UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE TECNOLOGÍAS DE LA INFORMACIÓN, TELECOMUNICACIONES E INDUSTRIAL

DIRECCIÓN DE POSGRADO

MAESTRÍA EN GERENCIA DE SISTEMAS DE INFORMACIÓN.

Tema: "Propuesta de un Plan de continuidad del negocio para una entidad pública del Ecuador"

Trabajo de Investigación para Titulación para la obtención del Grado Académico de Magister en Gerencia de Sistemas de Información

Autor: Ing. Glenda Marilyn Araujo Castro.

Director: Ing. Edison Homero Álvarez Mayorga Mg.

Ambato – Ecuador

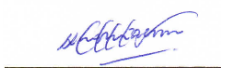
2019

A la unidad académica de titulación de la Facultad Tecnologías de la Información, Telecomunicaciones e Industrial.

El Tribunal receptor del Trabajo de Investigación presidido por la Ingeniera Elsa Pilar Urrutia Urrutia Magister, e integrado por los señores Ingeniero Carlos Israel Núñez Miranda, Magister., Ingeniero Edwin Hernando Buenaño Valencia, Magister, Ingeniero Félix Oscar Fernández Peña, PhD., designados por la Unidad Académica de Titulación de la Facultad Tecnologías de la Información, Telecomunicaciones e Industrial de la Universidad Técnica de Ambato, para receptar el Trabajo de Investigación con el tema: "Propuesta de un Plan de continuidad del negocio para una entidad pública del Ecuador", elaborado y presentado por la señora Ingeniera Glenda Marilyn Araujo Castro, para optar por el Grado Académico de Magister en Gerencia de Sistemas de Información; una vez escuchada la defensa oral del Trabajo de Investigación el Tribunal aprueba y remite el trabajo para uso y custodia en las bibliotecas de la UTA.

Ing. Elsa Pilar Urrutia Urrutia Mg,
Presidente del Tribunal

Ing. Carlos Israel Núñez Miranda Mg.
Miembro del Tribunal

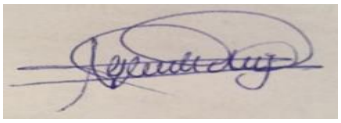


Ing. Edwin Hernando Buenaño Valencia Mg.
Miembro del Tribunal

Ing. Félix Oscar Fernández Peña PhD.
Miembro del Tribunal.

AUTORÍA DEL TRABAJO DE INVESTIGACIÓN

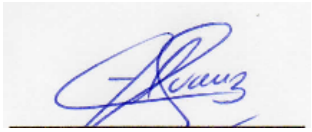
La responsabilidad de las opiniones, comentarios y críticas emitidas en el Trabajo de Investigación presentado con el tema: "Propuesta de un Plan de continuidad del negocio para una entidad pública del Ecuador" le corresponde exclusivamente a: Ingeniera Glenda Araujo Castro, Autor bajo la Dirección de Ing. Edison Homero Álvarez Mayorga Mg. Director (a) del Trabajo de Investigación; y el patrimonio intelectual a la Universidad Técnica de Ambato.



Ing. Glenda Marilyn Araujo Castro

c.c. 1803792439

AUTOR

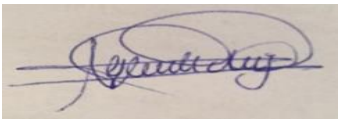


Ing. Edison Homero Álvarez Mayorga Mg.
c.c. 1801225960
DIRECTOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que el Trabajo de Investigación, sirva como un documento disponible para su lectura, consulta y procesos de investigación, según las normas de la Institución.

Cedo los Derechos de mi trabajo, con fines de difusión pública, además apruebo la reproducción de este, dentro de las regulaciones de la Universidad.



Ing. Glenda Marilyn Araujo Castro

C.I: 1803792439

ÍNDICE GENERAL

UNIVERSIDAD TÉCNICA DE AMBATO i

A la Unidad Académica de Titulación ii

INTRODUCCIÓN 1

CAPÍTULO I 3

1. EL PROBLEMA DE INVESTIGACIÓN 3
1.1 Tema de Investigación 3
1.2 Planteamiento del Problema 3
1.2.1 Contextualización 3
1.2.2 Análisis Crítico 5
1.2.3 Prognosis 6
1.2.4 Formulación del Problema 6
1.2.5 Interrogantes (Subproblemas) 6
1.2.5.1 Delimitación del objeto de investigación 6
1.2.5.2 Delimitación Espacial: 7
1.2.5.3 Delimitación Temporal: 7
1.2.5.4 Unidades de Observación: 7
1.3 Justificación 7
1.4 Objetivos 8
1.4.1 Objetivo General 8
1.4.2 Objetivos Específicos: 8
CAPITULO II 9

2. MARCO TEÓRICO 9
2.1 Antecedentes de Investigativos 9
2.2 Fundamentación Filosófica 10
2.3 Fundamentación Legal 10
2.4 Categorías Fundamentales 12
2.4.1 Constelación de Ideas, Variable Independiente u otros 13
2.4.2 Categorías de la Variable Independiente 14
2.4.3 Categorías de la Variable Dependiente 20
2.5 Hipótesis 22
2.6 Señalamiento de Variables 22
CAPÍTULO III 23

3. METODOLOGÍA 23
3.1 Enfoque 23
3.2 Modalidad básica de investigación 23
3.3 Nivel o tipo de investigación 23
3.4 Población y muestra 24
3.5 Operacionalización de variables 25
3.5.1 Variable independiente: Plan de Continuidad de Negocio 25
3.5.2 Variable dependiente: Disponibilidad Sistema de información. 26

3.6 Plan de recolección de información 26
3.7 Procesamiento y análisis de la información 27
CAPÍTULO IV 28
4. ANÁLISIS E INTERPRETACIÓN DE RESULTADOS 28
4.1 Análisis e interpretación de resultados 28
4.1.1 Cuestionario para el personal de Coordinación de Innovación Tecnológica del Servicio Nacional de Contratación Pública. 30
4.2 Verificación de la hipótesis 37
4.2.1 Planteamiento de la hipótesis 37
CAPÍTULO V 41
5. CONCLUSIONES Y RECOMENDACIONES 41
5.1 Conclusiones 41
5.2 Recomendaciones 42
CAPÍTULO VI 43
6. PROPUESTA 43
6.1 Datos informativos 43
6.2 Antecedentes de la propuesta 43
6.3 Justificación 45
6.4 Objetivos 46
6.4.1 General 46
6.4.2 Específicos 46
6.5 Análisis de factibilidad 46
6.5.1 Factibilidad operacional 46
6.5.2 Factibilidad técnica 47
6.5.3 Factibilidad financiera 47
6.6 Fundamentación 47
6.7 Metodología, modelo operativo 47
6.7.1 Alcance del modelo 49
6.7.2 Análisis del contexto 49
6.7.2.1 Definir características organizacionales 50
6.7.2.2 Identificación de los procesos organizacionales 52
6.7.3 Análisis de impacto en el negocio (BIA) 77
6.7.4 Análisis de riesgos 78
6.7.4.1 Metodología para el análisis de riesgos 78
6.7.4.2 Metodología Cualitativa 79
6.7.4.3 Metodología Cuantitativa 79
6.7.4.4 Criterios básicos 79
6.7.4.5 Criterios de valoración de activos 80
6.7.4.6 Criterios de probabilidad de ocurrencia de amenazas 81
6.7.4.7 Criterios de valoración de Impacto 82
6.7.4.8 Criterios de evaluación del riesgo. 83
6.7.4.9 Criterios para el tratamiento de riesgos 83

6.7.4.10 Criterios de prioridad en la aplicacón de controles. 84
6.7.4.11 Identificación de activos de la entidad 84
6.7.4.12 Identificación de amenazas..... 87
6.7.5 Proyección del plan de continuidad..... 103
6.7.5.1 Alcance 103
6.7.5.2 Políticas 103
6.7.5.3 Requisitos 103
6.7.5.4 Principios y valores 103
6.7.5.5 Objetivos..... 104
6.7.5.6 Definir estrategias de mitigación..... 104
6.8 Desarrollo del plan de continuidad de negocios. 107
6.8.1 Definir procedimientos e impactos. 108
Procedimiento para levantar la base de datos para la aplicación transaccional de la entidad:..... 123
6.8.2 Generación de informes de incidencias 124
6.9 Verificación y control del plan de continuidad..... 126
6.9.1 Análisis de informes de incidencias..... 126
6.10 Mejoramiento del plan de continuidad 126
6.10.1 Plan de mantenimiento..... 126
6.10.2 Propuesta de mejora..... 128
6.11 Análisis de resultados 128
6.12 Previsión de la evaluación 130
6.13 Conclusiones..... 131
6.14 Recomendaciones 131
6.15 Bibliografía 133
6.16 Anexos 144

ÍNDICE DE FIGURAS

Figura 2-1. Inclusiones Conceptuales 12
Figura 2-2. Constelación de ideas de la variable independiente. 13
Figura 2-3. Constelación de Ideas de la Variable Dependiente 13
Figura 4-4. Bases de un plan de continuidad. 14
Figura 4-5. Ciclo de retroalimentación del proceso de control. 17
Figura 4-1. Al no contar con un plan de continuidad de negocios afecta negativamente 30
Figura 4-2. Se aplican políticas de gestión de un plan de continuidad de negocios. 31
Figura 4-3. Existen estrategias de recuperación de los servicios críticos frente a una caída de los sistemas de información y comunicación. 32
Figura 4-4. Se realiza simulacros frente a una caída de los sistemas de información y comunicación. 33
Figura 4-5. Realización de tareas de monitoreo a los sistemas de información y comunicación. 34
Figura 4-6. Se realiza el control de los procesos críticos de los sistemas de información y comunicación 35
Figura 4-7. Considera que un Plan de continuidad de negocios, mejorará la disponibilidad de los Sistemas de información 36
Figura 4-8. Valor crítico. 39
Figura 4-9 Gráfica Chi Cuadrado 40
Figura 6-1. Alineación de la ISO 3100 e ISO 27005. 52
Figura 6-2. Oficinas del SERCOP a nivel nacional. 106

ÍNDICE DE TABLAS

Tabla 2-1. Alineación de estándares ISO 31000 e ISO 27005, con modelo PHVA. 19
Tabla 3-1. Población 24
Tabla 3-2. Operacionalización de la variable independiente: 25
Tabla 3-3. Operacionalización de la variable dependiente: 26
Tabla 5-4. Recolección de información. 26
Tabla 4-1. Al no contar con un plan de continuidad de negocios afecta negativamente la Coordinación de Innovación y Tecnología del Servicio Nacional de Contratación Pública. 30
Tabla 4-2. Se aplican políticas de gestión de continuidad de negocios. 31
Tabla 4-3. Existen estrategias de recuperación de los servicios críticos frente a una caída de los sistemas de información y comunicación. 32
Tabla 4-4. Se realiza simulacros frente a una caída de los sistemas de información y comunicación. 33
Tabla 4-5. Realización de tareas de monitoreo a los sistemas de información y comunicación. 34
Tabla 4-6. Se realiza el control de los procesos críticos de los sistemas de información y comunicación. 35
Tabla 4-7. Considera que un plan de continuidad de negocios mejorará la disponibilidad de los Sistemas de información de la entidad. 36
Tabla 4-8. Valores observados 38
Tabla 4-9. Valores esperados 38
Tabla 4-10. Cálculo del chi cuadrado 39
Tabla 4-11. Valor calculado 39
Tabla 6-1. Metodología para el plan de continuidad. 48
Tabla 6-2. Macroprocesos, procesos y subprocesos del servicio de contratación pública. 53
Tabla 6-3. Escala de clasificación de los procesos críticos. 59
Tabla 6-4. Matriz de calificación de procesos críticos. 60
Tabla 6-5. Recursos de soporte para procesos críticos. 71

Tabla 6-6. Matriz TOR y POR del proceso crítico de Gestión de Catálogo Electrónico. 74
Tabla 6-7. Matriz TOR y POR del proceso crítico de Gestión de Innovación Tecnológica. 75
Tabla 6-8. Matriz TOR y POR de la Gestión Técnica de Operaciones. 77
Tabla 6-9. Criterio de valoración de activos. 80
Tabla 6-10 Valor de cada activo 81
Tabla 6-11. Criterios de probabilidad de ocurrencia de amenazas 82
Tabla 6-12. Criterios de elaboración de impacto. 82
Tabla 6-13. Criterios de evaluación de riesgo. 83
Tabla 6-14. Criterios para el tratamiento de riesgos. 84
Tabla 6-15. Criterios de prioridad en la aplicación de controles. 84
Tabla 6-16. Activos primarios. 85
Tabla 6-17. Identificación de amenazas. 87
Tabla 6-18. Probabilidad de ocurrencias de amenazas. 88
Tabla 6-19. Calificación del nivel de impacto. 89
Tabla 6-20. Matriz de evaluación de nivel de riegos. 89
Tabla 6-21. Evaluación de las posibles amenazas y determinación del nivel de riesgo 91
Tabla 6-22. Matriz de impacto de la Gestión del Catálogo Electrónico. 94
Tabla 6-23. Matriz de impacto de Gestión de Innovación Tecnológica. 95
Tabla 6-24. Matriz de impacto de Gestión Técnica Operacional. 102
Tabla 6-25. Vías de recuperación tecnológica. 104
Tabla 6-26. Estrategias de recuperación de acuerdo a cada proceso crítico. 105
Tabla 6-27. Acciones ante una interrupción. 107
Tabla 6-28. Análisis de riesgo de los recursos críticos. 107
Tabla 6-29. Procedimiento para la declaración de emergencia. 109
Tabla 6-30. Procedimientos de Contingencia de Gestión de Servicios Informáticos. 112
Tabla 6-31. Procedimientos de Gestión de Desarrollo de Soluciones. 114
Tabla 6-32. Informe de incidencias. 124
Tabla 6-33. Plan de mantenimiento. 127

Tabla 6-34. Previsión de la evaluación 130

AGRADECIMIENTO

A mis padres y hermanos por su apoyo incondicional en esta etapa de mi vida.

Mi esposo a mi pequeño hijo por toda su paciencia y amor brindado.

A los docentes de la facultad de Tecnologías de Información Telecomunicaciones e Industrial por sus conocimientos impartidos herramientas claves para desarrollar el trabajo de investigación.

Glenda Araujo Castro.

DEDICATORIA

A Dios, a mi madre virgen María por la fortaleza y sabiduría brindada en este tiempo.

Con mucho amor a mi pequeño muñeco, Martín Valentino Henríquez Araujo.

Glenda Araujo Castro.

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE TECNOLOGÍAS DE LA INFORMACIÓN TELECOMUNICACIONES E INDUSTRIAL

MAESTRÍA EN GERENCIA DE SISTEMAS DE INFORMACIÓN

TEMA:

"Propuesta de un plan de continuidad del negocio para una entidad pública del Ecuador"

AUTOR: **Ing. Glenda Araujo**

DIRECTOR: Ing. Edison Álvarez

FECHA: 31 de mayo de 2019

RESUMEN EJECUTIVO

El presente trabajo de investigación trata sobre la importancia de disponer de un Plan de continuidad de negocios en el Servicio Nacional de Contratación Pública, siendo el propósito principal identificar los procesos tecnológicos primordiales, sus riesgos y amenazas a los que se encuentran expuestos, de esta manera adaptar a la realidad de la entidad una propuesta ideal de plan de continuidad de negocios. Es primordial tener un correcto manejo de riesgos y una visión clara de las actividades a realizar para recuperar las operaciones tecnológicas ante posibles amenazas materializadas, presencia de desastres naturales como terremotos, sismos, incendios, inundaciones o delincuencia que pueden afectar notoriamente el desempeño ideal de la institución. El Servicio Nacional de Contratación Pública es el ente rector de la contratación pública en el Ecuador y posee el mejor sistema de contratación de la región América Latina y el Caribe. Al realizar procesos de contratación en los que se transacciona millones de dólares del presupuesto general del estado se debe garantizar una estabilidad tecnológica para los principales actores como son entidades y proveedores; sin embargo esta institución se ha visto amenazada por hackers en los últimos años; por tal motivo, se propone un plan de continuidad de negocios, el mismo que se desarrollará en 5 fases que son: análisis de contexto (actividades, procesos y riesgos), proyección (alcance, políticas, requisitos, principios, objetivos y estrategias), desarrollo (procedimientos, análisis de impactos e informe de incidencias), verificación-control (análisis de informe de

incidencias, evaluación de desempeño) y mejoramiento (plan de mantenimiento, propuesta de mejora, informe de resultados).

Para garantizar esta investigación se analizaron varias normas y estándares internacionales que encierran todos los temas de seguridad de la información e informática.

Descriptores: Plan de continuidad, TOR, POR, análisis de contexto, verificación, control, mejoramiento.

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE TECNOLOGÍAS DE LA INFORMACIÓN TELECOMUNICACIONES E INDUSTRIAL

MAESTRÍA EN GERENCIA DE SISTEMAS DE INFORMACIÓN

THEME:

"Proposal for a business continuity plan for a public entity in Ecuador"

AUTHOR: Ing. Glenda Araujo

DIRECTED BY: Ing. Edison Álvarez

DATE: 31 de mayo de 2019

EXECUTIVE SUMMARY

This research work deals with the importance of having a business continuity plan in the National Public Procurement Service, the main purpose of which is to identify the main technological processes, their risks and threats to which they are exposed, in this way adapt an ideal proposal for a business continuity plan to the reality of the entity. It is essential to have a correct risk management and a clear vision of the activities to be carried out in order to recover technological operations in the event of materialized threats, the presence of natural disasters such as earthquakes, earthquakes, fires, floods or delinquency that can notably affect the ideal performance of the institution. The National Public Procurement Service is the governing entity of public procurement in Ecuador and has the best contracting system in the Latin America and the Caribbean region. When carrying out contracting processes in which millions of dollars of the general budget of the state are transacted, a technological stability must be guaranteed for the main actors such as entities and suppliers; however, this institution has been threatened by hackers in recent years; For this reason, a business continuity plan is proposed, which will be developed in 5 phases that are: analysis of context (activities, processes and risks), projection (scope, policies, requirements, principles, objectives and strategies), development (procedures, impact analysis and report of incidents), verification-control (analysis of incident report, performance evaluation) and improvement (maintenance plan, improvement proposal, report of results).

In order to guarantee this research, several international norms and standards that encompass all the information security and information issues were analyzed.

Descriptors: Continuity plan, TOR, POR, context analysis, verification, control, improvement.

INTRODUCCIÓN

Dentro de cualquier organización, sea esta pública o privada, el uso de la tecnología informática es vital para la gestión ordinaria de ámbitos diversos. Un factor alineado consecuentemente con el avance de las TIC que salvaguarda la continuidad y consistencia de la información almacenada en los sistemas informáticos es la disponibilidad de planes de continuidad del negocio.

La ejecución de un Plan de Continuidad de Negocios permite que los productos o servicios críticos sigan siendo entregados a los clientes internos o externos. Un plan de continuidad se enfoca en que los procesos críticos continúen estando disponibles.

Los productos o servicios críticos de una organización son aquellos que deben ser entregados para asegurar la supervivencia, evitar los problemas de no entregarlo y cumplir con obligaciones legales o contractuales existentes. El Plan de Continuidad de Negocio es un plan proactivo que busca asegurar que los productos o servicios continúen siendo entregados durante una interrupción no planeada (Camelo, 2016).

La investigación se ha elaborado de acuerdo a la organización de información que se detalla a continuación:

El CAPÍTULO I, EL PROBLEMA contiene: el tema de investigación, el planteamiento del problema, su contexto, análisis crítico, prognosis, formulación del problema, interrogantes, delimitación, justificación y objetivos en cuanto a los riesgos identificados que afectan a la información para tomar medidas de seguridad.

El CAPÍTULO II MARCO TEÓRICO contiene: antecedentes de la investigación, fundamentación filosófica, fundamentación legal, categorías fundamentales, hipótesis y señalamiento de variables.

El CAPÍTULO III METODOLOGÍA contiene: el enfoque de investigación, modalidad básica de la investigación, nivel o tipo de investigación, población y muestra, operacionalización de variables, plan de recolección de información y plan de procesamiento de la información.

El CAPÍTULO IV ANÁLISIS E INTERPRETACIÓN DE RESULTADOS contiene: análisis e interpretación de resultados, cuestionario para personal de Innovación Tecnológica, validación de las respuestas obtenidas, verificación de hipótesis, planteamiento de la hipótesis, prueba de χ^2 y datos estadísticos.

El CAPÍTULO V CONCLUSIONES Y RECOMENDACIONES contiene: conclusiones y recomendaciones.

El CAPÍTULO VI PROPUESTA contiene: la propuesta, los datos informativos, antecedentes de la propuesta, justificación, objetivos, análisis de factibilidad, fundamentación, metodología, modelo operativo, desarrollo del plan de continuidad de negocios y previsión de la evaluación.

CAPÍTULO I

1. EL PROBLEMA DE INVESTIGACIÓN

1.1 Tema de Investigación

Desarrollo de una propuesta de un Plan de Continuidad de negocio para una entidad pública

1.2 Planteamiento del Problema

1.2.1 Contextualización

En la actualidad, las instituciones públicas del Ecuador, tienen como objetivo proveer servicios tecnológicos de calidad a sus clientes internos y externos; sin embargo, esto no se ha llegado a cumplir ya que en los últimos años se ha intensificado los reclamos en los sistemas de tecnología e información debido a ataques cibernéticos, que causaron daños en las plataformas y en la operabilidad de los establecimientos (Agencia EFE, 2019) (Ortiz, 2019)

Unos de los ataques cibernéticos más conocidos fueron en la provincia de Pichincha hacia los portales de la Presidencia, del Ministerio del Interior y del Banco Central, donde hubo saturación de los servicios tecnológicos, que ocasionó cuantiosas pérdidas para el Estado (Patiño, 2019), Del mismo modo, el Servicio de Contratación Pública del Estado (SERCOP) no quedo absuelta, debido a la vulnerabilidad en sus sistemas de información y comunicación, por fallas en la infraestructura tecnológica y por no contar con un plan de contingencia para cada proceso crítico, afectando el proceso de contratación pública tanto en las entidades como a los proveedores (Vásquez, 2018).

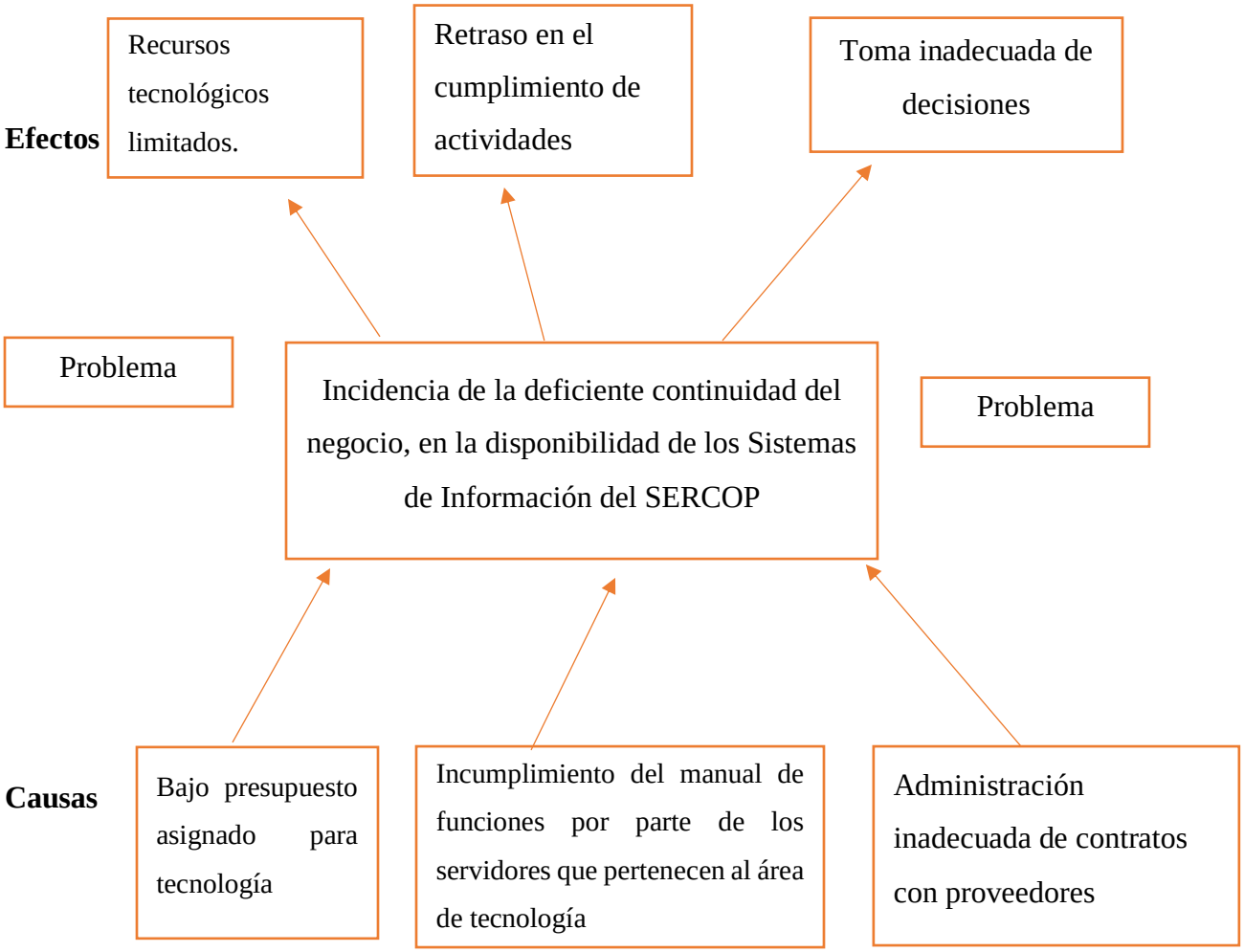
Estos ataques fueron monitoreados en cada establecimiento y se pidió a las instituciones del Gobierno central y otros poderes del Estado, que fortalezcan los sistemas de seguridad informática brindando capacitación, personal adecuado ante una emergencia y el apoyo económico para fortalecer los portales de las instituciones (Torres M. , 2019).

Hoy en día estas instituciones resguardan su información en el área de tecnologías informáticas, para evitar riesgos de pérdida o suspensión de servicios por fallas técnicas, mediante la activa participación del personal en la protección de la información; ya que, las personas no solo son las

primeras en ser afectadas, sino también las primeras en actuar frente una emergencia, antes que los mecanismos especializados de respuesta.

Por lo antes mencionado, es ideal que las entidades que ofrecen servicios on-line (oficinas públicas) o automatizados (líneas de producción) (Simplifica DC., 2009) implementen un plan de continuidad que identifique las debilidades en los servicios tecnológicos, que creen un estudio exhaustivo de los procesos críticos y que establezcan un contexto adecuado en caso de alguna catástrofe ya sea natural o humana (Torres & Torres, Plan de continuidad y plan de contingencia una forma de salvar tu negocio, 2018) (Benson, Estrategias de seguridad, 2000)

Árbol de problemas



1.2.2 Análisis Crítico

Con la finalidad de dar cumplimiento a lo dispuesto por la función ejecutiva el estado, sobre las medidas de austeridad, se reduce el presupuesto asignado a la entidad, por tal motivo la Coordinación de Innovación tecnológica se ve afectada al momento de realizar la adquisición para repotenciar la infraestructura tecnológica y así mantener los sistemas de información seguros y disponibles ante cualquier evento inesperado, retrasando de cierta manera las metas establecidas en la planificación anual de la Coordinación de innovación tecnológica.

Se encuentran creados un manual de funciones para cada puesto perteneciente a las cuatro direcciones de la Coordinación de innovación tecnológica, mismo que es administrado por los directores de cada dirección, al momento no se cumplen con las actividades que se encuentran destinadas para cada puesto de trabajo, esto se debe a que al momento de ingresar personal nuevo contratado, se le asigna tareas priorizadas, que no se encuentran plasmadas en dicho manual con el fin de cubrir necesidades de tareas incumplidas anteriormente, debido a una inadecuada planificación, de esta manera se prolonga el desarrollo de un plan de continuidad de negocios, y se desaprovecha los conocimientos del talento humano contratado.

Existen servicios contratados con proveedores externos, mismos que son administrador por el personal de la coordinación de innovación tecnológica, al presentarse inestabilidad de puestos de trabajo o rotación del personal se produce una ineficiente comunicación con los proveedores de servicios y soluciones ineficientes a los inconvenientes presentados, como resultado se toman decisiones incorrectas a nivel de dirección priorizando acciones que no garantizan una continuidad de negocio.

El uso creciente de las tecnologías por parte de las diversas instituciones, hacen que cada vez los sistemas informáticos sean frágiles y las redes de datos soporten las funciones más críticas de una organización; ocasionando una inconciencia sobre la importancia de garantizar la seguridad de los recursos involucrados en la información (INDECI, 2005).

Una de las entidades públicas expuesta a los ataques informáticos es el Servicio de Contratación Pública, debido a la falta de control y cumplimiento de las normas de seguridad informática (SERCOP, 2013), al no contar con un plan de continuidad que proteja los procesos críticos y

operativos del negocio contra desastres naturales o fallas mayores por la interrupción de las operaciones de una empresa, disminuye el impacto financiero, produce perdida de información crítica, credibilidad y productividad. A esto le podemos sumar enfermedades, huelgas o cortes en la cadena de suministros. (al contar con un plan de continuidad).

Debido a la necesidad de un plan de continuidad informática que contenga estrategias y soluciones que se pueden dar por diferentes factores, es indispensable definir una solución práctica y genérica para la identificación electrónica de un modelo conceptual que permita aplicar esta tecnología y mejorar la calidad de los procesos de identificación, brindando así información de mayor calidad para la toma de decisiones de autoridades.

1.2.3 Prognosis

De continuar con el problema, se seguirá observando la existencia de inconvenientes derivados a la no nula aplicación del plan de continuidad de negocio, incurriendo en pérdidas de tiempo, disponibilidad de los sistemas informáticos de la institución, afectando la eficiencia de los procesos institucionales y problemas económicos que se reflejan en la adquisición de bienes, servicios y obras para las entidades públicas provocando retraso en cronogramas y afectando a los activos del Estado.

1.2.4 Formulación del Problema

¿Incide la deficiente Continuidad del Negocio de la Coordinación de Innovación Tecnológica del Servicio Nacional de Contratación Pública en la disponibilidad de los sistemas de información y comunicación de la entidad?

1.2.5 Interrogantes (Subproblemas)

- ¿Cuál es el procedimiento primordial para iniciar con el desarrollo de un plan de continuidad de negocios?
- ¿Qué paso se debe ejecutar para iniciar con el desarrollo de una propuesta de un Plan de continuidad de negocios?
- ¿Cuál es la meta de desarrollar un Plan de Continuidad de negocio?

1.2.5.1 Delimitación del objeto de investigación

Campo: Sistema Nacional de Contratación Pública SERCOP

Área: Coordinación de Innovación Tecnológica

Aspecto: Control de la aplicación de un plan de continuidad informática.

1.2.5.2 Delimitación Espacial:

Servicio Nacional de Contratación Pública SERCOP matriz Quito

1.2.5.3 Delimitación Temporal:

Mes estimado: Mayo **año**: 2019

1.2.5.4 Unidades de Observación:

Servicio Nacional de Contratación Pública SERCOP matriz Quito

1.3 Justificación

El presente proyecto de investigación permitirá a la institución mantener un plan sustentable y sostenible para contrarrestar cualquier anomalía, problemas internos o externos de los que puedan ser afectados. Ya que; para esta institución, es indispensable identificar aquellos sistemas y recursos informáticos que son susceptibles de deterioro, violación o pérdida y que pueden ocasionar graves trastornos para el desenvolvimiento normal de la institución. Con el propósito de estructurar y ejecutar los procedimientos que admitan una pronta recuperación, así como asignar responsables de salvaguardar los componentes físicos, lógicos y sobre todo la información que permita su recuperación, garantizando la confidencialidad, integridad y disponibilidad de ésta en el menor tiempo posible, brindando un ambiente de tranquilidad y seguridad en cuanto a los activos de Tecnologías de Información (TI) así minimizando los costos en el levantamiento de la información y de los recursos informáticos.

- Factibilidad Técnica:

  Este proyecto es técnicamente factible de realizar debido a la disponibilidad de recursos tecnológicos, haciendo referencia a la infraestructura, herramientas hardware o software, acceso a datos e información requerida.

- Factibilidad Operativa:

El presente proyecto es factible operativamente porque cuenta con el apoyo de quienes están al frente de la Coordinación de Innovación Tecnológica del Servicio Nacional de Contratación Pública (SERCOP).

- Factibilidad Económica:

Y finalmente, este proyecto es económicamente factible ya que los costos que implican el análisis, estudio, tiempo empleado en estos temas son asumidos por el investigador.

1.4 Objetivos

1.4.1 Objetivo General

Desarrollar una propuesta de un plan de continuidad de negocios para los sistemas informáticos que administra la Coordinación de Innovación Tecnológica del Servicio Nacional de Contratación Pública.

1.4.2 Objetivos Específicos:

- Distinguir los posibles riesgos y amenazas a los que están expuestos los sistemas informáticos que administra la Coordinación de Innovación Tecnológica del Servicio Nacional de Contratación Pública.
- Identificar los procedimientos críticos que se encuentran en los sistemas informáticos que administra la Coordinación de Innovación Tecnológica del SERCOP, y a partir de esto proponer un Plan de Continuidad del Negocio.
- Obtener una probabilidad alta de continuidad en los procesos críticos informáticos de la Institución, en caso de que un incidente interrumpa las operaciones normales.
- Controlar el nivel de afectación a los procesos críticos de sistemas informáticos como consecuencia de una interrupción.

