cada organización, por esta razón, deben ser determinados en común acuerdo entre todo el equipo encargado y un representante de cada área de la organización.

Dentro de estos criterios se encuentran, entre otros, criterios de impacto, criterios de riego, criterios de probabilidad, criterios de cobertura, etc.

A continuación, se mostrarán unos ejemplos para crear una idea de criterios, se debe tomar en cuenta que estos ejemplos no pueden aplicar a todas las organizaciones:

Tabla 18.

Ejemplo de criterio de nivel de impacto.

Nivel del impacto	Valor	Descripción
Despreciable	1	De acuerdo con la organización
Ligeramente perjudicial	2	De acuerdo con la organización
Perjudicial	3	De acuerdo con la organización
Extremadamente perjudicial	5	De acuerdo con la organización

Tabla 19.

Ejemplo de criterio de nivel de probabilidad.

Nivel de la probabilidad	Valor	Descripción
Frecuente	>0,92	De acuerdo con la organización
Probable	>0,65 y <=0,92	De acuerdo con la organización
Ocasional	>0,39 y <=0,65	De acuerdo con la organización
Remoto	>0,15 y <=0,39	De acuerdo con la organización
Improbable	>=0 y <=0,15	De acuerdo con la organización

Tabla 20.

Ejemplo de criterio de nivel de riesgo.

Nivel del riesgo	Valor	Descripción
Extremo	5	De acuerdo con la organización
Altísimo	4	De acuerdo con la organización
Alto	3	De acuerdo con la organización
Medio	2	De acuerdo con la organización
Bajo	1	De acuerdo con la organización
Irrelevante	0,5	De acuerdo con la organización

4.1.2. Identificación, análisis y evaluación de riesgos

En este apartado se va a identificar y evaluar los activos, amenazas y vulnerabilidades, siendo compuesta por los siguientes pasos:

- **Identificación del riesgo:** determina los eventos que pueden causar pérdidas potenciales.
- **Análisis del riesgo:** determina la probabilidad de que ocurra un evento.
- **Evaluación del riesgo:** ordena los riesgos de acuerdo con los criterios de evaluación establecidos en la definición de contexto.

Después de identificar el contexto y la definición del alcance, con perfecto conocimiento de todo ambiente, se inicia el proceso de análisis/evaluación del riesgo. La figura 24 muestra las actividades en el proceso de gestión del riesgo. (Páez Parra, 2014)

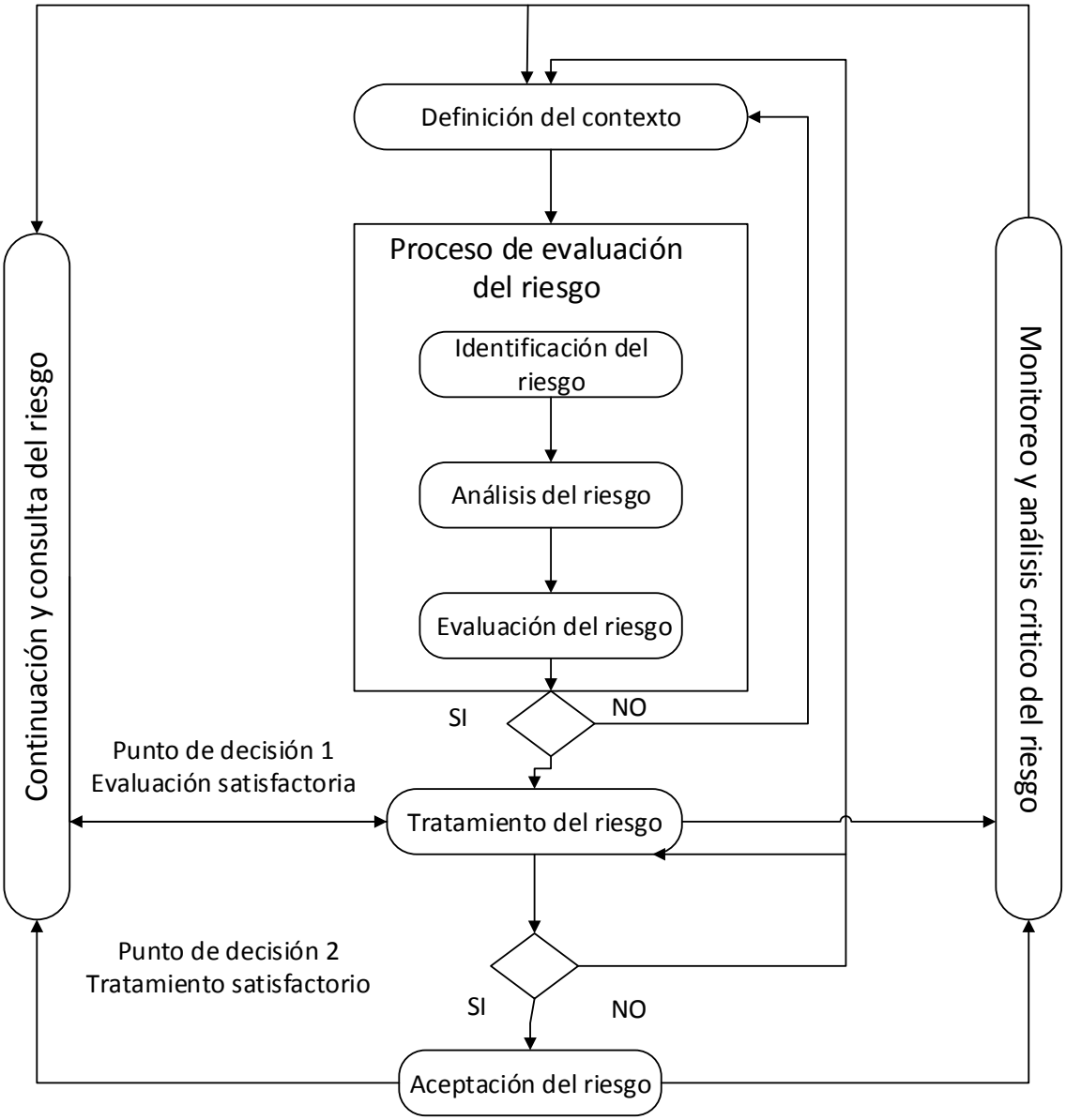

Figura 24. Proceso de gestión del riesgo.

Adaptado de (Páez Parra, 2014)

4.1.2.1. Identificación del riesgo

El objetivo principal de esta sección generar una lista de riesgos con sus causas y consecuencias.

En la etapa de análisis del riesgo, el primer paso que se debe hacer es la identificación del riesgo. Esta identificación se la realiza para poder conocer y

determinar los posibles eventos que tendrían un alto potencial de causar pérdidas en la organización. (Páez Parra, 2014)

Las actividades de identificación del riesgo se muestran en la figura 25:

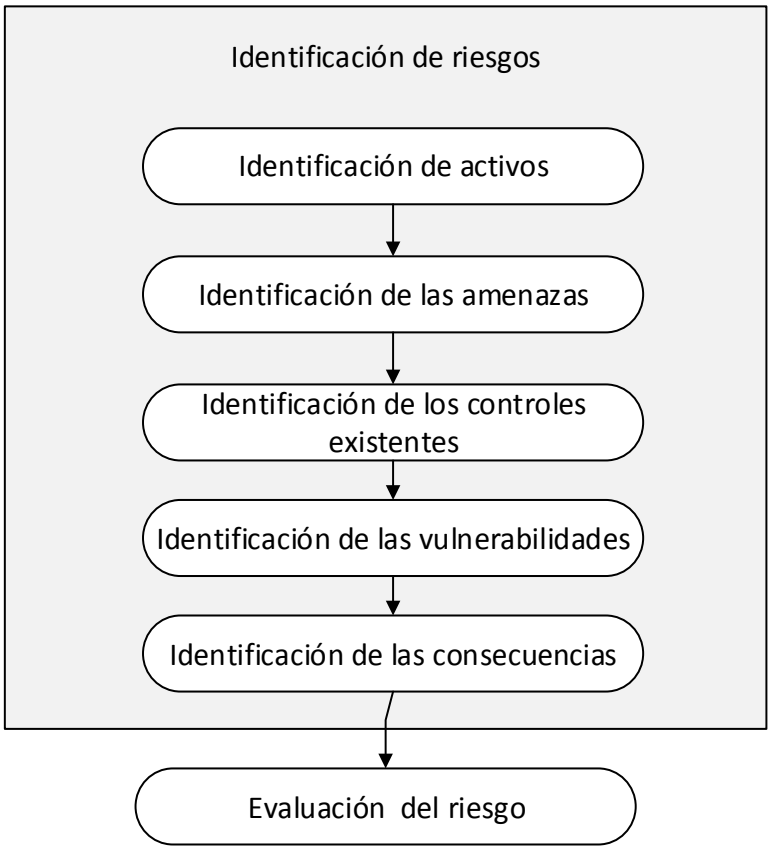

Figura 25. Actividades de la identificación del riesgo.

Tomado de (Páez Parra, 2014)

4.1.2.1.1. Identificación de activos

Cabe recordar que activo en relación con la seguridad de la información, se refiere a cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización. Cualquier cosa que tiene valor para la organización. Todos los activos deberían estar claramente identificados, confeccionando y manteniendo un inventario con los más importantes (ISO 27001, 2013).

En la actividad de la identificación de los activos:

- **Entrada**: contempla los resultados de la etapa de definición del alcance.
- **Acción:** Desarrollo de la actividad de identificación de los activos. La identificación de los activos debe ser hecha a un nivel de detalle que permite el suministro de información adecuada y suficiente para el análisis y evaluación del riesgo. Como el proceso define la necesidad de varias iteraciones, el detalle puede ser profundizado en cada iteración.
- **Salida:** Lista de los activos considerados sensibles para la organización y también una lista de los negocios relacionados a estos activos.

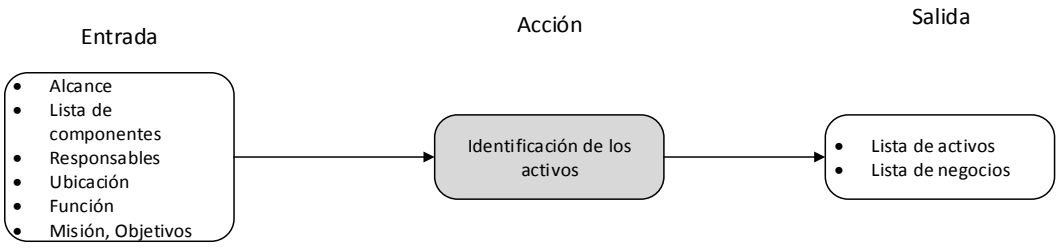

Figura 26. Actividades de la identificación de los activos.

Tomado de (Páez Parra, 2014)

Una clasificación general de los activos podría ser:

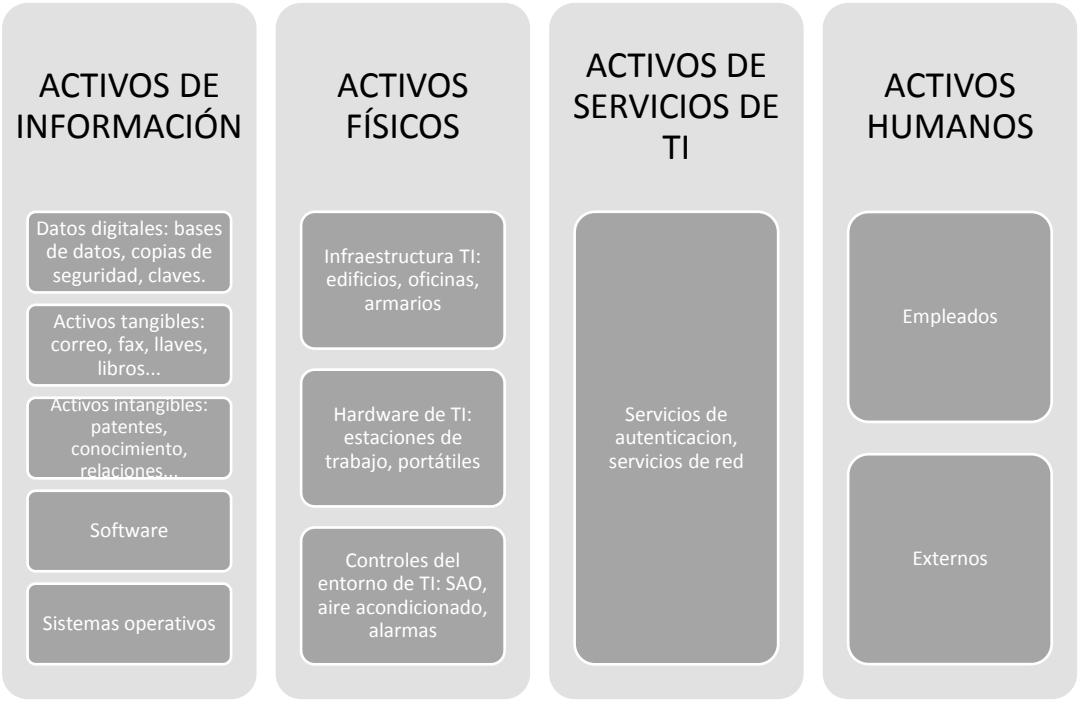

Figura 27. Clasificación general de los activos

Tomado de (ISO 27001, 2013)

La información más importante sobre un activo es quién es su responsable. Ya que este profesional es el que tiene toda la responsabilidad sobre la producción, desarrollo, mantenimiento, utilización y seguridad del activo. Es decir, tiene la mayor parte de la información sobre el activo y por lo general será la persona más apropiada para determinar el valor del activo (Páez Parra, 2014).

Dos tipos de activos pueden ser identificados:

- Activos primarios;
- Activos de soporte e infraestructura.

4.1.2.1.1.1. Identificación de activos primarios

Los activos primarios pueden ser tanto procesos y actividades de negocios, así como también toda la información relacionada. Una de las actividades más recomendadas para identificar estos activos es a través de entrevistas a un grupo heterogéneo de profesionales que representan el proceso, como gestores,

especialistas en los sistemas de información y usuarios. Se debe tomar en cuenta que es muy importante la participación de representantes de todos los niveles de la organización.

Por lo general, los activos primarios son los principales procesos e información de las actividades incluidas en el alcance. Los activos primarios pueden ser de dos tipos:

- Procesos o subprocesos y actividades de negocio. Por ejemplo:
    - Procesos cuya interrupción (así sea parcialmente) impide a la organización continuar con su negocio;
    - Procesos que contienen procedimientos secretos o que involucran tecnología patentada.
- La información primaria puede incluir:
    - Información vital para el ejercicio de las actividades de la organización;
    - Información de carácter personal, como las definidas en las leyes nacionales sobre la privacidad.

Normalmente, la información para la identificación detallada de los activos primarios es obtenida a nivel gerencial y de la alta dirección de la organización. Estos activos serán considerados sensibles para la organización. Cabe resaltar que existirán procesos e información que no serán sensibles, pero a menudo heredan los controles para la protección de procesos e información sensible (Páez Parra, 2014).

4.1.2.1.1.2. Identificación de activos de soporte e infraestructura

Es importante resaltar la importancia del detalle de esta información sobre los activos. Normalmente toda la información necesaria para el equipo de análisis de riesgo no será obtenida en una primera entrevista. La realización de otras reuniones y de entrevistas en los niveles gerenciales, técnicos y de usuarios,

junto con las observaciones in situ en la organización, permitirá que sea obtenida la información suficiente para identificar los activos.

