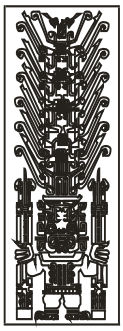


UNIVERSIDAD NACIONAL
FEDERICO VILLARREAL

Vicerrectorado de INVESTIGACIÓN

ESCUELA UNIVERSITARIA DE POSGRADO

"PROPUESTA DE UN MODELO DE CONTINUIDAD DE NEGOCIO Y BUENAS PRÁCTICAS PARA OPTIMIZAR LOS PROCESOS FORMATIVOS DE LAS UNIDADES ACADÉMICAS DE PREGRADO DE LAS ESCUELAS TÉCNICAS DE LA POLICÍA NACIONAL DEL PERÚ."

TESIS PARA OPTAR EL GRADO ACADÉMICO DE:
MAESTRO EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN GESTIÓN DE TECNOLOGIAS DE LA INFORMACIÓN

AUTOR:
DÍAZ CARRILLO, JIMMY TONY

ASESOR:
DR. MAYHUASCA GUERRA, JORGE VICTOR

JURADO:
DR. SOTO SOTO, LUIS
MG. GAMARRA MORENO, JUAN
MG. CARRILLO BALCEDA, JESÚS ELÍAS

LIMA – PERÚ
2019

DEDICATORIA

La presente Investigación está dedicada por el amor, admiración, respeto y agradecimiento que tengo, a mis Padres Doña Carmen Enriqueta Ortiz de Carrillo y Arturo Carrillo Contreras quienes con su dedicación, entrega y compromiso han hecho posible mi crecimiento y desarrollo Profesional.

INDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

TÍTULO DE LA TÉSIS:

“Propuesta de un modelo de Continuidad de Negocio y Buenas Prácticas para optimizar los procesos formativos de las Unidades Académicas de Pregrado de las Escuelas Técnicas de la Policía Nacional del Perú.”

AUTOR

La presente investigación es realizada por el Ingeniero de Sistemas Jimmy Tony Diaz Carrillo.

LUGAR DONDE SE DESARROLLO LA TESIS.

La Investigación se realizará en la Unidad Académica de la Escuela Técnica de la Policía Nacional del Perú “Capitán PNP Alipio Ponce Vásquez”, Ubicada en el Distrito de Puente Piedra, Provincia Lima, Departamento de Lima, Perú.

RESUMEN

Esta investigación propone obtener un "Modelo de Continuidad" basado en Estándares Internacionales dentro del marco de las "Tecnologías de la Información" con la intención de detallar un plan de respuesta y recuperación inmediata ante cualquier siniestro que pueda interrumpir los servicios Tecnológicos que brinda la Unidad Académica de Pregrado de la Institución Educativa Policial.

El estudio contiene seis capítulos. En el primero se define los antecedentes de estudio, el problema, Justificación e Importancia de la misma y se ha determino como objetivo principal el *"Optimizar los Procesos formativos de las Unidades Académicas de Pregrado de las Escuelas Técnicas de la Policía Nacional del Perú mediante la propuesta de un modelo de continuidad del negocio y buenas prácticas*".

En el ***segundo capítulo***, se precisa las teorías generales y relacionadas con el tema que facilite una teoría sólida que admita enaltecer los razonamientos para la obtención de la solución propuesta. Se define como hipótesis *"La Propuesta de un Modelo de Continuidad de negocio y Buenas Prácticas, optimiza los procesos formativos de las Unidades Académicas de Pregrado de las Escuelas Técnicas de la Policía Nacional del Perú."* la cual será validada o no durante el desarrollo de la investigación.

El ***capítulo tercero*** se desarrolla "la metodología y diseño de investigación" donde planteó un tipo de investigación aplicada orientada a problemas presentes suscitados en la institución en estudio, de nivel descriptivo utilizando un método Deductivo – Inductivo y debido a que los datos a utilizar son datos actuales se ha definido que será un diseño transversal. Además se trabajó con una población conformada por 22

personas pertenecientes a la Escuela Técnica de Policía “Capitán PNP Alipio Ponce Vásquez”, determinando por la cantidad de su población que será una muestra censal motivo por el cual se utiliza la herramienta probabilística de “T de Student” para realizar la prueba de la hipótesis.

En el ***cuarto capítulo*** describe “el resultado, su paráfrasis y procesamiento de la información, se resume la justificación de la hipótesis a través de los resultados alcanzados en función de los indicadores”.

El ***quinto capítulo*** denominado **“**desarrollo de la Propuesta” donde se plasma “la propuesta de solución, identificando y comprendiente la necesidad que la Escuela de Policía requiere para la continuidad de negocio de los procesos académicos”.

El ***sexto capítulo*** precisa la Discusión de la investigación, donde se registra de manera sintética y precisa: “las conclusiones y sugerencias, a su vez se plantea tácticas concretas en concordancia a la propuesta tecnológica del estudio realizado”.

En resumen el estudio va dirigido a las Institutos de Educación Superior Técnicas Profesionales de la Policía y Escuelas Militares a nivel nacional quienes podrán contar con un modelo de continuidad ágil y práctico, integrando normativas legales y técnicas adaptadas a sus necesidades, que les permita desarrollarse en un marco de competitividad organizacional, lo cual permitirá alcanzar uno de los objetivos fundamentales que es: “brindar una óptima preparación Policial”.