CAPITULO II

2. MARCO TEÓRICO

2.1 Antecedentes de Investigativos

“No existe un sistema 100% seguro, ya que los riesgos siempre están presentes, a pesar de las medidas que se tomen para prevenirlo.” (Narvaes & Mendez, 2012).

Luego de efectuar una revisión y análisis bibliográfico, en el repositorio de la Universidad no se encontró trabajos netamente relacionados a un plan de continuidad de negocio mediante la norma ISO 22301.

En la investigación de (Aucapiña, 2012), con tema “NORMA DE SEGURIDAD INFORMÁTICA ISO 27001 PARA MEJORAR LA CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD DE LOS SISTEMAS DE INFORMACIÓN Y COMUNICACIÓN EN EL DEPARTAMENTO DE SISTEMAS DE LA COOPERATIVA DE AHORRO Y CRÉDITO SAN FRANCISCOLTDA.” se propone elaborar una solución informática que mantenga y mejore la seguridad de los sistemas de información y comunicación en la Cooperativa de Ahorro y Crédito ―San Francisco Ltda., basada en el estándar ISO 27001, analizar los parámetros de confidencialidad, integridad y disponibilidad de los sistemas de información y comunicación del Departamento de Sistemas de la Cooperativa formato en su investigación titulado, una de las conclusiones que : “El contenido de la ISO 27001 está orientado al tratamiento de seguridad de la información mediante la gestión de riesgos, ya que describe la manera de mantener y mejorar la seguridad de los activos de información de cualquier organización”

Por otro lado se encontró en el trabajo de (Morales, 2019) titulado: “Balanced ScoreCard para seguridad de la información bajo el estándar ISO 27001 en Cooperativas de Ahorro y Crédito” sobre seguridad de la información aplicando la Norma ISO 27001, en el cual tiene como objetivo principal Diseñar un Balanced Score Card para seguridad de la información bajo el estándar ISO 27001 en Cooperativas de Ahorro y Crédito definiendo políticas de seguridad de la empresa, identificando los activos de la información y que tan vulnerable pueden ser los distintos departamentos de la institución financiera ante cualquier tipo de amenaza cuya principal

conclusión que describe es: La metodología planteada para este trabajo debe permitir un esquema apropiado de seguridad para la información, ya que durante el mismo se determina que son varios los activos como por ejemplo el computador personal del empleado que muestra debilidades a la hora de gestionar la información en cada uno de sus estados de gestión."

Además, se encontró una guía basada en definiciones de plan de continuidad de negocios escrita por (Gaspar Martinez, 2006), con título: "EL PLAN DE CONTINUIDAD DE NEGOCIO" guía práctica para su elaboración, defiende que un plan de continuidad de negocios debería hacer frente a:

- Aumentar la probabilidad de continuidad de las funciones críticas de la organización en caso de que un incidente interrumpa las operaciones informáticas en las que se apoya, además proporcionar un enfoque organizado y consolidado para dirigir actividades de respuesta y recuperación ante cualquier incidente o interrupción de trabajo imprevista, evitando confusión y reduciendo la situación de tensión.
- Reducir el tiempo de recuperación, y como consecuencias, las pérdidas económicas, directas e inducidas, como resultado de un desastre.

2.2 Fundamentación Filosófica

Esta investigación se guía por el paradigma critico-propositivo, es crítico debido a que realiza un análisis crítico de la problemática actual que surge al no existir una adecuada continuidad de negocio y es propositivo ya que se enfoca principalmente en la interpretación, comprensión y explicación de los fenómenos sociales en perspectiva de totalidad, donde busca analizarlos y se orienta a la obtención de resultados.

2.3 Fundamentación Legal

Con la elaboración de este plan de continuidad del negocio se beneficiará el recurso tecnológico de la institución en concordancia con los literales d), e) y f) del Artículo 1.3.2.4.1.de Gestión de Servicios Informáticos de la Ley Orgánica del Sistema Nacional de Contratación Pública del Registro Oficial Suplemento 395 de 04-ago.-2008 de estado vigente, los mismos que impulsan a la investigación y por ende promueve el desarrollo sustentable.

ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LAINFORMACION EGSI

Acuerdo Ministerial 166

Registro Oficial Suplemento 88 de 25-sep-2013

GESTION DE LA CONTINUIDAD DEL NEGOCIO 10.1. Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio

a) El responsable del área de Tecnologías de la Información o su similar será designado como coordinador de continuidad de los servicios informáticos, que se encargará de supervisar el proceso de elaboración e implantación del plan de continuidad, así como de la seguridad del personal.

b) Identificar los activos involucrados en los procesos críticos de los servicios informáticos, así como de las actividades que se deben realizar.

c) Elaborar la política de continuidad de los servicios informáticos determinando los objetivos y el alcance del plan, así como las funciones y responsabilidades; un documento que establezca a alto nivel los objetivos, el alcance y las responsabilidades en la gestión de la continuidad. Por ejemplo, la plantilla del documento debería contener:

INTRODUCCION: Detallando de forma resumida de que se trata, la estructura del documento y que se persigue.-

OBJETIVOS: que se satisfacen con la aplicación de la política, como se garantizará continuidad delas actividades y de los servicios, planes adicionales de contingencia.- ALCANCE: Procesos y operaciones que son cubiertos y recursos que utilizan los procesos u operaciones- RESPONSABILIDADES: Diferentes responsables implicados en la gestión de la continuidad de los servicios informáticos

d) Garantizar la continuidad incorporando los procesos generados en la estructura de la institución.

10.2. Continuidad del negocio y evaluación de riesgos

a) Definir los procesos y actividades de los servicios y aplicaciones,

b) Entender las complejidades e interrelaciones existentes entre equipamiento, personas, tareas, departamentos, mecanismos de comunicación y relaciones con proveedores externos, los cuales pueden prestar servicios críticos que deben ser considerados.

c) Identificar y valorar el impacto de las interrupciones de los procesos, aplicaciones y servicios de los servicios informáticos, para cuantificar y calificar los impactos y saber sus efectos.

d) Identificar el tiempo máximo de interrupción permitida para cada servicio o aplicación crítica; por ejemplo, 30 minutos, una hora o un día.

e) Analizar los riesgos, identificando las amenazas sobre los activos y su probabilidad de ocurrencia.

f) Analizar las vulnerabilidades asociadas a cada activo y el impacto que puedan provocar sobre la disponibilidad.

g) Obtener un mapa de riesgos que permita identificar y priorizar aquellos que pueden provocar una paralización de las actividades de la institución.

2.4 Categorías Fundamentales

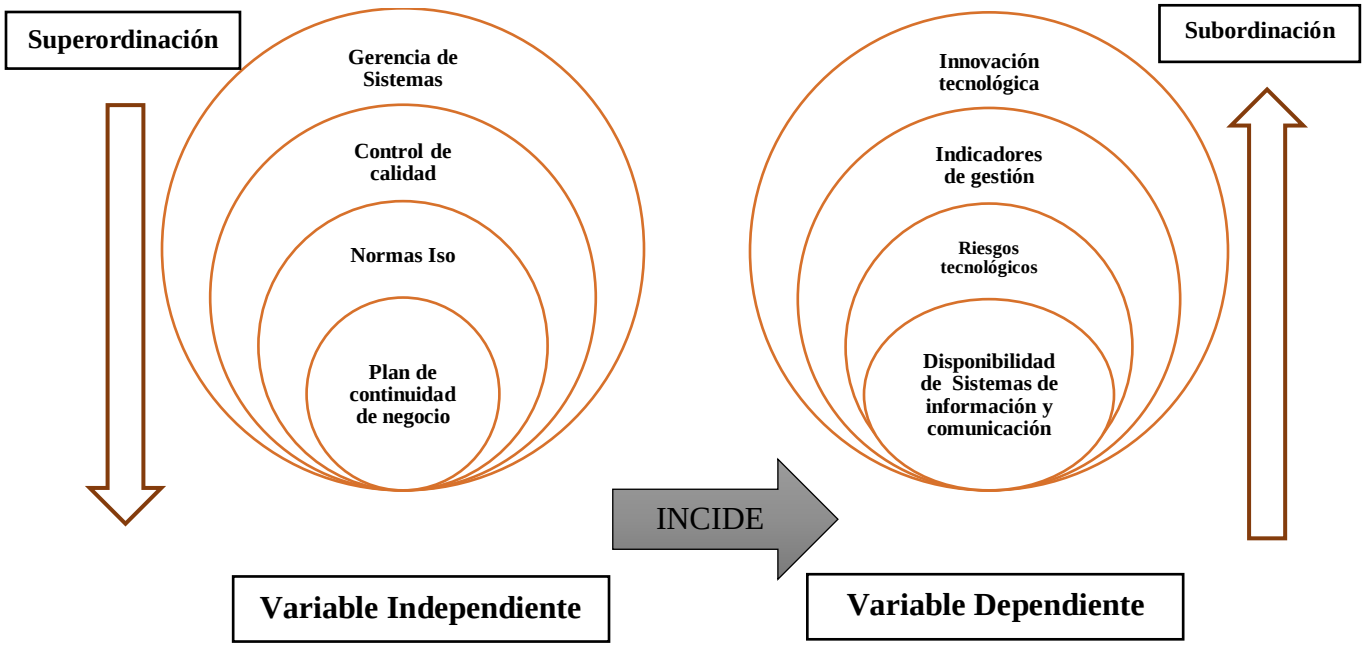


Figura 2-1. Inclusiones Conceptuales

Elaborado por: Investigador

2.4.1 Constelación de Ideas, Variable Independiente u otros

Figura 2-2. Constelación de ideas de la variable independiente.

Elaborado por: Investigador

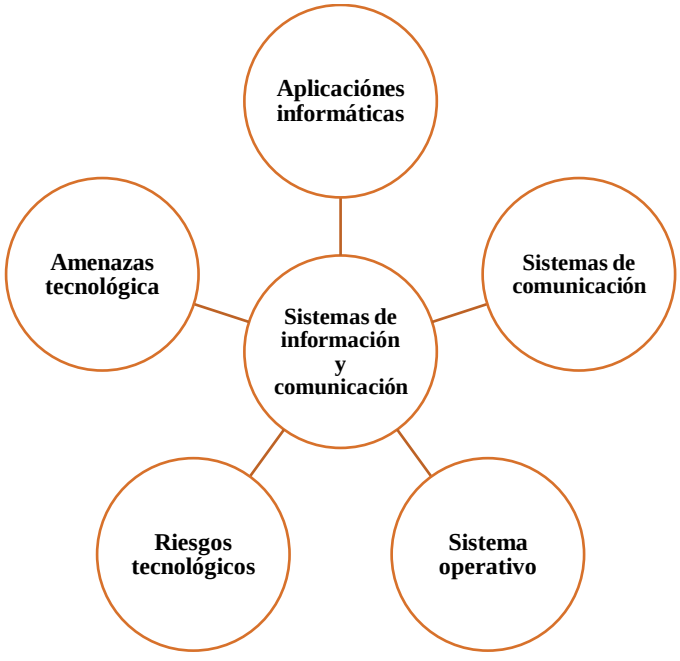


Figura 2-3. Constelación de Ideas de la Variable Dependiente

Elaborado por: Investigador

2.4.2 Categorías de la Variable Independiente

Plan de continuidad de negocio (BCP)

El plan de continuidad es un conjunto de actividades preventivas para minimizar los riesgos en caso de algún desastre de origen natural o humano (Rojas, 2017), manteniendo la operatividad de las actividades a un mínimo nivel hasta recuperar la totalidad de los sistemas y recursos; este, se encuentra conformado por tres acciones fundamentales que son: prevención (acciones para prevenir efectos) (ASI, 2009)., detección (acciones durante o después del desastre)y recuperación (restauración de los equipos y actividades) (Narvaes & Mendez, 2012) (Juarez, 2015).

Ya que no existe un sistema totalmente seguro; pero si un sistema confiable, el que se basa en 3 pilares fundamentales que se observan en la figura 2-4 (Alvarez, 2011).

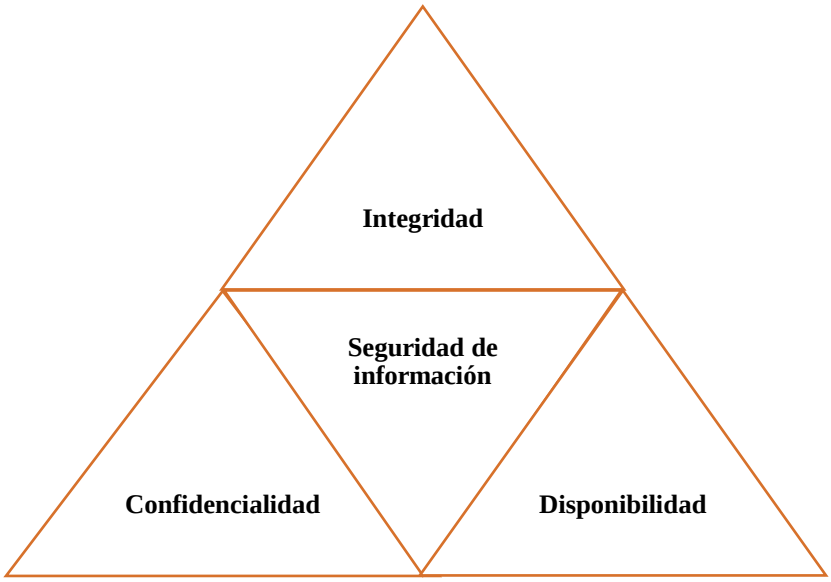


Figura 2-4. Bases de un plan de continuidad.

Elaborado por: (Ladine, 2017).

Los principales beneficios que brinda un plan de continuidad son los siguientes:

- Identificación de procesos críticos de la empresa (Pizzagalli, 2016)
- Definición un cronograma de recuperación (Vigo, Cardoso, & Mello, 2010).
- Prevención y minimización de pérdidas financieras.

- Clasificación los activos de la empresa otorgando prioridad para su protección.
- Es una ventaja competitiva.
- Es aplicable a empresas de cualquier tamaño.

Existe escenarios de riesgos tecnológicos por falta o deterioro de los sistemas informáticos, fallos de energía, sabotaje interno o por eventos catastróficos (Sánchez M. , 2013). Que pueden ser prevenidos cumpliendo las siguientes tareas:

- Elaboración de procedimientos técnicos de contingencias.
- Desarrollo del plan de recuperación de sistemas o plan de recuperación de desastres (PRS – DRP)
- Establecimiento de escenarios de recuperación operacional y preparación del plan de trabajo para recuperar la normalidad en las operaciones tecnológicas afectada por la contingencia (Jácomo, 2013).

Hay que tener en claro cuales con los desastres que puede sufrir una organización, para poder clasificarlos en tres niveles (Torres C. , 2013):

- Nivel menor. - Puede ocurrir durante todos los días de operación; debido, que los efectos causados son pequeños que puede ser reanudados por políticas del plan de continuidad.
- Nivel intermedio. – Ocurren con menos frecuencia y puede provocar interrupciones normales de la empresa.
- Nivel mayor. – La probabilidad de ocurrencia es muy baja; sin embargo, puede interrumpir la mayoría de procesos críticos.

Análisis de la gestión de riesgos

Esta información es vital para un plan de continuidad; ya que, se debe reportar los riesgos que puedo ocurrir en una organización (Torres C. , 2013), tomando en cuenta: amenazas y actividades críticas definiendo un modelo de análisis que se adecue a la empresa para implementar un control adecuado en la ejecución de las actividades de acuerdo a los niveles (Guirado, 2015):

- Aceptable: no se debe cambiar el procedimiento.

- Atención: es aceptable cierto grado, pero se debe realizar un seguimiento.
- Inaceptable: establecer un plan de acción para corregir el escenario actual.

Análisis de impacto sobre el negocio (BIA)

El impacto de riesgos es una herramienta que evalúa las consecuencias que podría sufrir una organización durante un desastre identificando los procesos críticos que son el foco principal para un plan de continuidad (Torres C. , 2013); además, este análisis es fundamental para elaborar un plan de recuperación ante desastre (DRP) que permite identificar y valorar las afectaciones económicas y funcionales de la empresa (Mendoza, 2014).

Para establecer el análisis de impacto sobre el negocio hay que tener claro los conceptos de: punto de recuperación objetivo o RTO (Tiempo de recuperación de las actividades de condiciones mínimas aceptables), tiempo de recuperación objetivo o MTD (Tiempo máximo tolerable de caída de un proceso antes de que se produzcan efectos desastrosos en la compañía y repercuta en el negocio) y periodo máximo tolerable de tiempo de inactividad o RPO (El grado de dependencia determina la cantidad máxima de información que se podría perder sin llegar a tener consecuencias inaceptables, formando parte de las políticas de respaldo que son definidas por la organización) (Instituto Nacional de Ciberseguridad, 2017).

Desarrollo de estrategias

El desarrollo de estrategias consiste en identificar alternativas de recuperación en los marcos de tiempos establecidos (Erazo, 2012); el cual, involucra los siguientes aspectos (MINTIC, 2015):

- Identificación de requerimientos.
- Evaluar la conexión de las estrategias contra los resultados sobre el impacto sobre el negocio.
- Establecer sitios de almacenamiento secundario (nubes) (ASPER, 2017).

Control de calidad

Son técnicas y actividades de acción operativa que se utilizan para obtener estándares de calidad del producto o servicio, cuya responsabilidad recae específicamente en el trabajador competente

(Guachi, 2012) (Sánchez E. , 2009). El proceso de control tiene la naturaleza de un ciclo de retroalimentación de la figura 4-5, que son aplicados en control de costos, de inventario, de calidad, etcétera (Valdas, 2015).

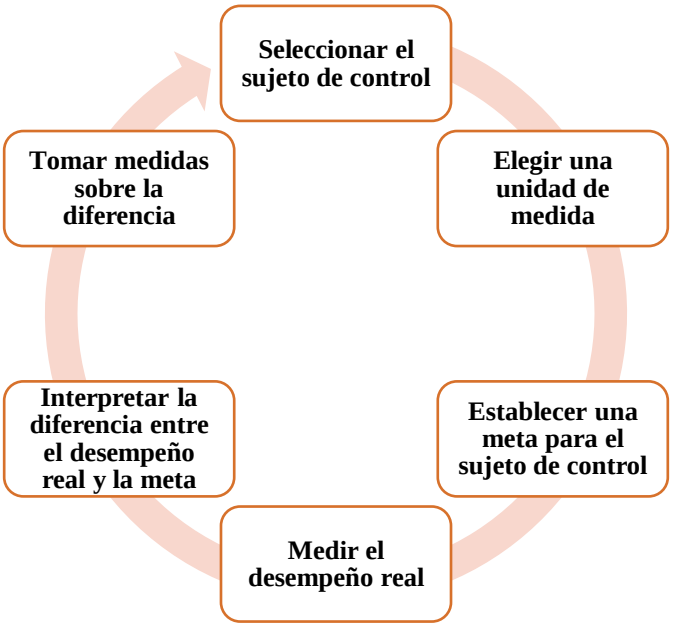


Figura 2-5. Ciclo de retroalimentación del proceso de control.

Elaborado por: (Ladine, 2017).

El seguimiento minucioso de los procesos dentro de una empresa o institución puede mejorar la calidad del producto y/o servicio si se realiza mediante la implantación de normas ISO.

Las ventajas de establecer procesos de control de calidad es el orden de la interrelación de los distintos procesos de la empresa, teniendo en cuenta un seguimiento detallado de las operaciones que se realizan con el fin de detectar los problemas para corregirlos eficientemente.

Normas ISO

Las normas ISO son diferentes programas, modelos, herramientas y/o técnicas utilizados por una empresa para mejorar de la calidad de sus productos y servicios; facilitando así, la coordinación y unificación de las normas internacionales e incorporando la idea de estandarización para adquirir beneficios de los productores y compradores de bienes y servicios.

Las normas ISO surgieron en el año 1987 por la Organización Internacional de Normalización (International Standard Organization ISO) (SPG, 2018), formada por más de noventa organismos, con el fin de internacionalizar los mercados con la competitividad de productos y servicios. La Organización ISO está compuesta por tres tipos de miembros:

- Miembros natos, conformado por un representante de cada nación.
- Miembros correspondientes, de los organismos de países en vías de desarrollo y que todavía no poseen un comité nacional de normalización. No toman parte activa en el proceso de normalización, pero están puntualmente informados acerca de los trabajos que les interesen.
- Miembros suscritos, países con reducidas economías a los que se les exige el pago de tasas menores que a los correspondientes.

Las series de normas ISO relacionadas con el riesgo y seguridad de la información constituyen lo que se denomina familia de norma (ISO tools, 2015) (Normas ISO, 2017), a las que se menciona a continuación:

- ISO 22301: Sistema de Gestión de Continuidad de Negocio.
- ISO 27001: Sistema de Gestión de Seguridad Informática.
- ISO 27005: Sistema de Gestión de Riesgos de Tecnologías de información.
- ISO 28000: Sistema de Gestión de la Seguridad para la Cadena de Suministro.
- ISO 31000: Sistema de Gestión de Riesgos.
- ISO 19600: Sistema de Gestión de Compliance.

Normas de seguridad informática

Teniendo en cuenta las normas ISO 27005 e ISO 22301, de seguridad de la información con relación al plan de continuidad de gestión de riesgos existe una alineación con un modelo PHVA (planificar- hacer- verificar- actuar) que se observa en la tabla 2-1 (Ramírez & Ortiz, 2011).

Tabla 2-1. Alineación de estándares ISO 31000 e ISO 27005, con modelo PHVA.

PHVAP	ISO 27005: 2013	ISO 22301: 2012
Planear	Definir plan de gestión de riesgos Establecimiento del contexto Identificación del riesgo Estimación del riesgo Evaluación del riesgo Desarrollo el plan de tratamiento del riesgo Aceptación del riesgo	Mandato y compromiso de dirección Diseño del marco de trabajo para gestión de riesgos Entender la organización y su contexto Definir responsabilidad Recursos Integración de procesos Establecer mecanismos de comunicación
Hacer	Implementar un plan de tratamiento Implementar un plan de comunicación de riesgo	Establecer políticas para la gestión de riesgo Implementación del marco de trabajo para la gestión de riesgos Implementar el proceso de gestión de riesgos
Verificar	Monitoreo y dirección de riesgo	Monitoreo y revisión del marco de trabajo
Actuar	Mantener y mejorar el proceso de gestión	Mejora continua del marco de trabajo

Elaborado por: (Rojas, 2017)(Ramírez & Ortiz, 2011) .

A pesar de que cada norma posee un enfoque distinto, todas identifican y analizan las actividades críticas que deben ser recuperadas en caso de existir interrupciones; además, proponen medidas para mitigar riesgos. A continuación, se mencionará a detalle las prioridades que poseen las distintas normas (Rojas, 2017):

ISO 27005: 2013. - Sistema de Gestión de Riesgos de Tecnologías de información, se enfoca en la gestión de seguridad de la información aportando diferentes recomendaciones y directrices para la gestión de riesgos (SGSI, 2017)(Espinoza, Martinéz, & Amador, 2014).

ISO 23001: 2012. - Sistema de Gestión de continuidad de negocios, se enfoca en determinar qué aspectos serán cubiertos y excluidos en el plan de continuidad de negocios con fin de comunicar al personal externo e interno de la institución para ayudar a minimizar el impacto que pueden perjudicar a los proveedores y clientes de la empresa (Sotres, 2012).

La materialización de riesgos puede implicar impactos grandes sobre el negocio, asociado a altos costos por recuperación e indisponibilidad de los servicios o productos que ofrece la organización. Cuando se realiza la valoración de riesgos dentro de la gestión de continuidad se tiene en cuenta la valoración del riesgo tecnológico y su efecto sobre los activos de información. Gracias a este análisis previo es posible realizar la identificación de los requerimientos mínimos para la

continuidad de las operaciones basado en las posibles interrupciones y con ello diseñar las alternativas estratégicas de operación y proceso.

Gerencia de sistemas

Órgano de apoyo, encargado de planificar, organizar, dirigir y evaluar la aplicación de las tecnologías de información para el adecuado uso y aprovechamiento de los recursos informáticos para la optimización de procesos (Slideshare, 2018)

Un Gerente de TI debe responder a las preguntas críticas del negocio y desde su área, aportar al logro de sus objetivos; es por ello que no basta con ser experto en tecnologías, ya que el cambio no es sólo de título, sino que conlleva cambio en actividades, actitud e impacto en la organización, por lo que también es indispensable un cambio en las habilidades y competencias de las personas desarrollando estos cargos. (Vanguardia, 2018)

2.4.3 Categorías de la Variable Dependiente

Disponibilidad de los sistemas de información y comunicación

Un sistema de información y comunicación se encuentra conformado por tres elementos que son: la información, recursos humanos y equipos computacionales que operan en conjunto para realizar actividades de administración, almacenamiento, procesamiento, transmisión o recepción datos e información (Paz, 2014) (Macua, 2004); con el único propósito de cumplir con los objetivos de la organización con partes definidas que son: entrada (captura de datos del interior y exterior del sistema de información), procesamiento (convertir datos e información de una manera más significativa para el negocio) y salida (transferir la información ya procesada a los usuarios para que desarrollen sus actividades diarias) (Rodríguez & Daureo, 2013) (Duménigo, 2012). En la actualidad el sistema de información y comunicación lo maneja el departamento informático de las instituciones.

El departamento de informática tiene un rol importante dentro de las organizaciones, debido al sustento técnico/tecnológico del procesamiento de datos (Palacios & Quiroz, 2013) (Macua, 2004); además, dirige las funciones de: gerencia de redes, soporte de usuarios, crear, administrar y dar seguimiento a las bases de datos, procurando siempre cuidar la integridad de equipos e

información, realizando aplicaciones y reportes que aporten insumos para la toma de decisiones, controlar usuarios y perfiles, etc. (Ladine, 2017)

El departamento informático debe ser proactivo al proponer decisiones de análisis con la suficiente capacidad de identificar los procesos que pueden ser automatizados, con el fin de reducir los problemas en las distintas áreas; siendo, un líder en la optimización de procesos y calidad, manteniéndose informados sobre los últimos avances tecnológicos y diseñar aplicabilidad en busca de la reducción de procesos y disminución de costos, así también dar seguimiento a los problemas de un sistema como una debilidad propia, debido a que dicha falla trae pérdidas económicas a la organización en general (Vigo, 2011).

Riesgos tecnológicos

Los riesgos tecnológicos que se pueden dar en una organización son por: materiales o procesos peligrosos, químicos o fenómenos debido a la interacción de estos puede causar consecuencias de salud, economía, medio ambiente e incluso al desarrollo integral de los sistemas (Estancio, 2016). Los riesgos tecnológicos pueden presentarse en una amplia gama de variedades, debe tenerse presente que no hay dos accidentes idénticos. Por ello los riesgos se clasifican según la variedad de la amenaza (Solis, 1997):

- Riesgo por Incendio o explosión. Presente sobre todo en plantas industriales y áreas de almacenamiento.
- Riesgo por escapes o derrames. Más común en plantas industriales y transporte de materiales peligrosos (sea por medio de tubería o por medio de vehículos automotores).
- Riesgo de intoxicación y exposición a radiaciones ionizantes. En procesos industriales y manejo inadecuado de desechos.

Indicadores de gestión.

Estos son los indicadores más representativos de la Dirección de Tecnología Informática relacionados con el proceso de planeación estratégica (Solozarno, 2018) (Robles, 2018):.

- Disponibilidad de infraestructura.
- Tiempo medio de atención.

- Porcentaje de identificaciones de servicios TIC activadas oportunamente.
- Porcentaje de identificaciones de servicios TIC desactivadas oportunamente.
- Nivel de oportunidad en la entrega de carné.
- Oportunidad en solución de incidentes, problemas y atención de solicitudes de productos e infraestructura TIC.
- Nivel de disponibilidad de los productos TIC.
- Eficacia de los controles de seguridad.
- Porcentaje de vulnerabilidades técnicas gestionadas.

2.5 Hipótesis

El Plan de continuidad de negocio de la Coordinación de Innovación Tecnológica del Servicio Nacional de Contratación Pública, si incide en la disponibilidad de los sistemas de información de la entidad.

2.6 Señalamiento de Variables

Variable Independiente: Plan de continuidad de negocio

Variable Dependiente: Disponibilidad Sistemas de información.

CAPÍTULO III

3. METODOLOGÍA

3.1 Enfoque

La investigación es cuantitativa porque se utilizará parámetros de medición para la variable dependiente y es cualitativa porque se emitirá juicios de valor sobre la investigación.

3.2 Modalidad básica de investigación

Investigación bibliográfica

Está investigación es bibliográfica porque se utilizará fuentes como libros, tesis, monografías, documentos, artículos, revistas, e incluso el internet para obtener información más profunda del marco teórico tanto de las normas y controles del plan de continuidad que se podría resumir en cuatro fases: planificación, identificación de amenazas, identificación de soluciones, estrategias.

Investigación de campo

La investigación además tiene la modalidad de campo porque se buscará obtener la información directa del Departamento de Innovación Tecnológica del SERCOP, en el lugar de los hechos para una adecuada documentación del proceso.

3.3 Nivel o tipo de investigación

Investigación exploratoria

Es una investigación exploratoria porque se analizará el problema, buscando obtener soluciones o alternativas actuales de la seguridad de los sistemas de información y comunicación con la implementación adecuado de los procedimientos.

Investigación descriptiva

La investigación es descriptiva porque se conocerá y analizará con profundidad el problema estableciendo las causas y consecuencias para una adecuada identificación de riesgos.

Investigación explicativa

Porque se buscará un control para verificar el cumplimiento de las políticas de un plan de continuidad del departamento de Coordinación e Innovación Informática del Servicio de Contratación Pública (SERCOP), partiendo de lo general a lo especifico (Método inductivo) y de lo específico a lo general (Método deductivo).

Investigación correlacional

Porque se buscará medir el grado de relación existente entre el cumplimiento de un plan de continuidad de negocio con la disponibilidad de los sistemas de información.

3.4 Población y muestra

El presente proyecto se desarrollará utilizando una muestra de población total que se beneficiará en el plan de contingencias para el sistema informático del Servicio de Contratación Pública (SERCOP)

Tabla 3-1. Población

Población	Número	Porcentaje
Coordinadora	1	12,5%
Director de seguridad informática	1	12,5%
Director de gestión de servicios informáticos	1	12,5%
Especialistas de seguridad informática	3	37,5%
Especialista de gestión de servicios informáticos	2	25,0%
Total	8	100 %

Elaborado por: Investigador

En referencia a la tabla 3-1, este trabajará la investigación con un grupo pequeño.

3.5 Operacionalización de variables

3.5.1 Variable independiente: Plan de Continuidad de Negocio

Tabla 3-2. Operacionalización de la variable independiente:

Conceptualización o Descripción	Dimensiones	Indicadores	Ítems Básicos	Técnicas e instrumentos
"Es un plan de emergencia con el objetivo de determinar los procesos críticos que afectarían el funcionamiento de los sistemas de información y comunicación de una organización a un nivel mínimo aceptable durante una contingencia"	- Ausencia de monitoreo en los sistemas de información y comunicación. - Coordinación con las autoridades. - Estrategias de recuperación. - Gestión de simulacros. - Gestión de riesgos. - Análisis de impacto en el negocio.	- Caídas del sistema cada año. - Políticas. - Lista de estrategias definidas. - Control de simulacros de la institución. - Análisis periódicos de los riesgos. - Identificación del tiempo de recuperación (RTO) y el punto de recuperación (RPO).	- ¿Al no contar con un plan de continuidad de negocios afecta negativamente la Coordinación de Innovación y Tecnológica? - ¿Existen políticas para la gestión de continuidad de negocios? - ¿Existe estrategias de recuperación de los servicios críticos frente a una caída de los sistemas de información y comunicación? - ¿Se realiza simulacros frente a una caída de los sistemas de información y comunicación? - ¿Se realiza tareas de monitoreo a los sistemas de información y comunicación? - ¿Se realiza el control de los procesos críticos?	- Encuesta

Elaborado por: Investigador

3.5.2 Variable dependiente: Disponibilidad Sistema de información.

Tabla 3-3. Operacionalización de la variable dependiente:

Conceptualización o Descripción	Dimensiones	Indicadores	Ítems Básicos	Técnicas e instrumentos
Un sistema de interacción de equipos y procedimientos, que hacen que la información pertinente esté disponible para la planificación, el análisis, la implementación y el control.	- Activación de los sitios de respaldo	- Tiempo necesario para reiniciar los sistemas críticos en el sitio de respaldo	- ¿Considera que un Plan de continuidad de negocios, mejorará la disponibilidad de los Sistemas de información?	- Encuesta

Elaborado por: Investigador

3.6 Plan de recolección de información

Para una adecuada recolección de información se utilizará técnicas como: observación y entrevista con registro de datos y un cuestionario para los empleados.

Tabla 3-4. Recolección de información.

Preguntas básicas	Explicación
¿Para qué?	Para evaluar el impacto de los procesos críticos.
¿De qué personas u objetos?	Clientes externos e internos.
¿Sobre qué aspectos?	Sistema de información.
¿Quién, Quiénes?	Investigador.
¿Cuándo?	Primera semana de la aprobación del plan.
¿Dónde?	Servicio Nacional de Contratación Pública
¿Cuántas veces?	Una vez
¿Qué técnicas de recolección?	Encuestas, Datos estadísticos
¿Con qué?	Cuestionario
¿En qué situación?	Horario laboral

Elaborado por: Investigador

3.7 Procesamiento y análisis de la información

Una vez recopilada la información, se seleccionará los datos con relación al problema planteado y serán analizados mediante una tabulación que permitirá visualizar los datos de forma más clara para relacionar las variables de investigación.