Para la actividad de identificación de los activos, el equipo de análisis tendrá como salida una lista de los activos considerados sensibles para la organización y también una lista de los negocios relacionados con estos activos.

Se puede registrar la información en una tabla como la siguiente:

Tabla 21.

Formato para la identificación de los activos

		Activos	**Responsable**	**Observaciones**
Activos primarios	1			
	2			
	3			
	4			
	5			
		Activos	**Responsable**	**Observaciones**
Activos de soporte e infraestructura	1			
	2			
	3			
	4			
	5			

4.1.2.1.1.3. Identificación de amenazas

La amenaza está definida como la probabilidad de ocurrencia de un evento potencialmente desastroso es decir que explote vulnerabilidades que puedan

causar un incidente no deseado, que puede resultar en daño a un sistema u organización durante un periodo de tiempo (Cardona A., 1993).

En la actividad de identificación de las amenazas serán realizadas acciones para levantar e identificar, dentro del alcance establecido, las amenazas existentes en la organización.

De esta actividad de identificación de las amenazas, el equipo de análisis tendrá como:

- **Entrada:** la información de su historial, obtenidas de los incidentes ocurridos, de observaciones realizadas por los responsables y usuarios de los activos, y aun a través de información recolectada de catálogos externos de amenazas.
- **Acción:** identificación de las amenazas y sus fuentes. La fuente de amenaza está relacionada a su agente, entidad que puede causar una amenaza explotando o evidenciando alguna vulnerabilidad. Uno de los principales y más peligrosas agentes de amenaza es el ser humano.
- **Salida:** una lista de amenazas con la identificación del tipo y de la fuente de las amenazas.

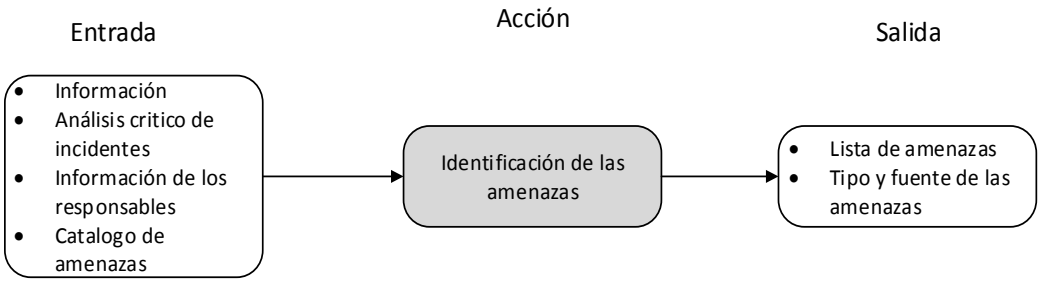

Figura 28. Actividades de la identificación de las amenazas.

Tomado de (Páez Parra, 2014)

Las amenazas pueden ser clasificadas como voluntarias, accidentales o de origen natural y ambiental.

La organización y los activos pueden estar comprometidos sin duda alguna por las amenazas, es por esto qué deben ser identificadas correctamente. Durante la identificación de amenazas se necesita crear un catálogo de amenazas de la organización. Este catálogo deberá contener la categoría de amenaza: si es interna es decir que el origen es dentro de la organización, externa si el origen es fuera de la organización o interna y externa simultáneamente.

Durante la identificación de amenazas, deben llevarse a cabo entrevistas, observaciones en el lugar y la realización de una *checklist*, a nivel gerencial, técnicos y de usuarios, para poder obtener la mayor información posible. Así puede ser obtenida la información como: datos de incidentes ocurridos, cantidad de ocurrencias, aspectos culturales y de ambiente de los activos, experiencias en ocurrencias anteriores, evaluaciones y otra información colectada en las reuniones. Toda la información debe ser registrada y compilada en un documento para su posterior utilización como prueba en caso de necesidad.

Fuentes de amenazas intencionales:

- Motivación para explotar, conflictos con superiores y la insatisfacción laborar.
- Habilidades y conocimientos: ciertas vulnerabilidades solo pueden ser explotadas si el atacante tiene elevado conocimiento técnico, para explotar otras vulnerabilidades simplemente desconectando la alimentación.
- Conocimiento de la vulnerabilidad, porque no todo el mundo puede percibir la existencia de la vulnerabilidad, aunque algunos ya saben dónde se almacena la contraseña.
- Poder de atracción de los activos: para un atacante motivado para causar gran daño, un servidor de e-mail no es suficiente, sin embargo, puede ser suficiente para otro atacante con el objetivo de provocar pequeños problemas, como sacar el servidor del aire.

Fuentes de amenazas accidentales:

- Proximidad a lugares insalubres y que pueden dañar los equipos;
- Eventos climáticos tales como tormentas, inundaciones y tormentas de viento;
- Factores facilitadores, que permiten que un error humano accidental (como la manipulación por personas no capacitadas técnicamente) impliquen errores, por ejemplo, red eléctrica inestable.

Es muy usual que algunas amenazas afecten negativamente sobre más de un activo. En estos casos, el equipo debe tener en cuenta que estas amenazas pueden actuar de manera diferente en cada activo, afectándolos de diferente forma a cada uno (Páez Parra, 2014).

Para poder registrar las amenazas de cada activo se puede usar la siguiente tabla como referencia:

Tabla 22.

Formato para identificación de las amenazas de los activos

	Activos	Amenazas	Categoría	Observaciones
1				
2				
3				
4				
5				

En el anexo 2 se enlista algunas posibles amenazas.

4.1.2.1.2. Identificar los controles existentes

Una vez que se ha identificado los activos y las amenazas, el siguiente punto es la identificación de controles existentes y los que están en proceso de implementación. Para cada activo y amenaza identificada, se debe verificar si ya existen controles implementados o que estén previstos para su implementación.

El control es cualquier procedimiento administrativo, físico u operacional capaz de tratar los riesgos de la ocurrencia de un incidente de seguridad. Ejemplos de controles incluyen políticas, procedimientos, estructuras organizaciones, antivirus, parches, cerraduras, extintor de incendio y *backups*, entre otros (Páez Parra, 2014).

En la acción de identificación de los controles existentes, el objetivo es identificar en el ambiente del alcance los controles que están planeados para implementación y los controles ya implementados y en uso corriente. En esta actividad:

- **Entrada**: documentación de los controles existentes y planes de implementación de control para el tratamiento del riesgo.
- **Acción:** identificación de los controles implementados y planificados.
- **Salida:** lista de todos los controles existentes y planeados, su implementación y estatus de uso.

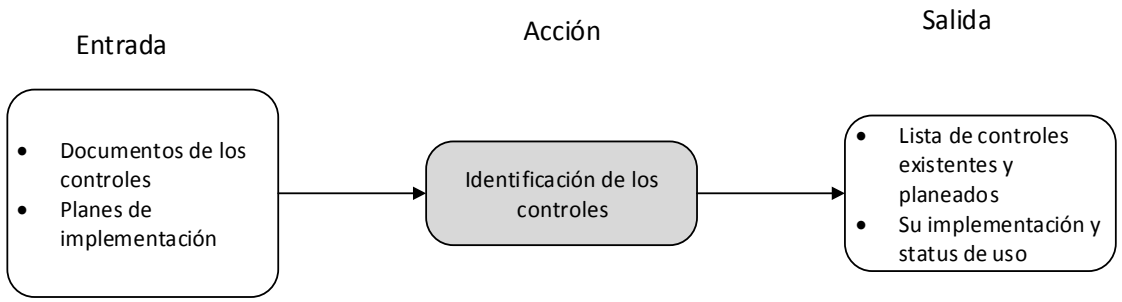

Figura 29. Identificación de los controles existentes.

Tomado de (Páez Parra, 2014)

Los objetivos de esta actividad son evitar reprocesos y costos adicionales para la duplicación de los controles, así como asegurar que los controles existentes estén funcionando adecuadamente, tratando eficazmente el riesgo. Una forma de realizar esta actividad es analizando informes de auditorías en el SGSI, los informes de análisis críticos de la dirección y los indicadores de la eficacia de los controles. Si esta información no está disponible, se recomienda la realización de:

- Reuniones con los responsables por la seguridad de la información;
- Entrevistas con usuarios para levantamiento de los controles existentes;
- Análisis crítico de la documentación sobre los controles existentes;
- Cuestionarios y listas de verificación;
- Inspecciones físicas y visitas a los locales.

Un control puede cumplir plenamente y fallar en el tratamiento del riesgo. Así, controles complementarios pueden ser necesarios para el tratamiento eficaz del riesgo. Otro punto es acerca de los controles ineficaces o insuficientes. En estos casos puede ser necesario que el control sea retirado y sustituido por otro. Estos puntos deben ser incluidos en el análisis de los controles existentes, realizado por el equipo de análisis. Controles planeados deben ser evaluados, sobre si realmente serán capaces de hacer frente a los riesgos a los que se refieren al cumplimiento (Páez Parra, 2014).

En la siguiente tabla se muestran algunos ejemplos de tipos de control:

Tabla 23.

Ejemplos de tipos de control.

Ejemplos Tipos de Control	
Controles de Gestión	Políticas claras aplicadas
	Seguimiento al plan estratégico operativo
	Indicadores de gestión
	Tableros de control
	Seguimiento a cronograma
	Evaluación del desempeño
	Informes de gestión
	Monitoreo de riesgos

Controles Operativos	Conciliaciones
	Consecutivos
	Verificación de firmas
	Lista de chequeo
	Registro controlado
	Segregación de funciones
	Niveles de autorización
	Custodia apropiada
	Procedimientos formales aplicados
	Pólizas
	Seguridad física
	Contingencias y respaldo
	Personal Capacitado
	Aseguramiento y calidad
Controles Legales	Normas claras y aplicadas
	Control de términos

Tomado de (DAFP, 2011)

4.1.2.1.3. Identificación de las vulnerabilidades

Cabe resaltar que la vulnerabilidad es cualquier debilidad que puede ser explotada y de esta manera convierta una amenaza en un riesgo para la operadora u organización y que además ponga en peligro la seguridad de la información (Jimenez, 2007).

Durante el desarrollo de esta sección, se recomienda observar las siguientes áreas para la identificación de las vulnerabilidades:

- Organización.
- Procesos y procedimientos.
- Rutinas de gestión y documentación.
- Recursos humanos (incluyendo contratistas y proveedores de servicios).
- Instalaciones físicas y prediales.
- Configuración de los sistemas de información (incluidos los sistemas operacionales y aplicaciones).
- Hardware, software y equipos de comunicación.
- Dependencias de entidades externas.

El principal objetivo de la identificación de vulnerabilidades es crear una lista que contenga todas las vulnerabilidades que estén asociadas a los activos, amenazas y controles que se ha identificado en los puntos anteriores. En esta sección se tiene como:

- **Entrada:** listas de amenazas conocidas, las listas de los activos y de los controles existentes, y todas las salidas de las actividades anteriores.
- **Acción:** actividad de identificación de las vulnerabilidades que podrían ser explotadas por amenazas con la posibilidad de poner en peligro los activos.
- **Salida:** lista de escenarios de incidentes con sus consecuencias asociadas con los activos y los procesos de negocio.

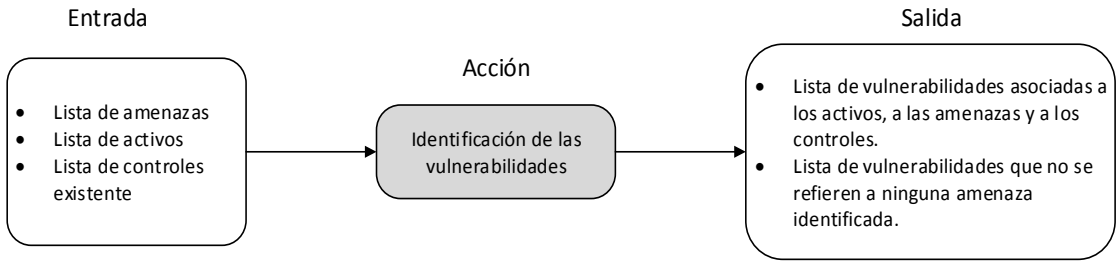

Figura 30. Actividades de la identificación de las vulnerabilidades.

Tomado de (Páez Parra, 2014)

Existen dos tipos de enfoques del que se deben analizar las vulnerabilidades, en la realización de esta sección: de afuera hacia adentro y de adentro hacia afuera. El primer enfoque desde adentro hacia afuera, se podría decir que es el punto de vista interno, que permite muchos privilegios. ¿Qué vulnerabilidades pueden existir o pueden ser explotadas? ¿Cómo los sistemas pueden verse comprometidos por el personal interno?

En el segundo enfoque, de afuera hacia adentro, los sistemas podrían verse afectados desde afuera. ¿Cuál del contenido accedido puede comprometer los activos e información de la organización? ¿Qué puede ser explorado para conferir privilegios no permitidos? (Páez Parra, 2014).

Estos dos tipos de enfoques ayudaran mucho a la hora de identificar las vulnerabilidades de la operadora ya que se tendrá en cuenta varios escenarios. Por lo general un atacante que quiere irrumpir el sistema, tiende a fijarse en los siguientes elementos: direcciones IP públicamente ruteables, los sistemas en la DMZ (Zona desmilitarizada), interfaces externas del firewall, etc.

Una buena práctica para la identificación de las vulnerabilidades es que el equipo encargado del análisis realice entrevistas en todas las áreas de la organización. Los entrevistados deben estar en su propio ambiente de trabajo ya que de esta manera se podría identificar los puntos débiles del área.

Además, se deben realizar cuestionarios basándose en las amenazas identificadas en los puntos anteriores. Otra práctica, aunque mucho más costosa, que se puede utilizar es la identificación de vulnerabilidades a través del uso de métodos proactivos. Entre los métodos proactivos se pueden citar:

- **Herramientas automatizadas para la búsqueda e identificación de las vulnerabilidades:** software creado para pruebas de seguridad y descubrimiento de las vulnerabilidades de forma automática, generando informes detallados de los problemas y vulnerabilidades identificados en el sistema. Las herramientas automatizadas son capaces de cruzar información, analizarlas y comprobar las vulnerabilidades encontradas de manera eficiente. Tales herramientas han madurado, catalogando en sus bases de conocimiento la mayoría de las vulnerabilidades existente, sin dejar de tener un costo relativamente alto.
- **Evaluación y pruebas de seguridad:** evaluación de la vulnerabilidad es un primer paso de verificación de la vulnerabilidad. Los resultados e información obtenida a través de las evaluaciones se utilizarán para la realización de las pruebas. La evaluación verifica vulnerabilidades potenciales y las pruebas de seguridad tratan de explotarlas.

- **Prueba de invasión:** tiene como objetivo comprobar la resistencia del activo con relación a los métodos de ataques conocidos.
- **Análisis crítico de código:** la identificación de las vulnerabilidades en el código fuente (Páez Parra, 2014).

Para poder registrar las vulnerabilidades se puede usar el siguiente formato:

Tabla 24.

Formato identificación de vulnerabilidades

	Activos	Amenazas	Vulnerabilidades
1			
2			
3			
4			
5			

En el anexo 3 se enlista algunos ejemplos de vulnerabilidades.

4.1.2.1.4. Identificación de las consecuencias

Se pude definir a las consecuencias como el resultado de un incidente o evento que puede tener un impacto en los objetivos de la organización. En esta parte del análisis del riesgo, una consecuencia puede ser, por ejemplo:

- La pérdida de eficacia en el funcionamiento operacional de los sistemas;
- La inestabilidad en el funcionamiento de sistemas;
- Condiciones adversas de operación;
- Pérdida de la oportunidad de negocios;
- Imagen y reputación afectadas;
- Violación de obligaciones reglamentarias;
- Pérdidas financieras;
- La pérdida de datos e información;
- La pérdida de vidas humanas;
- Pérdida de competitividad;

- Entre muchos otros, de acuerdo con los negocios de la organización.

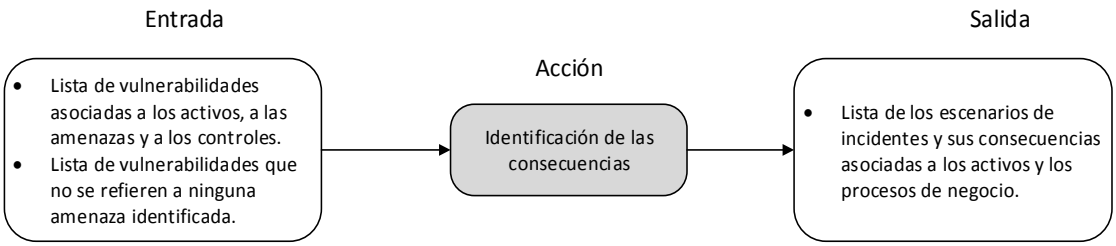

Figura 31. Actividades de las consecuencias.

Tomado de (Páez Parra, 2014)

Esta actividad tiene como objetivo identificar las consecuencias o daños para la organización que pueden ser el resultado de un escenario de incidentes, como resultado de las vulnerabilidades identificadas. La configuración de un escenario de incidentes se considera un defecto de seguridad.

Un escenario no es más que una descripción de una amenaza que explota una o más vulnerabilidades en un incidente de seguridad de la información y puede afectar a uno o más activos o apenas parte de un activo, de acuerdo con los criterios establecidos en la definición contexto. Como ejemplos de consecuencias operacionales se menciona:

- Pérdida de oportunidad;
- Salud y seguridad;
- Tiempo de investigación y tiempo de reparación;
- Tiempo de trabajo perdido;
- Costo financiero para reparar el daño;
- Imagen y reputación (Páez Parra, 2014).

Para registrar las consecuencias se puede utilizar el siguiente formato:

Tabla 25.

Formato para identificación de consecuencias.

	Activos	Amenazas	Vulnerabilidades	Consecuencias
1				
2				
3				
4				
5				

4.1.2.2. Análisis del riesgo

Después de la realización del proceso de identificación del riesgo, se necesita un proceso de asignación de valores a los activos, las amenazas, las vulnerabilidades y las consecuencias. Esto hace que sea posible poner los riesgos en orden de prioridad, para tratarlos de acuerdo con su urgencia o criticidad.

El análisis del riesgo se puede realizar con mayor o menor detalle, en función del riesgo, el objetivo del análisis, y de la información, datos y recursos disponibles. Se deben identificar los factores que afectan a la probabilidad y las consecuencias. Este análisis puede ser cualitativo, cuantitativo, o una combinación de ambos, dependiendo de las circunstancias (Páez Parra, 2014).

4.1.2.2.1. Metodologías

Dos metodologías se pueden utilizar para el análisis del riesgo:

- Análisis cualitativo de riesgos.
- Análisis cuantitativo de riesgos.

4.1.2.2.1.1. Metodología de análisis cualitativo

El análisis cualitativo se basa en la evaluación, a través de atributos calificadores y descriptivos, de la intensidad de las consecuencias y la probabilidad de

ocurrencia del riesgo identificado. En la metodología cualitativa no se asigna valores financieros a los activos, consecuencias o controles, sino que se utilizan escalas de atributos a través de valores descriptivos relativos.

Esta estimación es considerada demasiado subjetiva, siendo ideal para una verificación inicial de los riesgos, cuando no se dispone de suficientes datos numéricos (Páez Parra, 2014).

Ejemplos de uso del análisis cualitativo:

Para probabilidad:

- Alta, media y baja.
- Raro, poco probable, posible, probable y casi cierto.
- Remotamente posible, ocasionalmente, a menudo, varias veces al mes.
- Improbable, probable y cierto.
- Pequeña, mediana y grande.
- Bajo, medio, alto, muy alto y elevado.
- Improbable, remota, ocasional, probable, frecuente.

Para impactos:

- Alta, media y baja.
- Irrelevante, insignificante, marginal, critico, extremo y catastrófica.
- Extremo, alto, medio, bajo y despreciable.
- Grande, mediana, pequeña y banales.
- Trastornos muy graves, graves, limitados, ligeros y muy ligeros (Páez Parra, 2014).

4.1.2.2.1.2. Metodología de análisis cuantitativo

En la metodología de análisis cuantitativo es utilizada una escala de valores numéricos con el objetivo de intentar calcular valores numéricos para cada uno

de los componentes recolectados durante las actividades de identificación del riesgo. Un enfoque cuantitativo se adopta cuando hay un escenario que permita definir los valores financieros, aunque se aproximado de los activos priorizado, así como los impactos. Por ejemplo, se estima que el valor real de cada activo en función del costo de reemplazo o del costo asociado a la pérdida de productividad, y otros valores de acuerdo con el tipo de organización. Esta manera de calcular puede ser empleada para el levantamiento estimado del costo de los controles y otros valores identificados en la etapa anterior. El análisis cuantitativo se debe usar datos históricos y datos precisos y auditables. Si no existe tal información, este tipo de cálculo se convierte en falso (Páez Parra, 2014).

Ejemplos de uso de este análisis cuantitativo:

Para probabilidad:

- 50%;
- 0,2;
- 0,75

Para impactos:

- Valor de reposición del activo: US$ 12.000;
- Valor de mantenimiento del activo;
- Costo de implantación del control;
- Valor de la sanción por incumplimiento de contrato;
- Perjuicio por las horas de inactividad (Páez Parra, 2014).

4.1.2.2.2. Estimación del riesgo

Después de haber realizado la identificación del riesgo, activos, amenazas, vulnerabilidades y consecuencias, se realiza la estimación del riesgo que consta de las siguientes actividades:

- Evaluación del impacto
- Evaluación de la probabilidad de incidentes.
- Estimación del nivel del riesgo.

La figura 32 ilustra la secuencia de las actividades:

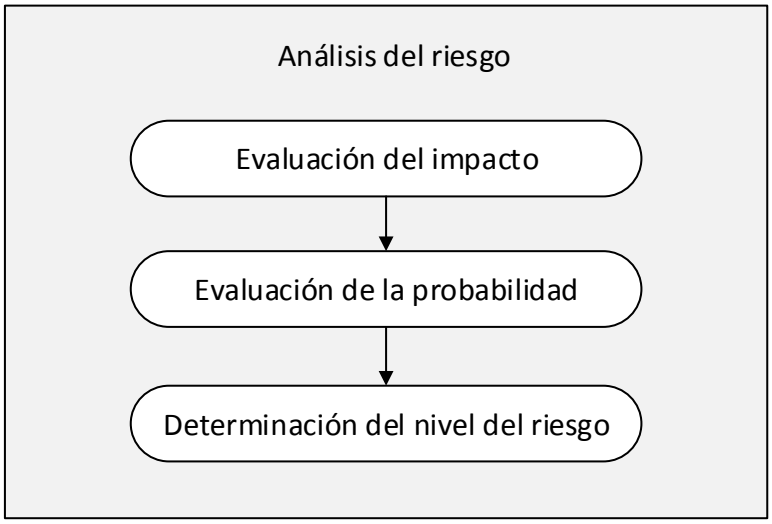

Figura 32. Actividades del análisis del riesgo.

Adaptado de (Páez Parra, 2014)

4.1.2.2.3. Evaluación del impacto

La evaluación del impacto tiene como objetivo principal evaluar los impactos que tendría sobre la organización la materialización del riesgo, teniendo en cuenta las consecuencias de una violación de seguridad de la información, tales como: la pérdida o degradación de la disponibilidad de los activos, la pérdida de la confidencialidad o la pérdida de integridad (DAFP, 2011).

Para esta evaluación, el equipo de análisis tendrá en cuenta los criterios y factores y adoptará una de las metodologías de estimativa: cualitativa o cuantitativa.

- **Entrada:** resultados de la etapa de identificación del riesgo.
- **Acción:** exactamente el desarrollo de la actividad de evaluación de las consecuencias sobre el negocio de la organización.
- **Salida:** lista de las consecuencias relativas a un escenario de incidente, estando relacionado a los activos y criterios de impacto.

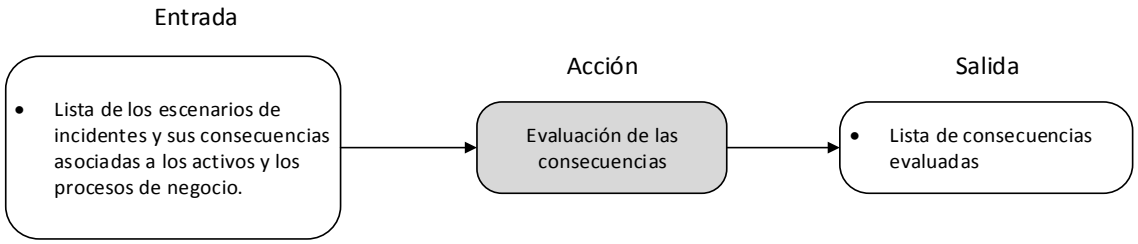

Figura 33. Actividades de la evaluación de las consecuencias.

Tomado de (Páez Parra, 2014)

Una de las primeras acciones es el ordenamiento de los activos de acuerdo con su criticidad e importancia para el logro de los objetivos de negocio de la organización. Es posible hacer esto de dos maneras:

- **A través del valor de reposición del activo:** donde se determina el costo financiero de recuperación o reposición del activo y también del valor de la información que contenga.
- **A través de las consecuencias al negocio:** el valor se determina por el impacto de las consecuencias en los negocios. Normalmente este valor es más significativo que solo el valor del activo.

Es muy importante la valoración de los activos y su clasificación por la criticidad para poder determinar el impacto que tendría un incidente en la organización, ya que el incidente podía afectar a uno o varios activos, por la interdependencia que tiene con los demás activos.

De esta manera, se obtiene una fuerte relación entre la evaluación del impacto con la valoración de los activos. Tomar en cuenta que las consecuencias pueden ser expresadas en términos de criterios monetarios, técnicos, humanos, del impacto en los negocios u otros criterios que la organización considere importante (Páez Parra, 2014).

Según el DAFP en el año 2001 definió que, bajo el criterio de impacto, el riesgo se debe medir a partir de las siguientes especificaciones:

Tabla 26.

Ejemplo de evaluación del impacto

NIVEL	DESCRIPTOR	DESCRIPCIÓN
1	Insignificante	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la entidad.
2	Menor	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad.
3	Moderado	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad.
4	Mayor	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad.
5	Catastrófico	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad.

Tomado de (DAFP, 2011)

4.1.2.2.4. Evaluación de la probabilidad de ocurrencia

Después de la identificación de los escenarios de incidentes y la evaluación del impacto, se debe realizar la evaluación de la probabilidad del riesgo en cada escenario y los impactos correspondientes. En esta actividad es importante utilizar el historial de ocurrencias de incidentes de seguridad.

En la actividad de la evaluación de la probabilidad de incidentes:

- **Entrada**: listas de escenarios de incidentes identificados como relevantes en la actividad de evaluación del impacto.
- **Acción**: evaluación de la probabilidad de ocurrencia de incidentes de seguridad.
- **Salida**: probabilidad de los escenarios de incidentes en el método cuantitativo o cualitativo.

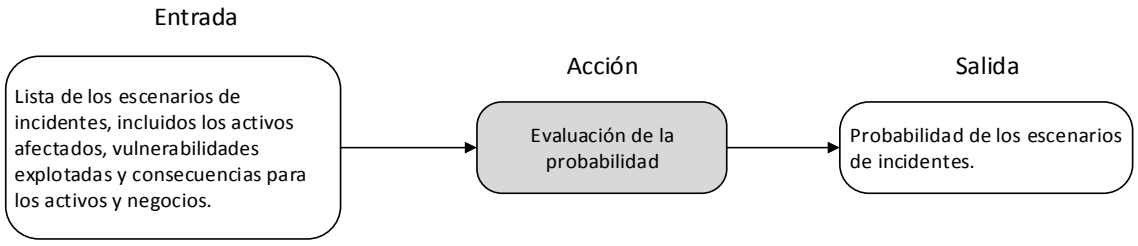

Figura 34. Evaluación de la probabilidad de los incidentes.

Tomado de (Páez Parra, 2014)

Para esta evaluación se utilizan metodologías para el análisis cuantitativo y cualitativo. Para que el equipo estime la probabilidad es necesario realizar el estudio del historial de ocurrencias y estadísticas pasadas, la frecuencia de ocurrencia de las amenazas y de la facilidad con la que las vulnerabilidades pueden ser explotadas.

Según el DAFP en el año 2001 definió que, bajo el criterio de Probabilidad, el riesgo se debe medir a partir de las siguientes especificaciones:

Tabla 27.

Ejemplo de evaluación de probabilidad.

NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
1	Raro	El evento puede ocurrir solo en circunstancias excepcionales.	No se ha presentado en los últimos 5 años.
2	Improbable	El evento puede ocurrir en algún momento.	Al menos de 1 vez en los últimos 5 años.
3	Posible	El evento podría ocurrir en algún momento.	Al menos de 1 vez en los últimos 2 años.
4	Probable	El evento probablemente ocurrirá en la mayoría de las circunstancias.	Al menos de 1 vez en el último año.
5	Casi Seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Mas de 1 vez al año.

Tomado de (DAFP, 2011)

4.1.2.2.5. Determinación del nivel del riesgo

La determinación del nivel del riesgo es una actividad en la cual el equipo de análisis va a medir el nivel el riesgo con el uso de los resultados obtenidos en las etapas anteriores. En esta actividad se confieren valores a la probabilidad e impactos del riesgo. Esta actividad es el inicio de la construcción de la tabla de análisis del riesgo.

En esta actividad de determinación del nivel del riesgo:

- **Entrada**: son las listas de escenarios de incidentes identificados con sus consecuencias y probabilidades en la actividad de evaluación de la probabilidad.
- **Acción**: determinación del nivel del riesgo para todos los incidentes considerados.
- **Salida**: una lista de riesgos con niveles de valores.

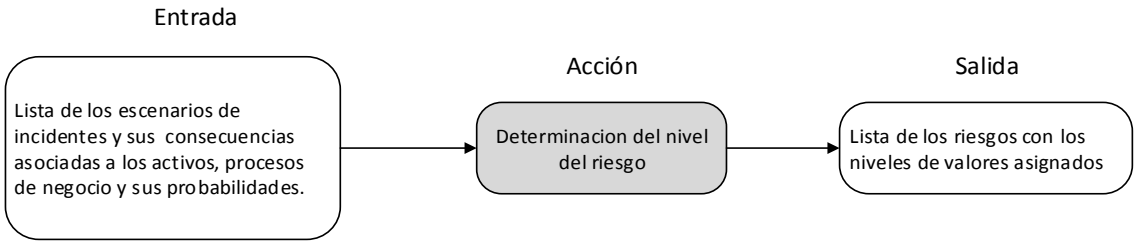

Figura 35. Determinación del nivel del riesgo.

Tomado de (Páez Parra, 2014)

El equipo de análisis deberá elegir el método que más se ajuste a las necesidades del giro de negocio de la organización. Tomando en cuenta que sea de fácil entendimiento para todos los miembros de esta (Páez Parra, 2014).

Un ejemplo de la matriz para la determinación del nivel de riesgo se muestra en la tabla 28:

Tabla 28.