CAPÍTULO IV

4. ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

4.1 Análisis e interpretación de resultados

Mediante la recolección de datos realizados en el personal de Coordinación de Innovación Tecnológica, se procedió a realizar la tabulación, análisis e interpretación de datos. Cuyo objetivo es verificar la utilización de un plan de continuidad de negocios.

Las alternativas de cada respuesta se representan en la tabla de frecuencias con su respectivo porcentaje del total recolectado.

Para verificar la hipótesis se utilizó en análisis estadístico chi cuadrado (X^2) con un nivel de significancia del 0,05 que da un nivel de confianza de 95%. Para realizar el cálculo es necesario determinar los grados de libertad mediante la ecuación 4-1.

$$gl = (f - 1) * (c - 1)$$

Ecuación 4-1. Grados de libertad.

Fuente: (Mendivelso & Rodríguez, 2018)

Donde, gl son los grados de libertad, f las filas y c las columnas.

Para determina el punto crítico de la hipótesis nula para la distribución X^2, se utiliza el alfa de 0.05, los grados de libertar y se consulta en la tabla de distribución de probabilidad. Posteriormente, se calcula el valor esperado mediante la ecuación 4-2.

$$E_I = \frac{T_i * T_P}{T_e}$$

Ecuación 4-2. Valor esperado.

Fuente: (Mendivelso & Rodríguez, 2018)

Donde, E_I son los valores esperados de cada ítem, T_i es la suma total de cada ítem, T_P la suma total de cada pregunta y T_e es el total de la encuesta.

Y finalmente. Se determina el valor de X^2 mediante la suma de los valores esperados (ecuación 4-3).

$$X^2 = \sum_{i=1}^{K} \frac{(O_i - E_i)^2}{E_i}$$

Ecuación 4-3. Cálculo del chi cuadrado.

Fuente: (Mendivelso & Rodríguez, 2018)

Donde, O_i son los valores observados, E_i los valores esperados e i las variables.

4.1.1 Cuestionario para el personal de Coordinación de Innovación Tecnológica del Servicio Nacional de Contratación Pública.

El cuestionario consta de siete puntos, que se menciona a continuación:

Punto 1: ¿Al no contar con un plan de continuidad de negocios afecta negativamente a la disponibilidad de los sistemas de información de la Coordinación de Innovación y Tecnológica?

Tabla 4-1. Al no contar con un plan de continuidad de negocios afecta negativamente la Coordinación de Innovación y Tecnología del Servicio Nacional de Contratación Pública.

Alternativas	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Si	6	75%	75%	75%
No	2	25%	25%	100%
Total	**8**	**100%**	**100%**	

Fuente: Encuesta

Elaborador por: Investigador

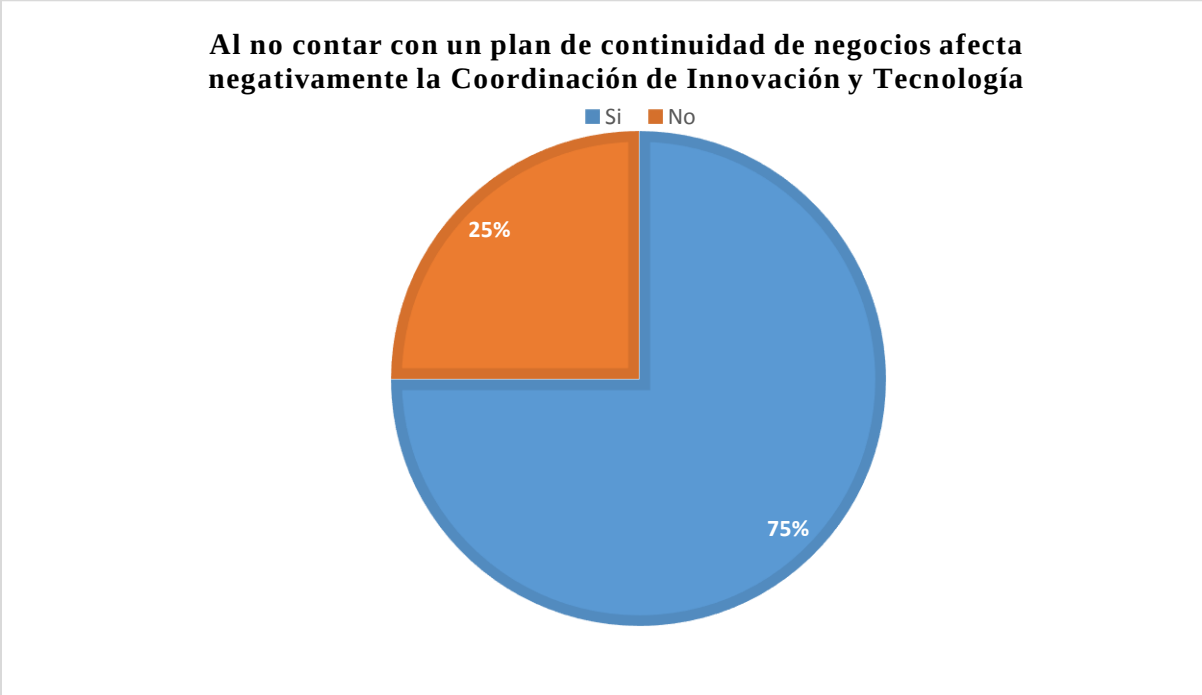


Figura 4-1. Al no contar con un plan de continuidad de negocios afecta negativamente
Fuente: Encuesta
Elaborado por: Investigador

Como se observa en la figura 4-1, se puede evidenciar que al no contar con un plan de continuidad de negocios afecta negativamente la Coordinación de Innovación Tecnológica del Servicio Nacional de Contratación pública con un 75% del "si", verificando la importancia de este proceso para el funcionamiento de la empresa en caso de ocurrir algún desastre.

Punto 2: ¿Existen políticas para la gestión de continuidad de negocios?

Tabla 4-2. Se aplican políticas de gestión de continuidad de negocios.

Alternativas	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Si	2	25%	25%	25%
No	6	75%	100%	100%
Total	**8**	**100%**	**100%**	

Fuente: Encuesta

Elaborado por: Investigador

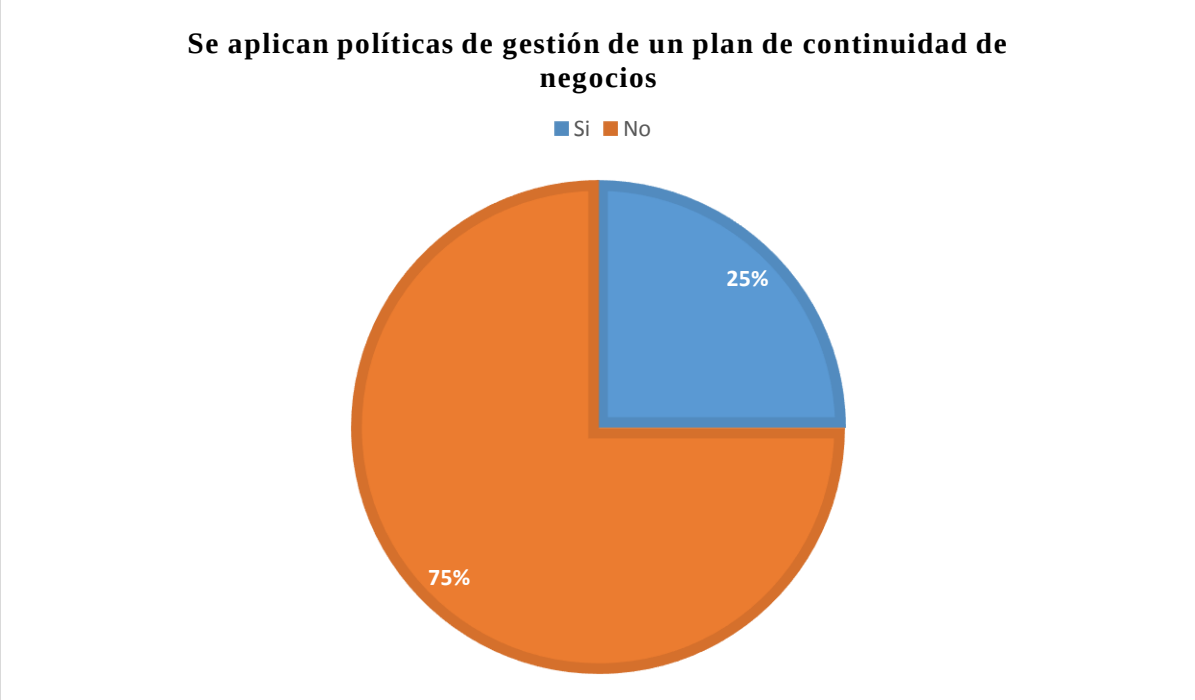


Figura 4-2. Se aplican políticas de gestión de un plan de continuidad de negocios.

Fuente: Encuesta

Elaborado por: Investigador

Como se observa en la figura 4-2, predomina el "no" con un 75%; ya que, al no existir un plan de continuidad de negocios no se evidencia la existencia de políticas de gestión. Justificando la necesidad de realizar un análisis del contexto en la institución.

Punto 3: ¿Existe estrategias de recuperación de los servicios críticos frente a una caída de los sistemas de información y comunicación?

Tabla 4-3. Existen estrategias de recuperación de los servicios críticos frente a una caída de los sistemas de información y comunicación.

Alternativas	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Si	2	25%	25%	25%
No	6	75%	100%	100%
Total	**8**	**100%**	**100%**	

Fuente: Encuesta

Elaborado por: Investigador

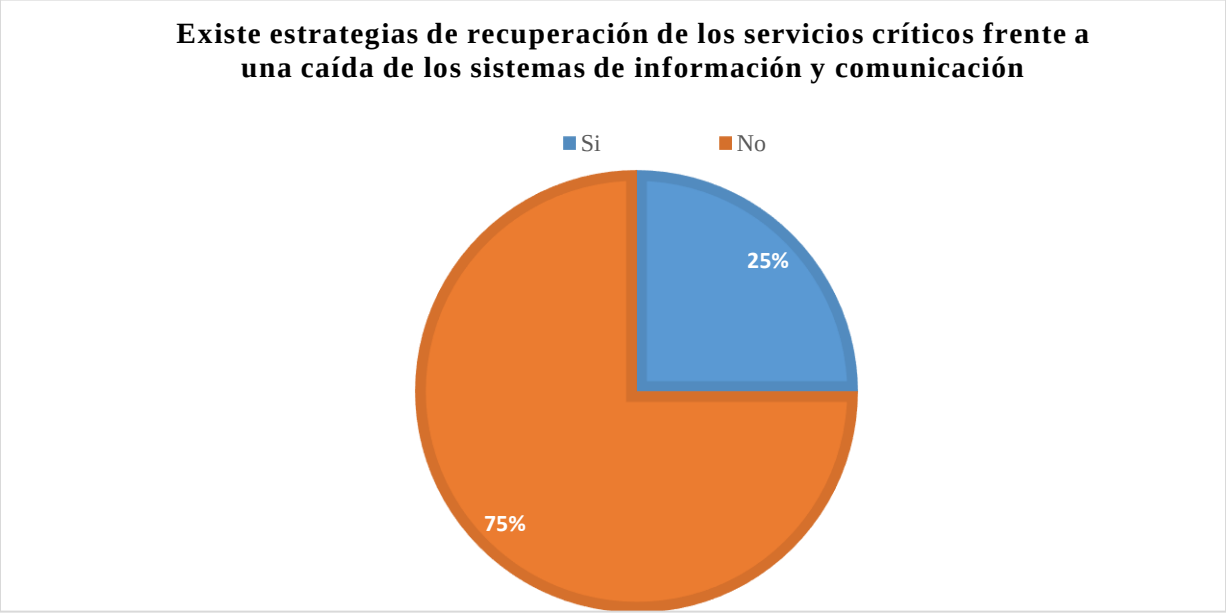


Figura 4-3. Existen estrategias de recuperación de los servicios críticos frente a una caída de los sistemas de información y comunicación.

Fuente: Encuesta

Elaborado por: Investigador

Como se muestra en la figura 4-3, con un 75% se puede verificar la ausencia de estrategias de recuperación de los servicios críticos frente a una caída de los sistemas de información y comunicación.

Punto 4: ¿Se realiza simulacros frente a una caída de los sistemas de información y comunicación?

Tabla 4-4. Se realiza simulacros frente a una caída de los sistemas de información y comunicación.

Alternativas	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Si	3	37,5%	37%	37%
No	5	62,5%	63%	100%
Total	**8**	**100%**	**100%**	

Fuente: Encuesta

Elaborado por: Investigador

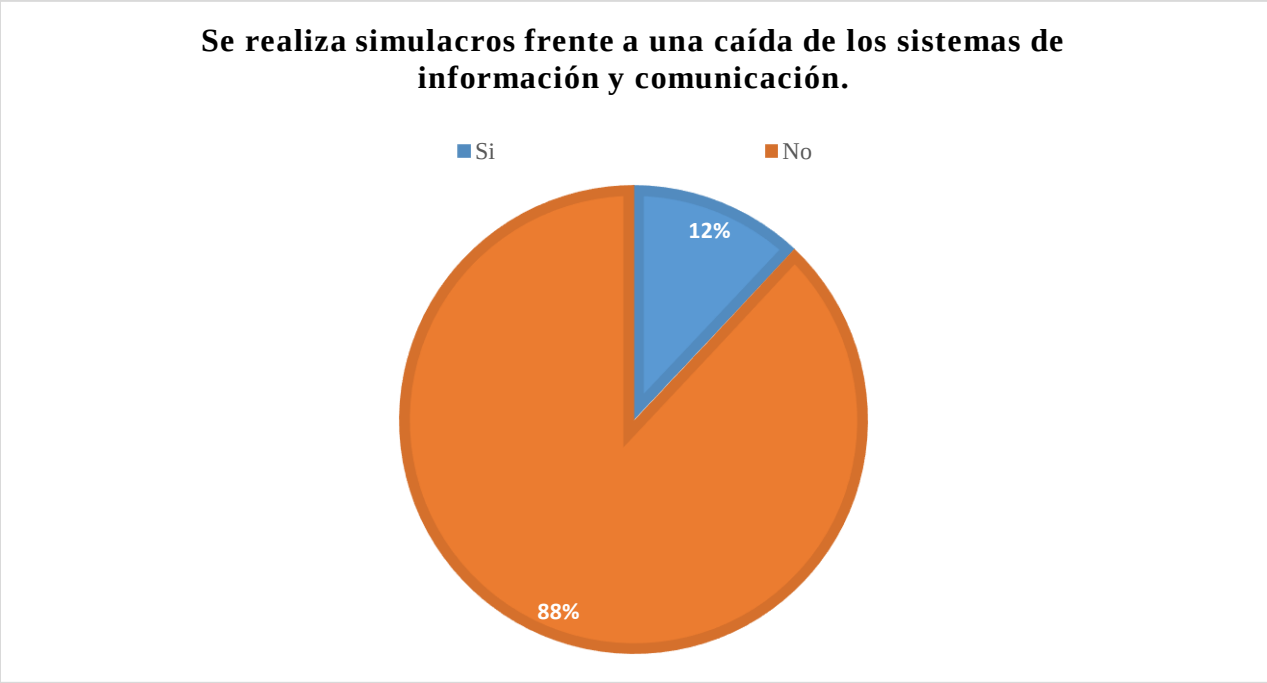


Figura 4-4. Se realiza simulacros frente a una caída de los sistemas de información y comunicación.

Fuente: Encuesta

Elaborado por: Investigador

Según los encuestados, no se realiza simulacros frente a la caída de los sistemas de información y de comunicación en un 88% con “no”; por ende, es necesario una adecuada proyección del plan de continuidad.

Punto 5: ¿Se realiza tareas de monitoreo a los sistemas de información y comunicación?

Tabla 4-5. Realización de tareas de monitoreo a los sistemas de información y comunicación.

Alternativas	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Si	1	12,5%	12%	12%
No	7	87,5%	88%	100%
Total	**8**	**100%**	**100%**	

Fuente: Encuesta

Elaborado por: Investigador

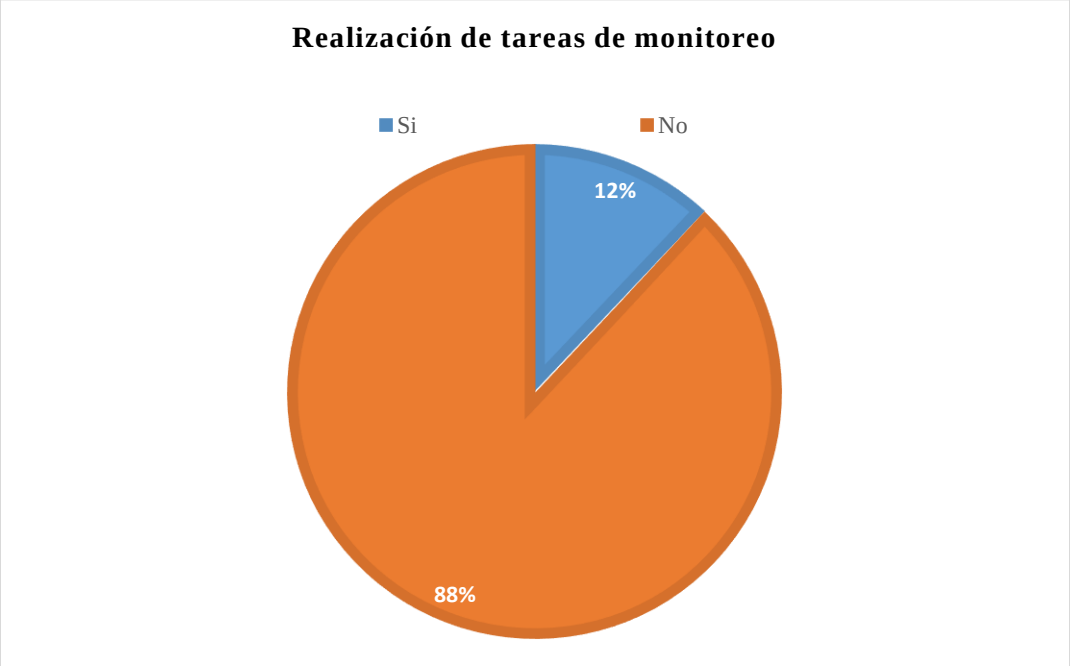


Figura 4-5. Realización de tareas de monitoreo a los sistemas de información y comunicación.

Fuente: Encuesta

Elaborado por: Investigador

Como se observa en la figura 4-5, predomina con el "no" del 88%; lo cual, se establece el inadecuado monitoreo de los sistemas de información y comunicación, por lo que es necesario la verificación y control del plan de continuidad propuesto.

Punto 6: ¿Se realiza el control de los procesos críticos de los sistemas de información y comunicación?

Tabla 4-6. Se realiza el control de los procesos críticos de los sistemas de información y comunicación.

Alternativas	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Si	2	25%	25%	25%
No	6	75%	75%	100%
Total	**8**	**100%**	**100%**	

Fuente: Encuesta

Elaborado por: Investigador

Figura 4-6. Se realiza el control de los procesos críticos de los sistemas de información y comunicación

Fuente: Encuesta

Elaborado por: Investigador

En la figura 4-6, se observa un “no” de 75%, lo que podría ocasionar fallas en el sistema y en los servicios de la institución.

Punto 7: ¿Un plan de continuidad de negocio mejorará la disponibilidad de los sistemas de información de la entidad?

Tabla 4-7. Considera que un plan de continuidad de negocios mejorará la disponibilidad de los Sistemas de información de la entidad.

Alternativas	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Si	8	100%	100%	100%
No	0	0%	0%	100%
Total	**8**	**100%**	**100%**	

Fuente: Encuesta

Elaborado por: Investigador

Figura 4-7. Considera que un Plan de continuidad de negocios, mejorará la disponibilidad de los Sistemas de información

Fuente: Encuesta

Elaborado por: Investigador

En la figura 4-7, se observa un "si" del 100%, evidenciando la necesidad de la existencia de un Plan de Continuidad de negocios para la recuperación de los sistemas ante una caída.

4.2 Verificación de la hipótesis.

Para verificar la hipótesis dentro de la investigación realizada al personal se utilizó el análisis estadístico del Chi Cuadrado, que permite evaluar directamente el impacto de la propuesta planteado del plan de continuidad de negocios para la administración y control de los procesos críticos en la Coordinación de Innovación Tecnología del Servicio Nacional de Contratación Pública.

4.2.1 Planteamiento de la hipótesis

Modelo lógico

Hipótesis nula (H_0).- La ejecución del plan de continuidad de negocios para la recuperación y restauración de funciones críticas informáticas NO impacta positivamente en la administración y control de la Coordinación de Innovación Tecnológica del Servicio Nacional de Contratación Pública.

Hipótesis alternativa (H_1).- La ejecución del plan de continuidad de negocios para la recuperación y restauración de funciones críticas informáticas impacta positivamente en la administración y control de la Coordinación de Innovación Tecnológica del Servicio Nacional de Contratación Pública.

Modelo matemático

H_0: Observado (O) ≠ Esperado (E)

H_1: Observado (O) = Esperado (E)

Modelo estadístico

Para verificar la hipótesis se utilizó la prueba del chi cuadrado en las preguntas, tomando en cuenta los valores observados en la encuesta (tabla 4-8).

Tabla 4-8. Valores observados

Preguntas	Ítems		Total
	Si	No	
1	6	2	8
2	2	6	8
3	2	6	8
4	3	5	8
5	1	7	8
6	2	6	8
7	8	0	8
Total	**24**	**32**	56

Elaborado por: Investigador

Por lo tanto, fue necesario determinar los valores esperados mediante la ecuación 4-9.

Tabla 4-9. Valores esperados

Preguntas	Ítems		Total
	Si	No	
1	3,43	4,57	8
2	3,43	4,57	8
3	3,43	4,57	8
4	3,43	4,57	8
5	3,43	4,57	8
6	3,43	4,57	8
7	3,43	4,57	8
Total	24	32	56

Elaborado por: Investigador

Y finalmente, se determinó el valor del chi cuadrado como se observa en la tabla 4-10

Tabla 4-10. Cálculo del chi cuadrado

Preguntas	Ítems		Total
	Si	No	
1	1,93	1,45	3,38
2	0,60	0,45	1,04
3	0,60	0,45	1,04
4	0,05	0,04	0,09
5	1,72	1,29	3,01
6	0,60	0,45	1,04
7	6,10	4,57	10,67
Total	11,58	8,69	**20,27**

Elaborado por: Investigador

La figura 4-8, muestra el valor crítico tomado a un nivel de significancia de 0,05 con el grado de libertad de 6 obteniendo el valor crítico de que se muestra en la tabla 4-18.

SIGNIFICANCIA

GRADOS DE LIBERTAD	0,05	0,025	0,01	0,005
1	3,841	5,024	6,635	7,879
2	5,991	7,378	9,210	10,597
3	7,815	9,348	11,345	12,838
4	9,488	11,143	13,277	14,860
5	11,07	12,832	15,086	16,750
6	**12,592**	14,449	16,812	18,548
7	14,067	16,013	18,475	20,278
8	15,507	17,535	10,09	21,955
9	16,919	19,023	21,666	23,589

Figura 4-8. Valor crítico.

Fuente: (Palacios E. , 2019).

Tabla 4-11. Valor calculado

Grados de libertad	7
Valor crítico	12,592
chi^2	20,270

Elaborado por: Investigador

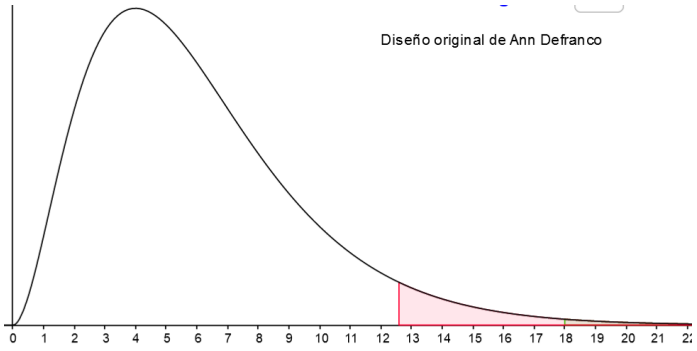


Figura 4-9 Gráfica Chi Cuadrado

Elaborado por: Investigador

Decisión

De acuerdo a los resultados en la encuesta, se rechaza la hipótesis nula y se acepta la hipótesis alterna; por lo tanto, es factible la propuesta del plan de continuidad de negocios SÍ impacta positivamente en la administración y control de la Coordinación de Innovación Tecnológica del Servicio Nacional de Contratación Pública.

CAPÍTULO V

5. CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- Posterior a la aplicación de la encuesta aplicada al personal de la Coordinación de Innovación Tecnológica del Servicio Nacional de Contratación Pública y análisis de la información recopilada, se puede concluir que, al no contar con un Plan de continuidad de negocio, se ve afectada la disponibilidad de los sistemas de información.
- Con base a los datos estadísticos obtenidos, es necesario definir las políticas de continuidad de negocio para la posterior aplicación y cumplimiento.
- Se requiere coordinar pruebas o simulacros frente una posible caída de los principales sistemas de información que administra la Coordinación de Innovación tecnológica del Servicio Nacional de Contratación Pública.
- Se observa que al momento no se cuenta con estrategias precisas con tareas y responsables, que permitan recuperar el normal funcionamiento de los sistemas de información de la entidad.
- No se cumple de manera eficiente el monitoreo del comportamiento adecuado de los sistemas de información y de la infraestructura tecnológica para detectar de manera temprana una posible interrupción o caída de los sistemas de información.
- Al momento, la entidad no cuenta con un plan de continuidad de negocio que permitan retomar las actividades normales de los sistemas de información en caso de presentar una caída o interrupción.

5.2 Recomendaciones

- Desarrollar un análisis de las características, procesos críticos y los riesgos de la empresa; además, crear una proyección de un plan de continuidad que integre el alcance, políticas, requisitos, principios y objetivos, por parte de las cuatro direcciones que forman parte de la Coordinación de Innovación Tecnológica.
- Es necesario disponer a las direcciones de Operaciones de Innovación Tecnológica y Seguridad Informática ejecutar un control y monitoreo de todas las actividades y funcionalidades relacionadas a los sistemas de información y de comunicación.
- La dirección de operaciones de Innovación Tecnológica y Seguridad informática debe generar la propuesta con los estándares adecuados de implementación del plan de continuidad para mejorar la confidencialidad, integridad y disponibilidad de los sistemas de información y comunicación.
- El especialista de Desarrollo de soluciones tecnológicas debe crear un instructivo en el que se plasme los pasos y persona responsable para ejecutar tareas de recuperación de los sistemas de información de la entidad.
- La Dirección de Seguridad Informática, debe crear estrategias e instructivos que permitan mejorar el monitoreo que se ejecuta a las aplicaciones e infraestructura tecnológica de la entidad.
- Los especialistas de Operaciones de Innovación tecnológica y Gestión de Servicios Informáticos, deben generar documentos técnicos que permitan tener una visión clara del proceso requerido para levantar los sistemas de información de la entidad, en el caso de que se reduzcan incidentes.
- Se recomienda la elaboración de un Plan de Continuidad de negocio para los sistemas de información del Servicio Nacional de Contratación Pública.

CAPÍTULO VI

6. PROPUESTA

6.1 Datos informativos

Tema:	"Propuesta de un Plan de continuidad del negocio para una entidad pública del Ecuador"
Institución:	SERCOP- Servicio Nacional de Contratación Pública
Provincia:	Pichincha
Cantón:	Quito
Dirección:	Av. De los Shyris, El Telégrafo 38-38 y, Quito 170135
Beneficiarios:	Personal de coordinación e innovación de tecnología.
Ejecución:	Inicia el 25 de mayo hasta el 26 de agosto de 2019.
Responsable:	Ing. Glenda Araujo
Director:	Ing. Edison Álvarez

6.2 Antecedentes de la propuesta

El exInstituto Nacional de Contratación Pública actualmente Servicio Nacional de contratación Pública fue creado por la Asamblea Constituyente a través de la Ley Orgánica del Sistema Nacional de Contratación Pública publicada en el Registro Oficial No. 395 del 4 de agosto del 2008. Al ser una institución de reciente creación fue muy importante que cuente con una visión clara de futuro para guiar a la institución a cumplir con los objetivos para los que fue creada.

El avance tecnológico cada vez cobra más importancia en el interior de organizaciones y empresas, por lo cual es necesario contar con un medio que garantice el correcto funcionamiento de la plataforma tecnológica en el menor tiempo posible en cualquier eventualidad, para se decide implementar un Plan de Continuidad Informático, el cual es un conjunto de actividades que nos permiten realizar acciones para minimizar los riesgos en caso de algún desastre de origen natural o humano, manteniendo la operatividad de las actividades a un mínimo nivel hasta recuperar la totalidad de los sistemas y recursos.

El procesamiento electrónico informático se ha convertido en estrategia para lograr una mayor optimización de la gestión empresarial.

Un plan de contingencia se encuentra conformado por tres acciones fundamentales que son: prevención, detección y recuperación.

Luego de efectuar una revisión y análisis bibliográfico, en el repositorio de la Universidad no se encontró trabajos netamente relacionados a un plan de continuidad de negocio mediante la norma ISO 22301, la misma que está orientada a la gestión de la continuidad de negocio, logrando que se minimice el impacto de algún tipo de incidente que provoque una interrupción a las actividades que se están realizando, según (BSI, 2019), tanto para sus activos como para sus procesos.

La investigación de (Guachi, 2012) trata de la confidencialidad de los sistemas de información aplicando la norma de seguridad ISO 27001 en la cual se resalta que, en la actualidad las empresas se enfrentan a muchos riesgos e inseguridades procedentes de focos diversos. Esto quiere decir que los activos de información de las empresas, uno de sus valores más importantes, se encuentran ligados o asociados a riesgos y amenazas que explotan una amplia tipología de vulnerabilidades; donde concluye que para garantizar y mejorar la seguridad en cuanto a la confiabilidad, disponibilidad e integridad de la información en el Departamento de Sistemas de la Institución Financiera se diseñó un Sistema de Gestión de Seguridad de la Información, en donde se determinó que algunos activos se encuentran desprotegidos por ende se definieron controles que aseguren la protección de la información.

Por otro lado se encontró en el trabajo de (Morales, 2019) una investigación sobre seguridad de la información aplicando la Norma ISO 27001 en el cual tiene como objetivo principal Diseñar un Balanced Score Card para seguridad de la información bajo el estándar ISO 27001 en Cooperativas de Ahorro y Crédito definiendo políticas de seguridad de la empresa, identificando los activos de la información y que tan vulnerable pueden ser los distintos departamentos de la institución financiera ante cualquier tipo de amenaza, donde concluyó que este modelo cubre los activos dependiendo de la actividad económica , es decir es factible aplicar el mismo modelo en otras entidades con las mismas características, garantizando que el área que gestiona los riesgos de la empresa pueda dar seguimiento fácilmente a los planes de acción que se encuentran en curso o aquellos que se encuentran próximos a alcanzar su fecha de ejecución o a su vez aquellos que ya

han cumplido su plazo, garantizando a la entidad financiera y a sus clientes información segura y por ende confianza en ellos.

Además, se encontró una guía basada en definiciones de plan de continuidad de negocios escrita por (Gaspar Martinez, 2006), defiende que un plan de continuidad de negocios debería hacer frente a:

- Aumentar la probabilidad de continuidad de las funciones críticas de la organización en caso de que un incidente interrumpa las operaciones informáticas en las que se apoya, además proporcionar un enfoque organizado y consolidado para dirigir actividades de respuesta y recuperación ante cualquier incidente o interrupción de trabajo imprevista, evitando confusión y reduciendo la situación de tensión.
- Reducir el tiempo de recuperación, y como consecuencias, las pérdidas económicas, directas e inducidas, como resultado de un desastre.

El propósito de la presente investigación es elaborar un Plan de Continuidad para mejorar la seguridad de los sistemas de información y comunicación del Servicio Nacional de Contratación Pública ya que es imperante disponer de una plataforma confiable debido a la compra pública de todas las entidades del estado incluyendo bienes, obras y servicios.

6.3 Justificación

En la actualidad la continuidad en todo tipo de negocio es importante debido a la prioridad que se proporciona a los clientes externos o internos y resultados de gestión. El Servicio de Contratación Pública necesita contar con un plan para proteger la continuidad de las operaciones y salvaguardar procesos tecnológicos ante un desastre; se utiliza la norma ISO 22301 que se refiere a la gestión de continuidad del negocio, Según (The British Standards Institution, 2017) “El sistema de gestión ISO 22301 permite identificar las amenazas relevantes y las funciones empresariales críticas que podrían sufrir consecuencias. También le permite establecer planes con antelación para asegurarse que su empresa no detiene su actividad.”, complementando a esta norma se utiliza la ISO 27005 que facilita las directrices para la gestión del riesgo en la seguridad de información; de esta forma

se logre mitigar el riesgo de divulgación o fallas en los sistemas por eventos infortunados y por el contrario recupere actividades, procesos operativos y tecnológicos de la institución.

6.4 Objetivos

6.4.1 General

Desarrollar una propuesta de un Plan de Continuidad para los sistemas informáticos que administra la Coordinación de Innovación Tecnológica del Servicio Nacional de Contratación Pública.