Matriz de calificación, evaluación y respuestas a riesgos

PROBABILIDAD	IMPACTO				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Raro (1)	B	B	M	A	A
Improbable (2)	B	B	M	A	E
Posible (3)	B	M	A	E	E
Probable (4)	M	A	A	E	E
Casi Seguro (5)	A	A	E	E	E
B: Zona de riesgo baja: Asumir el riesgo					
M: Zona de riesgo moderada: Asumir el riesgo, reducir el riesgo					
A: Zona de riesgo Alta: Reducir el riesgo, evitar, compartir o transferir					
E: Zona de riesgo extrema: Reducir el riesgo, evitar, compartir o transferir					

4.1.2.3. Evaluación del riesgo

Cabe recordar que el riesgo es la posibilidad de que se produzca un determinado impacto en la organización. El cálculo del riesgo es tan solo un indicador que está ligado a los valores calculados de la vulnerabilidad y el impacto, y estos a su vez están ligados a la relación entre el activo y la amenaza. Las ecuaciones 2 y 3 serán utilizadas para los cálculos de la probabilidad y del riesgo respectivamente:

$$Probabilidad = Amenaza \times Vulnerabilidad \quad \text{(Ecuación 2)}$$

$$Riesgo = Probabilidad \times Impacto \quad \text{(Ecuación 3)}$$

En esta fase los equipos de análisis en conjunto con la organización deben comparar los riesgos estimados con los criterios de evaluación establecidos durante la fase de contexto. La organización debe tomar decisiones en esta fase en función del nivel del riesgo aceptable. Sin embargo, factores como consecuencias, probabilidad y confianza deben ser considerados para una mejor toma de decisión.

Durante esta evaluación es importante que la organización considere:

- **Las propiedades de seguridad de la información (Confidencialidad, Integridad, Disponibilidad, Autenticidad):** si una de estas propiedades no es importante para la organización, ella podrá considerar como de bajo valor los riesgos que causan vulnerabilidades relacionadas a esta propiedad, y así encuádralos como riesgos aceptables.
- **La importancia de los procesos de negocio o de la actividad soportada por determinado activo o conjunto de activos**: si un proceso o actividad es valorada por la organización como de baja importancia, los riesgos asociados a él deben ser también menos tenidos en cuenta que los riesgos que causan impactos en procesos o actividades más importantes.

Otro punto importante para tener en cuenta durante la evaluación del riesgo es la suma de una serie de riesgos que se consideran pequeños o medianos para, a través de esta agregación, convertirlos en un riesgo total mucho más significativo, y así tratarlos adecuadamente.

En esta fase es importante que los equipos de análisis evalúen los requisitos contractuales, reglamentarios y legales. Esta actividad debe ser realizada en conjunto con la organización, porque sólo ella tiene la visión completa de sus objetivos estratégicos de negocio (Páez Parra, 2014).

Fase de evaluación del riesgo:

- **Entrada**: lista de los riesgos con los niveles de valores y criterios para la valuación del riesgo.
- **Acción**: comparación del nivel del riesgo con los criterios de evaluación.
- **Salida**: lista de riesgos ordenados por priorización, de acuerdo con los criterios de evaluación del riesgo.

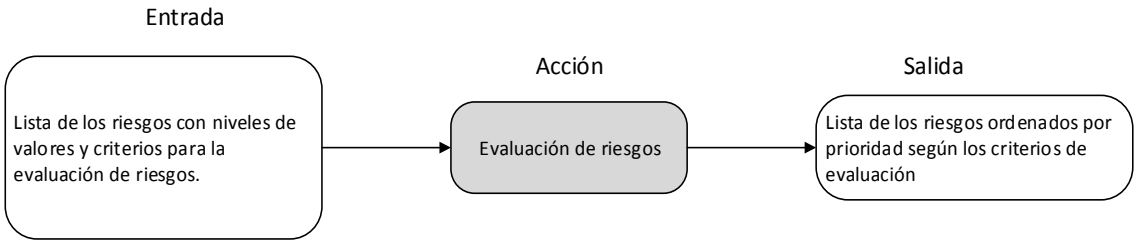

Figura 36. Fase de evaluación del riesgo.

Tomado de (Páez Parra, 2014)

Una vez que ya se han evaluado los riesgos, se debe decidir el tratamiento que se le va a dar al riesgo. Existen cuatro opciones que no son mutuamente excluyentes, es decir, que pueden ser combinadas entre sí:

- **Transferir el riesgo:** compartir el riesgo con una entidad externa, pueden ser los seguros que cubran incidentes.
- **Asumir el riesgo:** de acuerdo con los criterios de aceptación de la organización, es decir, “correr el riesgo”.
- **Reducir el riesgo:** implementar controles que permitan reducir los riesgos a un nivel aceptable.
- **Eliminar el riesgo:** mediante la eliminación de la fuente del riesgo.

Al final de este proceso se espera tener una lista como la siguiente:

Tabla 29.

Ejemplo de lista de evaluación de riesgos.

Riesgos	Calificación		Evaluación	Tratamiento
	Probabilidad	Impacto		

4.2. FASE 2: Análisis del impacto del negocio

Se puede definir al análisis del impacto del negocio, más conocido como BIA, como el proceso para determinar y documentar tanto las funciones como los procesos del negocio de nivel crítico. Asimismo, estimará el impacto financiero y operacional que tendría en la organización si ocurriera algún tipo de interrupción. Además, ayudará a la organización a identificar cual de todos sus productos o servicios son los más rentables y claves para el negocio, por añadidura el tiempo que tardará su recuperación.

Por consiguiente, con toda la información recolectada la organización comprenderá la importancia que tienen las funciones en el negocio, así como también las consecuencias negativas que tendría si alguna de las funciones críticas llegará a fallar. Dicho de otro modo, el BIA es la base para poder elaborar el plan de continuidad del negocio de la empresa u organización (Disaster Recovery, 2017).

4.2.1. Aspectos importantes

4.2.1.1. Preparar el equipo de trabajo

Para poder tener una buena organización y determinación del análisis se deben tomar en cuenta las siguientes recomendaciones:

- Definir los roles que tendrá cada uno de los participantes del equipo de trabajo, trazando claramente sus objetivos y el alcance.
- Definir un cronograma con todas las actividades que se realizarán tomando en cuenta los recursos necesarios que serán utilizados.
- Desarrollar uno o varios mecanismos para la recopilación de los datos.

4.2.1.2. Identificar los participantes

Para poder determinar el enfoque para la recopilación de los datos, se recomienda la selección de varios participantes de la organización, que representen cada una de las funciones de la empresa. Es decir, se necesita integrantes de cada nivel organizacional, los cuales sean representantes confiables de cada área (Hernandez & Galeano, 2016).

4.2.1.3. Métodos para obtención de información

El primero de los pasos para poder iniciar con el BIA es identificar las unidades del negocio de la empresa u organización. Es preciso señalar que el BIA es un proceso de recolección de información permanente, para lo cual se recomiendan algunos métodos como:

- **Encuesta**: En este tipo de método se utilizarán varias preguntas que serán realizadas a todas las áreas de la organización. Con el análisis y recopilación de todas las respuestas se puede llegar a obtener información muy valiosa como funciones, procesos y operaciones del negocio. Además, se identificarán los límites de los tiempos críticos y las prioridades cuando se deban recuperar.
- **Entrevistas**: En este tipo método se obtiene información de manera personal, haciendo entrevistas de forma individual o grupal. Estas entrevistas por lo general se las realiza a personas claves de cada nivel organizacional es decir a los participantes que se identificaron anteriormente.
- **Sesiones de facilitación**: Este método trata principalmente de reuniones con el personal de operaciones del negocio. Estas reuniones facilitarán la validación de la información y datos obtenidos de una manera concurrente. Se recomienda realizar una de estas sesiones si se tiene algún inconveniente al momento de la recolección de datos.

- **Combinación de los métodos**: Se puede utilizar una combinación de todos los métodos vistos anteriormente, con la finalidad de tener una recopilación de datos completa (Hernandez & Galeano, 2016).

4.2.2. Evaluación de impacto financiero y operacional

4.2.2.1. Impacto financiero

Para poder realizar el análisis del impacto financiero se lo debe evaluar de forma cualitativa en todos los casos, ya que por lo general las cifras reales de la organización son consideradas datos o información confidencial.

Según los autores Baños y Carrera, para poder determinar el impacto financiero se debe responder una pregunta muy importante: “Cuál será la magnitud del impacto de pérdida financiera si los procesos del negocio fueses interrumpidos?”(Baños Andi & Carrera Subía, 2010).

Existen varios factores que deben ser considerados para poder realizar una correcta evaluación del impacto financiero que se muestra en la siguiente tabla:

Tabla 30.

Costos considerados en el impacto financiero.

Costos financieros	Costos no financieros
Reducción de ingresos	Pérdida de credibilidad
Pérdida de activos	Requisitos legales, regulatorios y seguridad
Reducción de ganancias	
Pérdida de producción	
Aumento en los costos	
Multas	

4.2.2.2. Impacto operacional

Para realizar un correcto análisis del impacto operacional se debe realizar la clasificación, identificación y evaluación del impacto negativo, que en caso de

que ocurriera una interrupción o indisponibilidad de algún servicio, llegaría a tener la organización (Baños Andi & Carrera Subía, 2010).

Los principales factores que generan el impacto operacional que mencionan los autores Carrera y Baños son los siguientes:

- Falta de confiabilidad operacional de:
    - Equipos de TI
    - Recursos humanos
    - Procesos
    - Mantenibilidad de los equipos
- Suficiencia del servicio prestado
- Eficacia del servicio
- Satisfacción del cliente
- Posicionamiento en el mercado
- Confianza del cliente
- Control de la compañía
- Ética
- Moral, etc.

4.2.3. Requerimientos de tiempo de recuperación

Uno de los objetivos del Bia es ofrecer el tiempo máximo que se demora una organización en recuperarse, en caso de sufrir alguna amenaza. Esta información se divide de la siguiente manera:

- RTO
- RPO
- WRT
- MTD
- MTPoD

A continuación, se analizará más a detalle cada uno de ellos.

4.2.3.1. RTO

Recovery Time Objective, con sus siglas en ingles RTO, es el tiempo máximo en el que cada organización tiene para recuperar sus recursos o sistemas en caso de haber sufrido alguna alteración, al menos con sus niveles mínimos. Su principal objetivo es que la organización no tenga pérdidas financieras ni operacionales, por el contrario, lo que se espera es que pueda estar operando en un nivel normal todos sus servicios y procesos (MINTIC).

El RTO se lo realiza por proceso, y debe ser en lo posible, un valor mucho menor al tiempo máximo de interrupción que pueda soportar la organización.

4.2.3.2. RPO

Recovery Point Objective, con sus siglas en ingles RPO, es el punto antes de que ocurra el incidente, que sirve para determinar la pérdida de datos medida en términos de un periodo de tiempo que puede ser tolerado es decir la información que la organización está dispuesta a perder o recuperar manualmente(Baños Andi & Carrera Subía, 2010).

El RTO es considerado como el ultimo *backup* realizado antes del evento. Este respaldo será utilizado para restaurar las aplicaciones o sistemas que fueron afectados por el incidente.

4.2.3.3. WRT

Work Recovery Time, con sus siglas en ingles WRT, es el tiempo que se tiene para poder recuperar los datos, servicios y procesos, una vez que los sistemas han sido reparados (Hernandez & Galeano, 2016).

4.2.3.4. MTD

Máximun Tolerable Downtime, con sus siglas en ingles MTD, es el tiempo máximo de inactividad que la organización puede tolerar, sin tener pérdidas financieras y operacionales (Hernandez & Galeano, 2016).

4.2.3.5. MTPoD

Maximun Time Periodo of Disruption, con sus siglas en ingles MTPoD, es el plazo máximo de tiempo de interrupción, desde el momento que ocurre el incidente hasta el límite del RTO (MINTIC).

En el caso de que la organización supere el límite de tiempo establecido en el RTO y no logre restablecer sus servicios y procesos, al menos en sus niveles mínimos aceptables, esto es considerado como amenaza.

4.2.4. Metodología del análisis del impacto del negocio

La metodología del análisis del impacto de negocio define una serie de pasos para poder identificar los impactos de las interrupciones e incidentes. Para así, poder tomar decisiones sobre los procesos considerados como críticos para la organización y que afecten al giro de negocio (MINTIC).

A continuación, en la figura 37 se muestran los pasos de la metodología:

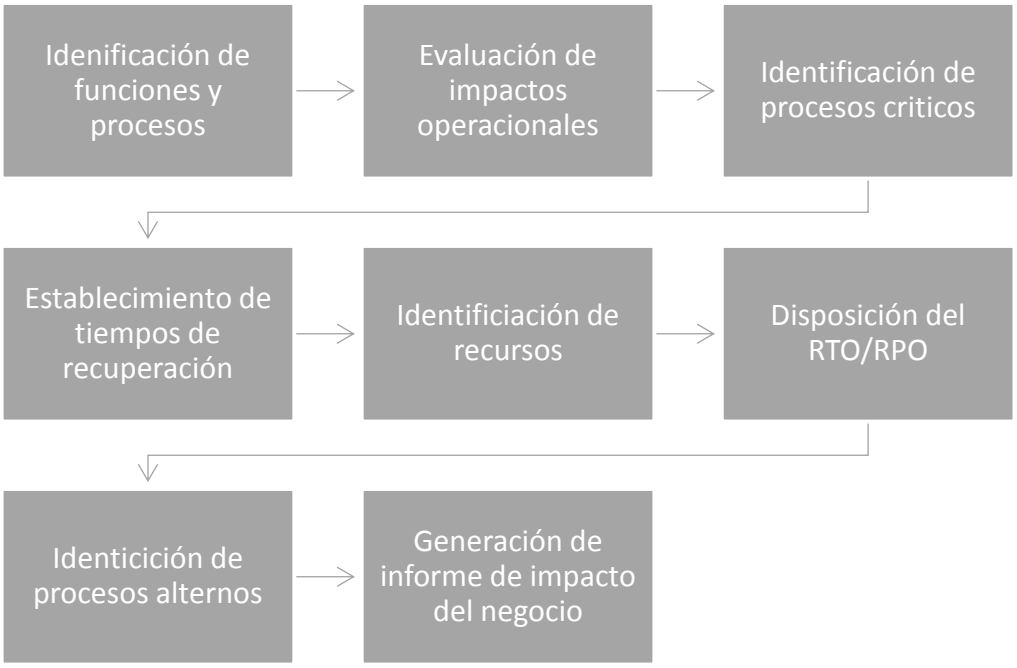

Figura 37. Metodología del análisis del impacto del negocio.

4.2.4.1. Identificación de funciones y procesos

En este paso de deben identificar las funciones del negocio que serán utilizadas para lograr alcanzar los objetivos de Sistema de Gestión de Seguridad de la información también conocido con el acrónimo SGSI.

Al final de este paso se obtendrá como resultado un listado donde constarán los roles y procesos, que servirán en los siguientes pasos para el análisis del impacto del negocio (MINTIC).

Para la obtención de datos se puede utilizar la siguiente tabla:

Tabla 31. Formato para la identificación de funciones y procesos

Procesos del negocio	Subprocesos del negocio	Roles	Responsabilidades

4.2.4.2. Evaluación de impactos operacionales

El impacto operacional permite a la organización evaluar el nivel negativo de una interrupción en varios aspectos de las operaciones del negocio. Para lo cual se han establecido unas métricas para evaluar el impacto, con los siguientes niveles: A, B y C (MINTIC).