6.4.2 Específicos

- Ejecutar los pasos necesarios para crear una propuesta de un plan de continuidad de negocios en los sistemas informáticos de la Coordinación de Innovación.
- Realizar un análisis de contexto donde se pueda evidenciar las actividades tecnológicas de la entidad.
- Identificar los procesos críticos y establecer los tiempos de recuperación mediante el método de RTO y RPO respectivamente para cada proceso.
- Determinar el alcance, políticas, requisitos, principios y estrategias de mitigación en la fase de proyección del Plan de continuidad del negocio.
- Desarrollar un Plan de continuidad del negocio basado en la definición de procedimientos, análisis de impacto y un informe de incidencias donde se detalle las pruebas realizadas y los responsables respectivamente.
- Establecer un plan de mantenimiento del Plan de continuidad del negocio, estableciendo tiempos, responsables, actividades para tener una propuesta de mejora y finalmente un informe de resultados.

6.5 Análisis de factibilidad

6.5.1 Factibilidad operacional

Este proyecto es factible operativamente porque se contaría con el apoyo de la gerencia de las organizaciones interesadas en aplicarlo y obtener los beneficios.

6.5.2 Factibilidad técnica

Este proyecto es técnicamente factible de realizar ya que se cuenta con los recursos tecnológicos requeridos, es decir, la infraestructura, herramientas tecnológicas o software, acceso a datos e información requerida, están disponibles.

6.5.3 Factibilidad financiera

Toda la parte económica que se emplee en la planificación y ejecución de la propuesta estará a cargo de la investigadora que desea proponer una propuesta acorde a la problemática del departamento de Coordinación e Innovación Tecnológica.

6.6 Fundamentación

El propósito principal de un plan de continuidad es levantar los sistemas en situaciones extremas (desastres naturales, ataques cibernéticos, virus informáticos, errores humanos, etc.) minimizando las consecuencias y ofreciendo servicios a sus clientes, proveedores y funcionarios en el menor tiempo posible (Córdoba, 2008). La colaboración de todos los involucrados de la empresa junto al respaldo de los directores de la organización optimiza la implementación del plan de continuidad para tener un mejor retorno de las operaciones minimizando las afectaciones (Rodriguez, 2018).

Los planes de continuidad son diferentes para cada empresa; sin embargo, todos comparten tres principios básicos que son: recuperar el funcionamiento normal de los procesos tecnológicos, mantener activo la empresa e incorporar los criterios de las autoridades (ISO tools, 2015). Es posible que varias organizaciones realicen los componentes del "Plan" de la ISO 27031 como parte de sus programas de recuperación de desastres de tecnología de la información la cual se centra en los aspectos críticos necesarios para el diseño e implementación exitosos de un Sistema de gestión de seguridad de la información (Ramiro, 2018). Por ende, es importante incorporar las normas en un plan de continuidad para un proceso efectivo de la propuesta.

6.7 Metodología, modelo operativo

Se utiliza la siguiente metodología para diseñar un plan de continuidad de negocios se puede apreciar el diseño de la tabla 6-1; donde, Ay B con la ISO 27005:2013 e ISO 22301:2012; además

cuenta con cinco fases: análisis de contexto, proyección, desarrollo, verificación, control y mejoramiento del PCN.

Tabla 6-1. Metodología para el plan de continuidad.

Actividades	Referente que sustenta la actividad
Fase I: Análisis del contexto	
Actividades y funciones de la organización	B
Identificar procesos y sus interrelaciones	A-B
Determinar procesos críticos (TRO y PRO)	A-B
Análisis de impacto (AIN)	A-B
Fase II: Proyección del PCN	
Determinar alcance	Autor
Determinar políticas	B
Determinar requisitos	B
Determinar principios	B
Determinar objetivos	B
Definir estrategias de mitigación	A-B
Fase III: Desarrollo del PCN	
Definir procedimientos	A-B
Análisis de impacto	A-B
Generación de informe de incidencias	Autor
Fase IV: Verificación y control del PCN	
Análisis de informes de incidencia	A-B

Elaborado por: (Rojas, 2017).

En la tabla 2-2 se puede observar la metodología del plan de continuidad, la misma que se va a desarrollar con la ayuda de cinco fases que comienza con el análisis de las actividades y funciones específicas de la organización hasta el mejoramiento y los informes de resultados que arroja la metodología.

La primera fase se encarga en la definición de las características organizacionales, debe ser lo más detallada posible con el propósito de conocer a qué tipo de organización se va a realizar el estudio; y, a partir de esto fundamentar las siguientes etapas.

La identificación de los procesos que realiza la institución se convierte en otra de las fases importantes que se debe cumplir para la implementación de un plan de continuidad; en esta fase se debe determinar las prácticas de la institución y la dependencia que tiene cada una de ellas.

Durante este procedimiento se debe considerar los factores que intervienen, tales como: recursos tecnológicos, financieros, humanos, entre otros.

Después de identificar los procesos generales de la organización se debe entrar en un estudio para clasificar aquellos que son críticos en la organización y continuidad de negocio; así, determinar el nivel de impacto que conlleva cada proceso en un plan de continuidad.

La última etapa de la primera fase es el análisis de riesgos (tecnológicos, humanos y naturales) a los que están expuestos los procesos, donde se debe realizar un estudio si las amenazas son externas o internas y el nivel de afectación a los procesos tecnológicos.

Ya teniendo claro de los procesos que realiza la institución y los aspectos que influyen en su entorno natural tanto positivos como negativos, se procede a ejecutar el BCP, es ahí donde comienza la segunda fase de proyección. En esta se fundamentan las políticas, el alcance requisitos, objetivos y principios del Plan de continuidad del negocio.

En la fase de desarrollo del Plan de continuidad del negocio se define los procesos, se realiza un análisis de impacto y se genera un informe de incidencias donde se detalla los procesos que se va a cumplir para un BCP junto con los responsables. En verificación y control del BCP interviene el análisis del informe de incidencias realizado en la fase anterior, la evaluación de desempeño.

6.7.1 Alcance del modelo

Se plantea como alcance de la propuesta del plan de continuidad de negocios la conformación de políticas, procesos críticos, los resultados del análisis de riesgos, las estrategias y procedimientos de mitigación y recuperación.

No es objetivo de esta investigación presentar una descripción técnica detallada de una implementación de la propuesta ni sugerir la mejor solución administrativa en la Coordinación e Innovación Tecnológica.

6.7.2 Análisis del contexto

De acuerdo a la ISO 22301: 2013 en el punto 4.1, el análisis de contexto es fundamental en la propuesta de un sistema de continuidad empresarial porque determina los asuntos internos y

externos convenientes a sus objetivos, llegando a determinar el tipo de metodología en cualquiera de las organizaciones empresariales. Esto implica que la organización debe identificar los factores que impactan en su cultura, objetivos y metas, la complejidad de los productos, el flujo de procesos e información, sus mercados, clientes, entre otros (Castañeda, 2016).

Es por esta razón que en la primera fase de implementación del BCP direccionado a los riesgos tecnológicos se analiza todos los elementos que intervienen en el comportamiento empresarial y que son importantes para las otras fases propuestas en esta investigación. Por lo tanto, es esencial establecer un análisis del contexto antes de iniciar una propuesta del plan de continuidad de negocios; para ello, es necesario establecer las partes interesadas y la determinación del alcance teniendo en cuenta las actividades de la empresa tales como: servicios, misiones, visiones, departamentos, líneas de estratégicas y bases legales; además, de definir los procesos, activos y relaciones con terceros que afecten a los procesos críticos de la empresa.

Del mismo modo es necesario definir una metodología para el mantenimiento del plan de continuidad, tanto a nivel organizativo como documental.

6.7.2.1 Definir características organizacionales

Todas las empresas tienen características organizacionales que las define de acuerdo a la ISO 22301: 2013 punto 4.2.2.

Los objetivos y metas por conseguir determinan cómo están organizadas las compañías en niveles jerárquicos, departamentales, funcionales, entre muchas otras unidades de negocio (Pérez, 2016).

Servicios

Los servicios que ofrece la institución son:

- Dirige y coordinara acciones oportunas en proyectos, acciones y actividades en el ámbito técnico del servicio de contratación pública.
- Manejo de compras públicas.
- Implementar estrategias para prevenir la corrupción.
- Mejora continua de procesos internos.

Misión

"Es el ente rector, técnico, regulador y autónomo de la contratación pública del Ecuador que brinda a instituciones públicas y proveedores un modelo de gestión que asesora, controla y supervisa, sobre la base de los principios de eficacia, eficiencia, transparencia, calidad y concurrencia, en los procedimientos de contratación" (SERCOP, 2018)

Visión

"Ser al 2021, la institución pública reconocida a nivel regional por su alto grado de transparencia y calidad en sus servicios, facilitando e innovando la contratación pública" (SERCOP, 2018)

Estrategia

Comprometidos con la calidad, eficiencia, transparencia, confianza y satisfacción de nuestros usuarios, mejoramos continuamente el Sistema Nacional de Contratación Pública, a través del uso eficiente del gasto público, la regulación, normalización de productos y servicios de la compra pública, innovación de nuestros procesos y servicios, capacitación a nuestros actores y prohibiendo expresamente la práctica de actos de corrupción y soborno, cumpliendo los requisitos técnicos y legales, incluyendo los relacionados a combatir la corrupción, apoyados en un equipo humano responsable y con valores y principios éticos.

Promovemos la participación de nuestras partes interesadas a que expongan y denuncien cualquier acto de corrupción, sin temor a represalias, amparados en la autoridad e independencia de la Función de Cumplimiento establecida por el SERCOP.

Líneas estratégicas

Objetivos estratégicos institucionales

- Incrementar la transparencia de la gestión de la contratación pública del Ecuador.
- Incrementar el aseguramiento de la calidad en normativas y técnicas para la gestión transparente de la contratación pública.
- Incrementar la efectividad de la gestión de la contratación pública del Ecuador.

- Incrementar el desarrollo del talento humano en el Servicio Nacional de Contratación Pública.
- Incrementar el uso eficiente del presupuesto en el Sistema Nacional de contratación Pública" (SERCOP, 2018).

Bases legales

"Registro Oficial No. 066 miércoles 18 de abril de 2007 FUNCIÓN EJECUTIVA DECRETOS: 258: Créase el Sistema Nacional de Compras Públicas Función Ejecutiva Decretos 258: Créase el Sistema Nacional de Compras Públicas" (Compras públicas, 2018).

6.7.2.2 Identificación de los procesos organizacionales

En la figura 6-1, se observa el resumen los procesos de servicios de la institución que se describe claramente en el sitio web (SERCOP, 2018).

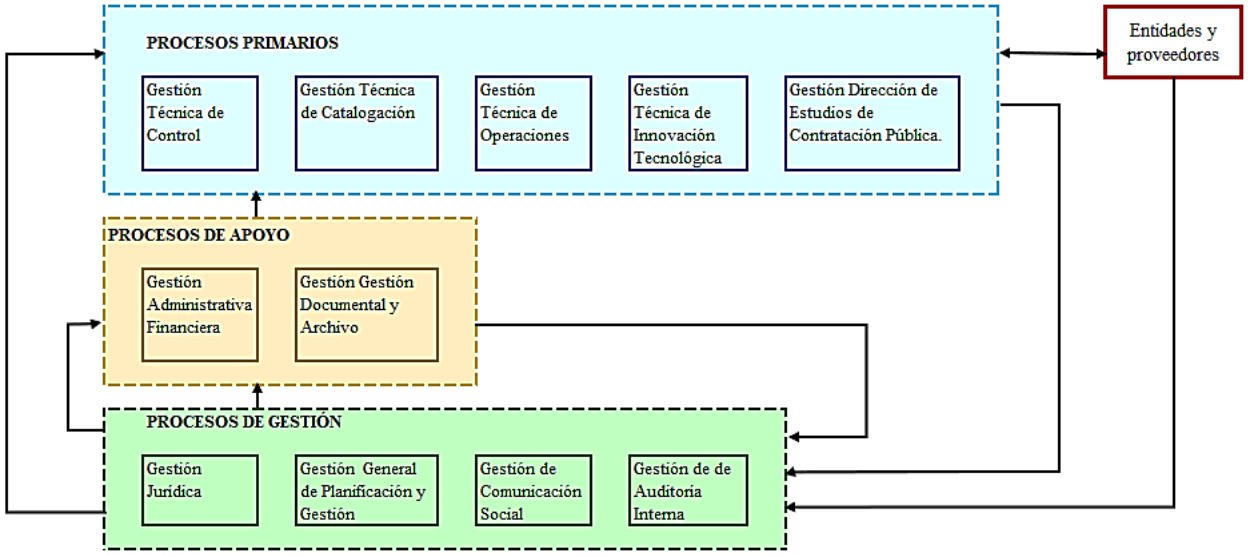


Figura 6-1. Alineación de la ISO 3100 e ISO 27005.

Elaborado por: Investigador

Se describe once macroprocesos son sus procesos y subprocesos respectivamente que se definen en la tabla 6-2; donde, cinco son los procesos primarios, cuatro son procesos de gestión y dos son procesos de apoyo.

Tabla 6-2. Macroprocesos, procesos y subprocesos del servicio de contratación pública.

MACROPROCESO	PROCESO	SUBPROCESO
GESTIÓN DE INNOVACIÓN TECNOLÓGICA	Gestión de Servicios Informáticos.	Planifica, establece, dirige y controla los procesos de tecnologías de la información y comunicación.
		Validación de las consultas técnicas de los usuarios en el sistema.
		Aprobar estudios, adquisición, mejora, mantenimiento y operación de los sistemas, plataformas y aplicaciones informáticas.
		Presentar propuestas para el desarrollo e implantación de las plataformas y aplicaciones informáticas utilizadas por la Institución.
		Coordinar la elaboración y ejecución del plan estratégico informático de la Institución.
		Articular con las unidades administrativas involucradas, la implementación de los sistemas informáticos.
		Articular la relación con los proveedores de las aplicaciones para la gestión de servicios informáticos.
	Gestión de Desarrollo de Soluciones.	Planifica, evalúa y controla las aplicaciones informáticas.
		Diseña y desarrolla pruebas de automatización y operación del Sistema Oficial de Contratación Pública del Ecuador.
		Código fuente de aplicaciones informáticas desarrolladas.
		Asesora la toma de decisiones para el desarrollo o adquisición de aplicaciones a terceros.
		Elabora términos de referencia para la estructuración de los proyectos de desarrollo de aplicaciones informáticas a medida.
		Gestiona las aplicaciones informáticas desarrolladas a medida por terceros para el Servicio Nacional de Contratación Pública.
		Realiza el análisis, diseño, arquitectura y mantenimiento de las herramientas del Servicio Nacional de Contratación Pública.
		Gestiona la integración e interoperabilidad de sistemas de información.
		Gestiona el desarrollo de las aplicaciones informáticas requeridas para el negocio.

MACROPROCESO	PROCESO	SUBPROCESO
G ESTIÓN DE INNOVACIÓN TECNOLÓGICA	Gestión TIC de Operaciones de Innovación Tecnológica.	Planifica, dirige, desarrolla, controla y mantiene el funcionamiento de las aplicaciones informáticas.
		Control y administración de la base de datos.
		Pruebas y producción de sistemas de información.
		Soporte técnico e instalación de hardware y software en las estaciones de trabajo.
		Desarrolla estándares para provisión del parque computacional.
		Administra las bases de datos de los sistemas de la institución.
		Administra el funcionamiento de los diferentes ambientes de cada una de las herramientas del Sistema Oficial de Contratación Pública del Ecuador.
		Implementa y mantiene los servicios de redes y comunicaciones.
		Articula mejoras a la infraestructura tecnológica de la institución.
		Aprueba la elaboración y ejecución del manual de procedimientos y estándares de infraestructura y operaciones de Innovación Tecnológica.
		Articula con el resto de unidades administrativas la implementación de nuevas tecnologías de la información.
		Gestiona la mejora de arquitecturas físicas y lógicas de tecnologías de información, así como de bienes y servicios tecnológicos.
		Gestiona las tareas de mantenimiento y soporte técnico a usuarios internos.
		Monitorea la disponibilidad del ambiente de producción del Servicio Nacional de Contratación Pública.
	Gestión de Seguridad Informática.	Planifica, elabora y controla la seguridad informática mediante políticas, normas, procedimientos y controles de la información de la Institución.
		Definir lineamientos técnicos para garantizar la confidencialidad, integridad y disponibilidad de la información
		Establecer los roles y perfiles para otorgar el acceso a los servicios de tecnologías de información de la Institución.
		Gestiona la implementación de controles de seguridad informática.
		Implementar acciones correctivas y preventivas en el ámbito de la seguridad informática para las aplicaciones de informáticas de la Institución.

MACROPROCESO	PROCESO	SUBPROCESO
GESTIÓN DE INNOVACIÓN TECNOLÓGICA	Gestión de Seguridad Informática.	Gestionar el monitoreo de la plataforma tecnológica en lo relacionado a la de seguridad informática de la Institución.
		Articular el análisis y respuesta a incidentes de seguridad informática.
		Elaborar informes de cumplimiento de políticas y normas de seguridad de la información en el ámbito de tecnologías de información.
DIRECCIÓN DE ESTUDIOS DE CONTRATACIÓN PÚBLICA.	Dirección de Estudios de Contratación Pública.	Administra los repositorios de precios de la contratación pública.
		Elabora estudios del comportamiento futuro del sector industrial del país, relacionado con el Valor Agregado Ecuatoriano.
		Articula el acceso a la información
GESTIÓN TÉCNICA DE OPERACIONES	Gestión de Atención al Usuario	Atención y asesoría de las actividades a los usuarios de contratación pública.
		Gestionar el registro único de proveedores.
		Gestionar la atención, asesoría y soporte a la ciudadanía y usuarios del Sistema Nacional SOCE Contratación Pública.
		Desarrolla canales para atención de la ciudadanía y al usuario Sistema Nacional de Contratación Pública
		Coordinar el seguimiento a la resolución de reclamos y quejas.
		Mide la percepción de uso y mejoramiento de los servicios del Sistema Nacional de Contratación Pública.
	Gestión de Herramientas de Contratación Pública.	Elabora y gestiona procedimientos y herramientas
		Reportes de pruebas de aceptación realizadas al Sistema Oficial de Contratación Pública del Ecuador para verificar su correcta aplicación.
		Efectúa mejoras en las herramientas informáticas del Sistema Nacional de Contratación Pública para socialización a usuarios.
		Monitorea incidencias de las herramientas del Sistema Oficial de Contratación Pública del Ecuador.

MACROPROCESO	PROCESO	SUBPROCESO
	Gestión de Capacitación y Certificación.	Planifica, ejecuta y controla actividades de capacitación a los usuarios de compras públicas.
		Establece manuales de usuarios de las herramientas informáticas del Sistema Oficial de Contratación Pública del lidiador.
		Analiza información de los procesos de capacitación y certificación.
GESTIÓN TÉCNICA DE CATALOGACIÓN	Gestión de Catálogo Electrónico	Planifica, controla y elabora los convenios marco y el catálogo electrónico.
		Oferta los bienes y servicios de la industria ecuatoriana (micro/ maro empresas).
		Procesos de bienes y servicios normalizados.
		Inclusión de bienes y servicios en el catálogo electrónico
		Instalación, configuración y acceso de aplicaciones externas.
	Gestión de Compras Inclusivas	Planifica, ejecuta y controla procedimientos de compras de producción ecuatoriana.
		Realiza el análisis técnico y normativo de factibilidad para la inclusión de bienes y servicios en el catálogo dinámico inclusivo.
		Genera el modelo tic gestión de catalogación de bienes y servicios para las compras inclusivas, que incluya ferias inclusivas, incorporación de actores de la economía popular y solidaria, y artesanos, micro y pequeñas empresas en la contratación pública.
	Gestión de Desarrollo de Compras Corporativas	Planifica, elabora y controla subastas corporativas.
		Realiza el análisis de factibilidad para la inclusión de bienes y servicios en el catálogo electrónico para compras corporativas.
		Modelo de gestión para el desarrollo para los usuarios del catálogo electrónico e inclusivo.
GESTIÓN DE ASESORÍA JURÍDICA	Gestión de Asesoría Jurídica	Asesora en materia jurídica a los usuarios de la institución, dentro de las políticas y demás áreas de derecho.
	Gestión Normativa	Planifica, analiza y desarrolla normas e instructivos, mediante el diagnóstico de las políticas para mejorarla gestión.
GESTIÓN DE COMUNICACIÓN SOCIAL	Gestión de Planificación, Seguimiento y Evaluación	Controla la elaboración, ejecución de la planificación estratégica y operativa institucional.
	Gestión de Servicios y Procesos	Gestiona la administración de los procesos para la prestación de los servicios a los usuarios.

MACROPROCESO	PROCESO	SUBPROCESO
GESTIÓN DE COMUNICACIÓN SOCIAL	Dirección de Comunicación Social	Difunde y promociona los procesos de comunicación, imagen y relaciones públicas.
	Dirección de Auditoria Interna	Evalúa el sistema de control interno, riesgos institucionales, operaciones y el control de leyes aplicables que permitan el logro de los objetivos institucionales.
GESTIÓN DE ADMINISTRACIÓN FINANCIERA	Gestión Administrativa	Administra los recursos materiales y logística de la institución
	Gestión Financiera	Dirige, gestiona, suministra y controla los recursos financieros para la ejecución de proyectos y servicios.
	Gestión de la Administración del Talento Humano	Administra, gestiona y vigila el desarrollo e implementación de los subsistemas de talento humano.
GESTIÓN DOCUMENTAL Y ARCHIVO	Dirección de Gestión Documental y Archivo	Controla y mantiene el sistema de gestión documental y archivo de la información oficial, y biblioteca.
		Certifica la documentación solicitada por usuarios internos y/o externos.
GESTIÓN TÉCNICA DE CONTROL	Gestión de Denuncias en Contratación Pública	Establecimiento de personas naturales en los procesos de contratación
		Formaliza denuncias ante la Fiscalía General del Estado.
	Gestión de Control Participativo	Controla la participación pública en contratación.
		Elabora metodologías, certificados y autorizaciones establecidas por la institución.
GESTIÓN DE AUDITORÍA INTERA	Gestión de Auditoría Interna	Realizar la evaluación posterior de las operaciones y actividades de la entidad a través de auditorías de gestión y exámenes especiales, por disposición expresa del Contralor General del Estado o de la máxima autoridad de la entidad.
		Identificar y evaluar los procedimientos y sistemas de control y de prevención internos para evitar actos ilícitos y de corrupción que afecten a la entidad.
		Efectuar el seguimiento al cumplimiento de las recomendaciones establecidas en los informes de auditoría interna y externa, sobre la base del cronograma preparado por los funcionarios responsables de su aplicación y aprobado por la máxima autoridad;

Fuente: (SERCOP, 2013)

En la tabla 6-1, se determinó los macroprocesos, subprocesos de la entidad, siendo el paso siguiente determinar los procesos críticos. Para determinar la criticidad de los procesos primeramente se determinan 5 aspectos fundamentales que pueden influir en el nivel de criticidad de un proceso. En este caso se toman como elementos determinantes los siguientes

- Proceso de entidades y proveedores: Cumple con actividades que ejecutan directamente los clientes externos principales de la entidad como son los proveedores y entidades del estado.
- Procesos de contratación pública: Atiende el principal core del negocio de la entidad, siendo las principales: Publicaciones de procedimientos de contratación, pujas, adjudicaciones de procesos.
- Proceso de cumplimiento de políticas: al ser una entidad pública debe cumplir con todas las políticas internas que sean mandatarias para el normal funcionamiento de los sistemas de información
- Procesos de cumplimiento de regulatorios: Cumpliendo con los requisitos que solicitan los organismos de control.
- Procesos transaccionales: A través del sistema se transacciona cantidades el presupuesto general de estado en etapas de adjudicación de proceso de contratación

Utilizando la tabla 6-1, se elaboró una tabla 6-4 cuantitativa para determinar los procesos críticos, donde se indica el subproceso y su evaluación entre uno a cinco; donde, uno significa no está reconocido y cinco como una alta relación. Los criterios de calificación serán: muy elevada (5), elevada (4), media (3), baja (2), muy baja (1) y se determina el promedio para definir su criticidad de acuerdo a la tabla 6-3.

Tabla 6-3. Escala de clasificación de los procesos críticos.

Calificación	Clasificación	Significado
20-25	Crítico	• Las aplicaciones no pueden ejecutarse y deben ser reemplazadas con otras funciones. • No se reemplazan con funciones manuales. • El costo de interrupción es muy elevado. • No tolera interrupciones
16-19	Vital	• Las funciones pueden ser manejadas manualmente durante un corto plazo. • El costo de interrupciones no es muy alto si es en un periodo de 5 días. • Tolera interrupciones.
5-15	Deseable	• Las funciones pueden ser manejadas manualmente durante un largo plazo. • El costo de interrupción es muy bajo

Elaborado por: Investigador

Tabla 6-4. Matriz de calificación de procesos críticos.

Macroproceso	Proceso	Subproceso	Responsable	Calificación					Total	Criticidad
				Proceso de entidades y proveedores	Proceso de contratación pública	Proceso de cumplimiento de políticas	Procesos de cumplimiento de regulatorios	Procesos transaccionales		
GESTIÓN DE INNOVACIÓN TECNOLÓGICA	Gestión de Servicios Informáticos.	Planifica, establece, dirige y controla los procesos de tecnologías de la información y comunicación. GSISP1	Director/a de Gestión de Servicios Informáticos.	4	4	2	2	4	16	Vital
		Validación de las consultas técnicas de los usuarios en el sistema. GSISP2	Director/a de Gestión de Servicios Informáticos.	5	4	3	4	4	20	Crítico
		Aprobar estudios, adquisición, mejora, mantenimiento y operación de los sistemas, plataformas y aplicaciones informáticas. GSISP3	Director/a de Gestión de Servicios Informáticos.	2	3	4	5	3	17	Vital
		Presentar propuestas para el desarrollo e implantación de las plataformas y aplicaciones informáticas utilizadas por la Institución. GSISP4	Director/a de Gestión de Servicios Informáticos.	4	5	3	3	4	19	Vital
		Coordinar la elaboración y ejecución del plan estratégico informático de la Institución. GSISP5	Director/a de Gestión de Servicios Informáticos.	2	3	5	5	2	17	Vital
		Articular con las unidades administrativas involucradas, la implementación de los sistemas informáticos. GSISP6	Director/a de Gestión de Servicios Informáticos.	4	4	3	3	2	16	Vital
		Articular la relación con los proveedores de las aplicaciones para la gestión de servicios informáticos. GSISP7	Director/a de Gestión de Servicios Informáticos.	2	4	4	3	3	16	Vital

Macroproceso	Proceso	Subproceso	Responsable	Calificación					Total	Criticidad
				Proceso de entidades y proveedores	Proceso de contratación pública	Proceso de cumplimiento de políticas	Procesos de cumplimiento de regulatorios	Procesos transaccionales		
GESTIÓN DE INNOVACIÓN TECNOLÓGICA	Gestión de Desarrollo de Soluciones.	Planifica, evalúa y controla las aplicaciones informáticas.GDSSP1	Director/a de Gestión de Desarrollo de Soluciones.	5	4	3	2	2	16	Vital
		Diseña y desarrolla pruebas de automatización y operación del Sistema Oficial de Contratación Pública del Ecuador. GDSSP2	Director/a de Gestión de Desarrollo de Soluciones.	5	5	4	3	4	21	Crítico
		Código fuente de aplicaciones informáticas desarrolladas. GDSSP3	Director/a de Gestión de Desarrollo de Soluciones.	5	5	4	3	4	21	Crítico
		Asesora la toma de decisiones para el desarrollo o adquisición de aplicaciones a terceros. GDSSP4	Director/a de Gestión de Desarrollo de Soluciones.	4	4	3	2	3	16	Vital
		Elabora términos de referencia para la estructuración de los proyectos de desarrollo de aplicaciones informáticas a medida. GDSSP5	Director/a de Gestión de Desarrollo de Soluciones.	2	2	1	1	1	7	Deseable
		Gestiona las aplicaciones informáticas desarrolladas a medida por terceros para el Servicio Nacional de Contratación Pública. GDSSP6	Director/a de Gestión de Desarrollo de Soluciones.	5	5	3	4	3	20	Crítico
		Realiza el análisis, diseño, arquitectura y mantenimiento de las herramientas del Servicio Nacional de Contratación Pública. GDSSP7	Director/a de Gestión de Desarrollo de Soluciones.	5	5	4	2	4	20	Crítico
		Gestiona la integración e interoperabilidad de sistemas de información. GDSSP8	Director/a de Gestión de Desarrollo de Soluciones.	5	5	3	2	4	19	Vital

Macroproceso	Proceso	Subproceso	Responsable	Calificación					Total	Criticidad
				Proceso de entidades y proveedores	Proceso de contratación pública	Proceso de cumplimiento de políticas	Procesos de cumplimiento de regulatorios	Procesos transaccionales		
GESTIÓN DE INNOVACIÓN TECNOLÓGICA	Gestión TIC de Operaciones de Innovación Tecnológica.	Implementa y mantiene los servicios de redes y comunicaciones..GOITSP1	Director/a de Gestión de Desarrollo de Soluciones.	5	5	4	3	4	21	Crítico
		Gestiona las tareas de mantenimiento y soporte técnico a usuarios internos. GOITSP2	Director/a de Gestión TIC de Operaciones de Innovación Tecnológica	5	5	5	3	4	22	Crítico
		Control y administración de la base de datos. GOITSP3	Director/a de Gestión TIC de Operaciones de Innovación Tecnológica	5	5	5	5	5	25	Crítico
		Administración de los ambiente de pruebas y producción de sistemas de información. GOITSP4	Director/a de Gestión TIC de Operaciones de Innovación Tecnológica	4	5	4	4	5	22	Crítico
		Soporte técnico e instalación de hardware y software en las estaciones de trabajo. GOITSP5	Director/a de Gestión TIC de Operaciones de Innovación Tecnológica	1	3	5	4	2	15	Deseable
		Desarrolla estándares para provisión del parque computacional. GOITSP6	Director/a de Gestión TIC de Operaciones de Innovación Tecnológica	1	2	5	2	1	11	Deseable
		Administra las bases de datos de los sistemas de la institución. GOITSP7	Director/a de Gestión TIC de Operaciones de Innovación Tecnológica	5	5	5	4	3	22	Crítico

Macroproceso	Proceso	Subproceso	Responsable	Calificación					Total	Criticidad
				Proceso de entidades y proveedores	Proceso de contratación pública	Proceso de cumplimiento de políticas	Procesos de cumplimiento de regulatorios	Procesos transaccionales		
GESTIÓN DE INNOVACIÓN TECNOLÓGICA	Gestión de Seguridad Informática.	Monitorea la disponibilidad del ambiente de producción del Servicio Nacional de Contratación Pública. GSISP1	Director/a de Gestión TIC de Operaciones de Innovación Tecnológica	3	4	5	5	3	20	Crítico
		Planifica, elabora y controla la seguridad informática mediante políticas, normas, procedimientos y controles de la información de la Institución. GSISP2	Director/a de Gestión de Seguridad Informática	2	5	5	5	3	20	Crítico
		Definir lineamientos técnicos para garantizar la confidencialidad, integridad y disponibilidad de la información GSISP3	Director/a de Gestión de Seguridad Informática	2	5	5	5	4	21	Crítico
		Establecer los roles y perfiles para otorgar el acceso a los servicios de tecnologías de información de la Institución. GSISP4	Director/a de Gestión de Seguridad Informática	3	4	5	5	3	20	Crítico
		Gestiona la implementación de controles de seguridad informática. GSISP5	Director/a de Gestión de Seguridad Informática	2	2	5	5	2	16	Vital
		Implementar acciones correctivas y preventivas en el ámbito de la seguridad informática para las aplicaciones de informáticas de la Institución. GSISP6	Director/a de Gestión de Seguridad Informática	2	5	5	5	1	18	Vital
		Gestionar el monitoreo de la plataforma tecnológica en lo relacionado a la de seguridad informática de la Institución. GSISP7	Director/a de Gestión de Seguridad Informática	2	2	5	4	3	16	Vital

Macroproceso	Proceso	Subproceso	Responsable	Calificación					Total	Criticidad
				Proceso de entidades y proveedores	Proceso de contratación pública	Proceso de cumplimiento de políticas	Procesos de cumplimiento de regulatorios	Procesos transaccionales		
GESTIÓN DE INNOVACIÓN TECNOLÓGICA	Gestión de Seguridad Informática.	Articular el análisis y respuesta a incidentes de seguridad informática. GSISP8	Director/a de Gestión de Seguridad Informática	2	3	5	5	2	17	Vital
GESTIÓN DE ESTUDIOS DE CONTRATACIÓN PÚBLICA.	Gestión de Estudias de Contratación Pública.	Gestiona, elabora herramientas y controla lineamientos de estudio de levantamiento de información.	Directo/a de Dirección de Estudios de Contratación Pública.	2	2	5	5	2	16	Vital
	Gestión de Estudios de Contratación Pública.	Elabora estudios del comportamiento futuro del sector industrial del país, relacionado con el Valor Agregado Ecuatoriano.	Directo/a de Dirección de Estudios de Contratación Pública.							
	Gestión de Estudias de Contratación Pública.	Articula el acceso a la información	Directo/a de Dirección de Estudios de Contratación Pública.	5	4	4	4	5	22	Crítico