- **Nivel A**: “La operación es crítica para el negocio. Una operación es crítica cuando al no contar con esta, la función del negocio no puede realizarse”.
- **Nivel B**: “La operación es una parte integral del negocio, sin esta el negocio no podría operar normalmente, pero la función no es crítica”.
- **Nivel C**: “La operación no es una parte integral del negocio”.

Para realizar la evaluación de impactos operacionales se puede utilizar el siguiente formato:

Tabla 32.

Formato para la evaluación de impactos operacionales.

Procesos del negocio	Subprocesos del negocio	Nivel de impacto	Observaciones

4.2.4.3. Identificación de procesos críticos

Para poder identificar los procesos críticos de la organización se debe basar en la clasificación de los impactos operacionales realizados en el ítem anterior, según la siguiente tabla:

Tabla 33.

Identificación de procesos críticos.

Valor	Interpretación del proceso crítico
A	Crítico para el negocio, la función del negocio no puede realizarse

B	No es crítico para el negocio, pero la operación es una parte integral del mismo
C	La operación no es parte integral del negocio.

Tomado de (MINTIC)

4.2.4.4. Establecimiento de tiempos de recuperación

Después de identificar los procesos críticos de la organización, se realiza la identificación del MTD, que es el tiempo máximo tiempo de inactividad que puede tolera una organización y se jerarquiza de acuerdo con las prioridades de recuperación. Es decir, se les otorga mayor prioridad a los procesos que tienen menor tolerancia a la inactividad (Hernandez & Galeano, 2016).

Se puede utilizar el siguiente formato para establecer los tiempos de recuperación:

Tabla 34.

Formato de establecimiento de tiempos de recuperación.

Procesos críticos	Prioridad de recuperación	MTD (Días)	Observaciones

4.2.4.5. Identificación de recursos críticos

Cada función critica del negocio está conformada por varias actividades, estas deben ser consideradas de vital importancia en el momento de evaluar los procesos críticos del negocio. Por lo tanto, en este punto se deben identificar los recursos críticos del sistema para así poder tomar acciones que nos permitan medir el impacto del negocio en la organización.

Utilice el siguiente formato para identificar los recursos:

Tabla 35.

*Formato para identificación de recursos críticos***.**

Procesos críticos	Recursos críticos	Observaciones

4.2.4.6. Disposición de los RTO/RPO

En este punto el principal objetivo es determinar el tiempo que se requerirá disponer de un servicio, el cual ha estado fuera de uso como consecuencia de un incidente, y que está impidiendo dar una alta disponibilidad y una continuidad de negocios a la organización.

Para poder medir este tiempo se debe tomar en cuenta desde el momento que el servicio estuvo fuera de operación, es decir el momento del incidente, hasta que se retome nuevamente su funcionamiento, dicho de otro modo, se calcula el RTO, RPO y WRT.

Tabla 36.

Formato para disposición de RTO, RPO y WRT.

Procesos críticos	Recursos Críticos	MTD (Días)	RTO (horas)	WRT (horas)	RPO (horas)

4.2.4.7. Identificación de procesos alternos

Las organizaciones deben tener preparado procesos alternos en caso de que se presente algún incidente o interrupción, de manera que los procesos del negocio puedan seguir operando. Para lo cual se deben usar métodos alternativos de manera temporal, es decir, procedimientos manuales que ayuden a superar la crisis que ha generado el incidente dando una continuidad en el negocio.

Tabla 37.

Formato para identificación de procesos alternos.

Procesos del negocio	Procesos alternos	Observaciones

4.2.4.8. Generación de informe de impacto del negocio

El BIA finaliza con la generación de informe el cual se presenta toda la información que se obtuvo de los tiempos de recuperación y recursos críticos del negocio para que la organización no sufra de un colapso financiero ni operacional, utilizando varias estrategias alternativas para garantizar la continuidad del negocio.

El informe del impacto del negocio debe contener lo siguiente como mínimo:

- Listado de los procesos críticos.
- Listado de prioridades de recursos, sistemas y aplicaciones de TI.
- Listado de los MTD y criticidad de cada uno de los procesos.
- Listado de los RTO.
- Listado de los RPO.
- Listado de los WRT.
- Listado de procesos alternos.

4.3. FASE 3: Selección de la estrategia

Según la ISO 22301, la selección de estrategias se trata básicamente de la elaboración de un plan genérico de emergencias. Es decir, crear un plan alternativo que garantice la continuidad del negocio, este plan puede contener la definición de las estrategias para garantizar la restauración de los procesos

críticos de la organización en un periodo menor al definido anteriormente (ISO 22301, 2012).

No existe un modelo fijo de estrategia, sino que depende totalmente de cada organización. Independientemente de la estrategia que se escoja, para asegurar una continuidad en el negocio siempre se debe contar con un centro alternativo, propio o subcontratado.

4.3.1. Centro alternativo

Para empezar, se definirá a un centro de control como un lugar donde se realizan reuniones con todo el equipo encargado de la continuidad del negocio de la organización. En este lugar se toman decisiones, se coordina y se planifica todo acerca de los riesgos del negocio.

Dentro de los centros alternativos, se deben elegir un tipo de centro según la criticidad de los procesos y de los tiempos de recuperación obtenidos en la fase de análisis del impacto.

- **Centro frio:** se trata de una sala que contiene todos los equipos informáticos necesarios para poder brindar los procedimientos alternativos. Este tipo de centro está acondicionado perfectamente para soportar este tipo de equipamiento.

- **Centro caliente:** se trata de una locación con un Data Center que se encuentra perfectamente configurado para poder brindar el servicio, es decir, tiene una disponibilidad en pocas horas.

- **Centro espejo:** se trata de dos instalaciones configuradas de manera idéntica que deben estar actualizadas permanentemente. Su principal objetivo es que si una llega a fallar la otra se hace cargo inmediatamente de brindar los servicios.

- **Centro móvil:** se trata de un contenedor que se encuentra acondicionado y equipado, que puede ser rápidamente configurado para recuperar los servicios críticos de la organización. Muy útiles para obtener un sitio rápidamente en casos de emergencia, hay que tener en cuenta que su espacio es muy limitado.

4.3.1.1. Localización dentro de la organización

Por lo general, las organizaciones cuentan con más de un centro de procesos de datos, una estrategia es que uno de estos centros funcione como respaldo y ayuda de otro. Es decir, utilizar la misma infraestructura de la organización, pero para almacenar diferentes respaldos.

Para lograr esto se necesita de mucha planificación ya que se debe tener en cuenta que deberían estar ubicados lo suficientemente lejos para que los dos no sean afectados por el incidente, pero a su vez, la recuperación de datos no debe tomar más del tiempo establecido.

4.3.1.2. Acuerdos recíprocos

Dentro de estos acuerdos, también llamados de ayuda mutua, se realizan acuerdos con otras organizaciones que tengan el mismo giro de negocio o parecido. Además, deben contar con instalaciones de hardware y software compatibles, lo que permitirá recuperar algunos procesos en la otra localización.

Para lograr este tipo de acuerdo, debe existir un documento legal donde se especifican todos los términos y condiciones, afirmando que ambas empresas estén totalmente de acuerdo.

4.3.1.3. Acuerdos con proveedores de equipos

Algunos proveedores de equipos ofrecen el servicio de respaldo. De la misma forma que en los casos anteriores estos deben estar reflejados en un documento legal.

4.3.1.4. Empresas de servicio

Se contrata espacios alternativos a empresas dedicadas a este tipo de sitios. Estas empresas brindan el servicio de *backup* temporal. De esta manera, se puede recuperar los procesos principales de la organización. Estas empresas especializadas cuentas con varias alternativas, se debe elegir la que más se ajuste a la organización.

4.3.2. Comunicaciones alternativas o trabajo remoto

Dependiendo del alcance del incidente, muchas veces se necesita trabajar desde lugares exteriores a la organización por medio de conexiones remotas. Para lo cual se requiere disponer de una red de comunicaciones alternativas.

4.3.3. Procedimientos de backup

La mayoría de las organizaciones tienen un departamento especializado en realizar las copias de seguridad de todas las áreas. Pero esto no es suficiente, por lo que se recomienda que un encargado de cada área realice sus propias copias de seguridad y estas sean almacenadas en un centro externo.

4.3.4. Centro de almacenamiento externo

Este es uno de los puntos más importantes, ya que absolutamente todas las organizaciones sin importar su giro de negocio, debe tener sus copias de seguridad fuera del área de riesgos de su *Data Center*.

Para lo cual existen dos soluciones que son:

- **Solución propia:** Esta es considerada la solución más costosa ya que se requiere un espacio dedicado y acondicionado, una logística de traslado y personal especializado dedicado a la gestión del almacenamiento externo. Pero también es una de las soluciones más efectivas por su accesibilidad y rapidez de recuperación.

  Si la organización decide implementar esta solución para tener un sitio de almacenamiento externo se recomienda las siguientes condiciones:

  - Accesibilidad
  - Resistencia al fuego;
  - Temperatura controlada;
  - Humedad controlada;
  - Resistencia de aplastamiento;
  - Hermeticidad ante gases;
  - Hermeticidad ante agua;
  - Sistema de detección;
  - Sistema de extinción;
  - Cierre rápido;
  - Protección contra el robo (Martinez, 2010).

- **Solución externa:** Existen compañías dedicadas al almacenamiento de respaldos y copias de seguridad. Para asegurar un servicio confiable se debe exigir entre otras condiciones:

  - **Requisitos de instalaciones:** Vigilancia, soportes presurizados, sistema de extinción de incendios, redundancia en fuentes eléctricas, etc.
  - **Requisitos de transporte:** Vehículos con aire acondicionado, contenedores, transporte con comunicación con la base, etc.
  - **Requisitos de servicio:** Alta disponibilidad, Cobertura de seguro adecuada, software de administración y logística integrados, Confidencialidad, etc.

Cualquier opción de estrategia se debe considerar otros factores que influyen mucho en la toma de decisiones como: costos, hardware, software, recursos requeridos tanto técnicos como humanos. Pero sobre todo se debe tomar en cuenta que mientras menor sea el tiempo de recuperación mayor será el costo.

4.4. FASE 4: Ejecución y desarrollo del plan

Después de seleccionar la estrategia se debe definir los procedimientos para poner en marcha el plan de continuidad del negocio. Esta fase constara de las siguientes actividades:

- Organización de equipos de recuperación
- Funciones de los equipos
- Plan de acción
- Procedimientos de emergencia
- Procedimientos de respuestas
- Procedimientos de recuperación
- Plan de vuelta a la normalidad

4.4.1. Organización y funciones de los equipos de recuperación

Un equipo de recuperación se podría definir como un grupo de personas que tendrán la responsabilidad de realizar una serie de actividades del plan de continuidad del negocio para lograr obtener un proceso de recuperación favorable.

Cada equipo estará compuesto por un jefe, un suplente y un grupo de personas. Cabe recalcar que un grupo puede estar compuesto por una sola persona, y que una persona puede pertenecer a uno o más equipos, en caso de que se lo requiera.

Dependerá totalmente de cada organización, el número y funciones de los equipos ya que se deberán ajustar a las necesidades de cada una. Con el fin de

orientar y ejemplificar, se enlistarán algunos tipos de equipos que se creen necesarios para cualquier organización (Martinez, 2010).

- **Equipo de gestión de incidentes**: Este equipo estará conformado por los jefes de todos los equipos restantes de la organización, y estará dirigido por una persona que se encuentre en un nivel jerárquico alto para que pueda tomar decisiones dentro de la empresa. Sus principales funciones se muestran a continuación.

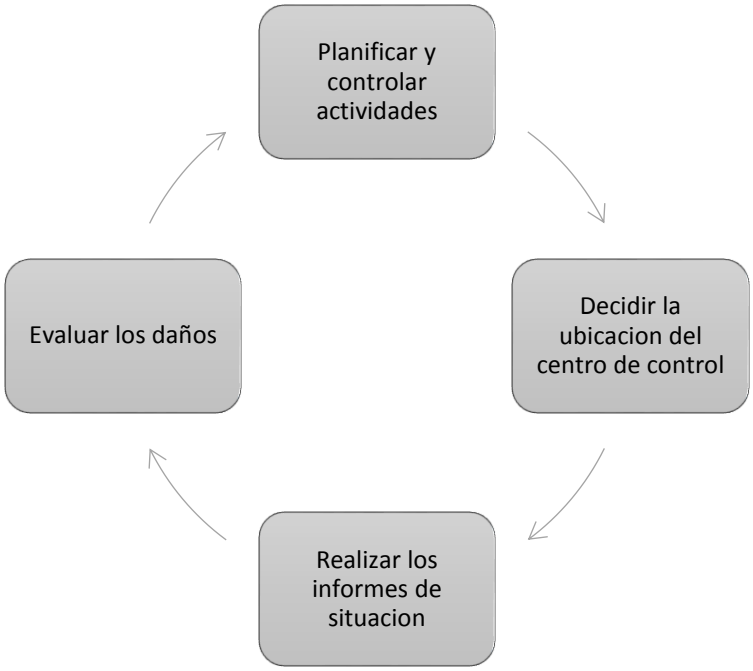

Figura 38. Funciones del equipo de gestión de incidentes.

Para poder obtener una lista con todos los miembros del equipo de gestión de incidentes se recomienda usar el siguiente formato:

Tabla 38.

Formato para miembros del equipo de gestión de incidentes.

Miembros del equipo de gestión de incidentes				
Nombres y Apellidos	**Cargo (dentro de la operadora)**	**Teléfono y extensión**	**Teléfono móvil**	**Email**

- **Equipo de operaciones informáticas**: Este equipo tiene como principal responsabilidad la de restablecer todas las instalaciones informáticas después de ocurrir el incidente. Sus funciones básicas se muestran en la siguiente figura.

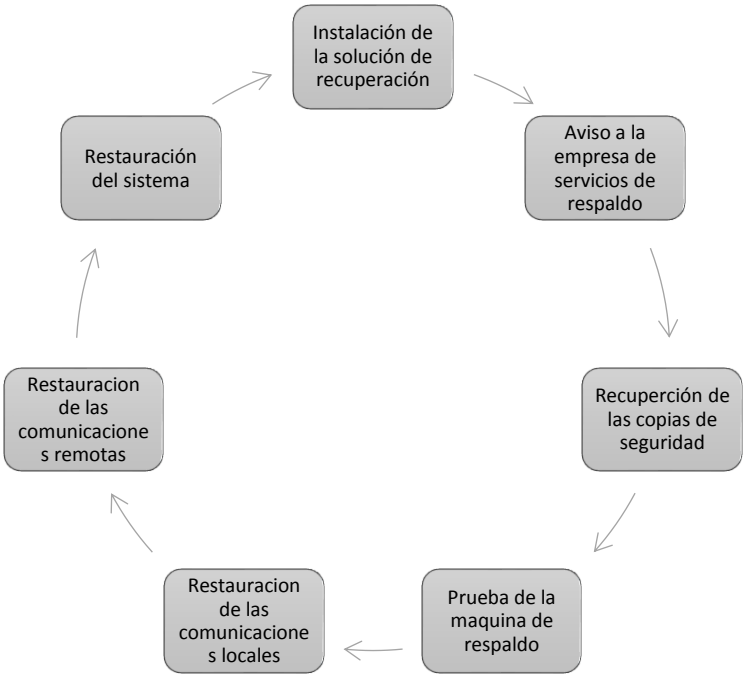

Figura 39. Funciones del equipo de operaciones informáticas

Para poder obtener una lista con todos los miembros del equipo de operaciones informáticas se recomienda usar el siguiente formato:

Tabla 39.

Formato para miembros del equipo de operaciones informáticas.

Miembros del equipo de operaciones informáticas				
Nombres y Apellidos	**Cargo (dentro de la operadora)**	**Teléfono y extensión**	**Teléfono móvil**	**Email**

- **Equipo de administración**: Este equipo tiene la principal responsabilidad de provisionar de recursos a los demás equipos. Sus funciones básicas se muestran en la siguiente figura.

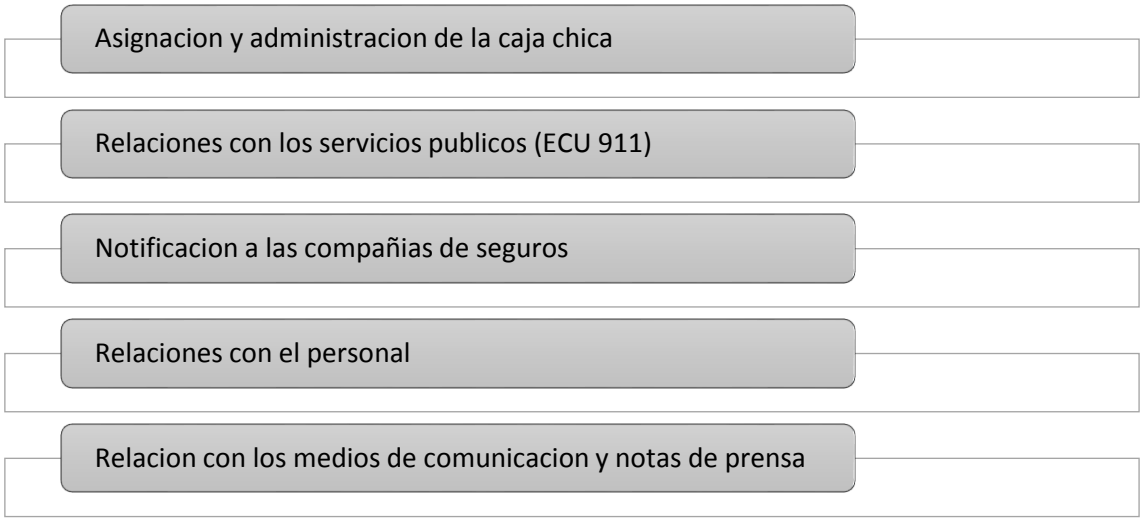

Figura 40. Funciones del equipo de administración

Para poder obtener una lista con todos los miembros del equipo de administración se recomienda usar el siguiente formato:

Tabla 40.

Formato para miembros del equipo de administración.

Miembros del equipo de administración				
Nombres y Apellidos	**Cargo (dentro de la operadora)**	**Teléfono y extensión**	**Teléfono móvil**	**Email**

- **Equipo de atención a usuarios**: Este equipo se encargará de comunicar a los departamentos usuarios por medio de boletines informativos sobre

todo el proceso de recuperación. En el caso de que exista algún cambio en el proceso de restauración, este equipo es el responsable de tomar esa decisión.

Para poder obtener una lista con todos los miembros del equipo de atención a usuarios se recomienda usar el siguiente formato:

Tabla 41.

Formato para miembros del equipo de atención a usuarios.

Miembros del equipo de atención a usuarios				
Nombres y Apellidos	**Cargo (dentro de la operadora)**	**Teléfono y extensión**	**Teléfono móvil**	**Email**

- **Equipo de inmuebles**: Este equipo tiene la responsabilidad de reconstruir y reacondicionar las salas. Para realizar esto, el equipo debe contactarse con los subcontratistas y suministros.

Para poder obtener una lista con todos los miembros del equipo de inmuebles se recomienda usar el siguiente formato:

Tabla 42.

Formato para miembros del equipo de inmuebles.

Miembros del equipo de inmuebles				
Nombres y Apellidos	**Cargo (dentro de la operadora)**	**Teléfono y extensión**	**Teléfono móvil**	**Email**

- **Equipo de servicios generales**: Este equipo tiene la responsabilidad de dar soporte de servicios auxiliares que sean necesarios para la recuperación de las áreas afectadas.

Para poder obtener una lista con todos los miembros del equipo de servicios generales se recomienda usar el siguiente formato:

Tabla 43.

Formato para miembros del equipo de inmuebles.

Miembros del equipo de servicios generales				
Nombres y Apellidos	**Cargo (dentro de la operadora)**	**Teléfono y extensión**	**Teléfono móvil**	**Email**

Para tener claro las funciones que debe realizar cada equipo de recuperación se debe seleccionar muy bien de que se va a ocupar cada equipo, lo más claro posible y teniendo en cuenta que no existan ambigüedades para evitar fallos en la realización del plan de continuidad del negocio.

Se recomienda realizar la siguiente tabla para especificar las funciones de cada equipo de recuperación:

Tabla 44.

Formato para funciones de los equipos de recuperación.

Funciones del Equipo de gestión de incidentes	
Función N.º	**Descripción de a función**

4.4.2. Plan de acción

En esta sección se procede a la activación del plan, esta decisión la toma el jefe del equipo de gestión de incidentes. En el caso de que se afirme la puesta en marcha del plan se inicia la ejecución de los procedimientos indicados, se desarrolla el plan de acción y se moviliza al personal apropiado (Martinez, 2010).

4.4.2.1. Definición de desastres

Para poder poner en marcha el plan de continuidad del negocio se debe conocer el nivel del desastre al que se está enfrentando la empresa en función del tiempo de interrupción de los procesos. Para lo cual se tiene la siguiente figura como referencia:

Desastre menor	Desastre mayor	Desastre catastrófico
• Desastre que provoca una parada en sus procesos que no supere las 4 horas.	• Desastre que provoca una parada en sus procesos mayor a 4 horas y menor a 24 horas.	• Desastre que provoca una parada en sus procesos por más de un día y que no supere una semana

Figura 41. Definición de desastres

4.4.2.2. Procedimientos para la continuidad del negocio

Lo principal dentro del plan de acción para que exista una correcta continuidad en el negocio es notificar de manera inmediata a la persona responsable sobre la ocurrencia de cualquier tipo de incidente. De esta manera, el encargado del plan tomará acciones rápidas, realizando los procedimientos señalados anteriormente por el equipo responsable.

Se ha dividido estos procedimientos en tres grupos:

- **Procedimientos de emergencia**: se trata de procedimientos que se realizan inmediatamente de la ocurrencia del incidente, lo que busca es proteger la integridad de las personas, evitar la propagación del incidente y parar el incidente si es posible. Algunos ejemplos son:
    - Notificación de primera alerta
    - Escalado de problemas
    - Ejecución del plan
    - Informe de emergencia
    - Evaluación de daños
- **Procedimientos de respuesta**: se trata de actuaciones que las realiza cada departamento en caso de algún incidente que sustituyen los procedimientos habituales por alternativos, lo que permite atender necesidades críticas de manera inmediata. A continuación, unos ejemplos:
    - Coordinación de actuaciones por el equipo de gestión de incidentes.
    - Procedimientos de cada departamento de la organización.
    - Procedimientos de traslado de personas y recursos.
    - Procedimientos de utilización del centro de control.

- **Procedimientos de recuperación**: se trata de actividades que tienen que ver con los sistemas de información. Es decir, los procedimientos que permiten la reutilización de los datos, aplicaciones, sistemas, etc. Por lo general, estos procedimientos toman más tiempo para ser puestos en marcha. Algunos ejemplos son:
    - Coordinar la preparación del lugar de recuperación
    - Traslado al centro de respaldo
    - Procedimientos de gestión y soporte
    - Procedimientos de restauración del sistema operativo
    - Procedimientos de restauración de datos

- Procedimientos de restauración de aplicaciones

4.4.3. Plan de vuelta a la normalidad

El plan de vuelta a la normalidad o fase de vuelta a la normalidad es una actividad que está dirigida hacia el desarrollo y establecimiento de varias acciones, con la finalidad de regresar al estado normal de las actividades de la organización.

El principal objetivo de este plan es que una vez que se reanuden las operaciones críticas de la organización no exista un riesgo adicional. Para poder obtener este resultado se debe planificar minuciosamente las actividades de vuelta a la normalidad. Para lo cual, se pueden realizar las siguientes acciones:

- Realizar una reunión con el equipo de gestión de incidentes, para planificar la restauración de los procesos críticos en los centros alternativos. Además, se tocarán temas como las estrategias temporales de regreso.
- Cada equipo de recuperación realizará una reunión para revisar y actualizar los procedimientos de la continuidad del negocio.
- Todos los equipos de recuperación participantes deberán desarrollar, aprobar y revisar un programa final que contenga una valoración de los equipos e instalaciones dañados por el evento.
- Poner en marcha todos los procedimientos de vuelta a la normalidad que han sido modificados de esta manera se podrá reanudar las operaciones.

4.5. FASE 5: Plan de evaluación y mantenimiento

Contar con un plan de continuidad del negocio no garantiza que la organización estará fuera de peligro, para lo cual se recomienda poner a prueba los planes e instalaciones para así poder garantizar que se cumplan los requerimientos mínimos fundamentales que necesita la organización para seguir prestando sus servicios.

No basta con tener el plan de continuidad, sino saber si realmente este funciona y cumple las necesidades esperadas por todo el equipo de recuperación. Para esto se realizan pruebas constantemente y se definen los procedimientos de mantenimiento que tendrá el plan.

Después de cada prueba realizada se recomienda actualizar el plan, aumentando o disminuyendo los cambios efectuados en el mismo y este a su vez debe ser aprobado nuevamente por todos los responsables de la gestión de la continuidad de la organización. La principal idea de esta fase es la mejora continua del plan, intentando no dejar brechas vacías.

4.5.1. Plan de evaluación

Los planes de evaluación o pruebas se deben llevar a cabo periódicamente, al menos una o dos veces al año, según las necesidades de la organización. Estas pruebas, deben estar basadas en escenarios reales y en incidentes que sean comunes dentro de la organización.

Los objetivos y beneficios principales de la realización de un plan de evaluación son las siguientes:

- Validación de los planes de continuidad de negocio mediante la capacitación, y conocimiento de los equipos responsables de la continuidad del negocio.
- Asegurarse de que se cumplirán con los tiempos de críticos establecidos por la organización como el RTO y RPO.
- Actualización de los planes en caso de que se necesite mejorar algunos procedimientos o por cambios existentes en la organización.
- Asegurarse de que los planes de continuidad del negocio cumplen con las funciones requeridas.
- Verificar la capacidad de recuperación de los planes.

Uno de los procesos más simples y recomendados por otras organizaciones para la verificación de los planes de continuidad es el modelo PDCA (Plan-Do-Check-Act) como se muestra en la figura 42.

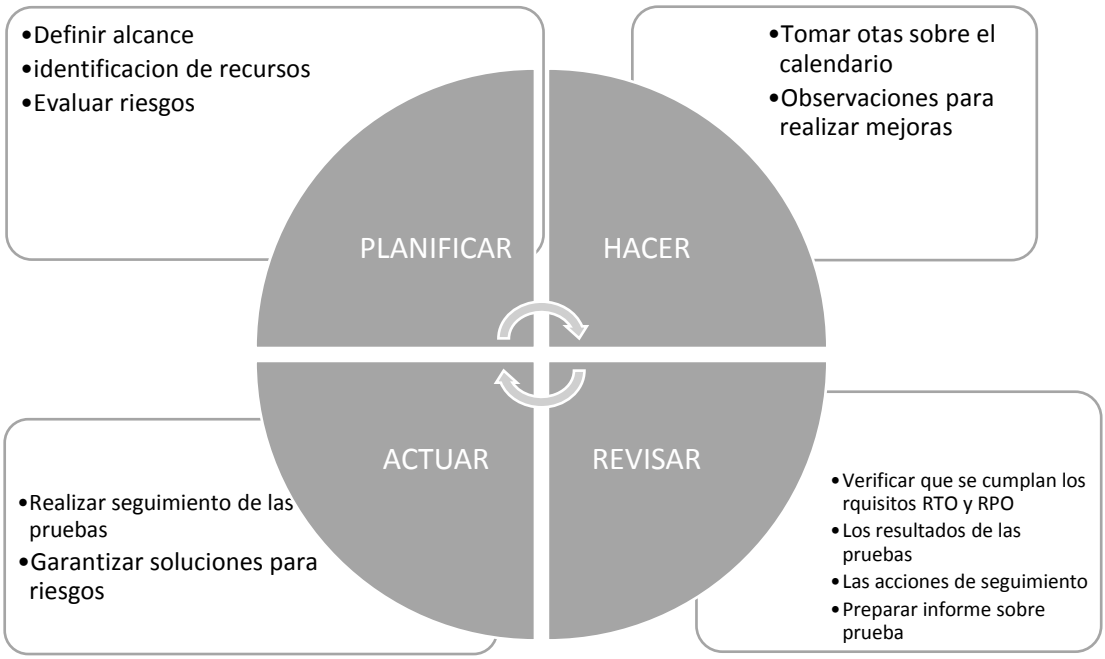

Figura 42. Proceso de verificación del plan de continuidad de negocio

El plan de evaluación debe constar como mínimo de los siguientes elementos:

- **Revisiones periódicas**: su objetivo es verificar y comprobar que el plan aun cumpla con las premisas de partida. Es decir, si existen nuevas funciones críticas, si hay disponibilidad de los recursos de recuperación, si los tiempos de recuperación aún son apropiados para la organización, etc.
- **Ejercicios de entrenamiento**: se trata de reuniones con todos los jefes y suplentes de los equipos de recuperación, en donde su objetivo es volver a familiarizarse y entrenarse sobre las estrategias y procedimientos de recuperación del plan. Por lo general se trata de varias actividades como, banco de preguntas, lecturas sobre el plan y encuestas que deben ser realizadas por cada persona que interviene en el proceso de continuidad.

- **Pruebas técnicas**: para asegurar la efectividad del plan se recomienda realizar pruebas técnicas anuales, están pueden estar compuestas por restaurar y comprobar la idoneidad de todos los *backups*, verificar la disponibilidad de los suministradores de los recursos críticos, etc.

4.5.2. Mantenimiento

Las organizaciones están en un cambio constantes de personal, infraestructura, tecnología, procesos, productos y servicios. Por lo que es muy importante que los planes de continuidad del negocio estén vigentes con todos esos cambios efectuados.

Cada cambio realizado en la organización debe ser analizado para verificar si afecta la capacidad de recuperación de la empresa establecida anteriormente. Ya que una modificación en sus procesos o el ingreso de un nuevo producto puede cambiar totalmente el análisis del impacto, o los procesos y subprocesos que antes no eran críticos, después del cambio lo pueden ser, o también los tiempos de recuperación como el RTO y RPO pueden modificarse.

Cada equipo de recuperación es responsable de mantener el plan al día y comprobar que sea preciso y completo. Para lo cual se realizan revisiones y validaciones de las necesidades y estrategias para después realizar las actualizaciones correspondientes. Existen dos tipos de revisiones que se pueden utilizar:

- **Evaluaciones**: se trata de revisar los procedimientos que se establecieron en la estrategia del plan de continuidad del negocio para comprobar que funcionan correctamente y que tengan una adecuada aplicación dentro de la organización. Existen muchas empresas dedicadas a las evaluaciones de la continuidad del negocio que por lo general es una buena recomendación.

- **Auditorias**: se trata de verificar que el proceso del plan de continuidad de negocio se haya seguido de manera correctamente. Las auditorias pueden ser realizadas de manera interna o externa, donde la externa es la más recomendada ya que lo realiza una entidad especializada con profesionales que se apegan a reglamentos y normas legales, que están fuera de la propia organización y se evitarían las auto-auditorias (Martinez, 2010).