Macroproceso	Proceso	Subproceso	Responsable	Calificación					Total	Criticidad
				Proceso de entidades y proveedores	Proceso de contratación pública	Proceso de cumplimiento de políticas	Procesos de cumplimiento de regulatorios	Procesos transaccionales		
GESTIÓN TÉCNICA DE OPERACIONES	Gestión de Atención al Usuario	Atención y asesoría de las actividades a los usuarios de contratación pública.	Director/a de Gestión de Atención al Usuario	4	3	2	2	3	14	Deseable
		Gestionar el registro único de proveedores.	Director/a de Gestión de Atención al Usuario	5	5	3	3	2	18	Vital
		Gestionar la atención, asesoría y soporte a la ciudadanía y usuarios del Sistema Nacional SOCE Contratación Pública.	Director/a de Gestión de Atención al Usuario	5	5	2	4	2	18	Vital
		Desarrolla canales para atención de la ciudadanía y al usuario Sistema Nacional de Contratación Pública	Director/a de Gestión de Atención al Usuario	1	2	2	1	2	8	Deseable
		Coordinar el seguimiento a la resolución de reclamos y quejas.	Director/a de Gestión de Atención al Usuario	2	2	2	1	2	9	Deseable
		Mide la percepción de uso y mejoramiento de los servicios del	Director/a de Gestión de Atención al Usuario	2	1	2	1	2	8	Deseable

Macroprocesos	Proceso	Subproceso	Responsable	Calificación					Total	Criticidad
				Proceso de entidades y proveedores	Proceso de contratación pública	Proceso de cumplimiento de políticas	Procesos de cumplimiento de regulatorios	Procesos transaccionales		
GESTIÓN TÉCNICA DE OPERACIONES	Gestión de Herramientas de Contratación Pública.	Elabora y gestiona procedimientos y herramientas	Director/a de Gestión de Herramientas de contratación pública	2	2	4	2	3	13	Deseable
		Reportes de pruebas de aceptación realizadas al Sistema Oficial de Contratación Pública del Ecuador para verificar su correcta aplicación.	Director/a de Gestión de Herramientas de contratación pública	2	2	5	4	4	17	Vital
		Efectúa mejoras en las herramientas informáticas del Sistema Nacional de Contratación Pública para socialización a usuarios.	Director/a de Gestión de Herramientas de contratación pública	5	5	3	2	1	16	Vital
		Monitorea incidencias de las herramientas del Sistema Oficial de Contratación Pública del Ecuador.	Director/a de Gestión de Herramientas de contratación pública	1	1	2	1	1	6	Deseable
	Gestión de Capacitación y Certificación.	Planifica, ejecuta y controla actividades de capacitación a los usuarios de compras públicas.	Director/a de Gestión de Capacitación y Certificación	5	2	2	1	2	12	Deseable
		Establece manuales de usuarios de las herramientas informáticas del Sistema Oficial de Contratación Pública del lidiador.	Director/a de Gestión de Capacitación y Certificación	4	1	2	1	1	9	Deseable
		Analiza información de los procesos de capacitación y certificación.	Director/a de Gestión de Capacitación y Certificación	4	1	2	1	1	9	Deseable

Macroprocesos	Proceso	Subproceso	Responsable	Calificación					Total	Criticidad
				Proceso de entidades y proveedores	Proceso de contratación pública	Proceso de cumplimiento de políticas	Procesos de cumplimiento de regulatorios	Procesos transaccionales		
GESTIÓN TÉCNICA DE CATÁLOGO ELECTRÓNICO	Gestión de Catálogo Electrónico	Planifica, controla y elabora los convenios marco y el catálogo electrónico.GCESP1	Director/a de Gestión de Catálogo Electrónico	2	2	2	1	2	9	Deseable
		Oferta los bienes y servicios de la industria ecuatoriana (micro/ maro empresas). GCESP2	Director/a de Gestión de Catálogo Electrónico	1	2	1	1	2	7	Deseable
		Procesos de bienes y servicios normalizados. GCESP1	Director/a de Gestión de Catálogo Electrónico	2	2	2	2	3	11	Deseable
		Inclusión de bienes y servicios en el catálogo electrónico GCESP3	Director/a de Gestión de Catálogo Electrónico	4	3	3	3	4	17	Vital
		Instalación, configuración y acceso de aplicaciones externas. GCESP4	Director/a de Gestión de Catálogo Electrónico y director/a de Operaciones de Innovación Tecnológica	4	4	3	3	4	18	Vital
	Gestión de Compras Inclusivas	Planifica, ejecuta y controla procedimientos de compras de producción ecuatoriana.	Director/a de Gestión de Compras Inclusivas	3	2	2	1	2	10	Deseable
		Realiza el análisis técnico y normativo de factibilidad para la inclusión de bienes y servicios en el catálogo dinámico inclusivo.	Director/a de Gestión de Compras Inclusivas	1	2	2	1	1	7	Deseable

Macroprocesos	Proceso	Subproceso	Responsable	Calificación					Total	Criticidad
				Proceso de entidades y proveedores	Proceso de contratación pública	Proceso de cumplimiento de políticas	Procesos de cumplimiento de regulatorios	Procesos transaccionales		
GESTIÓN TÉCNICA DE CATÁLOGO ELECTRÓNICO	Gestión de Compras Inclusivas	Genera el modelo tic gestión de catalogación de bienes y servicios para las compras inclusivas, que incluya ferias inclusivas, incorporación de actores de la economía popular y solidaria, y artesanos, micro y pequeñas empresas en la contratación pública.	Director/a de Gestión de Compras Inclusivas	3	2	2	1	1	9	Deseable
	Gestión de Desarrollo de Compras Corporativas	Planifica, elabora y controla subastas corporativas.	Director/a de Desarrollo de Compras Corporativas	4	3	2	3	3	15	Deseable
		Realiza el análisis de factibilidad para la inclusión de bienes y servicios en el catálogo electrónico para compras corporativas.	Director/a de Desarrollo de Compras Corporativas	1	3	2	3	3	12	Deseable
		Modelo de gestión para el desarrollo para los usuarios del catálogo electrónico e inclusivo.	Director/a de Desarrollo de Proveedores	4	3	2	2	1	12	Deseable
GESTIÓN DE ASESORÍA JURÍDICA	Gestión de Asesoría Jurídica	Asesora en materia jurídica a los usuarios de la institución, dentro de las políticas y demás áreas de derecho.	Director/a de Asesoría Jurídica	2	1	2	1	1	7	Deseable
	Gestión Normativa	Planifica, analiza y desarrolla normas e instructivos, mediante el diagnóstico de las políticas para mejorarla gestión.	Director/a de Normativa	2	1	2	1	1	7	Deseable

Macroprocesos	Proceso	Subproceso	Responsable	Calificación					Total	Criticidad
				Proceso de entidades y proveedores	Proceso de contratación pública	Proceso de cumplimiento de políticas	Procesos de cumplimiento de regulatorios	Procesos transaccionales		
GESTIÓN DE COMUNICACIÓN SOCIAL	Gestión de Planificación, Seguimiento y Evaluación	Controla la elaboración, ejecución de la planificación estratégica y operativa institucional.	Director/a de Planificación, Siguiente y Evaluación	2	2	2	1	1	8	Deseable
	Gestión de Servicios y Procesos	Gestiona la administración de los procesos para la prestación de los servicios a los usuarios.	Director/a de Servicios y Procesos	3	1	1	1	2	8	Deseable
GESTIÓN DE COMUNICACIÓN SOCIAL	Dirección de Comunicación Social	Difunde y promociona los procesos de comunicación, imagen y relaciones públicas.	Director/a de Comunicación Social	1	1	1	1	2	6	Deseable
	Dirección de Auditoria Interna	Evalúa el sistema de control interno, riesgos institucionales, operaciones y el control de leyes aplicables que permitan el logro de los objetivos institucionales.	Director/a de Auditoria Interna	1	1	2	1	1	6	Deseable
GESTIÓN DE ADMINISTRACIÓN FINANCIERA	Gestión Administrativa	Administra los recursos materiales y logística de la institución	Director/a de Administrativa	1	1	1	3	2	8	Deseable
	Gestión Financiera	Dirige, gestiona, suministra y controla los recursos financieros para la ejecución de proyectos y servicios.	Director/a Financiera	1	1	1	2	1	6	Deseable
	Gestión de la Administración del Talento Humano	Administra, gestiona y vigila el desarrollo e implementación de los subsistemas de talento humano.	Director/a de Administración del Talento Humano	2	1	1	1	2	7	Deseable

Macroprocesos	Proceso	Subproceso	Responsable	Calificación					Total	Criticidad
				Proceso de entidades y proveedores	Proceso de contratación pública	Proceso de cumplimiento de políticas	Procesos de cumplimiento de regulatorios	Procesos transaccionales		
GESTIÓN DOCUMENTAL Y ARCHIVO	Dirección de Gestión Documental y Archivo	Controla y mantiene el sistema de gestión documental y archivo de la información oficial, y biblioteca.	Director/a de Gestión Documental y Archivo	2	1	2	1	1	7	Deseable
		Certifica la documentación solicitada por usuarios internos y/o externos.	Director/a de Gestión Documental y Archivo	1	1	2	1	1	6	Deseable
GESTIÓN TÉCNICA DE CONTROL	Gestión de Denuncias en Contratación Pública	Establecimiento de personas naturales en los procesos de contratación	Director/a de Denuncias de Contratación Pública	2	2	1	1	1	7	Deseable
		Formaliza denuncias ante la Fiscalía General del Estado.	Director/a de Denuncias de Contratación Pública	2	1	2	1	1	7	Deseable
	Gestión de Control Participativo	Controla la participación pública en contratación.	Director/a de Control de Participativo	1	1	2	1	2	7	Deseable
		Elabora metodologías, certificados y autorizaciones establecidas por la institución.	Director/a de Control para Producción Nacional	1	1	1	1	1	5	Deseable

Elaborado por: Investigador

Una vez identificados los procesos críticos considerados vitales y críticos es necesario determinar los recursos para su ejecución como se observa la tabla 6-5.

Tabla 6-5. Recursos de soporte para procesos críticos.

PROCESO	SUBPROCESOS								RECURSO TI
	GSISP1	GSISP2	GSISP3	GSISP4	GSISP5	GSISP6	GSISP7		
GESTIÓN DE SERVICIOS INFORMÁTICOS		x				x	x		Bases de datos PostgreSql
		x					x		Bases de datos SQL Server
		x				x	x		Sistema SOCE
	x	x	x	x	x	x	x		Red de datos
	x	x	x	x	x	x	x		Internet
	x		x	x	x		x		Central telefónica
	x	x	x	x	x	x	x		PCs de usuario final
	x	x				x	x		Servidor de correo
	GDSSP1	GDSSP2	GDSSP3	GDSSP4	GDSSP5	GDSSP6	GDSSP7	GDSSP8	
GESTIÓN DE DESARROLLO DE SOLUCIONES		x	x			x	x	x	Bases de datos PostgreSql
		x	x	x		x	x	x	Bases de datos SQL Server
		x	x	x	x	x	x	x	Sistema SOCE desarrollo
	x	x	x	x	x	x	x	x	Red de datos
	x	x	x	x	x	x	x	x	Internet
	x		x	x	x	x	x	x	Central telefónica
	x	x	x	x	x	x	x	x	PCs de usuario final
	x	x	x	x	x	x	x	x	Correo electrónico
	GOITSP1	GOITSP2	GOITSP3	GOITSP4	GOITSP5	GOITSP6	GOITSP7		
GESTIÓN DE OPERACIONES DE INNOVACIÓN TECNOLÓGICA			x	x			x		Bases de datos PostgreSql
			x	x			x		Bases de datos SQL Server
	x			x			x		Servidor web sistema SOCE
	x	x	x	x	x	x	x		Red de datos

	x	x	x	x	x	x	x		Internet
	x	x	x	x	x	x	x		Hardware red (hubs, switch, routers, etc.).
	x	x	x	x	x	x	x		PCs de usuario final
		x	x	x	x	x	x		Servidor de correo
	GSISP1	GSISP2	GSISP3	GSISP4	GSISP5	GSISP6	GSISP7	GSISP8	
GESTIÓN DE SEGURIDAD INFORMATICA	x	x	x	x		x	X	x	Bases de datos PostgreSql
	x	x	x	x		x	X	x	Bases de datos SQL Server
	x	x	x	x	x	x	X	x	Servidor web sistema SOCE
	x	x	x	x	x	x	X	x	Red de datos
	x	x				x	X	x	Internet
	x				x			x	Central telefónica
	x	x	x	x	x	x	X	x	PCs de usuario final
	x			x	x	x		x	Servidor de correo
	x	x	x		x	x	X	x	Antivirus
	x	x	x		x	x	X	x	Equipos de seguridad perimetral
GESTIÓN TÉCNICA DE CATÁLOGO ELECTRÓNICO	GCESP1		GCESP2		GCESP3		GCESP4	GCESP5	
			x		x		x		Bases de datos PostgreSql
	x		x		x		x		Servidor web sistema SOCE y catalogo electrónico
	x		x		x		x	x	Red de datos
	x		x		x		x	x	Internet
	x		x		x		x	x	Central telefónica
	x		x		x		x	x	PCs de usuario final
	x		x		x		x	x	Correo Electrónico

Elaborado por: Investigador

Después de realizar el análisis de los procesos críticos y sus recursos se determinó el Tiempo Objetivo de Recuperación (TOR) y el Punto Objetivo de Recuperación (POR).

Establecimiento de los tiempos de recuperación

Según (ccn, 2014) Es un parámetro importante en la concepción de un plan de continuidad. Concretamente se plantea un tiempo límite para que un cierto servicio vuelva a estar en funcionamiento. A partir de este objetivo, empleado como techo, se van planteando los mecanismos de respaldo y los procesos asociados.

Realmente, el RTO a veces tiene diferentes interpretaciones. Desde que un servicio deja de estar operativo hasta que se restaura, podemos diferenciar 3 fases:

1. T_1 = desde que el servicio deja de estar operativo hasta que se detecta.
2. T_2 = desde que se detecta hasta que se toma la decisión de activar el plan de recuperación.
3. T_3 = desde que se toma la decisión de restaurar el servicio, hasta que se consuma el plan de recuperación.

Como parte del proceso de construcción del Plan de continuidad del negocio, se identificó aquellos tiempos críticos que la institución puede tolerar en un proceso que se encuentre detenido, entre los principales tiempos se detalla:

- **RTO:** Indica el tiempo disponible para recuperar sistemas y/o recursos que han sufrido una alteración
- **RPO:** Se refiere a la magnitud de la pérdida de datos, medida en términos de un período de tiempo que un proceso de negocios puede tolerar

Para el caso de Servicio Nacional de Contratación Pública, se tomará en cuenta principalmente los tiempos RPO y RTO, además se debe recordar que estos tiempos fueron definidos por los responsables de los procesos, y servirán como marco de referencia para dos temas puntuales:

De esta forma se determinó los tiempos máximos de los procesos críticos podrían estar suspendidos por la pérdida de información y comunicación sin afectar significativamente a la empresa del mismo modo el tiempo máximo de respaldo del servicio. Los cuales se determinaron en las siguientes tablas 6-6, 6-7 y 6-8.

Tabla 6-6. Matriz TOR y POR del proceso crítico de Gestión de Catálogo Electrónico.

Macroproceso	Proceso	Subproceso	RTO	RPO
GESTIÓN TÉCNICA DE CATÁLOGO ELECTRÓNICO	Gestión de Catálogo Electrónico	Inclusión de bienes y servicios en el catálogo electrónico	2 horas	2 horas
	Gestión de Catálogo Electrónico	Instalación, configuración y acceso de aplicaciones externas.	1 día	2 horas

Elaborado por: Investigador

Tabla 6-7. Matriz TOR y POR del proceso crítico de Gestión de Innovación Tecnológica.

Macroproceso	Proceso	Subproceso	RTO	RPO
GESTIÓN DE INNOVACIÓN TECNOLÓGICA	Gestión de Servicios Informáticos.	Planifica, establece, dirige y controla los procesos de tecnologías de la información y comunicación.	2 horas	4 horas
		Validación de las consultas técnicas de los usuarios en el sistema.	4 horas	4 horas
		Aprobar estudios, adquisición, mejora, mantenimiento y operación de los sistemas, plataformas y aplicaciones informáticas.	3 horas	4 horas
		Presentar propuestas para el desarrollo e implantación de las plataformas y aplicaciones informáticas.	5 horas	6 horas
		Coordinar la elaboración y ejecución del plan estratégico informático de la Institución.	3 horas	4 horas
		Articular con las unidades administrativas involucradas, la implementación de los sistemas informáticos.	2 horas	4 horas
		Articular la relación con los proveedores de las aplicaciones para la gestión de servicios informáticos.	2 horas	4 horas
	Gestión de Desarrollo de Soluciones.	Planifica, evalúa y controla las aplicaciones informáticas.	2 horas	3 horas
		Diseña y desarrolla pruebas de automatización y operación del Sistema Oficial de Contratación Pública del Ecuador.	4 horas	5 horas
		Código fuente de aplicaciones informáticas desarrolladas.	4 horas	5 horas
		Asesora la toma de decisiones para el desarrollo o adquisición de aplicaciones a terceros.	5 horas	6 horas
		Gestiona las aplicaciones informáticas desarrolladas a medida por terceros.	8 horas	10 horas
		Realiza el análisis, diseño, arquitectura y mantenimiento de las herramientas.	12 horas	24 horas
		Gestiona la integración e interoperabilidad de sistemas de información.	8 horas	2 horas
		Gestiona el desarrollo de las aplicaciones informáticas requeridas para el negocio.	24 horas	24 horas
	Gestión TIC de Operaciones de Innovación Tecnológica.	Planifica, dirige, desarrolla, controla y mantiene el funcionamiento de las aplicaciones informáticas.	5 horas	6 horas
		Control y administración de la base de datos.	24 horas	24 horas
		Pruebas y producción de sistemas de información.	12 horas	24 horas

Macroproceso	Proceso	Subproceso	RTO	RPO
GESTIÓN DE INNOVACIÓN TECNOLÓGICA	Gestión TIC de Operaciones de Innovación Tecnológica	Administra las bases de datos de los sistemas de la institución.	12 horas	12 horas
		Administra el funcionamiento de los diferentes ambientes de cada una de las herramientas del Sistema Oficial de Contratación Pública del Ecuador.	8 horas	12 horas
		Implementa y mantiene los servicios de redes y comunicaciones.	4 horas	6 horas
		Articula mejoras a la infraestructura tecnológica de la institución.	6 horas	6 horas
		Articula con el resto de unidades administrativas la implementación de nuevas tecnologías de la información.	8 horas	8 horas
		Gestiona la mejora de arquitecturas físicas y lógicas de tecnologías de información, así como de bienes y servicios tecnológicos.	6 horas	8 horas
		Gestiona las tareas de mantenimiento y soporte técnico a usuarios internos.	12 horas	24 horas
		Monitorea la disponibilidad del ambiente de producción del Servicio Nacional de Contratación Pública.	4 horas	8 horas
	Gestión de Seguridad Informática.	Planifica, elabora y controla la seguridad informática mediante políticas, normas, procedimientos y controles de la información de la Institución.	2 horas	4 horas
		Definir lineamientos técnicos para garantizar la confidencialidad, integridad y disponibilidad de la información	2 horas	3 horas
		Establecer los roles y perfiles para otorgar el acceso a los servicios de tecnologías de información de la Institución.	4 horas	5 horas
		Gestiona la implementación de controles de seguridad informática.	2 horas	3 horas
		Implementar acciones correctivas y preventivas en el ámbito de la seguridad informática para las aplicaciones de informáticas de la Institución.	2 horas	4 horas
		Gestionar el monitoreo de la plataforma tecnológica en lo relacionado a la de seguridad informática de la Institución.	2 horas	3 horas
		Articular el análisis y respuesta a incidentes de seguridad informática.	3 horas	4 horas

Elaborado por: Investigador

Tabla 6-8. Matriz TOR y POR de la Gestión Técnica de Operaciones.

Macroproceso	Proceso	Subproceso	RTO	RPO
GESTIÓN TÉCNICA DE OPERACIONES	Dirección de Estudias de Contratación Pública.	Gestiona, elabora herramientas y controla lineamientos de estudio de levantamiento de información.	12 horas	24 horas
		Articula el acceso a la información	4 horas	4 horas
	Gestión de Atención al Usuario	Gestionar el registro único de proveedores.	5 horas	8 horas
		Gestionar la atención, asesoría y soporte a la ciudadanía y usuarios del Sistema Nacional SOCE Contratación Pública.	8 horas	12 horas
	Gestión de Herramientas de Contratación Pública.	Reportes de pruebas de aceptación realizadas al Sistema Oficial de Contratación Pública del Ecuador para verificar su correcta aplicación.	12 horas	24 horas
		Efectúa mejoras en las herramientas informáticas del Sistema Nacional de Contratación Pública para socialización a usuarios.	24 horas	24 horas

Elaborado por: Investigador

6.7.3 Análisis de impacto en el negocio (BIA)

En esta fase se determinó las acciones de restauración y continuidad de los procesos críticos donde se cuantifica los impactos que pueden causar en la institución.

En esta sección posee mayor prioridad aquellos procesos que podría perjudicar los servicios de la empresa cuya interrupción podría causar malestar a sus clientes (entidades y proveedores), los daños que podría generarse causarían interrupción en algunas operaciones. Por esta razón, para determinar el impacto en cada de los servicios se cualifica de manera objetiva la realidad institucional, social y financiera.

El análisis de impacto en el negocio proporciona información sobre potenciales impactos, posibles costos, prioridad y estrategias de recuperación.

A continuación, se menciona las áreas que se verían mayor afectadas en la ejecución de sus actividades en caso de alguna catástrofe tecnológica:

- Entidades y proveedores.
- Políticas de la institución.
- Reputación.
- Administración.

De acuerdo al análisis de las tablas 6-5, indica que la Gestión del Catálogo Electrónico el proceso de servicios de catálogo, instalación, configuración y acceso aplicaciones externas revela un alto impacto en el negocio de un RTO de 24 horas, incidiendo en todas las áreas anteriormente planteadas.

En el proceso de Gestión de Innovación Tecnológica de la tabla 6-6, en la gestión de desarrollo de aplicaciones y el control y administración de la base de datos 24 horas; siendo el soporte técnico e instalación de hardware y software en las estaciones de trabajo el de mayor incidencia en el análisis de los procesos críticos, ocasionando perjuicios en todas las áreas excepto en las políticas de la institución.

Y finalmente, en la tabla 6-7 de la Gestión Técnica de Operaciones se observa una interrupción máxima de 4 horas en la articulación de acceso a la información mediante la interconexión de plataformas interfiriendo en las áreas de entidades, proveedores y en la reputación de la institución.

6.7.4 Análisis de riesgos

A continuación, se identifica los riesgos tecnológicos que pueden ocasionar problemas y daños en el servicio de la institución que fueron obtenidos de acuerdo a la observación del desarrollo de los procesos tecnológicos, donde se identificaron posibles amenazas que pueden causar daños en el hardware, software y sistemas eléctricos. De acuerdo a lo mencionado se enlista los posibles riesgos que se expone el Servicio de Contratación Pública:

6.7.4.1 Metodología para el análisis de riesgos

La ISO/IEC 27005 proporciona una guía para realizar el análisis de riesgos de la seguridad de la información especificando parámetros que se debe cumplir en las diferentes fases del proceso; sin embargo, se debe apoyar en una metodología, la misma que facilita la estimación del riesgo. Esta

metodología puede ser cualitativa, cuantitativa o una combinación de las dos, esto dependerá del nivel de detalle con que se desee analizar, así como también de la información que se tenga.

6.7.4.2 Metodología Cualitativa

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

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

6.7.4.3 Metodología Cuantitativa

Esta metodología es menos utilizada pues consiste en recolectar datos, realizar cálculos y usar técnicas de modelamiento, etc., que pueden dar como resultado información difícil de estimar. Usa escalas de valoración numérica ya sea para la evaluación de probabilidades de ocurrencia como para el impacto de estas en base a varios datos lo que permite calcular el nivel de riesgo. La complejidad y exactitud de los valores numéricos, así como la validez del modelo utilizado determina el éxito del uso de esta metodología.

6.7.4.4 Criterios básicos

De acuerdo a lo descrito en las dos metodologías anteriores para llevar a cabo el análisis de riesgos tecnológicos en la entidad Servicio Nacional de Contratación Pública, se establecen los criterios básicos en base a la combinación de éstas, ya que por un lado se califica los atributos como define la metodología cualitativa y junto con ello se da una valoración numérica, que no representa exactamente el uso de la metodología cuantitativa pues no se realizan cálculos matemáticos complejos, sin embargo ayuda a que la estimación del riesgo tenga mayor exactitud. A continuación, se definen los parámetros a tomar en cuenta para la valoración cualitativa de cada atributo de los diferentes criterios que se utilizan para el análisis de riesgo. Estos criterios se basan en la información recopilada de visitas efectuadas dentro de la entidad.

6.7.4.5 Criterios de valoración de activos

Se dan de acuerdo a la importancia, funciones dentro de la red y dependencia de estos hacia otros activos. La evaluación de los activos utilizará los criterios de cualificación y valoraciones numéricas que se muestra en la Tabla 6-9.

Tabla 6-9. Criterio de valoración de activos.

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

Elaborado por: Investigador

El producto de los valores obtenidos de cada parámetro identificado en la tabla anterior determinará el valor de cada activo, que a su vez pertenecerá a un nivel de importancia, el cual será evaluado de acuerdo a la Tabla 6-10 que se muestra a continuación.

Tabla 6-10 Valor de cada activo

Calificación	Valor	Calificación	Significancia
1-8	1	POCO IMPORTANTE	El activo tiene poca importancia para la entrega de servicios a través de la red de datos, de acuerdo a los criterios de dependencia, funcionalidad y confidencialidad, integridad y disponibilidad
9-26	2	IMPORTANTE	El activo es importante para la entrega de servicios a través de la red de datos, de acuerdo a los criterios de dependencia, funcionalidad y confidencialidad, integridad y disponibilidad.
27-64	3	CRÍTICO	El activo es vital para la entrega de servicios a través de la red de datos, de acuerdo a los criterios de dependencia, funcionalidad y confidencialidad, integridad y disponibilidad.
VALOR DEL ACTIVO = DEPENDENCIA * FUNCIONALIDAD * (CONFIDENCIALIDAD, INTEGRIDAD, DISPONIBILIDAD)			

Elaborado por: Investigador

6.7.4.6 Criterios de probabilidad de ocurrencia de amenazas

En la Tabla 6-9, se muestran los criterios calificativos y los valores numéricos a ser utilizados para la valoración de la probabilidad de amenazas que podrían explotar alguna vulnerabilidad existente.

Tabla 6-11. Criterios de probabilidad de ocurrencia de amenazas

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

Elaborado por: Investigador

6.7.4.7 Criterios de valoración de Impacto

El impacto es medir la consecuencia de la materialización de un riesgo, además de ser el valor promedio entre los impactos de integridad, confidencialidad y disponibilidad, siendo así un punto importante al momento de la toma de decisiones para la puesta en marcha de los controles. Criterios de valoración para valorar el impacto: Confidencialidad, integridad y disponibilidad. La tabla 6-12, presenta los criterios de valoración de impacto

Tabla 6-12. Criterios de elaboración de impacto.

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

Elaborado por: Investigador

6.7.4.8 Criterios de evaluación del riesgo.

Se calcula mediante el producto entre la probabilidad de ocurrencia de una amenaza y el impacto que esta pudiese ocasionar, el resultado del producto es el nivel de riesgo de cada activo, la tabla 6- 13 presenta los criterios de evaluación de riesgo.

Tabla 6-13. Criterios de evaluación de riesgo.

Valor	Criterio	Significancia
1-2	BAJO	El riesgo del activo es bajo
3-4	MODERADO	El riesgo del activo es moderador
5-8	ALTO	El riesgo del activo es alto
9-12	CRÍTICO	El riesgo del activo es crítico
NIVEL DE RIESGO= PROBABILIDAD*IMPACTO		

Elaborado por: Investigador

6.7.4.9 Criterios para el tratamiento de riesgos

Cuando los daños provocados por la materialización de un riesgo no han afectado mayormente las actividades y funcionalidades tecnológicas de la entidad se deberá aceptar el riesgo.

Cuando los daños provocados por la materialización de un riesgo han afectado las actividades y funcionalidades tecnológicas de la entidad, se deberá reducir dicho riesgo, es por tal motivo que la Coordinación de Innovación Tecnológica con sus cuatro direcciones tiene la obligación de reducir el riesgo implementado controles que mitiguen el impacto que provocaría la materialización de un riesgo.

Para la mecionada tarea se definen los siguientes criterios para el tratamiento de riesgos en la tabla 6-14:

Tabla 6-14. Criterios para el tratamiento de riesgos.

BAJO	Aceptar el riesgo
MODERADO	
ALTO	Reducir el riesgo
CRÍTICO	

Elaborado por: Investigador

6.7.4.10 Criterios de prioridad en la aplicacón de controles.

Se debe tomar en consideración la prioridad en la que deben ser implementados los controles. El nivel de riesgo por el nivel de importancia de la aplicación del control en la taba 6-15 se plasma los criterios de aplicación de los controles:

Tabla 6-15. Criterios de prioridad en la aplicación de controles.

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

Elaborado por: Investigador

6.7.4.11 Identificación de activos de la entidad

En la tabla 6-16, se observa los activos primeros de la institución.

Tabla 6-16. Activos primarios.

Servicio	Activos	Dependencia	Funcionalidad	Confidencialidad integridad y disponibilidad	Total
Servicios de Negocio	Sistema Oficial de Contratación del Estado	4	3	4	48
	Procedimientos dinámicos	4	3	4	48
	Procedimientos comunes	4	3	4	48
	Procedimientos de consultoría	4	3	4	48
	Procedimientos especiales	4	3	4	48
	Procedimientos de Régimen Especial	4	3	4	48
	Búsqueda de procesos	4	3	4	48
	Registro único de proveedores	4	3	4	48
	Envío de notificaciones	4	3	4	48
	PAC	2	4	4	32
	Portal de capacitación	2	3	2	12
	ELearning	2	3	2	12
	Capacitación Virtual	2	3	2	12
	Servicios WEB	4	3	4	48
	Business Intelligence	3	3	4	36
	Ventanilla única ecuatoriana (VUE)	4	2	3	24
	Catálogo Electrónico	4	3	4	48
	Ushay	4	3	4	48
	SI – Control	2	3	2	12

	Portal Institucional	4	2	3	24
	Esigef	2	1	3	6
	Alfresco	3	3	2	18
	Correo Electrónico	2	2	3	12
	Mesa de Servicio	2	3	2	12
	Usuarios del Soce	4	3	4	48
	Intranet	2	2	1	4
	Equipos	4	3	3	36
	MANTIS Desarrollo	2	4	3	24
Servicio Técnico	Soporte Telefonía IP	2	4	1	8
	Servicio de Base de Datos	4	4	4	64
	Turnero	2	2	2	8
	Correos Masivos	4	4	5	80
	Impresión y Escaneo	2	2	2	8
	Almacenamiento	2	3	2	12
	Redes e Internet	3	4	2	24
	Energía	4	4	2	32
	Climatización	3	2	3	18
	Gestión de Seguridad	4	4	4	64
	Gestión de Operaciones	4	4	4	64
	Gestión de Técnica	4	4	4	64
	Gestión de Red	4	4	4	64
	Redes	2	2	2	8
	Soporte de Aplicaciones del Negocio	4	4	4	64

	Soporte de Escritorio	3	2	1	6
	Soporte de Impresión	2	3	2	12
	Soporte Software Base	4	4	4	64
	Antivirus	3	2	2	12
	Mantis (SEGURIDAD)	3	2	2	12

Elaborado por: Investigador

6.7.4.12 Identificación de amenazas

Las amenazas pueden ocasionar riesgo al explotar las vulnerabilidades, estas amenazas se determinarán para los recursos críticos que sustentan la ejecución de los procesos críticos identificados anteriormente. Para identificar las amenazas se optó por analizar lo siguiente:

Tabla 6-17. Identificación de amenazas.

Items
Ubicación de las instalaciones
Seguridad interna y externa
Ambiente físico
Protección de activos
Protección del personal
Protección de la información

Elaborado por: Investigador

Según la ISO 22031: 2013 punto 8.2.2, se identifica los riesgos tecnológicos que pueden ocasionar problemas y daños en el servicio de la institución de acuerdo a la observación del desarrollo de los procesos tecnológicos, donde se identificaron posibles amenazas que pueden causar daños en el hardware, software y sistemas eléctricos. De acuerdo a lo mencionado se enlista los posibles riesgos que se expone el Servicio de Contratación Pública:

- USB infectadas.
- Ingreso no autorizado al sistema con el fin de obtener o alterar información.
- Utilización de software no adecuado.

- Perdida o falla en el almacenamiento de información en la base de datos.
- Caída del sistema.
- Daños en los equipos de la institución.
- Errores humanos.
- Ataques cibernéticos.
- Fallo eléctrico por causas naturales.
- Fallas o daños en las redes de la institución (Muncaster, 2017).

De acuerdo a la norma ISO 31000 de gestión de riesgos, indica que la definición de estos criterios debe estar alineada a la cultura de la organización y ser acorde a sus necesidades (Gutierrez & Ortiz, 2018) (Guerra, 2013), por esta razón la calificación de las probabilidades e impactos se elaboró con apoyo del Coordinador de Innovación Tecnológica. Donde, se evaluó las posibles amenazas de la institución de acuerdo a la probabilidad con la tabla 6-18 y para calificar el impacto con la tabla 6-19, y se estableció cinco niveles cada uno: baja, media baja, media, medio alta y alta (Sosa, 2018).