Al finalizar las pruebas y el mantenimiento se recomienda que el plan de continuidad sea distribuido a todo el personal que participa en el proceso de recuperación para que se mantengan informados.

La información que contiene el plan de continuidad del negocio debe ser manejada de carácter confidencial para la organización, por lo tanto, al existir un cambio en los miembros de los equipos, las personas desplazadas deben devolver toda la información correspondiente a los procesos de recuperación. Firmando y aceptando documentos que acrediten que no retienen alguna copia del PCN.

5. CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

Después del desarrollo del presente trabajo de investigación, se concluye que un plan de continuidad de negocio es una parte fundamental dentro de cualquier organización; independiente de su tamaño y actividad; ya que, de éste dependerá gran parte el aseguramiento de la información, protegiéndola contra los riesgos; a más de que la operadora sabrá cómo actuar ante cualquier tipo de incidente; afianzando siempre la disponibilidad, integridad y confidencialidad de dicha información.

Se propuso una guía para el desarrollo de planes de continuidad de negocio de TI, enfocada a las operadoras móviles de Ecuador, basándose en normas y estándares, tanto nacionales como internacionales, que están relacionadas con la seguridad de la información, gestión del riesgo, gestión de la continuidad del negocio etc., por ejemplo; la ISO 27001, ISO 22301, ISO 27005, ISO 27031 y la norma nacional que regula la presentación de planes de contingencia emitido por la ARCOTEL.

El principal objetivo de esta guía es brindar un formato o una base con los requerimientos mínimos que necesita un plan de continuidad de negocio, para que las operadoras móviles de Ecuador puedan basarse y realizar sus propios planes, acoplándose a sus propias necesidades; pero a su vez sometiéndose al cumplimiento de las leyes nacionales; evitando así, algún tipo de sanción por parte de los entes reguladores. Sobre todo, esta guía evitará que sus servicios sean interrumpidos o eliminados, en caso de que ocurriera algún tipo de incidente, beneficiando así directamente a los usuarios y por ende a la misma organización.

Se determinó la importancia de que las organizaciones cuenten con sus propios planes de continuidad de negocio; para que de esta manera tengan la capacidad

de saber cómo recuperar y restaurar sus funciones críticas, ya sea de una forma parcial o total, y que esta recuperación se la realice dentro de los tiempos establecidos. Lo más importante de esta guía, es que cada operadora puede desarrollar sus propios planes según sus necesidades, ya que ninguna organización es igual a otra.

Adicionalmente, se realizó un análisis de la criticidad de las amenazas naturales a nivel país; donde se determinó cuáles son las zonas más vulnerables con mayor impacto de riesgo en el Ecuador. Éste señala que, la zona costera del país es una de las más afectadas en caso de ocurrencia de alguna amenaza.

Los datos obtenidos en el análisis asistirán a las operadoras, al momento de montar sus infraestructuras o de escoger los lugares para sus centros de control alternativos. Asimismo, favorecerá a las organizaciones para tener precauciones y realizar procedimientos de protección según los riesgos que puedan ocurrir en las diferentes zonas. Esta información, será muy importante y ayudará en la toma de decisiones a lo largo de toda la elaboración del plan de continuidad del negocio de la organización.

Después de la investigación de normas y estándares nacionales relacionados con la continuidad del negocio en las organizaciones, se pudo identificar que existe mucho desconocimiento del tema en Ecuador, y que las empresas nacionales aún no cuentan con una ley o norma nacional, a la cual regirse para realizar sus planes.

Al final, se determinó que el análisis del negocio es uno de los pasos fundamentales del plan de continuidad de negocio, ya que al concluir esta sección se obtendrá una lista de los activos y procesos críticos mínimos necesarios para la operación de la organización. Es decir, se conocerán los recursos indispensables que se necesitan para poder brindar sus servicios a los usuarios, dándoles mayor protección a éstos y así evitar la interrupción de los mismos, lo que conllevaría grandes pérdidas financieras para las operadoras.

5.2. Recomendaciones

Dentro de la primera fase del plan de continuidad de negocio, en la sección de identificación de vulnerabilidades se recomienda, el uso de herramientas automatizadas para la identificación de las vulnerabilidades ya que se obtienen mejores resultados y mucho más precisos.

Para la organización de los equipos de recuperación se requiere, que las personas que vayan a formar parte de cualquiera de éstos sean personas que conozcan muy bien las funciones principales del área en la que se desempeñan, y sobre todo tener un alto conocimiento de los procesos críticos de la organización.

Después del análisis de criticidad de riesgos a nivel país se advierte, que las operadoras móviles de Ecuador ubiquen sus centros de control alternativos e infraestructura critica de preferencia en la región sierra y amazónica. En caso de ubicarlas en la zona costera, se sugiere ubicarlas en los cantones menos afectados por las amenazas naturales.

Para ayudar a la elaboración de un correcto plan de continuidad se exhorta a seguir las fases definidas en la guía, en el orden planteado para así evitar que existan confusiones. Cabe recordar que esta guía se basa en la norma ISO 22301; la misma que, recomienda mantener esta secuencia para asegurar la continuidad del negocio en las organizaciones.

Se aconseja implementar esta guía, para el desarrollo de planes de continuidad de negocio para cualquier tipo de organización; ya que el presente trabajo de titulación se enfocó solamente a las operadoras móviles de Ecuador. Esto deja abierta una puerta para seguir perfeccionando y adaptando esta guía para los demás proveedores de servicios.

REFERENCIAS

ARCOTEL. (2018). Agencia de Regulacion y Control de las Telecomunicaciones. Recuperado el 28 de marzo de 2018 de http://www.arcotel.gob.ec/

Areitio Bertolin, J. (2008). Seguridad de la información. Redes, informática y sistemas de información. Editorial Paraninfo.

Bilait. (s.f.). Recuperado el 06 de abril de 2018 de http://bilait.co/continuidad/wp-content/uploads/2012/11/PCN1.png

Cardona A., O. (1993). Evaluacion de la amenaza,la vulnerabilidad y el riesgo. En A. Maskey, Los desastre no son naturales. La red.

DAFP. (2011). Guia para la Administracion del Riesgo. Bogota.

D'Ercole, R., & Trujillo, M. (2003). Amenazas, vulnerabilidades, capacidades y riesgo en el Ecuador. Quito: COOPI, IRD, OXFAM.

Disaster Recovery. (2017). Universidad Virtual. Recuperado el 20 de mayo de 2018 de https://universidadvirtual.sdr.com.mx/pluginfile.php/1014/mod_resource/content/1/BR%20Unidad%202.pdf

FAO. (2008). Organizacion de las Naciones Unidas para la Alimentacion y Agricultura. Recuperado el 19 de abril de 2018 de http://www.fao.org/docrep/013/i1255b/i1255b02.pdf

Fluidsignal Group. (s.f.). Recuperado el 12 de abril de 2018 de https://fluidattacks.com/web/es/blog/etiquetas/rpo/

Giménez Albacete, J. (2015). Seguridad en equipos informáticos. IFCT0109. IC Editorial.

Hernandez, L., & Galeano, R. (2016). Universidad Piloto de Colombia. Recuperado el 21 de abril de 2018 de http://polux.unipiloto.edu.co:8080/00000815.pdf

IGEPN. (s.f.). Instituto Geofísico de la Escuela Politécnica Nacional. Recuperado el 07 de mayo de 2018 de http://www.igepn.edu.ec

INAMHI. (s.f.). Instituto Nacional de Meteorología e Hidrología. Recuperado el 14 de abril de 2018 de http://www.serviciometeorologico.gob.ec/

ISO 22301. (2012). ISOTools. Recuperado el 17 de abril de 2018 de https://www.isotools.org/normas/riesgos-y-seguridad/iso-22301

ISO 27001. (2013). ISOTools. Recuperado el 13 de mayo de 2018 de https://www.isotools.org/2013/12/05/en-inventario-de-activos-en-la-implementacion-de-la-norma-iso-27001/

ISO 27001. (2013). Sistemas de Gestión la Seguridad de la Información.

Jimenez, L. d. (2007). Guia de Desarrollo de un Plan de Continuidad de Negocio. Madrid.

Kosutic, D. (2016). 27001 Academy. Recuperado el 11 de abril de 2018 de https://advisera.com/27001academy/es/que-es-iso-27001/

Machi, J. (2018). Dialogic. Recuperado el 09 de abril de 2018 de https://www.dialogic.com/glossary/mobile-network-operator-mno

Martinez, J. G. (2010). El plan de continuidad de negocio: guía práctica para su elaboración. Recuperado el 28 de marzo de 2018 de http://ebookcentral.proquest.com

Mendoza, M. (s.f). WeLiveSecurity. Recuperado el 12 de mayo de 2018 de https://www.welivesecurity.com/la-es/2014/11/06/business-impact-analysis-bia/

MINTIC. (s.f.). Ministerio de Tecnologías de la Información y las Comunicaciones. Recuperado el 16 de mayo de 2018 de https://www.mintic.gov.co/gestionti/615/articles-5482_G11_Analisis_Impacto.pdf

OPS. (s.f.). Organizacion Panamericana de la Salud . Recuperado el 28 de junio de 2018 de http://www.paho.org/ecu/index.php?option=com_content&view=article&id=349:vulnerabilidad-desastres&Itemid=972

Páez Parra, I. P. (2014). Gestión del riesgo de las TI NTC 27005. Bogota: RENATA.

Roble, H. (s.f.). Desastres Naturales Recuperado el 28 de abril de 2018 de https://www.vix.com/es/btg/curiosidades/2011/02/05/tipos-de-desastres-naturales-que-existen

Secretaría de Gestión de Riesgos. (s.f.). Secretaría de Gestión de Riesgos. Recuperado el 12 de mayo de 2018 de http://www.gestionderiesgos.gob.ec/

SGCI. (2018). Blog especializado en Sistemas de Gestión. Recuperado el 05 de mayo de 2018 de SGCI:https://www.pmg-ssi.com/2014/01/isoiec-27005-gestion-de-riesgos-de-la-seguridad-la-informacion/

SISTESEG. (2007). METODOLOGIA DE ANALISIS DE RIESGO. Recuperado el 15 de abril de 2018 de http://www.sisteseg.com/files/Microsoft_Word_-_METODOLOGIA_DE_ANALISIS_DE_RIESGO.pdf

Villamil, H. P. (2014). Gestion de la seguridad de la información . Bogota: RENATA-Escuela Superior de Redes.

ANEXOS

ANEXO 1

CANTONES CLASIFICADOS SEGÚN EL GRADO DE AMENAZA (POR TIPO DE AMENAZA Y GLOBAL)

Tabla 45.

Cantones del Ecuador clasificados según el grado de amenaza

Cantón	Provincia	Grado de amenaza sísmica	Grado de amenaza de tsunami	Grado de amenaza volcánica	Grado de amenaza inundación	Grado de amenaza de deslizamiento	Grado de amenaza de sequía	Valor amenaza global	Grado amenaza global
Portoviejo	Manabí	3	2	0	3	2	2	12	muy alto
Esmeraldas	Esmeraldas	3	2	1	3	2	1	12	muy alto
Santa Elena	Santa Elena	3	2	0	3	1	2	11	muy alto
Sucre	Manabí	3	2	0	3	1	2	11	muy alto
Puerto López	Manabí	3	2	0	2	2	2	11	muy alto
Eloy Alfaro	Esmeraldas	3	2	1	2	3	0	11	muy alto
San Lorenzo	Esmeraldas	3	2	1	2	3	0	11	muy alto
Atacames	Esmeraldas	3	2	0	2	2	1	10	muy alto
Rio Verde	Esmeraldas	3	2	0	2	2	1	10	muy alto
Jipijapa	Manabí	3	2	0	2	2	1	10	muy alto
Montecristi	Manabí	3	2	0	2	1	2	10	muy alto
Pedernales	Manabí	3	2	0	2	2	1	10	muy alto
Jama	Manabí	3	2	0	2	2	1	10	muy alto
Jaramijó	Manabí	3	2	0	2	1	2	10	muy alto
Guano	Chimborazo	3	0	3	0	3	0	9	alto
Penipe	Chimborazo	3	0	3	0	3	0	9	alto
El Guabo	El Oro	2	1	0	3	2	1	9	alto
Quinindé	Esmeraldas	3	0	1	3	2	0	9	alto
Naranjal	Guayas	2	1	0	3	2	1	9	alto
Salinas	Santa Elena	3	2	0	2	0	2	9	alto
La Libertad	Santa Elena	3	2	0	2	0	2	9	alto
Chone	Manabí	3	0	0	3	2	1	9	alto
Junín	Manabí	3	0	0	3	2	1	9	alto

Manta	Manabí	3	2	0	2	0	2	9	alto
Santa Ana	Manabí	3	0	0	3	2	1	9	alto
Archidona	Napo	3	0	3	0	3	0	9	alto
Quito	Pichincha	3	0	3	0	3	0	9	alto
Mejía	Pichincha	3	0	3	0	3	0	9	alto
San Miguel/Bancos	Pichincha	2	0	3	2	2	0	9	alto
Baños	Tungurahua	3	0	3	0	3	0	9	alto
Gonzalo Pizarro	Sucumbíos	3	0	2	1	3	0	9	alto
Latacunga	Cotopaxi	3	0	3	0	2	0	8	alto
La Maná	Cotopaxi	2	0	2	1	3	0	8	alto
Pujilí	Cotopaxi	3	0	2	0	3	0	8	alto
Muisne	Esmeraldas	3	2	0	2	1	0	8	alto
Guayaquil	Guayas	2	1	0	3	0	2	8	alto
Duran	Guayas	2	1	0	3	0	2	8	alto
Playas	Guayas	3	2	0	2	0	1	8	alto
Ibarra	Imbabura	3	0	1	0	3	1	8	alto
Ventanas	Los Ríos	2	0	1	3	1	1	8	alto
Valencia	Los Ríos	2	0	1	3	2	0	8	alto
Bolívar	Manabí	2	0	0	3	2	1	8	alto
Pajan	Manabí	3	0	0	2	2	1	8	alto
Rocafuerte	Manabí	3	0	0	3	0	2	8	alto
Olmedo	Manabí	3	0	0	2	2	1	8	alto
Palora	Morona Santiago	2	0	1	2	3	0	8	alto
Huamboya	Morona Santiago	2	0	2	1	3	0	8	alto
Tena	Napo	2	0	1	2	3	0	8	alto
El chaco	Napo	3	0	2	0	3	0	8	alto
Quijos	Napo	3	0	2	0	3	0	8	alto
Cayambe	Pichincha	3	0	2	0	3	0	8	alto
Patate	Tungurahua	3	0	2	0	3	0	8	alto
Pelileo	Tungurahua	3	0	3	0	2	0	8	alto
Guaranda	Bolívar	3	0	1	0	3	0	7	Rel Alto
Chimbo	Bolívar	3	0	1	0	3	0	7	Rel Alto
Las naves	Bolívar	2	0	1	2	2	0	7	Rel Alto
La troncal	Cañar	2	0	0	3	1	1	7	Rel Alto
Bolívar	Carchi	3	0	0	0	3	1	7	Rel Alto
Mira	Carchi	3	0	0	0	3	1	7	Rel Alto
Parigua	Cotopaxi	2	0	1	1	3	0	7	Rel Alto
Salcedo	Cotopaxi	3	0	2	0	2	0	7	Rel Alto

Saquisilí	Cotopaxi	3	0	2	0	2	0	7	Rel Alto
Sigchos	Cotopaxi	2	0	2	0	3	0	7	Rel Alto
Riobamba	Chimborazo	3	0	1	0	3	0	7	Rel Alto
Chambo	Chimborazo	3	0	1	0	3	0	7	Rel Alto
Machala	El Oro	2	1	0	3	0	1	7	Rel Alto
Santa Rosa	El Oro	2	0	0	3	1	1	7	Rel Alto
Balao	Guayas	2	1	0	3	0	1	7	Rel Alto
El triunfo	Guayas	2	0	0	3	1	1	7	Rel Alto
Samborondón	Guayas	2	0	0	3	0	2	7	Rel Alto
Yaguachi	Guayas	2	0	0	3	0	2	7	Rel Alto
Otavalo	Imbabura	3	0	1	0	3	0	7	Rel Alto
Tosagua	Manabí	3	0	0	3	0	1	7	Rel Alto
Santo Domingo	Sto. Domingo de los Tsáchilas	2	0	1	1	3	0	7	Rel Alto
Loreto	Orellana	2	0	2	2	1	0	7	Rel Alto
San Miguel	Bolívar	3	0	0	0	3	0	6	Rel Alto
Caluma	Bolívar	2	0	1	0	3	0	6	Rel Alto
Tulcán	Carchi	3	0	0	0	3	0	6	Rel Alto
Espejo	Carchi	3	0	0	0	3	0	6	Rel Alto
Montufar	Carchi	3	0	0	0	3	0	6	Rel Alto
San Pedro de Huaca	Carchi	3	0	0	0	3	0	6	Rel Alto
Colta	Chimborazo	3	0	0	0	3	0	6	Rel Alto
Guamote	Chimborazo	2	0	1	0	3	0	6	Rel Alto
Pallatanga	Chimborazo	3	0	0	0	3	0	6	Rel Alto
Atahualpa	El Oro	2	0	0	1	3	0	6	Rel Alto
Huaquillas	El Oro	2	0	0	2	0	2	6	Rel Alto
Pasaje	El Oro	2	0	0	2	2	0	6	Rel Alto
Piñas	El Oro	2	0	0	1	2	1	6	Rel Alto
A. Baquerizo Moreno	Guayas	2	0	0	3	0	1	6	Rel Alto
Balzar	Guayas	2	0	0	3	0	1	6	Rel Alto
Daule	Guayas	2	0	0	3	0	1	6	Rel Alto
Milagro	Guayas	2	0	0	3	0	1	6	Rel Alto
Naranjito	Guayas	2	0	0	3	0	1	6	Rel Alto
Palestina	Guayas	2	0	0	3	0	1	6	Rel Alto
Pedro Carbo	Guayas	3	0	0	1	1	1	6	Rel Alto
Santa Lucia	Guayas	2	0	0	3	0	1	6	Rel Alto

Urbina Jado	Guayas	2	0	0	3	0	1	6	Rel Alto
Crnl M. Maridueña	Guayas	2	0	0	3	0	1	6	Rel Alto
Nobol	Guayas	2	0	0	3	0	1	6	Rel Alto
Isidro Ayora	Guayas	2	0	0	2	1	1	6	Rel Alto
Cotacachi	Imbabura	2	0	1	0	3	0	6	Rel Alto
Pimampiro	Imbabura	3	0	0	0	3	0	6	Rel Alto
Urcuqui	Imbabura	2	0	1	0	3	0	6	Rel Alto
Célica	Loja	2	0	0	0	3	1	6	Rel Alto
Maracá	Loja	2	0	0	0	3	1	6	Rel Alto
Babahoyo	Los Ríos	2	0	0	3	0	1	6	Rel Alto
Baba	Los Ríos	2	0	0	3	0	1	6	Rel Alto
Puebloviejo	Los Ríos	2	0	0	3	0	1	6	Rel Alto
Quevedo	Los Ríos	2	0	0	3	0	1	6	Rel Alto
Urdaneta	Los Ríos	2	0	0	3	1	0	6	Rel Alto
Vinces	Los Ríos	2	0	0	3	0	1	6	Rel Alto
Palenque	Los Ríos	2	0	0	3	0	1	6	Rel Alto
Buena Fé	Los Ríos	2	0	1	3	0	0	6	Rel Alto
Mocache	Los Ríos	2	0	0	3	0	1	6	Rel Alto
Flavio Alfaro	Manabí	3	0	0	0	2	1	6	Rel Alto
Pichincha	Manabí	2	0	0	1	2	1	6	Rel Alto
24 de mayo	Manabí	3	0	0	0	2	1	6	Rel Alto
Mera	Pastaza	2	0	0	2	2	0	6	Rel Alto
Pedro Moncayo	Pichincha	3	0	1	0	2	0	6	Rel Alto
Rumiñahui	Pichincha	3	0	3	0	0	0	6	Rel Alto
Ambato	Tungurahua	3	0	1	0	2	0	6	Rel Alto
Mocha	Tungurahua	3	0	1	0	2	0	6	Rel Alto
Quero	Tungurahua	3	0	1	0	2	0	6	Rel Alto
Píllaro	Tungurahua	3	0	1	0	2	0	6	Rel Alto
Tisaleo	Tungurahua	3	0	1	0	2	0	6	Rel Alto
Isabela	Galápagos	2	0	2	0	0	2	6	Rel Alto
Sucumbíos	Sucumbíos	3	0	0	0	3	0	6	Rel Alto
Cuenca	Azuay	2	0	0	0	3	0	5	Rel. Bajo
Pucara	Azuay	2	0	0	0	3	0	5	Rel. Bajo
Santa Isabel	Azuay	1	0	0	0	3	1	5	Rel. Bajo

Oña	Azuay	1	0	0	0	3	1	5	Rel. Bajo
Chillanes	Bolívar	2	0	0	0	3	0	5	Rel. Bajo
Echeandia	Bolívar	2	0	1	0	2	0	5	Rel. Bajo
Cañar	Cañar	2	0	0	0	3	0	5	Rel. Bajo
El Tambo	Cañar	2	0	0	0	3	0	5	Rel. Bajo
Suscal	Cañar	2	0	0	0	3	0	5	Rel. Bajo
Alausí	Chimborazo	2	0	0	0	3	0	5	Rel. Bajo
Chunchi	Chimborazo	2	0	0	0	3	0	5	Rel. Bajo
Cumandá	Chimborazo	2	0	0	0	3	0	5	Rel. Bajo
Arenillas	El Oro	2	0	0	2	0	1	5	Rel. Bajo
Marcabeli	El Oro	2	0	0	0	2	1	5	Rel. Bajo
Zaruma	El Oro	1	0	0	1	3	0	5	Rel. Bajo
Las lajas	El Oro	2	0	0	0	2	1	5	Rel. Bajo
Simón Bolívar	Guayas	2	0	0	2	0	1	5	Rel. Bajo
Catamayo	Loja	1	0	0	0	3	1	5	Rel. Bajo
Espíndola	Loja	1	0	0	0	3	1	5	Rel. Bajo
Gonzanamá	Loja	1	0	0	0	3	1	5	Rel. Bajo
Paltas	Loja	2	0	0	0	3	0	5	Rel. Bajo
Saraguro	Loja	1	0	0	0	3	1	5	Rel. Bajo
Sozoranga	Loja	1	0	0	0	3	1	5	Rel. Bajo
Pindal	Loja	2	0	0	0	2	1	5	Rel. Bajo
Montalvo	Los Ríos	2	0	0	2	1	0	5	Rel. Bajo
El Carmen	Manabí	2	0	0	2	1	0	5	Rel. Bajo
Morona	Morona Santiago	1	0	2	0	2	0	5	Rel. Bajo
C. J Arosemena Tola	Napo	2	0	0	2	1	0	5	Rel. Bajo
San Cristóbal	Galápagos	2	0	1	0	0	2	5	Rel. Bajo
Santa Cruz	Galápagos	2	0	1	0	0	2	5	Rel. Bajo
Girón	Azuay	1	0	0	0	3	0	4	Rel. Bajo
Nabón	Azuay	1	0	0	0	3	0	4	Rel. Bajo
Paute	Azuay	1	0	0	0	3	0	4	Rel. Bajo
San Fernando	Azuay	1	0	0	0	3	0	4	Rel. Bajo
El Pan	Azuay	1	0	0	0	3	0	4	Rel. Bajo
Sevilla de Oro	Azuay	1	0	0	0	3	0	4	Rel. Bajo
Guachapéala	Azuay	1	0	0	0	3	0	4	Rel. Bajo
Biblián	Cañar	2	0	0	0	2	0	4	Rel. Bajo
Balsas	El Oro	2	0	0	0	1	1	4	Rel. Bajo
Chillanes	El Oro	1	0	0	0	3	0	4	Rel. Bajo

Portovelo	El Oro	1	0	0	0	3	0	4	Rel. Bajo
Colimes	Guayas	2	0	0	1	0	1	4	Rel. Bajo
El Empalme	Guayas	2	0	0	1	0	1	4	Rel. Bajo
Lomas de Sargentillo	Guayas	2	0	0	1	0	1	4	Rel. Bajo
Loja	Loja	1	0	0	0	3	0	4	Rel. Bajo
Calvas	Loja	1	0	0	0	3	0	4	Rel. Bajo
Chaguarpamba	Loja	1	0	0	0	2	1	4	Rel. Bajo
Puyango	Loja	2	0	0	0	2	0	4	Rel. Bajo
Quilanga	Loja	1	0	0	0	3	0	4	Rel. Bajo
Gualaquiza	Morona Santiago	1	0	0	0	3	0	4	Rel. Bajo
Limón Indanza	Morona Santiago	1	0	0	0	3	0	4	Rel. Bajo
Santiago	Morona Santiago	1	0	0	0	3	0	4	Rel. Bajo
Sucúa	Morona Santiago	1	0	0	0	3	0	4	Rel. Bajo
San Juan Bosco	Morona Santiago	1	0	0	0	3	0	4	Rel. Bajo
Logroño	Morona Santiago	1	0	0	0	3	0	4	Rel. Bajo
P. Vicente Maldonado	Pichincha	2	0	1	1	0	0	4	Rel. Bajo
Puerto Quito	Pichincha	2	0	1	1	0	0	4	Rel. Bajo
Cevallos	Tungurahua	3	0	1	0	0	0	4	Rel. Bajo
Zamora	Zamora Chinchipe	1	0	0	0	3	0	4	Rel. Bajo
Chinchipe	Zamora Chinchipe	1	0	0	0	3	0	4	Rel. Bajo
Nangaritza	Zamora Chinchipe	1	0	0	0	3	0	4	Rel. Bajo
Yacuambi	Zamora Chinchipe	1	0	0	0	3	0	4	Rel. Bajo
Yantzaza	Zamora Chinchipe	1	0	0	0	3	0	4	Rel. Bajo
El pangui	Zamora Chinchipe	1	0	0	0	3	0	4	Rel. Bajo
Palanda	Zamora Chinchipe	1	0	0	0	3	0	4	Rel. Bajo
La Concordia	Sto. Domingo de los Tsáchilas	2	0	0	2	0	0	4	Rel. Bajo

El Piedrero	Cañar	2	0	0	0	2	0	4	Rel. Bajo
Gualaceo	Azuay	1	0	0	0	2	0	3	Rel. Bajo
Sigsig	Azuay	1	0	0	0	2	0	3	Rel. Bajo
Chordeleg	Azuay	1	0	0	0	2	0	3	Rel. Bajo
Azogues	Cañar	1	0	0	0	2	0	3	Rel. Bajo
Bucay	Guayas	2	0	0	0	1	0	3	Rel. Bajo
Antonio Ante	Imbabura	3	0	0	0	0	0	3	Rel. Bajo
Zapotillo	Loja	2	0	0	0	0	1	3	Rel. Bajo
Olmedo	Loja	1	0	0	0	2	0	3	Rel. Bajo
Taisha	Morona Santiago	1	0	0	1	1	0	3	Rel. Bajo
Centinela del Condor	Zamora Chinchipe	1	0	0	0	2	0	3	Rel. Bajo
Cascales	Sucumbíos	2	0	0	0	1	0	3	Rel. Bajo
Orellana	Orellana	1	0	0	2	0	0	3	Rel. Bajo
Deleg	Cañar	1	0	0	0	1	0	2	Bajo
Pastaza	Pastaza	1	0	0	1	0	0	2	Bajo
Santa Clara	Pastaza	2	0	0	0	0	0	2	Bajo
Lago Agrio	Sucumbíos	1	0	0	1	0	0	2	Bajo
La joya de los Sachas	Orellana	1	0	0	1	0	0	2	Bajo
Arajuno	Pastaza	1	0	0	0	0	0	1	Bajo
Shushufindi	Sucumbíos	0	0	0	1	0	0	1	Bajo
Aguarico	Orellana	0	0	0	1	0	0	1	Bajo
Putumayo	Sucumbíos	0	0	0	0	0	0	0	Bajo
Cuyabeno	Sucumbíos	0	0	0	0	0	0	0	Bajo

Adaptado de (D'Ercole & Trujillo, 2003)

ANEXO 2

LISTA DE POSIBLES AMENAZAS

AMENAZAS	
Abuso de privilegios	Virus
Accidente grave	Exceso de humedad
Contaminación	Fallo del aire acondicionado
Copia ilegal de software	Vandalismo
Derechos de forja	Robo de documentos
Destrucción de equipos o medios	Fenómeno climático
Explosivos	Denegación de servicios
Falla de equipos	Repudio de acciones
Falla en las copias de seguridad	Divulgación indebida
Falla equipos de telecomunicaciones	Falla del hardware
Falta de disponibilidad de recursos	Software malicioso
Fenómeno volcánico	Subida de tensión
Fuego fortuito	Incendios
Huracanes	Humo, gases tóxicos
Incumplimientos legales	Datos de fuentes no confiables
Ingeniería social	Robo de hardware/software
Interrupción fuente de energía	Accidentes del personal
Inundaciones	Accidente grave
Pérdida de confidencialidad	Equipo defectuoso
Polvo, corrosión, congelación	Sismos
Radiación electromagnética	Falla de las comunicaciones
Radiación térmica	Errores de operación
Robo de equipos	Cambio del hardware
Sanciones y multas	Cambio del software
Troyanos	Descargas no controladas
Uso no autorizado de equipos	Saturación del sistema

ANEXO 3

EJEMPLOS DE POSIBLES TIPOS DE VULNERABILIDAD

TIPOS DE VULNERABILIDADES	
Almacenamiento no protegido	Antivirus no actualizado
Ausencia de control de activos	Antivirus no disponible
Ausencia de políticas de respaldos	Ausencia de acuerdos de confidencialidad
Control de acceso inadecuado	Ausencia de *backups*
Derechos de accesos incorrectos	Ausencia de plan de recuperación de desastres
Políticas de firewall inadecuadas	Ausencia planes de continuidad
Ausencia de pruebas	Cableado inapropiado
No definición de reemplazos	Dependencia de proveedores
Ausencia de políticas de seguridad	Desastre natural
Inadecuada clasificación de archivos	Descargas no controladas de software
Arquitectura insegura de la red	Falta de capacitación
Ausencia de logs	Falta de monitoreo
Ausencia de actualizaciones	Falta de parches
Ausencia de protección contra código malicioso	No definición de puestos
Degradación de equipos	Personal sin formación adecuada
Control inadecuado de cambios	Privilegios inadecuados
Incumplimientos legales	Proveedor único en el mercado
Falta de licencias	Puertos o servicios activos no requeridos
Inadecuada protección física	Uso de software ilegal