Tabla 6-18. Probabilidad de ocurrencias de amenazas.

Probabilidad de ocurrencia	**Calificación cuantitativa**	**Criterio**	**Presencia de la situación**
Baja	1	Improbable	Una vez en 3 años
Media baja	2	Raramente	Una vez en 2 años con seis meses
Media	3	Moderada	Una vez en 2 años
Media alta	4	Frecuente	Una vez en 1 año con seis meses
Alta	5	Siempre	Una vez en 1 año

Fuente: (Sosa, 2018).

Tabla 6-19. Calificación del nivel de impacto.

Impacto	Calificación cuantitativa	Criterio
Baja	1	Incomoda
Media baja	2	Controlable
Media	3	Regulable
Media alta	4	Crítico
Alta	5	Irreparable

Fuente: (Sosa, 2018).

Los niveles anteriormente para probabilidad e impacto generan una matriz que visualiza la criticidad del riesgo. El modelo genérico de ésta se encuentra en la Tabla 6-20. El cruce de la probabilidad y el impacto da como resultado el nivel de riesgo.

Tabla 6-20. Matriz de evaluación de nivel de riegos.

		IMPACTO				
PROBABILIDAD		**1 Bajo**	**2 Medio bajo**	**3 Medio**	**4 Medio alto**	**5 Alto**
	5 Alta	*Alto*	*Alto*	*Muy alto*	*Muy alto*	*Muy alto*
	4 Media alta	*Medio*	*Alto*	*Alto*	*Muy alto*	*Muy alto*
	3 Media	*Bajo*	*Medio*	*Alto*	*Muy alto*	*Muy alto*
	2 Media baja	*Bajo*	*Bajo*	*Medio*	*Alto*	*Muy alto*
	1 Baja	*Bajo*	*Bajo*	*Medio*	*Alto*	*Alto*

Fuente: (Sosa, 2018) (Guerra, 2013) (Ramirez & Ortiz, 2011).

En la tabla 6-21, se evaluó las amenazas en forma cualitativa, mientras que en las tablas 6-22, 6-23 y 6-24 se evaluó los procesos críticos en forma cuantitativa (probabilidad e impacto) y

cualitativa en nivel de riesgo de acuerdo al tiempo de recuperación establecido con el apoyo de la coordinadora de Innovación Tecnológica.

Tabla 6-21. Evaluación de las posibles amenazas y determinación del nivel de riesgo

Amenazas	Control	Vulnerabilidad	Daños	Complicaciones	Probabilidad	Impacto	Nivel de riesgo
USB infectadas. De acuerdo a que riesgo?	Charlas del manejo de la USB. Controles de virus en los equipos tecnológicos. Instalación de software de antivirus.	No existe control en la limpieza de las USB cada cierto periodo.	Interrupción de los servicios tecnológicos.	Fallas en los servicios a las entidades y proveedores.	Alta	Medio	Muy alto
Ingreso no autorizado al sistema con el fin de obtener o alterar información.	Instalación de servicios de seguridad en el sistema. Charlas de concientización de la discreción de la información. Controles y avisos de ingresos de los usuarios.	Falta de creación de usuarios y contraseña para la modificación de información.	Pérdida parcial/ total de la información.	Fallas en la información de la página de la institución.	Baja	Media alto	Alto
Utilización de software no adecuado.	Instalación de softwares con los permisos adecuados. Controles de los softwares obsoletos.	No existe control en los permisos de instalación de programas.	Pérdida parcial de información.	Fallas de los procesos de servicios tecnológicos.	Media Baja	Bajo	Bajo
Pérdida o falla en el almacenamiento de información en la base de datos.	Capacitación del ingreso de información en la base de datos. Creación de respaldos de la base de datos. Ingreso del personal autorizado en la base de datos.	No existe la creación de usuarios y contraseña para el ingreso de información.	Pérdida total de información.	Interrupción del portal de la institución.	Baja	Alto	Alto

Amenazas	Control	Vulnerabilidad	Daños interrupciones	Complicaciones	Probabilidad	Impacto	Nivel de riesgo
Caída del sistema.	Capacitación de simulacros de recuperación de comunicación. Generación de software para recuperar la información.	No existe simulacros ante la ciada del sistema.	Pérdida parcial de la información.	Interrupción de los servicios de la institución.	Medio	Alto	Muy Alto
Daños en los equipos de la institución.	Capacitación en el uso adecuado de los recursos de la institución. Mantenimiento de los equipos cada cierto periodo. Renovación de los equipos dañados.	Falta de recursos para cambiar los equipos.	Reducción de la eficiencia del trabajo. Perdida de comunicación con las entidades e instituciones.	Reducción de atención en los servicios.	Baja	Medio	Medio
Errores humanos.	Capacitación del personal en los servicios. Charlas de concientización del uso adecuado del sistema. Centro de información de dudas de los procesos.	Falta del centro de atención para los empleados.	Dificultad en el ambiente de trabajo.	Interrupción de las labores de la institución.	Muy Bajo	Medio	Medio
Ataques cibernéticos.	Creación de sistemas de seguridad para el control de la información. Ante algún ataque bloquear el portal de la institución.	No existe personal encargado en la creación de sistemas de seguridad.	Infiltración de la información.	Interrupción total de la información.	Baja	Alto	Alto

Amenazas	Control	Vulnerabilidad	Daños interrupciones	Complicaciones	Probabilidad	Impacto	Nivel de riesgo
Fallo eléctrico por causas naturales	Tener un generador de energía en la institución. Control y mantenimiento del generador. Monitoreo de fluctuaciones de la energía.	No existe una persona encargada en el mantenimiento del generador.	Perdida de la información.	Interrupción total del portal de la institución.	Media baja	Alto	Muy alto
Fallas o daños en las redes comunicación de la institución	Controles de las redes de la institución.	No existe personal encargado para el control.	Perdida de comunicación.	Interrupción parcial de la información.	Baja	Bajo	Bajo

Elaborado por: Investigador

Tabla 6-22. Matriz de impacto de la Gestión del Catálogo Electrónico.

Macroproceso	Proceso	Subproceso	Área impactada	Impacto del proceso								
				Menos de 4 horas			Menos de 4 horas			Menos de 4 horas		
				Probabilidad	Impacto	Nivel de riesgo	Probabilidad	Impacto	Nivel de riesgo	Probabilidad	Impacto	Nivel de riesgo
GESTIÓN TÉCNICA DE CATÁLOGO ELECTRÓNICO	Gestión de Catálogo Electrónico	Inclusión de bienes y servicios en el catálogo electrónico	Entidades y proveedores	1	2	Bajo	2	2	Bajo	2	3	Medio
			Políticas de la institución	2	1	Bajo	2	3	Medio	3	2	Medio
			Reputación	1	1	Bajo	1	2	Bajo	2	3	Medio
			Administración	2	1	Bajo	3	1	Medio	2	3	Medio
		Instalación, configuración y acceso de aplicaciones externas.	Entidades y proveedores	1	1	Bajo	2	3	Medio	3	2	Medio
			Políticas de la institución	2	1	Bajo	1	3	Medio	2	3	Medio
			Reputación	2	1	Bajo	2	3	Medio	4	2	Alto
			Administración	1	2	Bajo	2	2	Bajo	2	3	Medio

Elaborado por: Investigador

Tabla 6-23. Matriz de impacto de Gestión de Innovación Tecnológica.

Macroproceso	Proceso	Subproceso	Área impactada	Impacto del proceso								
				Menos de 4 horas			4-8 horas			8-24 horas		
				Probabilidad	Impacto	Nivel de riesgo	Probabilidad	Impacto	Nivel de riesgo	Probabilidad	Impacto	Nivel de riesgo
GESTIÓN DE INNOVACIÓN TECNOLÓGICA	Gestión de Servicios Informáticos.	Planifica, establece, dirige y controla los procesos de tecnologías de la información y comunicación.	Entidades y proveedores	3	3	Bajo	3	3	Alto	4	3	Alto
			Políticas de la institución	2	1	Bajo	2	1	Bajo	3	2	Medio
			Reputación	1	1	Bajo	1	2	Bajo	2	3	Medio
			Administración	2	1	Bajo	3	1	Bajo	4	2	Alto
		Validación de las consultas técnicas de los usuarios en el sistema.	Entidades y proveedores	2	2	Bajo	3	2	Medio	4	3	Alto
			Políticas de la institución	2	2	Bajo	2	2	Bajo	3	3	Alto
			Reputación	1	2	Bajo	1	3	Medio	2	4	Alto
			Administración	2	1	Bajo	3	2	Medio	4	3	Alto
		Aprobar estudios, adquisición, mejora, mantenimiento y operación de los sistemas, plataformas y aplicaciones informáticas.	Entidades y proveedores	2	3	Medio	3	4	Muy alto	4	5	Muy alto
			Políticas de la institución	2	2	Bajo	2	2	Bajo	3	3	Alto
			Reputación	1	2	Bajo	4	5	Muy alto	5	5	Muy alto
			Administración	2	2	Bajo	3	3	Alto	4	4	Muy alto
		Presentar propuestas para el desarrollo e implantación de las plataformas y aplicaciones informáticas utilizadas por la Institución.	Entidades y proveedores	2	3	Medio	3	4	Muy alto	4	5	Muy alto
			Políticas de la institución	2	2	Bajo	2	2	Bajo	3	3	Alto
			Reputación	3	4	Muy alto	4	5	Muy alto	5	5	Muy alto
			Administración	2	2	Bajo	3	3	Alto	4	4	Muy alto

Macroproceso	Proceso	Subproceso	Área impactada	Impacto del proceso								
				Menos de 4 horas			Menos de 4 horas			Menos de 4 horas		
				Probabilidad	Impacto	Nivel de riesgo	Probabilidad	Impacto	Nivel de riesgo	Probabilidad	Impacto	Nivel de riesgo
GESTIÓN DE INNOVACIÓN TECNOLÓGICA	Gestión de Servicios Informáticos.	Presentar propuestas para el desarrollo e implantación de las plataformas y aplicaciones informáticas utilizadas por la Institución.	Entidades y proveedores	1	2	Bajo	1	2	Bajo	2	3	Medio
			Políticas de la institución	2	1	Bajo	2	2	Bajo	3	3	Alto
			Reputación	1	3	Medio	2	3	Medio	3	4	Muy alto
			Administración	2	2	Bajo	2	3	Medio	3	3	Alto
		Coordinar la elaboración y ejecución del plan estratégico informático de la Institución.	Entidades y proveedores	1	1	Bajo	2	3	Medio	4	3	Alto
			Políticas de la institución	1	2	Bajo	2	1	Bajo	3	2	Medio
			Reputación	1	1	Bajo	1	2	Bajo	2	3	Medio
			Administración	1	2	Bajo	3	1	Medio	4	2	Alto
		Articular con las unidades administrativas involucradas, la implementación de los sistemas informáticos.	Entidades y proveedores	2	3	Medio	3	4	Muy alto	4	5	Muy alto
			Políticas de la institución	2	2	Bajo	2	2	Bajo	3	3	Alto
			Reputación	3	4	Muy alto	4	5	Muy alto	5	5	Muy alto
			Administración	2	2	Bajo	3	3	Alto	4	4	Muy alto
		Articular la relación con los proveedores de las aplicaciones para la gestión de servicios informáticos.	Entidades y proveedores	1	2	Bajo	2	3	Medio	3	4	Muy alto
			Políticas de la institución	1	1	Bajo	1	2	Bajo	1	2	Bajo
			Reputación	1	1	Bajo	2	1	Bajo	2	2	Bajo
			Administración	1	3	Medio	2	3	Medio	3	3	Alto

Macroproceso	Proceso	Subproceso	Área impactada	Impacto del proceso								
				Menos de 4 horas			Menos de 4 horas			Menos de 4 horas		
				Probabilidad	Impacto	Nivel de riesgo	Probabilidad	Impacto	Nivel de riesgo	Probabilidad	Impacto	Nivel de riesgo
GESTIÓN DE INNOVACIÓN TECNOLÓGICA	Gestión de Servicios Informáticos.	Planifica, evalúa y controla las aplicaciones informáticas.	Entidades y proveedores	2	3	Medio	3	4	Muy alto	4	5	Muy alto
			Políticas de la institución	2	2	Bajo	2	2	Bajo	3	3	Alto
			Reputación	3	4	Muy alto	4	5	Muy alto	5	5	Muy alto
			Administración	2	2	Bajo	3	3	Alto	4	4	Muy alto
		Diseña y desarrolla pruebas de automatización y operación del Sistema Oficial de Contratación Pública del Ecuador.	Entidades y proveedores	2	3	Medio	3	4	Muy alto	4	5	Muy alto
			Políticas de la institución	2	2	Bajo	2	2	Bajo	3	3	Alto
			Reputación	3	4	Muy alto	4	5	Muy alto	5	5	Muy alto
			Administración	2	2	Bajo	3	3	Alto	4	4	Muy alto
		Código fuente de aplicaciones informáticas desarrolladas.	Entidades y proveedores	2	3	Medio	3	4	Muy alto	4	5	Muy alto
			Políticas de la institución	2	2	Bajo	2	3	Medio	2	5	Muy alto
			Reputación	3	3	Alto	3	4	Muy alto	3	5	Muy alto
			Administración	2	3	Medio	3	4	Muy alto	4	5	Muy alto
		Asesora la toma de decisiones para el desarrollo o adquisición de aplicaciones a terceros.	Entidades y proveedores	0	0	N/A	1	1	Bajo	1	2	Bajo
			Políticas de la institución	1	1	Bajo	1	2	Bajo	1	3	Medio
			Reputación	1	2	Bajo	2	2	Bajo	3	2	Medio
			Administración	0	0	N/A	1	1	Bajo	1	1	Bajo
		Gestiona las aplicaciones informáticas desarrolladas a medida por terceros para el SERCOP	Entidades y proveedores	1	2	Bajo	2	2	Bajo	2	3	Medio
			Políticas de la institución	2	1	Bajo	2	3	Medio	3	2	Medio
			Reputación	1	1	Bajo	1	2	Bajo	2	3	Medio
			Administración	2	1	Bajo	3	1	Medio	4	2	Alto

Macroproceso	Proceso	Subproceso	Área impactada	Impacto del proceso								
				Menos de 4 horas			Menos de 4 horas			Menos de 4 horas		
				Probabilidad	Impacto	Nivel de riesgo	Probabilidad	Impacto	Nivel de riesgo	Probabilidad	Impacto	Nivel de riesgo
GESTIÓN DE INNOVACIÓN TECNOLÓGICA	Gestión de Servicios Informáticos.	Realiza el análisis, diseño, arquitectura y mantenimiento de las herramientas del Servicio Nacional de Contratación Pública.	Entidades y proveedores	1	2	Bajo	2	2	Bajo	2	3	Medio
			Políticas de la institución	2	2	Bajo	2	3	Medio	3	3	Alto
			Reputación	2	3	Medio	2	4	Alto	3	5	Muy alto
			Administración	2	2	Bajo	3	3	Alto	4	4	Muy alto
		Gestiona la integración e interoperabilidad de sistemas de información.	Entidades y proveedores	1	1	Bajo	1	2	Bajo	2	2	Bajo
			Políticas de la institución	2	2	Bajo	2	2	Bajo	3	3	Alto
			Reputación	3	4	Muy alto	4	5	Muy alto	5	5	Muy alto
			Administración	3	2	Medio	3	3	Alto	4	4	Muy alto
		Gestiona el desarrollo de las aplicaciones informáticas requeridas para el negocio.	Entidades y proveedores	1	1	Bajo	1	1	Bajo	1	1	Bajo
			Políticas de la institución	1	2	Bajo	1	3	Medio	2	4	Alto
			Reputación	3	4	Muy alto	4	5	Muy alto	5	5	Muy alto
			Administración	2	3	Medio	3	3	Alto	4	4	Muy alto
	Gestión de Desarrollo de Soluciones.	Planifica, dirige, desarrolla, controla y mantiene el funcionamiento de las aplicaciones informáticas.	Entidades y proveedores	2	3	Medio	3	4	Muy alto	4	5	Muy alto
			Políticas de la institución	2	2	Bajo	2	2	Bajo	3	3	Alto
			Reputación	3	4	Muy alto	4	5	Muy alto	5	5	Muy alto
			Administración	2	2	Bajo	3	3	Alto	4	4	Muy alto
		Control y administración de la base de datos.	Entidades y proveedores	1	1	Bajo	1	3	Medio	3	4	Muy alto
			Políticas de la institución	1	2	Bajo	2	2	Bajo	3	3	Alto
			Reputación	1	3	Medio	1	3	Medio	2	4	Alto
			Administración	2	1	Bajo	3	3	Medio	4	3	Alto

Macroproceso	Proceso	Subproceso	Área impactada	Impacto del proceso								
				Menos de 4 horas			Menos de 4 horas			Menos de 4 horas		
				Probabilidad	Impacto	Nivel de riesgo	Probabilidad	Impacto	Nivel de riesgo	Probabilidad	Impacto	Nivel de riesgo
GESTIÓN DE INNOVACIÓN TECNOLÓGICA	Gestión de Desarrollo de Soluciones.	Pruebas y producción de sistemas de información.	Entidades y proveedores	2	3	Medio	2	4	Alto	3	5	Muy alto
			Políticas de la institución	1	2	Bajo	3	3	Alto	4	4	Muy alto
			Reputación	1	1	Bajo	1	2	Bajo	2	2	Bajo
			Administración	2	2	Bajo	2	3	Medio	3	3	Alto
		Administra las bases de datos de los sistemas de la institución.	Entidades y proveedores	3	4	Muy alto	4	5	Muy alto	5	5	Muy alto
			Políticas de la institución	2	3	Medio	3	3	Alto	4	4	Muy alto
			Reputación	2	3	Medio	3	4	Muy alto	4	5	Muy alto
			Administración	1	1	Bajo	2	2	Bajo	3	3	Alto
		Administra el funcionamiento de los diferentes ambientes de cada una de las herramientas del Sistema.	Entidades y proveedores	2	3	Medio	3	4	Muy alto	4	5	Muy alto
			Políticas de la institución	2	2	Bajo	2	3	Medio	2	5	Muy alto
			Reputación	3	3	Alto	3	4	Muy alto	3	5	Muy alto
			Administración	3	3	Medio	3	4	Muy alto	4	5	Muy alto
		Implementa y mantiene los servicios de redes y comunicaciones.	Entidades y proveedores	1	2	Bajo	1	2	Bajo	2	3	Medio
			Políticas de la institución	1	2	Bajo	3	1	Medio	4	2	Alto
			Reputación	2	3	Medio	3	4	Muy alto	4	5	Muy alto
			Administración	2	2	Bajo	2	2	Bajo	3	3	Alto
		Articula mejoras a la infraestructura tecnológica de la institución.	Entidades y proveedores	2	3	Medio	3	4	Muy alto	4	5	Muy alto
			Políticas de la institución	1	1	Bajo	2	2	Bajo	3	3	Alto
			Reputación	3	4	Muy alto	4	5	Muy alto	5	5	Muy alto
			Administración	2	1	Bajo	3	4	Muy alto	4	5	Muy alto

Macroproceso	Proceso	Subproceso	Área impactada	Impacto del proceso								
				Menos de 4 horas			Menos de 4 horas			Menos de 4 horas		
				Probabilidad	Impacto	Nivel de riesgo	Probabilidad	Impacto	Nivel de riesgo	Probabilidad	Impacto	Nivel de riesgo
GESTIÓN DE INNOVACIÓN TECNOLÓGICA	Gestión de Desarrollo de Soluciones.	Articula con el resto de unidades administrativas la implementación de nuevas tecnologías de la información.	Entidades y proveedores	1	2	Bajo	1	2	Bajo	1	3	Alto
			Políticas de la institución	2	1	Bajo	2	1	Bajo	3	2	Medio
			Reputación	1	1	Bajo	1	2	Bajo	2	3	Medio
			Administración	2	1	Bajo	3	1	Bajo	4	2	Alto
		Gestiona la mejora de arquitecturas físicas y lógicas de tecnologías de información, así como de bienes y tecnologías.	Entidades y proveedores	2	1	Bajo	2	2	Bajo	3	3	Alto
			Políticas de la institución	1	3	Medio	2	3	Medio	3	4	Muy alto
			Reputación	1	2	Bajo	1	3	Medio	2	3	Medio
			Administración	1	1	Bajo	2	3	Medio	4	3	Alto
		Gestiona las tareas de mantenimiento y soporte técnico a usuarios internos.	Entidades y proveedores	1	2	Bajo	2	2	Bajo	2	3	Medio
			Políticas de la institución	2	1	Bajo	2	3	Medio	3	2	Medio
			Reputación	1	1	Bajo	1	2	Bajo	1	2	Bajo
			Administración	1	1	Bajo	2	1	Bajo	2	2	Bajo
		Monitorea la disponibilidad del ambiente de producción del Servicio Nacional de Contratación Pública.	Entidades y proveedores	1	3	Medio	2	3	Medio	3	4	Muy alto
			Políticas de la institución	2	2	Bajo	2	3	Medio	3	3	Alto
			Reputación	1	1	Bajo	1	3	Medio	4	3	Alto
			Administración	1	2	Bajo	2	1	Bajo	3	2	Medio
		Planifica, elabora y controla la seguridad informática con políticas, normas, procedimientos y controles de la información.	Entidades y proveedores	1	1	Bajo	1	1	Bajo	1	2	Bajo
			Políticas de la institución	2	3	Medio	3	3	Alto	4	4	Muy alto
			Reputación	4	1	Medio	4	4	Muy alto	4	5	Muy alto
			Administración	2	2	Bajo	2	2	Bajo	3	3	Alto

Macroproceso	Proceso	Subproceso	Área impactada	Impacto del proceso								
				Menos de 4 horas			Menos de 4 horas			Menos de 4 horas		
				Probabilidad	Impacto	Nivel de riesgo	Probabilidad	Impacto	Nivel de riesgo	Probabilidad	Impacto	Nivel de riesgo
GESTIÓN DE INNOVACIÓN TECNOLÓGICA	Gestión TIC de Operaciones de Innovación Tecnológica	Define lineamientos técnicos para garantizar la confidencialidad, integridad y disponibilidad de la información	Entidades y proveedores	1	2	Bajo	2	4	Alto	3	3	Alto
			Políticas de la institución	2	1	Bajo	3	3	Alto	4	3	Alto
			Reputación	1	2	Bajo	1	2	Bajo	1	3	Medio
			Administración	3	1	Bajo	2	3	Medio	2	4	Alto
		Establece los roles y perfiles para el acceso a los servicios de tecnologías de información	Entidades y proveedores	2	2	Bajo	2	4	Alto	5	5	Muy alto
			Políticas de la institución	2	3	Medio	3	3	Alto	4	4	Muy alto
			Reputación	1	3	Medio	1	2	Bajo	4	5	Muy alto
			Administración	2	2	Bajo	2	2	Bajo	3	3	Alto
		Gestiona la implementación de controles de seguridad informática.	Entidades y proveedores	2	2	Bajo	3	2	Medio	4	5	Muy alto
			Políticas de la institución	2	3	Medio	2	3	Medio	3	3	Alto
			Reputación	2	3	Medio	4	2	Alto	5	5	Muy alto
			Administración	1	1	Bajo	3	3	Alto	4	5	Muy alto
		Implementa acciones correctivas y preventivas en la seguridad informática para las aplicaciones.	Entidades y proveedores	3	1	Bajo	3	2	Medio	3	2	Medio
			Políticas de la institución	2	1	Bajo	4	1	Medio	4	3	Alto
			Reputación	2	2	Bajo	5	1	Medio	5	3	Alto
			Administración	1	2	Bajo	1	3	Medio	1	4	Alto
		Gestiona el monitoreo de la plataforma tecnológica en lo relacionado a la de seguridad informática	Entidades y proveedores	0	0	N/A	1	1	Bajo	1	1	Bajo
			Políticas de la institución	4	2	Alto	4	3	Alto	4	5	Muy alto
			Reputación	4	1	Medio	5	1	Alto	5	2	Alto
			Administración	5	1	Alto	5	3	Muy alto	5	5	Muy alto
		Articula el análisis y respuesta a incidentes de seguridad informática.	Entidades y proveedores	1	2	Bajo	1	2	Bajo	1	3	Alto
			Políticas de la institución	2	1	Bajo	2	1	Bajo	3	2	Medio
			Reputación	1	1	Bajo	1	2	Bajo	2	3	Medio
			Administración	2	1	Bajo	3	1	Bajo	4	2	Alto

Elaborado por: Investigador

Tabla 6-24. Matriz de impacto de Gestión Técnica Operacional.

Macroproceso	Proceso	Subproceso	Área impactada	Impacto del proceso								
				Menos de 4 horas			Menos de 4 horas			Menos de 4 horas		
				Probabilidad	Impacto	Nivel de riesgo	Probabilidad	Impacto	Nivel de riesgo	Probabilidad	Impacto	Nivel de riesgo
GESTIÓN TÉCNICA DE OPERACIONES	Dirección de Estudias de Contratación Pública.	Gestiona, elabora herramientas y controla el estudio de levantamiento de información.	Entidades y proveedores	1	2	Bajo	2	2	Bajo	2	3	Medio
			Políticas de la institución	2	1	Bajo	2	3	Medio	3	2	Medio
			Reputación	1	1	Bajo	1	2	Bajo	2	3	Medio
			Administración	2	1	Bajo	3	1	Medio	4	2	Alto
		Articula el acceso a la información	Entidades y proveedores	1	3	Medio	2	3	Medio	3	4	Muy alto
			Políticas de la institución	1	2	Bajo	1	3	Medio	2	3	Medio
			Reputación	1	1	Bajo	2	3	Medio	4	3	Alto
			Administración	1	2	Bajo	2	2	Bajo	2	3	Medio
	Gestión de Atención al Usuario	Gestionar el registro único de proveedores.	Entidades y proveedores	3	4	Muy alto	4	5	Muy alto	5	5	Muy alto
			Políticas de la institución	2	3	Medio	3	3	Alto	4	4	Muy alto
			Reputación	2	3	Medio	3	4	Muy alto	4	5	Muy alto
			Administración	1	1	Bajo	2	2	Bajo	3	3	Alto
		Gestionar la atención, asesoría y soporte a la ciudadanía y usuarios del Sistema Nacional SOCE	Entidades y proveedores	2	3	Medio	3	3	Alto	4	4	Muy alto
			Políticas de la institución	1	3	Medio	1	2	Bajo	4	5	Muy alto
			Reputación	2	2	Bajo	2	2	Bajo	3	3	Alto
			Administración	2	2	Bajo	3	2	Medio	4	5	Muy alto
	Gestión de Herramientas de Contratación Pública	Reportes de pruebas de aceptación realizadas al Sistema para verificar su correcta aplicación.	Entidades y proveedores	1	1	Bajo	1	2	Bajo	2	3	Medio
			Políticas de la institución	2	1	Bajo	3	1	Bajo	4	2	Alto
			Reputación	2	1	Bajo	2	2	Bajo	3	3	Alto
			Administración	1	2	Bajo	1	3	Medio	1	4	Alto
		Efectúa mejoras en las herramientas informáticas del Sistema para socialización a usuarios.	Entidades y proveedores	1	1	Bajo	1	3	Medio	1	4	Alto
			Políticas de la institución	1	2	Bajo	2	2	Bajo	3	3	Alto
			Reputación	1	3	Medio	1	3	Medio	2	4	Alto
			Administración	2	1	Bajo	3	3	Medio	4	3	Alto

Elaborado por: Investigador

6.7.5 Proyección del plan de continuidad

La proyección es un pronóstico de diversas gestiones que parten de un análisis de procesos en base a la información estadística de departamentos institucionales. A partir del análisis de la información se logra entender el comportamiento de todos los procesos informáticos, ello permitirá realizar las proyecciones mediante diversos métodos.

6.7.5.1 Alcance

El alcance del plan de continuidad de negocios del Servicio de Contratación Pública está encaminado a una propuesta del uso adecuado de los funcionarios, entidades, proveedores en los servicios en caso de un desastre o amenaza que paralice la institución.

6.7.5.2 Políticas

Establecer los escenarios de ejecución y respuesta rápida para garantizar el funcionamiento del plan de continuidad y ofrecer mayor estabilidad en los servicios a las entidades y proveedores del estado, durante la ocurrencia de algún desastre que provoque la falla de los sistemas de los procesos críticos y el colapso de la atención, minimizando el tiempo y la pérdida de los recursos, para evitar desprestigio de la organización.

6.7.5.3 Requisitos

- Capacitación de las posibles amenazas a los funcionarios de la entidad de acuerdo a las bases y fundamentos de un plan de continuidad.
- Utilización de los recursos tecnológicos en los procesos para la actuación de algún desastre no previsto por parte de los funcionarios de la institución.
- Concientización de los beneficios que provoca la indagación de los procesos críticos y cómo contrastarlos en beneficio de las entidades y proveedores.

6.7.5.4 Principios y valores

Mediante los principios y valores de la institución se establece un plan de continuidad para proteger los procesos críticos, mitigando los riesgos de desastres operacionales y el desprestigio de la institución de ese modo satisfaciendo las necesidades de las entidades y proveedores mediante canales alternativos de precaución y respaldo de la información (LEXISFINDER, 2018).

6.7.5.5 Objetivos

1. Garantizar la calidad de ejecución de la contratación y la aplicación efectiva de las normas, políticas y procedimientos de la institución; además, avalar la transparencia de los procesos.
2. Simplificar el tiempo de respuesta frente la interrupción de los procesos tecnológicos.
3. Mantener la seguridad y la reputación de la institución.

6.7.5.6 Definir estrategias de mitigación

Mediante la identificación de los tiempos de recuperación y de operacionalización de los procesos críticos, se determinó vías de recuperación tecnológica para mitigar los riesgos y el tiempo de respuesta, como se indica en la tabla 6-25.

Tabla 6-25. Vías de recuperación tecnológica.

Estrategias de recuperación	Descripción	Tiempos de recuperación estimados (tiempo en condiciones ideales- tiempo máximo)
Sitio Alterno Duplicado (Mirrored Site)	Sitio alterno de información paralela al sitio de la institución mantenido la integridad y la discreción al 100%	5 – 60 min
Sitio Alterno Equipado (Hot Site)	Sitio alterno de procesamiento de datos, totalmente operacional equipado con hardware y software usado para cualquier amenaza.	16- 48 horas
Sitio alterno Semi-equipado (Warm Site)	Sitio de almacenamiento parcial para el funcionamiento de un centro alterno tales como: hardware software, pero sin ordenador principal a menudo este sitio se encuentra equipado con una CPU de menor capacidad.	1-4 semanas
Sitio Alterno sin equipos (Cold Site)	Dispone de un eje de respaldo propio con los medios básicas, para eliminar la dependencia de un servicio fuera de la institución.	1-3 meses
Sitio Alterno Contratado con Proveedores	Ofrecer seguridad a la institución y son capaces de mantener la continuidad de los procesos ante algún desastre.	Depende del tiempo de contratación.

Fuente: (Puente, 2014), (Ávila, 2013), (CIBERSEGURIDAD, 2018), (TRIARA, 2018)

Como se indica en la tabla 6-26, se determinó la estrategia de recuperación para cada proceso crítico, tomando en cuenta el menor tiempo de interrupción (TOR) involucrando las aplicaciones de la institución.

Tabla 6-26. Estrategias de recuperación de acuerdo a cada proceso crítico.

Proceso	Subproceso	Responsable	TOR	Estrategia de recuperación
Gestión de Catálogo Electrónico	Inclusión de bienes y servicios en el catálogo electrónico	Director/a de Catálogo Electrónico.	2 horas	Sitio Alterno Duplicado
	Fichas técnicas de bienes y servicios normalizados	Director/a de Catálogo Electrónico.	4 horas	Sitio Alterno Duplicado
	Instalación, configuración y acceso a aplicaciones externas	Director/a de Catálogo Electrónico.	24 horas	Sitio Alterno Equipado
Gestión de Innovación Tecnológica	Validación de las consultas técnicas de los usuarios en el sistema	Coordinador/a Técnica de Innovación Tecnológica.	4 horas	Sitio Alterno Duplicado
	Código fuente de aplicaciones informáticas desarrolladas	Director/a de Gestión de Desarrollo de Soluciones.	4 horas	Sitio Alterno Duplicado
	Control y administración de la base de datos.	Director/a de Operaciones de Innovación Tecnológica.	5 horas	Sitio Alterno Duplicado
	Pruebas y producción de sistemas de información: SOCE Catálogo Electrónico, USHAY	Director/a de Operaciones de Innovación Tecnológica.	24 horas	Sitio Alterno Equipado
	Administración de equipos de Seguridad Perimetral	Director/a de Seguridad Informática	4 horas	Sitio Alterno Duplicado
Gestión Técnica de Operaciones	Capacitación a usuarios en el manejo de los sistemas de información	Coordinador/a Técnico/a de Operaciones.	2 horas	Sitio Alterno Duplicado
	Articular el acceso a la información mediante la interconexión de plataformas	Coordinador/a Técnico/a de Operaciones	4 horas	Sitio Alterno Duplicado

Elaborado por: Investigador

De acuerdo a los tiempos de recuperación de los procesos críticos del Servicio de Contratación Pública, se recomienda utilizar la estrategia del "Sitio Alterno Duplicado" o "Sitio Alterno Equipado", que permita recuperar los servicios dentro de 4 hasta 48 horas.

El Servicio Nacional de Contratación Pública cuenta con diferentes sitios estratégicos (figura 6-2), cada uno de estos cuentan con recursos tecnológicos necesarios para mantener la ejecución de los procesos críticos durante algún desastre no previsto.

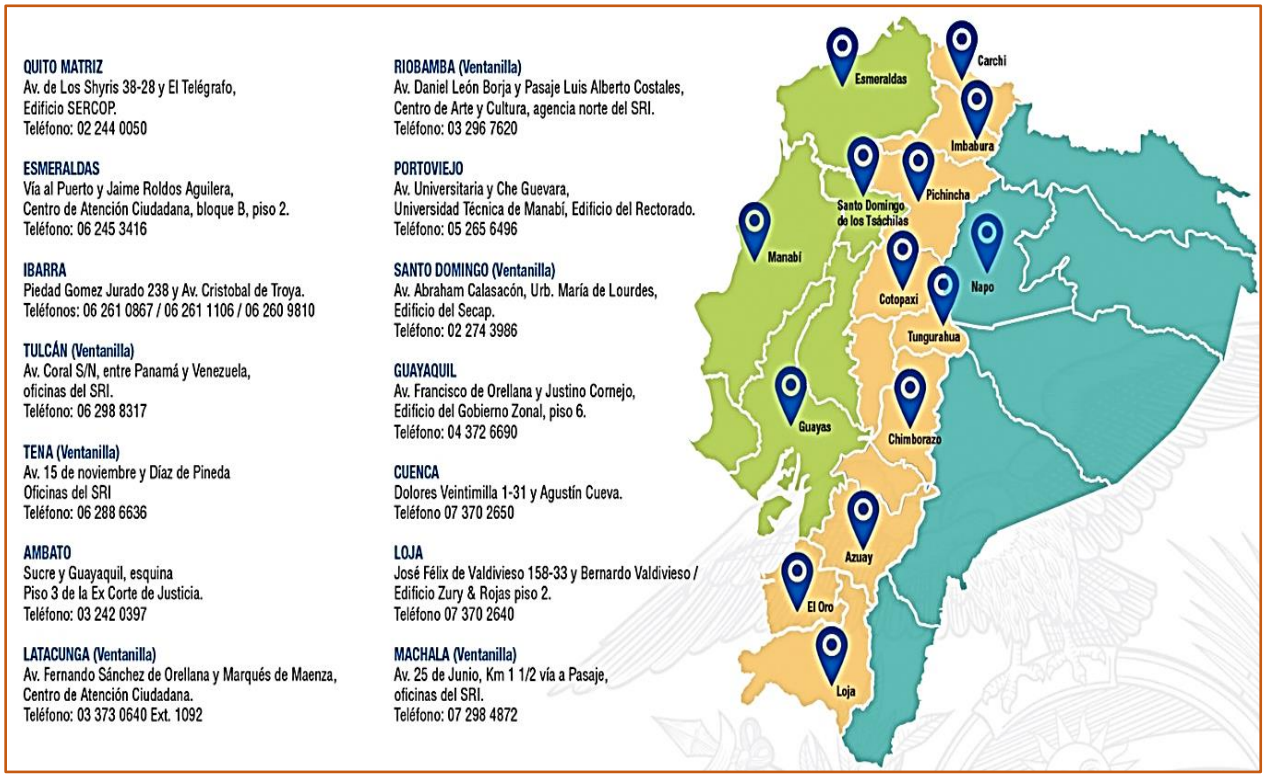


Figura 6-2. Oficinas del SERCOP a nivel nacional.

Fuente: (SERCOP, 2019)**.**

Sin embargo, existen acciones que podrían afectar la recuperación de un plan de continuidad los más relevantes se menciona la tabla 6-27.

Tabla 6-27. Acciones ante una interrupción.

Escena: perdida de información	Suceso	Operación de recuperación
En forma total (a nivel nacional)	Eventos naturales que ocasionen daños la infraestructura de la organización.	Levantamiento de la configuración, datos de respaldo de los sistemas de información en un sitio alterno.
	Daños en la base de datos y el sistema no permite el acceso a los usuarios.	
En forma parcial (operatividad)	Fallas del funcionamiento de operatividad en alguna oficina.	El personal debe buscar una oficina para realizar la operabilidad con normalidad.

Elaborado por: Investigador

En la tabla 6-28, se observa el análisis de riesgo y el proceso de operación de recuperación de los recursos críticos.

Tabla 6-28. Análisis de riesgo de los recursos críticos.

Recursos críticos	Riesgo	Operación de recuperación
Personal backup	Interrupción de los servicios del portal de la institución por daños causados por el personal	Capacitar al personal de respaldo.
Información de los procesos de contratación.	Deterioro de la información perteneciente a los procedimientos de contratación	Ejecutar copias de respaldo de la información de los procedimientos de contratación en sitios o dispositivos descentralizados

Elaborado por: Investigador

6.8 Desarrollo del plan de continuidad de negocios.

El desarrollo del presente trabajo de investigación se puede definir como la integración de una serie de procesos y actividades: la definición de procesos, análisis de impacto y la generación un informe de incidencias, haciendo uso de una metodología definida que permita lograr los objetivos y metas de la manera más eficiente y efectiva, donde está presente.

6.8.1 Definir procedimientos e impactos.

Para evitar la divulgación, modificación o eliminación de la información confidencial e impedir interrupciones de los procesos críticos de la institución se recomienda definir los procedimientos con herramientas adecuadas en cada caso.

Se establecen los procedimientos para el plan de continuidad de negocio, mismos que permitirán enfrentar la ocurrencia de eventos inesperados y trae consigo la paralización de los eventos críticos la los siguientes:

- Procedimiento para la declaración de emergencia
- Procedimiento de capacitación.
- Procedimientos de Operación de Contingencia del Gestión de servicios informáticos.
- Procedimientos de Operación de Contingencia de Innovación Tecnológica.
- Procedimientos de Operación de Contingencia Técnica de Operación.

En las siguientes tablas, se hace un resumen de los procedimientos con los respectivos objetivos, alcances, responsables y lineamientos.

Tabla 6-29. Procedimiento para la declaración de emergencia.

PROCEDIMENTO DE DECLARACIÓN DE EMERGENCIA	
OBJETIVO	Informar a los funcionarios de la entidad los pasos que se deben seguir al momento de presentar un incidente que afecte los servicios de información y comunicación que impacte en los procesos críticos y servicios de la entidad.
ALCANCE	Se cubre las actividades que se deben desarrollar desde el momento que se identifica un incidente que puede paralizar las operaciones de la entidad hasta el momento en que el Coordinar de innovación tecnológica o el encargado de comité de crisis declaran la emergencia y disponen activar los "Planes de continuidad del negocio y recuperación de desastres"
RESPONSABLE	Coordinador de innovación tecnológica, Comité de crisis
LINEAMIENTOS	Eventos de Riesgo: Los que puedan ocasionar la interrupción del servicio informático de la entidad
RESPONSABLES	**ACTIVIDADES**
Funcionarios de la Coordinación de Innovación Tecnológica	Inmediatamente se identifique un incidente que comprometan la funcionalidad de los sistemas de información se debe comunicar a las autoridades que forma parte de la coordinación de innovación tecnológica, en el caso de presentarse siniestros naturales, se debe comunicar de manera inmediata a los organismos de socorro estatales. Tomar en cuenta que la notificación se la debe ejecutar vía correo electrónico y llamada telefónica o de manera presencial en el caso de la interrupción de los servicios mencionados.
Equipo para evaluación del incidente	Las autoridades de la coordinación de innovación tecnológica evaluaran el incidente analizarán el impacto del mismo no sea totalmente evidente.

	Determinarán si el incidente ha ocasionado u ocasionará la suspensión del servicio informático, para lo cual se utilizará los siguientes niveles de alerta: Nivel de Alerta 1 (Baja) Cuando la situación de riesgo está controlada, no se afecta las operaciones del negocio ni el servicio tecnológico. Nivel de Alerta 2 (Media) El evento de riesgo impide las operaciones en oficinas puntuales pero no existe una afectación en la continuidad del negocio. Nivel de Alerta 3 (Alta) El evento de riesgo afecta o afectará el servicio informático o la operación de la entidad impactando en la continuidad del negocio.
Coordinador de innovación tecnológica	Informará al Director Ejecutivo Nacional la activación del Plan de Contingencia en el caso que el incidente sea considerado en nivel 2 y 3
Directores de la Coordinación de innovación tecnológica.	Determinarán el tiempo requerido en el los Servicios afectados sean colocados nuevamente de manera operativa de acuerdo al tiempo estimado en el plan de contingencia. Organizarán el equipo de trabajo con analistas y especialistas de las diferente direcciones con el fin de coordinar el trabajo del plan de contingencia. Determinarán el momento en que los sistemas de información se encuentren nuevamente operativos.
Director de atención al cliente	Comunicación constante con los directores de la coordinación de innovación tecnológica durante la ejecución del plan de contingencia Coordinar actividades para mantener informados a los clientes externos como proveedores y entidades sobre la reanudación del normal comportamiento de los Sistemas de información.
Director General	Notificará la decisión de activar el Plan de contingencia a través del medio más efectivo. Notificará el momento en que los sistemas de información o el recurso afectado regresen a su normal funcionamiento.

Tabla 6-30. Procedimiento para la declaración de emergencia.

Objetivos	Informar a todo el personal involucrado en el BCP de la secuencia a seguir en caso de algún desastre en los sistemas de comunicación e información y causar alguna falla en los procesos críticos de la institución.
Alcance	El manual de funcionamiento estará disponible para todo el personal.
Responsable operativo	Director/a de Gestión de Servicios Informáticos.
Lineamientos	Creación de un manual para el plan de continuidad Establecer tareas de recuperación y reanudación de los procesos críticos. Los programas de capacitación deberán aprobar el director /a de Gestión de Servicios Informáticos. Capacitar al personal con casos problemas del plan de continuidad. Semestralmente se informará al personal de los lineamientos y pruebas que se realizarán.
Responsables	
Coordinador de Gestión de Servicios Informáticos.	Realiza un cronograma de actividades para la capacitación.
	Envía comunicados al responsable del riesgo operativo con 48 horas de anterioridad con el respectivo cronograma de actividades.
Responsable del Riesgo Operativo	Se encarga de informal al personal de la capacitación con 24 horas de antelación. Realiza la capacitación exponiendo los puntos clases del plan de continuidad, los procesos críticos y las mediadas de respaldo a tomar.
Responsable de Riesgos en Contratación Pública	Analiza los resultados de la capacitación con el responsable del Riesgo Operativo y emiten al responsable del área.
Coordinador del Riesgo Operativo	En caso de no cumplir con las expectativas y objetivos de la capacitación se enviará al responsable del Riesgo Operativo, caso contrario se emitirá un informe final y pone en conocimiento al director/a de Gestión de Servicios Informáticos.

Elaborado por: Investigador

Tabla 6-30. Procedimientos de Contingencia de Gestión de Servicios Informáticos.

Objetivos	Establecer acciones ante algún incidente para minimizar los impactos que podría causar.
Alcance	El alcance es todo el personal de la institución en la ciudad de Quito.
Responsable operativo	Director/a de Gestión de Servicios Informáticos..
ACTIVIDADES	
Validación de las consultas técnicas de los usuarios en el sistema.	
El *"Procedimientos de Gestión de Servicios Informáticos"*- Validación de las consultas técnicas de los usuarios en el sistema deberá ser puesto en marcha en caso de presentarse los siguientes escenarios: • Indisponibilidad del sistema oficial de contratación del estado • Indisponibilidad en el servicio del internet. **Actividades del proceso** • Monitoreo de la infraestructura • Realizar pruebas internas de consulta. • Verificación de la disponibilidad del sistema. **Recursos críticos** *Recursos humanos* • Analista de Gestión de Servicios Informáticos *Página web* • SOCE *Servicios* • Teléfono • Correo electrónico • Internet *Recursos informáticos* • 1 computadoras • Conexiones. **Plan de contingencia** • En el caso de la indisponibilidad en el servicio del internet, se deberá ingresar a la base de datos con la ayuda del servidor actualizado recientemente, pero si existe fallas a nivel nacional el proceso de "Validación de las consultas técnicas de los usuarios en el sistema" no podrá ser efectuada hasta su activación.	
Planifica, establece, dirige y controla los procesos de tecnologías de la información y comunicación, valida funcionamiento del SOCE. Y catálogo electrónico.	
El *"Planifica, establece, dirige y controla los procesos de tecnologías de la información y comunicación, valida funcionamiento del SOCE. Y catálogo electrónico."* deberá ser puesto en marcha en caso de presentarse los siguientes escenarios: • Caídas del sistema. **Actividades del proceso** • Ejecución de pruebas internas. • Verificación de conexiones a los servidores del sistema. • Notificación a las direcciones correspondientes. **Recursos críticos** *Recursos humanos* • Analistas de Gestión de Servicios Informáticos. *Página Web*	

- SOCE.
- Catálogo electrónico.

Servicios

- Conexiones.
- Accesos remotos.
- Internet

Recursos informáticos

- 3 computadoras
- 1 impresora
- 1 scanner

Plan de contingencia

En el caso existir inconsistencias en el proceso de validación del funcionamiento del SOCE y catálogo electrónico no podrá ser efectuada hasta su activación en el ambiente de producción de las aplicaciones.

Verificación del funcionamiento de aplicaciones externas.

El *"Procedimiento de Gestión de Servicios Informáticos- Verificación del funcionamiento de aplicaciones externas"* deberá ser puesto en marcha en caso de presentarse los siguientes escenarios:

- Indisponibilidad de la aplicación externa.

Actividades del proceso

- Ejecución de pruebas funcionales.
- Vinculación a las aplicaciones externas.
- Notificar a los proveedores de los sistemas externos.

Recursos críticos

Recursos humanos

- Analista de Gestión de Servicios Informáticos.

Aplicaciones

- Repositorio documental.

Servicios

- Teléfono
- Correo electrónico
- Internet

Recursos informáticos

- 2 computadoras
- 1 impresora
- 1 scanner

Plan de contingencia

En el caso de la indisponibilidad de las aplicaciones externas" se deberá notificar a los respectivos proveedores respetando los SLA.

Elaborado por: Investigador

Tabla 6-31. Procedimientos de Gestión de Desarrollo de Soluciones.

Objetivos	Establecer acciones ante algún incidente para minimizar los impactos que podría causar la indisponibilidad del sistema por código fuente.
Alcance	Personal de la institución en la ciudad de Quito.
Responsable operativo	Director/a de Desarrollo de Soluciones Tecnológicas.
ACTIVIDADES	
Código fuente de aplicaciones informáticas desarrolladas.	
El *"*Procedimientos de Gestión de Desarrollo de Soluciones - **Código fuente de aplicaciones informáticas desarrolladas***"*, deberá ser puesto en marcha en caso de presentarse los siguientes escenarios: • Deterioro, pérdida de código fuente de las aplicaciones de la entidad. **Actividades del proceso** • Verificar las versiones del código fuente en los diferentes ambientes. • Verificación del repositorio de código fuente • Revisión de los servidores del ambiente de desarrollo. **Recursos críticos** *Recursos humanos* • Analista de desarrollo tecnológico. *Página web* • Soce, catálogo electrónico, ambiente de desarrollo • Catálogo electrónico. *Servicios* • Teléfono • Correo electrónico • Internet • Conexión a servidores *Recursos informáticos* • 1 computadoras • 1 impresora Plan de contingencia • En el caso de la indisponibilidad o deterioro del código fuente de las aplicaciones de la entidad, se deberá acudir a las versiones publicadas en los ambientes de pruebas y producción.	
Diseña y desarrolla pruebas de automatización y operación del Sistema Oficial de Contratación Pública del Ecuador.	
El *"*Procedimiento de Gestión de Desarrollo de Soluciones - **desarrolla pruebas de automatización y operación del Sistema Oficial de Contratación Pública del Ecuador.***"* deberá ser puesto en marcha en caso de presentarse el siguiente escenario: • Fallas en la codificación de las aplicaciones informáticas. **Actividades del proceso** • Implementación y pruebas de codificación de aplicaciones informáticas. • Evaluación semestral de código fuente. • Realización de informes del correcto funcionamiento del código fuente. **Recursos críticos** *Recursos humanos* • Analista de Desarrollo de soluciones tecnológicas *Aplicación*	

- Software de soportes de la institución.
- SOCE
- Catálogo electrónico.

Servicios

- Teléfono
- Correo electrónico
- Internet
- Conexión a servidores.

Recursos informáticos

- 2 computadoras
- 1 impresora
- 1 scanner

Plan de contingencia

En el caso de existir inconsistencias de la codificación de las aplicaciones se deberá mejorarlo o cambiarlo de acuerdo la decisión que se tome en el comité de Innovación Tecnológica.

Gestiona las aplicaciones informáticas desarrolladas a medida por terceros para el Servicio Nacional de Contratación Pública.

El *"*Procedimientos de Gestión de Desarrollo de Soluciones Gestiona las aplicaciones informáticas desarrolladas a medida por terceros para el Servicio Nacional de Contratación Pública.*"* deberá ser puesto en marcha en caso de presentarse los siguientes escenarios:

- Indisponibilidad de las aplicaciones desarrolladas a medida por terceros.

Actividades del proceso

- Vinculación a las aplicaciones externas.
- Validación de conectividad aplicaciones externas.
- Ejecución de pruebas de aplicaciones externas

Recursos críticos

Recursos humanos

- Analista, especialista de desarrollo tecnológico

Aplicaciones

- Enlaces a sistemas desarrollados por terceras personas

Servicios

- Código fuente

Recursos informáticos

- 2 computadoras
- 1 impresora
- 1 scanner

Plan de contingencia

En el caso de la indisponibilidad de la aplicación adecuado, para el proceso de "Gestiona las aplicaciones informáticas desarrolladas a medida por terceros para el Servicio Nacional de Contratación Pública." no podrá ser efectuada hasta su comunicación y gestión con los proveedores externos encargados del soporte a las aplicaciones externas

Integración e interoperabilidad de sistemas de información

El *"Procedimiento de Contingencia de Desarrollo de soluciones* – "Integración e interoperabilidad de sistemas de información*"* deberá ser puesto en marcha en caso de presentarse los siguientes escenarios:

- Falla en la integración e interoperabilidad con los sistemas de información.

Actividades del proceso

- Verificación de los enlaces de conexión para las aplicaciones.

- Verificación del estado de las aplicaciones

Recursos críticos

Recursos humanos

- Analista de Desarrollo de Soluciones
- Especialista de Desarrollo de Soluciones

Documentación

- Manual de desarrollo de soluciones

Servicios

- Correo electrónico
- Internet
- Acceso a los servidores en los que se encuentran los sistemas de información ambiente de desarrollo.

Recursos informáticos

- 1 computadoras
- 1 impresora
- 1 scanner

Plan de contingencia

En el caso de existir fallas en la integración e interoperabilidad de sistemas de información, se debe verificar la disponibilidad de los sistemas, de las conexiones, analizar la solución al problema de interoperabilidad con las herramientas de desarrollo.

Gestiona el desarrollo de las aplicaciones informáticas requeridas para el negocio.

Procedimientos de Contingencia de Desarrollo tecnológico Innovación Tecnológica- Gestiona el desarrollo de las aplicaciones informáticas requeridas para el negocio." deberá ser puesto en marcha en caso de presentarse el siguiente escenario:

- Indisponibilidad del ambiente de desarrollo.

Actividades del proceso

- Verificación de la conectividad a los servidores.
- Verificación de los equipos de seguridad perimetral.
- Análisis de la última versión del código fuente.

Recursos críticos

Recursos humanos

- Analista, especialista de desarrollo tecnológico.

Aplicaciones

- Software para desarrollo
- Sistema operativo de servidores

Servicios

- Teléfono
- Correo electrónico
- Internet

Recursos informáticos

- 3 computadoras
- 1 impresora
- 1 scanner

Plan de contingencia

En el caso de la disponibilidad de Gestiona el desarrollo de las aplicaciones informáticas requeridas para el negocio, se deberá obtener la última versión del código fuente y publicarlos en servidores de desarrollo.

Tabla 6-2. Procedimientos de Gestión de Operaciones de Innovación Tecnológica.

Objetivos	Establecer acciones ante algún incidente para minimizar los impactos que podría causar la indisponibilidad del sistema por servidores y equipos de comunicación
Alcance	Personal de la institución en la ciudad de Quito.
Responsable operativo	Director/a de Operaciones Tecnológicas.
ACTIVIDADES	
Administra el funcionamiento de los diferentes ambientes de cada una de las herramientas del Sistema Oficial de Contratación Pública del Ecuador	

El *Procedimiento de Gestión de Operaciones de Innovación tecnológica* -Administra el funcionamiento de los diferentes ambientes de cada una de las herramientas del Sistema Oficial de Contratación Pública del Ecuador.*",* deberá ser puesto en marcha en caso de presentarse los siguientes escenarios:

- Fallo en el funcionamiento de las aplicaciones de la entidad

Actividades del proceso

- Verificación de la conectividad a los equipos de comunicaciones
- Verificación del estado de los equipos de comunicación y cómputo
- Verificar las versiones de los sistemas de información.

Recursos críticos

Recursos humanos

- Analista de operaciones de Innovación tecnológica.
- Especialista de operaciones de Innovación tecnológica

Página web

- SOCE, catálogo electrónico, ambiente de producción, pruebas y desarrollo
- Catálogo electrónico ambiente de producción, pruebas y desarrollo

Servicios

- Teléfono
- Correo electrónico
- Internet
- Conexión a servidores

Recursos informáticos

- 1 computadoras
- Correo electrónico
- Servidores

Plan de contingencia

- En el caso de algún inconveniente en la administración de los sistemas de información de la entidad en los diferentes ambientes, se debe levantar el ambiente en servidores alternos que se encuentren configurados e instalados las herramientas requeridas.

Servidores WEB

- Instalar y configurar el Sistema Operativo RED HAT Linux Server n.n
- Instalar y configurar APACHE
- Instalar y configurar SEND MAIL
- Instalar y configurar TOMCAT 5
- Instalar y configurar PHP.
- Enganchar el servidor en REDHAT
- Instalación de servidor de aplicaciones.

ACTIVIDADES
Administración de las bases de datos de la entidad

El *"Procedimiento de Gestión de Operaciones de Innovación tecnológica- Administra las bases de datos de la entidad."* deberá ser puesto en marcha en caso de presentarse el siguiente escenario:

- No disponibilidad de los servicios de base de datos
- Comportamiento inadecuado de los servicios de base de datos

Actividades del proceso

- Verificación de la conectividad a los servidores de base de datos.
- Verificación del estado de los servidores en los que se encuentran las bases de datos

Recursos críticos

Recursos humanos

- Analista de operaciones de Innovación Tecnológica
- Especialista de operaciones de Innovación Tecnológica

Aplicación

- Base de datos de la entidad
- Servidores
- SOCE
- Catálogo electrónico.

Servicios

- Teléfono
- Correo electrónico
- Internet
- Conexión a servidores.

Recursos informáticos

- 2 computadoras
- 1 impresora
- 1 scanner

Plan de contingencia

En el caso de existir no disponibilidad de las bases de datos de la entidad se debe:

1. Instalar y configurar el Sistema Operativo RED HAT Linux Server
2. Instalar y configurar Postgresql 1.0
3. Instalar y configurar Sendmail.

- **BASE DE DATOS.**
  1. Instalar y configurar el Sistema Operativo RED HAT Linux Server
  2. Instalar y configurar Postgresql
  3. Instalar y configurar Sendmail
  4. Editar el fichero de configuración #vim /var/lib/pgsql/data/n.n/data/pg_hba.conf
  5. Reiniciar el servicio.

Tabla 6-3. Procedimientos de Gestión de Seguridad Informática

Objetivos	Establecer acciones ante algún incidente para minimizar los impactos que podría causar la indisponibilidad del sistema por fallos en equipos de seguridad perimetral.
Alcance	Personal de la institución Dirección de seguridad informática en la ciudad de Quito.
Responsable operativo	Director/a de Seguridad Informática
ACTIVIDADES	
Monitorea la disponibilidad del ambiente de producción del Servicio Nacional de Contratación Pública.	
El *"Procedimiento de Seguridad Informática de Innovación tecnológica- Monitorea la disponibilidad del ambiente de producción de los sistemas del Servicio Nacional de Contratación Pública."* deberá ser puesto en marcha en caso de presentarse el siguiente escenario: • No disponibilidad de los servicios de monitoreo de los sistemas de información ambiente productivo • Error en los sistemas de información ambiente productivo **Actividades del proceso** • Verificación de la conectividad a los servidores de herramientas de monitoreo • Verificación del estado de los servidores en los que se encuentran los sistemas de información. **Recursos críticos** *Recursos humanos* • Analista de operaciones de Seguridad Informática • Especialista de Seguridad Informática *Aplicación* • Base de datos de la entidad • Servidores • SOCE • Catálogo electrónico. • Sistema de monitoreo *Servicios* • Teléfono • Correo electrónico • Internet • Conexión a servidores. *Recursos informáticos* • 2 computadoras • 1 impresora Plan de contingencia En el caso de existir no disponibilidad de los sistemas de monitoreo se debe: Verificar la conectividad al servidor de la herramienta de monitoreo Verificar el estado del servidor de monitoreo en los equipos de seguridad perimetral en la sección Virtual server. Ejecutar el cambio de estado del servidor en mención en los virtual server de los equipos de seguridad perimetral. Verificar estado de las conexiones al servidor de monitoreo.	

Comprobar el funcionamiento del sistema de monitoreo.
En caso de ser necesario, tomar contacto con el proveedor del sistema de monitoreo

Definir lineamientos técnicos para garantizar la confidencialidad, integridad y disponibilidad de la información.

El "Procedimiento de Seguridad Informática de Innovación tecnológica- Definir lineamientos." deberá ser puesto en marcha en caso de presentarse el siguiente escenario:

- Presencia de ataques a los sistemas de información de la entidad
- Vulneración de la seguridad informática.

Actividades del proceso

- Verificación de los posibles ataques en los equipos de seguridad perimetral.
- Control del posible ataque a los sistemas de información.

Recursos críticos

Recursos humanos

- Analista de operaciones de Seguridad Informática
- Especialista de Seguridad Informática

Aplicación

- Base de datos de la entidad
- Servidores
- SOCE
- Catálogo electrónico.
- Equipos de Seguridad perimetral

Servicios

- Teléfono
- Correo electrónico
- Internet
- Conexión a servidores.

Recursos informáticos

- 2 computadoras
- 1 impresora

Plan de contingencia

En el caso de existir la presencia de un ataque a los sistemas de información de la entidad se debe:
Verificar el estado de los servidores que contienen los sistemas de información de la entidad.
Ingresar a los equipos de seguridad perimetral, a la sección tráfico de los servidores.
Identificar el tráfico inusual existente en los servidores de aplicaciones y base de datos
Controlar el ataque, mediante las herramientas de los equipos de seguridad perimetral.
Verificar el comportamiento de los sistemas de información de la entidad.
En caso de ser necesario tomar contacto con el proveedor de los equipos de seguridad perimetral.
Documentar todos los pasos ejecutados.

Elaborado por: Investigador.

Tabla 6-4. Procedimiento para levantar un proceso Crítico

Proceso: Control y administración de la base de datos.

Proceso	**Responsable**	**Área Responsable**	**Aplicaciones**	**Herramientas de oficina**	**Servicios tecnológicos**	**Recursos humanos, personal principal y backup**	**Proveedores externos**	**Recursos de soporte**	**Cantidad de recursos tecnológicos existentes**	**Cantidad de recursos tecnológicos mínimos en caso de existir un desastre**
Control y administración de la base de datos.	Director de operaciones de Innovación Tecnológica	Dirección de operaciones de Innovación tecnológica	Posgresql	Reportar incidente a los funcionarios involucrados Generar informe de incidencia	Internet Correo electrónico Servidores Telefonía	Especialistas Administradores de servidores. Director de operaciones de Innovación tecnológica. DBA	Servicio de soporte posgres	Manual de administración de base de datos. Instructivo administración servidor de base de datos.	Un servidor principal de base de datos transaccional. Un servidor de base de datos de lectura. Dos servidores de backup.	Un servidor principal de base de datos transaccional. Un servidor de base de datos de lectura. Un servidores de backup

Procedimiento para levantar la base de datos para la aplicación transaccional de la entidad:

- Un servidor que cumpla con las características mínimas del servidor actual trabajando en el ambiente de producción.
- Instalar las herramientas requeridas Sistema Operativo, motor d base de datos posgres.
- Obtener el backup de la data.

Descripción de los pasos a seguir para proceder a la obtención del backup de la data.

Pasos previos

- Base de datos transaccional posgres con un servidor de réplica en línea.
- Puerto por el que atiende la base de datos 5432
- Nombre de la base de datos principal
- Esquemas con los que cuenta la base de datos principal

Actividades que debe ejecutar el Administrador de la base de datos para la obtención de backups de la data.

- Definir el conjunto de tablas que forman pare de históricos y pasarlas al esquema correspondiente
- Implementar reglas en las cuales se establece en los inicios de mes las tablas historias y log's y el esquema al que deben pertenecer.
- Implementar y Ejecutar un crond diario que permita ejecutar un respaldo full diario de las data.
- Verificar la hora ideal para ejecutar el crond de respaldo.
- Implementar el mecanismo que permitirá ejecutar cambios de esquemas de la data histórica.
- Implementar archivos logs que permita almacenar los resultados de los trabajos de los diferentes crones
- Implementar el directorio en el que se almacenará los respaldos
- El backup debe ser identificad fácilmente, para ello se debe incluir fecha de obtención y responsable de la generación del backup.
- El operador de las cintas de backup deberá ejecutar

- Tomar el backup diario y con la librería adecuada copiar a la cinta para backup
- Tomar el backup mensual y copiarlo en las cintas
- Cambiar las cintas cada vez que se hay culminado es espacio de almacenamiento
- Llevar las cintas grabadas a un lugar físico seguro dentro de la entidad fuera del data center
- Etiquetar de manera clara con nombre del responsable y fecha de obtención del backup cada cinta
- Proveer al BDA la cinta de acuerdo a cada backup requerido.

6.8.2 Generación de informes de incidencias

Tabla 6-32. Informe de incidencias

Nombre del Informe	Informe de incidencias
Fecha de elaboración	13/05/2019
Destinatario / Cargo	Coordinador de Innovación Tecnológica
Objetivo	Describir las acciones realizadas por los servidores públicos de la entidad ante la presencia de eventos inesperados.
Alcance	Coordinación Nacional de Innovación Tecnológica.
Participantes	Servidores públicos de la dirección de seguridad informática. Personal de operaciones de innovación tecnológica.
Proveedor	En caso de afectación de equipos ubicados en el datacenter de Cnt y datacenter de Matriz, los proveedores deberán participar en el diagnóstico, este ítem se incluye en la etapa contractual de la prestación de servicios.
Pruebas ejecutadas	1- Se verificó el compromiso de las cuatro direcciones que conforman la coordinación nacional de innovación tecnológica con la ejecución del BCP. 2- Se observó que existe un oficial de seguridad de la información, responsable de asignar los permisos de acuerdo con cada perfil de usuario y velar el cumplimiento de los controles de seguridad establecidos. 3- Se pudo observar que no se encuentran difundidas las políticas de tecnologías de información al personal de la coordinación de innovación

	tecnológica, así como los procedimientos a seguir para cumplir dichas políticas. 4- Se verificó que no existe la suficiente capacitación para el personal Backup en el manejo de equipos tecnológicos como servidores, equipos de seguridad perimetral y equipos de redes. Los instructivos no se encuentran aprobados por la coordinadora de innovación tecnológica. 5- Existe un inventario de los equipos de tecnología identificando cada responsable de su uso. 6- Existen acuerdos de niveles de servicio SLA con los proveedores externos de los equipos de tecnología. 7- Existe una adecuada comunicación interna con los funcionarios responsables de la administración de los equipos tecnológicos 8- Los funcionarios administradores de contratos involucrados en la prestación de servicios informáticos se encuentran en constante comunicación con las diferentes áreas involucradas para procesos de cumplimiento y sanciones o multas por incumplimientos.
Conclusiones	Al realizar las pruebas detalladas en este informe de incidencia se pudo identificar una serie de contratiempos que deben ser analizados en la entidad para que el plan de continuidad se elabore con éxito, se debe considerar que los involucrados en la administración de la entidad deben realizar controles adecuados a todos los datos y documentación informática. Todos los objetivos deben ser orientados a la resolución de problemas detectados en el desarrollo de pruebas.
Recomendaciones	1- Realizar capacitaciones técnicas al personal Backup sobre la administración de equipos y servidores informáticos. 2- Elaborar los procedimientos necesarios para poder ejecutar de manera exitosa las políticas de tecnología. 3- Automatizar el proceso de asignación de accesos que lleva el oficial de seguridad de la información.

Elaborado por: Investigador

Con ayuda del informe de incidencia en la parte de verificación (tabla 6-31) se puede observar que para aplicarse todas las pruebas establecidas se necesitan algunos controles, capacitaciones y procedimientos en la entidad para llegar a establecer un Plan de Continuidad exitoso. La entidad es la encargada de seleccionar al personal que esté a cargo, deben aportar con su experiencia y conocimientos en el desarrollo de un BCP.

6.9 Verificación y control del plan de continuidad

6.9.1 Análisis de informes de incidencias

Es importante conocer la forma de cómo se está aplicando el plan de continuidad en la organización, para de esa forma comprobar el correcto funcionamiento del mismo, controlando el número de posibles interrupciones y en caso de que se presente alguna, verificando que los tiempos de recuperación de los procesos sean el mínimo o se reduzca paulatinamente, controlar que los procesos críticos del sistema no representen una preocupación en caso de una interrupción, y por último concluir con que se cumplan todas las metas y objetivos planteados por la organización.

El siguiente informe de incidencia muestra los aspectos verificados de la organización.

6.10 Mejoramiento del plan de continuidad

6.10.1 Plan de mantenimiento

En un plan de Continuidad de negocio es muy importante tener el respaldo de un mantenimiento y actualización continua, para ello se realizan una serie de pruebas de entrenamiento, pruebas técnicas, simulacros. El objetivo principal de un plan de mantenimiento es detallar todos los cambios y estrategias del plan de Continuidad. El potencial mantenimiento se evaluará cada vez que existan modificaciones o cambios importantes en:

- Procesos
- Servicios
- Proveedores
- Eventos externos

En la tabla 6-33 se realiza el plan de mantenimiento.

Tabla 6-33. Plan de mantenimiento.

N°	Actividades del plan de mantenimiento	Responsabilidad	Frecuencia
1	Perfeccionar el direccionamiento estratégico y procedimientos de la tecnología de información.	Director/a de gestión de servicios Informáticos.	Actividad del día a día.
2	Incentivar al personal del área tecnológica de la información con capacitaciones sobre el plan de continuidad de negocios.	Director/a de gestión de servicios Informáticos.	Cada Cuatrimestre.
3	Revisar los planes de recuperación por área.	Director/a de gestión de servicios Informáticos.	Bianual
4	Mantener un directorio que contenga los documentos del BCP. - Operaciones tecnológicas - Análisis de impacto - Plan de respuesta a crisis - Plan de restauración de actividades.	Director/a de gestión de servicios Informáticos.	Actividad del día a día.
5	Desarrollar ejercicios de simulación que permitan una reconstrucción de los servidores necesarios para reanudar los procesos de forma inmediata.	Director/a de gestión de servicios Informáticos.	Anual
6	Medir los resultados de las pruebas según lo acordado en el TOR y POR.	Director/a de gestión de servicios Informáticos.	Bianual

Elaborado por: Investigador

El plan de mantenimiento expuesto en la tabla 6-33 puede ser modificado de acuerdo a las necesidades previo a una evaluación por parte de la administración, ya que se pueden presentar problemas o casos nuevos que no estén o formen parte de este plan de trabajo.

6.10.2 Propuesta de mejora

Es importante que el plan de negocio este expuesto a mejoras continuas y así lograr obtener todos los beneficios que pueda brindas; según (APE, 2014) existe una lista de los aspectos considerados importantes para una mejora continua redactadas a continuación:

1- Adaptarse de forma inmediata a los nuevos cambios y mejoras tecnológicas presentes en el medio.
2- Realizar un estudio de proveedores, para así llegar a identificar los que se encuentren en estado crítico y con los que se debe trabajar de forma continua.
3- Nombrar un líder para la ejecución del BCP, quien tendrá la capacidad de direccionar las actividades del BCP en toda la organización.
4- Involucrar en el BCP personal capacitado para el manejo del plan, ya que se encuentran actividades que requieren la participación activa y la cooperación de distintos sectores.
5- La dirección debe actualizar y asegurar los recursos necesarios, incluyendo un presupuesto disponible para el líder del BCP y el equipo que desempeñe las actividades encomendadas.

6.11 Análisis de resultados

En el presente trabajo de investigación se deja planteado la propuesta de un plan de continuidad de negocios para el Servicio Nacional de Contratación Pública, con el mismo se pretende reducir o eliminar cualquier daño que se pueda presentar en caso de un evento no programado o desastre que interrumpa las operaciones normales de funcionamiento en el departamento de gestión de servicios informáticos.

La información confidencial se ha convertido en uno de los puntos más importantes que contiene cualquier organización, en caso de un desastre el principal objetivo es proteger toda esta información, parte de sus operaciones, funcionamientos y/o servicios en red que pueden quedar inoperantes. La preparación de un plan llega a ser la clave para sobrevivir ante eventos externos.

En el presente trabajo de investigación, se verificó los procesos que se realizan en la organización, el compromiso de las cuatro direcciones que conforman la coordinación nacional de innovación tecnológica con la ejecución del BCP.

Se lograron identificar que en el entorno de la información tecnológica existen una serie de recursos (humanos, naturales, técnicos, etc.) que están expuestos a diferentes tipos de eventualidades: los normales, comunes a cualquier entorno, y los excepcionales, originados por situaciones concretas que afectan o pueden afectar a toda o parte del Servicio Nacional de Contratación Pública, como la inestabilidad política del país; para tratar de minimizar los efectos de un problema de seguridad se realizó un análisis de riesgos. La implementación del plan se transforma en una ventaja competitiva para el sector.

Una vez que se conoció y evaluó los riesgos a los que se enfrenta la organización se pudo definir las políticas e implementar las soluciones prácticas, los mecanismos para minimizar los efectos ante cualquier tipo de desastre.

El plan de continuidad se diseñó para que la institución logre enfrentar un desastre, proporciona información suficiente para que funcione normalmente después de efectuarse un desastre.

Se definieron las características de la institución donde se determinó que es un ente rector que brinda a instituciones públicas y proveedores un modelo de gestión que asesora, controla y supervisa en base a transparencia y calidad en los procedimientos de contratación y que existen acuerdos de niveles de servicio SLA con los proveedores externos de los equipos de tecnología.

Se estudió y se determinó tanto el tiempo de recuperación objetivo como el punto de recuperación objetivo; donde, el RTO se utiliza para plantearse un tiempo límite para que un cierto servicio vuelva a estar en funcionamiento y el RPO se refiere al tiempo que transcurre entre el momento del desastre y el último punto de restauración, parecen iguales, pero sirven para un diferente propósito.

6.12 Previsión de la evaluación

Tabla 6-34. Previsión de la evaluación

Preguntas básicas	Explicación
¿Qué evaluar?	La propuesta del plan de continuidad de negocios en el departamento de Coordinación e Innovación Tecnológica.
¿Por qué evaluar?	Para conocer el efecto del plan de continuidad de negocios propuesto
¿Para qué evaluar?	Para conocer el impacto del plan de continuidad de negocios sobre la institución.
¿Quién evalúa?	El director
¿Cuándo evalúa?	Posterior a la ejecución de la propuesta
¿Con que evaluar?	Aplicando indicadores
¿Fuentes de información?	Usuarios del proceso del control y administración de los riegos críticos.

Elaborado por: Investigador

6.13 Conclusiones

La propuesta del plan de continuidad de negocios dentro de la coordinación e innovación de tecnología involucra el análisis de los procesos y la creación de estrategias para identificar riesgos críticos sobre los sistemas tecnológicos en la Coordinación e Innovación Tecnológica, con el fin de crear acciones de respuesta efectiva para resguardar los intereses de la institución. Para este tipo de análisis se utilizó el esquema de continuidad de negocios de basado en el modelo PHVA (Planear, Hacer, Verificar y Actuar).

En conclusión, es importante contar con estándares y esquemas de medición que permitan identificar la posición en que se encuentra la organización, pero el gran riesgo es confiar en que solo la teoría y la documentación que brinda protección y confiabilidad sin mantener el control en un evento de catástrofe, es en este sentido importante, resaltar que para contar con una exitosa preparación ante desastres, las pruebas y ejercicios se convierten en un elemento fundamental de las estrategias y arquitecturas tanto de TIC como operativas; las cuales deben ser realizadas de manera programada y constante, ya que nos permiten desarrollar confianza en nuestras capacidades de reacción, así como fortalecer las habilidades y experiencia de los equipos de encargados de la continuidad. Estas pruebas y ejercicios se deben hacer tanto de "escritorio" como "simuladas", con escenarios de fallas totales o parciales de todos y cada uno de los recursos críticos para el negocio.

Es importante superar el temor que nos representa "simular" una falla o crisis, mediante la preparación de todas las áreas, no solo de tecnología, sino también de las áreas operativas, ante la posibilidad de una falla severa a nivel de la provisión de recursos (personal clave, infraestructura, potencia, ambiente, tecnología, etc.), todo esto orientado al final, a minimizar la "incertidumbre" y conocer las propias vulnerabilidades, trabajar en ellas y aumentar la capacidad de "resiliencia" para la organización como un todo y así garantizar una real "continuidad del negocio".

6.14 Recomendaciones

- Resaltar que la administración de la institución debe tener presente la propuesta de un plan de continuidad ya que nos encontramos en un país donde los desastres naturales como terremotos, inundaciones, etc realmente pueden ocurrir.

- Incentivar al personal Backup a tomar capacitaciones técnicas sobre el manejo de equipo tecnológicos ya sea para servidores, seguridad perimetral o equipos de redes.
- Automatizar el proceso de asignación de accesos que lleva el oficial de seguridad de la información.
- Difundir las políticas de tecnologías de informacion al personal de la coordinación de innovación tecnológica, y los procedimientos a seguir para cuplir dichas políticas.
- Es necesario actualizarse periódicamente con un análisis de riesgos que puedan ocurrir en la institucion e incluirle de forma inmediata la plan de continuidad.

6.15 Bibliografía

Agencia EFE. (15 de Abril de 2019). *Ecuador denuncia 40 millones de ciberataques tras retiro de asilo a Assange*. Obtenido de https://www.elcomercio.com/actualidad/ecuador-denuncia-millones-ciberataques-assange.html

Alvarez, J. (14 de 11 de 2011). *Retroalimentación del control de calidad.* Recuperado el 9 de 3 de 2019, de La empresa: https://todoparaemprendedores.wordpress.com/2011/11/14/la-retroalimentacion-y-el-control-en-la-empresa/

APE. (2014). Guía para Pequeñas y Medianas Empresas sobre el Plan de Continuidad de Negocios. 61.

ASI. (9 de 3 de 2009). *Plan de continuidad informática.* Recuperado el 9 de 3 de 2019, de https://www.auditoria.com.mx/not/boletin/2006/0601_40.htm

ASPER. (26 de Octubre de 2017). *Plan de continuidad.* Recuperado el 14 de Marzo de 2019, de https://blog.apser.es/2017/10/26/plan-de-continuidad-tic-por-que-tenerlo

Aucapiña, T. V. (Julio de 2012). *Repositorio Universidad Técnica de Ambato.* Recuperado el 12 de 3 de 2019, de http://repositorio.uta.edu.ec/bitstream/123456789/2361/1/Tesis_t715si.pdf

Ávila, M. (2013). *Diseño e implementación de un DRP (Disaster Recovery Plan) para Departamento de Ingenierías de la Empresa Continental Tire Andina.* Universidad de Cuenca. Recuperado el 13 de Mayo de 2019, de http://dspace.ucuenca.edu.ec/jspui/bitstream/123456789/5265/1/TESIS.pdf

Bautista, M. (2014). Marco de referencia de formulación de un Plan de Continuidad de Negocio para TI, un caso de estudio. *8*(1), 200- 207. Recuperado el 26 de Febrero de 2019, de https://web.b.ebscohost.com/abstract?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=13905074&AN=95648743&h=J2LffZDWEJo8y%2bys4ltQt7FXJWr4eRt7GGdTFXBWjSxVSr%2bJmxah%2fe8rHFaeJsFhfw0u1H%2bAF8TUz6M5YxdWPQ%3d%3d&crl=c&resultNs=AdminWebAuth&resultL

Benson, C. (2000). *Estrategias de seguridad*. (Microsoft Solutions) Recuperado el 27 de Febrero de 2019, de https://www.segu-info.com.ar/politicas/seguridad.htm

Benson, C. (2000). *Estrategias de seguridad*. Obtenido de https://www.segu-info.com.ar/politicas/seguridad.htm

Betancourt, E., & Salguero, J. (2014). *Propuesta del plan de continuidad del negocio (BCP), caso de aplicación.* Escuela Politécnica Nacional, Facultad de Ingenieria de Sistemas, Quito. Recuperado el 10 de Marzo de 2019

BSI. (2019). *bsigroup*. Obtenido de https://www.bsigroup.com/es-ES/ISO-22301-continuidad-de-negocio/

Camelo, L. (10 de 2016). *Seguridad de la información en Colombia*. Recuperado el 23 de 2 de 2019, de http://seguridadinformacioncolombia.blogspot.com/2010/06/plan-de-continuidad-de-negocios-o.html.

Castañeda, C. (28 de Septiembre de 2016). *Como hacer el análisis de contexto para la empresa*. Recuperado el 12 de Febrero de 2019, de Acerta: http://acertacomunicaciones.com/analisis-de-contexto-la-empresa/

ccn. (12 de 02 de 2014). *Análisis de Impacto. Continuidad de operaciones.* Obtenido de https://www.ccn-cert.cni.es/publico/herramientas/Pilar-5.4.5/Pilar_5.4.5/bcm_es/index.html?n=6.html

CIBERSEGURIDAD. (12 de Mayo de 2018). *Estrategias de recuperación para un plan de continuidad*. Recuperado el 13 de Mayo de 2019, de https://ciberseguridad.blog/estrategias-de-recuperacion-para-un-plan-de-continuidad-del-negocio/

Compras públicas. (18 de Abril de 2018). *Decreto 258*. Recuperado el 4 de Mayo de 2019, de https://portal.compraspublicas.gob.ec/sercop/wp-content/uploads/files/99/Decreto_258.pdf

Constituyente, A. (Abril de 2008). *http://www.cpccs.gob.ec/wp-content/uploads/2017/03/LOSNCP.pdf*.

Contreras, J. (27 de 02 de 2019). *Las cuatro modalidades de la seguridad laboral*. Obtenido de Docente de prevención de riesgos: http://www.emb.cl/hsec/articulo.mvc?xid=177&edi=8&xit=modelo-seguridad-total-las-cuatro-modalidades-de-la-seguridad-laboral

Córdoba, A. (15 de Julio de 2008). *Centro de recursos*. Recuperado el 3 de Abril de 2019, de El plan de continuidad de negocios debe ser una prioridad: http://www.itcio.es/planes-contingencia/analisis/1004786016902/plan-continuidad-negocio-debe-prioridad.1.html

Cutili, J. A. (Abril de 2009). *Seguridad Total: las 4 Modalidades de la Seguridad para la Prevención de Riesgos del Trabajo*. Obtenido de Instituto Argentino: http://www.seguridad-laboral.es/instituciones/asociaciones-y-fundaciones/seguridad-total-las-4-modalidades-de-la-seguridad-para-la-prevencion-de-riesgos-del-trabajo

Dueñas, A. (27 de Julio de 2014). *Cálculo del alfa de Cronbach*. Obtenido de https://asesoriatesis1960.blogspot.com/2014/07/coeficiente-alfa-de-cronbach.html

Duménigo, D. (2012). Sistema de información, aplicación en empresas. *1*(1), 8-16.

ejecutiva, F. (Octubr de 2013). *http://www.espol.edu.ec/sites/default/files/espol/LEY-ORGANICA-DE-EFICIENCIA-DE-LA-CONTRATACION-PUBLICA.pdf*.

Erazo, C. (Agosto de 2012). *Plan de continuidad de negocio.* Recuperado el 14 de Marzo de 2019, de http://siguex.blogspot.com/2012/08/plan-de-continuidad-del-negocio-pcn.html

Espinoza, D., Martinéz, J., & Amador, S. (Julio de 2014). Gestión del riesgo en la seguridad de la información con base en la norma ISO/ IEC 27005. 2011, proponiendo una adeptación de metodología OCTAVE-S. Caso de estudio proceso de inscripciones y adminisiones en la división de la admisión registro y control. *2*(5). Obtenido de http://web.usbmed.edu.co/usbmed/fing/v5n2/pdf/Articulo_Gestion_Riesgo_Seguridad_Informacion

Estancio, J. (2016). *Los riesgos tecnológicos en el DMQ: la paradoja del desarrollo urbano y el síndrome de nuevos escenarios de riesgos y desastres*. Recuperado el 14 de Marzo de 2019, de https://flacsoandes.edu.ec/sites/default/files/agora/files/1218664438.ponencia_final_de_jairo_estacio_2.pdf

Gaspar Martinez, J. (22 de 08 de 2006). Recuperado el 12 de 3 de 2019, de http://www.editdiazdesantos.com/wwwdat/pdf/9788479787783.pdf

Guachi, T. (Julio de 2012). *Norma de seguridad informática ISO 27001 para mejorar la conficialidad, integridad y disponibilidad de los sistemas de información y comunicación en el departamento de sistemas de la Cooperativa de Ahorro y Crédito San Francisco LTDA.*

Guerra, R. (2013). *Para calificar la probabilidad de ocurrencia y el nivel de impacto se utilizó la tabla 6-17 y 6-18 que poseen valores de 1 a 5 permitiendo evaluar cuantitativamente y los colores en forma cualitativamente los procesos de la institución. .* Bogota: Universidad Libre .

Guirado, R. (Octubre de 2015). *Gestión de riesgos y continuidad operativa en IT: Recomendaciones prátcias.* Recuperado el 14 de Marzo de 2019, de http://m.isaca.org/chapters8/Montevideo/cigras/Documents/CIGRAS2015/CIGRAS-2015.09.09-09-Gestion%20de%20Riesgos%20y%20Continuidad%20Operativa%20de%20IT%20Recomendaciones%20Practicas-Rodrigo%20Guirado.pdf

Gutierrez, Y., & Ortiz, A. (Agosto de 2018). Diseño de un Modelo de Gestión de Riesgos basado en ISO 31.000:2012 para los Procesos de Docencia de Pregrado en una Universidad Chilena. *Scielo, 11*(4). doi:doi.org/10.4067/S0718-50062018000400015

Herrera, M. &. (2010). *http://biblioteca.casadelacultura.gob.ec/cgi-bin/koha/opac-detail.pl?biblionumber=18937*.

Instituto Nacional de Ciberseguridad. (1 de 2 de 2017). *Pasos a seguir para realizar un análisis de impacto en nuestro negocio*. Recuperado el 11 de 3 de 2019, de https://www.incibe.es/protege-tu-empresa/blog/pasos-seguir-realizar-analisis-impacto-negocio

ISO tools. (2 de 4 de 2015). *Normas ISO.* Recuperado el 10 de 3 de 2019, de https://www.isotools.org/normas/

Jácomo, W. (2013). *Administración de continuidad de negocio en el deaprtamento TI.* Recuperado el 9 de 3 de 2019, de http://repositorio.puce.edu.ec/bitstream/handle/22000/12656/Tesis_JacomeWilsonMGTI.pdf?sequence=1&isAllowed=y

Juarez, S. (10 de 9 de 2015). *Plan de continuidad informática.* Recuperado el 9 de 3 de 2019, de http://normasiso2700.blogspot.com/2015/09/plan-de-continuidad-del-negocio.html

Lab, K., & Raiu, C. (12 de 05 de 2017). *Un ciberataque afecta a compañías e instituciones estatales alrededor del mundo*. Obtenido de https://www.eltelegrafo.com.ec/noticias/94/30/varias-companias-espanolas-victimas-de-un-ciberataque

Ladine, K. (28 de Agosto de 2017). *Plan informático de contingencia para la seguridad de la información del departamento de TIC de la PUCESE.*

Leiva, A. (2008). *Desarrollo del plan de continuidad del negocio para el departamento de la TI en una empresa farmacéutica.* Escuela Politécnica Nacional, Facultad de Ingeniería en Sistemas, Quito. Recuperado el 25 de Febrero de 2019

LEXISFINDER. (18 de Enero de 2018). *Estatuto orgánico de gestión organicional por procesos del Sercop*. Obtenido de https://portal.compraspublicas.gob.ec/sercop/wp-content/uploads/2018/01/ESTATUTO-ORGANICO-DE-GESTION-ORGANIZACIONAL-POR-PROCESOS-DEL-SERCOP.pdf

Macua, R. (Septiembre de 2004). Funciones de las tecnologías de la información y las comunicaciones de las organizaciones. *Universidad y Sociedad del Conocimiento, 1*(1), 12- 24. Recuperado el 310 de 2019, de https://www.raco.cat/index.php/Rusc/article/viewFile/28809/28643

Mendivelso, F., & Rodríguez, M. (2018). Prueba chi cuadrado de independencia aplicada a tablas 2xn. *Medica.Sanitas, 21*(2), 92- 95. Recuperado el 3 de Marzo de 2019

Mendoza, M. (6 de 11 de 2014). *El Business Impact Analysis permite a empresas estimar el impacto operacional y financiero de interrupciones. Revisaremos sus características y desarrollo.* Recuperado el 11 de 3 de 2019, de https://www.welivesecurity.com/la-es/2014/11/06/business-impact-analysis-bia/

MINTIC. (Noviembre de 2015). *Guía para la preparación de un plan de continuidad del negocio.* Recuperado el 14 de Marzo de 2019, de https://www.mintic.gov.co/gestionti/615/articles-5482_G10_Continuidad_Negocio.pdf

Molina, A. (3 de 6 de 2016). *Los cinco principios de COBIT 5.* Recuperado el 11 de 3 de 2019, de https://www.esan.edu.pe/apuntes-empresariales/2016/06/los-cinco-principios-de-cobit-5/

Morales, L. R. (Enero de 2019). *Repositorio Universidad Técnica de Ambato.* Recuperado el 12 de 3 de 2019, de http://repositorio.uta.edu.ec/handle/123456789/29216

Muncaster, P. (25 de Julio de 2017). *¿Porque se caen las redes? y como evitarlos*. Recuperado el 8 de Mayo de 2019, de http://www.think-progress.com/es/eficiencia-en-el-lugar-de-trabajo/por-que-se-caen-las-redes-y-como-evitarlo/

Narvaes, L., & Mendez, K. (Octubre de 2012). *Plan de Contingencia Para la Unidad de Sistemas y Tecnología de Información del Gobierno Autónomo Descentralizado Antonio Ante en Base a la Norma Iso/Iec 27002.*

Normas ISO. (7 de 4 de 2017). *Asesoría y formación en sistemas de gestión.* Recuperado el 10 de 3 de 2019, de https://www.normas-iso.com/

Ortega, J. (24 de 01 de 2015). *Cibermafias atacaron a 17 empresas ecuatorianas*. Obtenido de https://www.elcomercio.com/actualidad/cibermafias-ciberataque-17empresas-ecuador-seguridadinformatica.html

Ortiz, S. (16 de Abril de 2019). *Hackers lanzaron ofensiv global para atacar web estatales*. Obtenido de https://www.elcomercio.com/actualidad/hackers-ofensiva-global-ataque-ecuador.html

Palacios, A., & Quiroz, J. (23 de Septiembre de 2013). *Plan de contigencias de los equipos y sistemas informáticos del gobierno autónomo decentralizado del Municipio del Cantón Junín.* Recuperado el 7 de Marzo de 2019

Palacios, E. (30 de Abril de 2019). *Chi cuadrado*. Recuperado el 22 de Mayo de 2019, de https://vefuentespalacios.wordpress.com/2014/06/01/tarea-del-seminario-numero-9-la-chi-cuadrado/

Patiño, S. (2017). *Plan informático de contigencia para la seguridad de la información del departamento de TIC de la PUCESE*. Recuperado el 27 de 02 de 2019, de https://repositorio.pucese.edu.ec/bitstream/123456789/1010/1/LADINES%20GARC%C3%89S%20KATHERINE%20STEFANIA.pdf

Patiño, S. (12 de Abril de 2019). Obtenido de https://www.eluniverso.com/noticias/2019/04/12/nota/7281890/exjefe-inteligencia-militar-recomienda-gobierno-fusion-sus-sistemas

Paz, J. (11 de 7 de 2014). *Sistemas de información y comunicación*. Recuperado el 10 de 3 de 2019, de http://controlinternopublico.blogspot.com/2009/05/sistemas-de-informacion-y-comunicacion.html

Pérez, J. (28 de Noviembre de 2016). *Estructura organizacional*. Recuperado el 14 de Febrero de 2019, de SINNAPS: https://www.sinnaps.com/blog-gestion-proyectos/estructura-organizacional

Pizzagalli. (17 de 6 de 2016). *Beneficios de un plan de continuidad de negocios.* Recuperado el 9 de 3 de 2019, de http://pizzagalli.cl/prensa/beneficios-de-un-plan-de-continuidad-de-negocio/

Puente, D. (2014). *Diseño de un plan de recuperación de desastre que garantice de continuidad de operaciones de medicamenta ecuatoriana S.A.* Recuperado el 13 de Mayo de 2019, de http://dspace.udla.edu.ec/bitstream/33000/1557/1/UDLA-EC-TMGSTI-2014-01.pdf

Puricica, C. A. (03 de 05 de 2018). *veeam*. Obtenido de https://www.veeam.com/blog/es-lat/rto-rpo-definitions-values-common-practice.html

Ramirez, & Ortiz. (14 de Agosto de 2011). *Nivel de Riesgo*. Recuperado el 10 de Mayo de 2019

Ramírez, A., & Ortiz, Z. (2011). Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios. *Ingeniería, 16*(2), 56- 66. Obtenido de https://dialnet.unirioja.es/descarga/articulo/4797252.pdf

Ramiro, R. (28 de Julio de 2018). *Cyberseguridad*. Recuperado el 14 de Febrero de 2019, de Comparación de algunos estandares de continuidad de negocios: https://ciberseguridad.blog/comparacion-de-algunos-estandares-de-continuidad-de-negocio/

Robles, J. (10 de 4 de 2018). *Cinco indicadores para una efectiva gestión de los departamentos de TICS e informática*. Recuperado el 12 de 3 de 2019, de http://www.itmadrid.com/5-indicadores-o-kpi-clave-para-una-efectiva-gestion-de-los-departamentos-tic-o-informatica/

Rodriguez, C. (23 de Agosto de 2018). *Seguridad en América*. Recuperado el 10 de Enero de 2019, de Importancia de un plan de continuidad: https://www.seguridadenamerica.com.mx/noticias/articulos/16851/la-importancia-del-plan-de-continuidad-del-negocio

Rodríguez, J., & Daureo, M. (Febrero de 2013). *Sistemas de información: Aspectos técnicos y legales.* Recuperado el 10 de 3 de 2019, de https://w3.ual.es/~jmrodri/sistemasdeinformacion.pdf

Rojas, J. (2017). *Propuesta de un plan de continuidad de negocio para institución financiera del sector privado bancario del Ecuador.* Recuperado el 9 de 3 de 2019, de http://dspace.udla.edu.ec/bitstream/33000/7531/1/UDLA-EC-TMGSTI-2017-08.pdf

Sánchez, E. (23 de 11 de 2009). *Calidad y seguridad informática.* Recuperado el 9 de 3 de 2019, de https://e-archivo.uc3m.es/bitstream/handle/10016/8510/proyectoEsmeralda.pdf

Sánchez, M. (2013). *Peores escenarios de riesgos tecnológicos en el comercio: guía para el comité de dirección.* Recuperado el 9 de 3 de 2019, de https://ssa-asesores.es/html/wordpress/

SERCOP. (31 de Octubre de 2013). *Incidente Portal de Compras Públicas 31/10/2013*. Recuperado el 14 de Marzo de 2019, de https://portal.compraspublicas.gob.ec/sercop/comunicado-incidente-portal-de-compras-publicas-31102013/

SERCOP. (2018). *Servicio de Contratación Pública* . Recuperado el 14 de Enero de 2019, de Valores: https://portal.compraspublicas.gob.ec/sercop/valores/

SERCOP. (Enero de 2019). *Servicio de Contratación Pública*. Recuperado el 5 de Marzo de 2019, de La institución: https://portal.compraspublicas.gob.ec/sercop/la-institucion/

SGSI. (5 de 1 de 2017). *Sistema de gestión de seguridad informática*. Recuperado el 11 de 3 de 2019, de https://www.pmg-ssi.com/2017/01/iso-27005-como-identificar-los-riesgos/

Simplifica DC . (Mayo de 2009). *Continuidad de negocios*. Obtenido de https://www.simplificadc.com/Brochure_SimplificaDC.pdf

Simplifica DC. (Mayo de 2009). *Continuidad de negocios*. Obtenido de https://www.simplificadc.com/Brochure_SimplificaDC.pdf

Slideshare. (2018). Obtenido de https://es.slideshare.net/mangones/gerencia-de-sistemas-52508917

Solis, A. (Enero de 1997). *Desastres y emergencias tecnológicas*. Recuperado el 14 de Marzo de 2019, de http://helid.digicollection.org/en/d/Jcne05/1.1.html#Jcne05.1.1

Solozarno, W. (11 de 11 de 2018). *La gestión de TI es un aspecto fundamental para empresas de todos los tamaños.* Recuperado el 12 de 3 de 2019, de https://blogmexico.comstor.com/cuales-son-las-metricas-esenciales-para-el-departamento-de-ti

Sosa, N. (6 de Junio de 2018). *Cálculo de matriz de riesgos*. Recuperado el 22 de Mayo de 2019, de https://www.soltia.com.mx/blog/noticias-1/post/calculo-de-la-matriz-de-riesgos-39

Sotres, P. (9 de 2012). *ISO 23001- Continuidad del negocio.* Recuperado el 11 de 3 de 2019, de https://www.interempresas.net/FeriaVirtual/Catalogos_y_documentos/87942/Continuidad_Negocio-ISO-22301.pdf

SPG. (4 de 2 de 2018). *Que es ISO.* Recuperado el 10 de 3 de 2019, de https://www.certificadoiso9001.com/que-es-iso/

Torres, C. (2013). *Plan de continuidad de negocios.* México. Recuperado el 12 de Febrero de 2013

Torres, C., & Torres, M. (2018). *Plan de continuidad y plan de contigencia una forma de salvar tu negocio*. Obtenido de Ciberseguridad: https://www.scprogress.com/NOTICIAS/CyberNoticia46-20170727.pdf

Torres, C., & Torres, M. (2018). *Plan de continuidad y plan de contingencia una forma de salvar tu negocio*. Obtenido de Ciberseguridad: https://www.scprogress.com/NOTICIAS/CyberNoticia46-20170727.pdf

Torres, M. (4 de Junio de 2019). *Se activó el protocolo de seguridad para prevenir ataques informáticos*. Obtenido de https://www.pichinchauniversal.com.ec/se-activo-el-protocolo-de-seguridad-para-prevenir-ataques-informaticos/

TRIARA. (3 de Diciembre de 2018). *Sitio Alterno para la Continuidad de un Negocio*. Recuperado el 13 de Mayo de 2019, de http://triara.com/sitio-alterno-para-continuidad-de-negocio

Ulloa, G. (14 de 6 de 2009). *Redes informáticas*. Recuperado el 11 de 3 de 2019, de http://ticsredesinformaticas.blogspot.com/2009/07/estructura-de-las-redes-las-redes.html

Valdas, C. (6 de 7 de 2015). *Importancia del control en la retroalimentación del ciclo administrativo.* Recuperado el 9 de 3 de 2019, de https://www.grandespymes.com.ar/2012/09/19/importancia-del-control-en-la-retroalimentacion-del-ciclo-administrativo/

Vallejo, S. (30 de 10 de 2015). *Ataque informatico a SERCOP*. Obtenido de http://www.teleamazonas.com/2015/09/denuncian-ataque-informatico-a-sercop/

Vanguardia. (2018). Obtenido de https://www.vanguardia.com/tecnologia/el-nuevo-papel-del-gerente-de-ti-en-la-transformacion-digital-de-las-empresas-IFVL378246

Vásquez, S. (30 de Septiembre de 2018). *Sercop denuncia vulneración del Sistema Nacional de Conratación Pública*. Obtenido de https://www.eltelegrafo.com.ec/noticias/informacion/1/sercop-denuncia-vulneracion-del-sistema-nacional-de-contratacion-publica

Vigo, G. M. (Febrero de 2011). *Softeam*. Recuperado el 7 de Marzo de 2019, de http://www.softeam1.com.ar/utn/Documentos%20Seguridad/plan_de_contingencia.pdf

Vigo, M., Cardoso, C., & Mello, W. (3 de 2010). *Plan de contigencia y continuidad de negocio.* Recuperado el 9 de 3 de 2019, de https://www.colibri.udelar.edu.uy/jspui/bitstream/123456789/217/1/M-CD4039.pdf

6.16 Anexos

ANEXO 1 ENCUESTA APLICADA

Encuesta aplicada al personal de Coordinación de Innovación Tecnológica del Servicio Nacional de Contratación Pública

MAESTRÍA EN GERENCIA DE SISTEMAS DE INFORMACIÓN

ESTUDIO DE INVESTIGACIÓN

ENCUESTA APLICADA AL PERSONAL DE COORDINACIÓN DE INNOVACIÓN TECNOLÓGICA DEL SERVICIO NACIONAL DE CONTRATACIÓN PÚBLICA

Instrucciones: Marque con una X la alternativa que considere más adecuada.

1. ¿Al no contar con un plan de continuidad de negocios afecta negativamente la Coordinación de Innovación y Tecnológica?
Si_____ No_____

2. ¿Existen políticas para la gestión de continuidad de negocios?

Si_____ No_____

3. ¿Existe estrategias de recuperación de los servicios críticos frente a una caída de los sistemas de información y comunicación?
Si_____ No_____

4. ¿Se realiza simulacros frente a una caída de los sistemas de información y comunicación?

Si_____ No_____

5. ¿Se realiza tareas de monitoreo a los sistemas de información y comunicación?

Si_____ No_____

6. ¿Se realiza el control de los procesos críticos de los sistemas de información y comunicación?
Si_____ No_____

7. ¿Un plan de continuidad de negocio mejorará la disponibilidad de los sistemas de información de la entidad?
Si_____ No_____