Palabras Clave: Modelo de Continuidad, Buenas Prácticas, Procesos Formativos.

ABSTRACT

This research proposes to obtain a "Business Continuity Model" based on International Standards within the framework of "Information Technologies" with the purpose of detailing an immediate response and recovery plan in case of any accident that could interrupt the technological services provided the Undergraduate Academic Unit of the Police Educational Institution

The study contains six chapters. The first one defines the background of the study, the problem, Justification and Importance of the same and the main objective has been the "Optimizing the formative processes of the Undergraduate Academic Units of the Technical Schools of the National Police of Peru through the proposal of a model of business continuity and good practices ".

In the second chapter, the general and related theories are specified to facilitate a solid theory that admits the reasoning to obtain the proposed solution. It is defined as a hypothesis "The Proposal for a Business Continuity Model and Good Practices, optimizes the training processes of the Undergraduate Academic Units of the Technical Schools of the National Police of Peru" which will be validated or not during the development of the investigation.

The third chapter develops "the methodology and design of research" where he proposed a type of applied research oriented to present problems raised in the institution under study, of descriptive level using a Deductive - Inductive method and because the data to be used are data current has been defined as a cross-

sectional design. Also worked with a population consisting of 22 people belonging to the Technical School of Police "Captain PNP Alipio Ponce Vásquez", determining by the amount of its population that will be a census sample reason why the probabilistic tool of "T of Student "to perform the hypothesis test.

In the fourth chapter describes "the result, its interpretation and processing of information, the justification of the hypothesis is summarized through the results achieved according to the indicators".

The fifth chapter called "development of the Proposal" where "the solution proposal is defined, identifying and understanding the need that the Police School requires for the business continuity of the academic processes".

The sixth chapter requires the Discussion of the investigation, where it is recorded in a synthetic and precise manner: "the conclusions and suggestions, in turn, raises specific tactics in accordance with the technological proposal of the study carried out".

In summary, the study is aimed at the Institutes of Higher Education Professional Techniques of the Police and Military Schools nationwide who can count on an agile and practical continuity model, integrating legal regulations and techniques adapted to their needs, allowing them to develop in a framework of organizational competitiveness, which will allow achieving one of the fundamental objectives that is: "to provide an optimal police preparation".

Keywords: Model of Continuity, Good Practices, Training Processes.

INTRODUCCIÓN

El presente proyecto se realizó con el fin de adquirir información actualizada, veraz y confiable. El resultado que se espera obtener de esta Investigación es un Marco de Trabajo que permita optimizar los procesos académicos que se realizan en la Escuela de Policía.

La ejecución de esta investigación busca una medida orientada a la agilización y mejoramiento de los procesos que están inmersos en la formación Policial de los Alumnos que se encuentran en la etapa de preparación.

El servicio que presta el obtener un Modelo de Continuidad no solamente es de asegurar el almacenamiento de información y generar reportes inmediatos, éstos pueden preservar la continuidad de los procesos formativos que se realizan en la Institución; en este estudio se busca implementar esta ventaja que puede ofrecer esta propuesta, que a través de su implementación brindará las herramientas para enfrentar siniestros y así asegurar que los objetivos trazados por la institución respecto a la calidad de la formación se cumplan. Todo gracias a los aportes adquiridos con la implementación del estudio.

Esta investigación busca obtener un estándar práctico de continuidad de negocio congruente a los requerimientos de la Institución Policial que le permita optimizar su operatividad y efectividad bajo cualquier circunstancia optimizando los procesos formativos que están inmersos en la formación Policial de los Alumnos internados.

CAPITULO I. PLANTEAMIENTO DEL PROBLEMA.

1.1 DESCRIPCIÓN DEL PROBLEMA

Perú cuenta con una población estimada en 30 millones de personas, según datos del INEI (Instituto Nacional de Estadística e Informática)[1], es reconocido como un país altamente turístico y de grandes oportunidades para los negocios; debido a estos factores el Perú, ha tenido a través de los años un crecimiento en su economía, es por ello que capitalistas nacionales y extranjeros han visto conveniente realizar grandes inversiones en diferentes localidades de nuestro territorio nacional, lo cual se ve reflejado en grandes centros comerciales como "Real Plaza", "Saga Falabella", "Totus", "Maestro Home Center", Centros Particulares de Estudio, Cadena de Hoteles, Crecimiento del Parque Automotor, entre otros; todo esto ha generado que tengamos una economía creciente y favorable.

Paralelamente con el crecer económico, se ha ido incrementando anualmente el accionar delincuencial, llegando en los últimos años a cifras alarmantes (Tabla 01 y 02), esto según información policial respecto a la cifra de denuncias reconocidas en las dependencias Policiales a nivel nacional; es por ello que en la actualidad los principales problemas sociales del país percibidos por la población son la delincuencia y la falta de seguridad ciudadana[2], por tal motivo la ciudadanía reclama un mayor compromiso por parte de las instituciones encargadas de salvaguardar la seguridad y tranquilidad de la población, es así que esta

[1] INEI, Informe OCT2016, consultado el 01oct2017 en htpps:www.inei.gob.pe
[2] INEI, encuesta Nacional del hogares, consultado el 01oct2017 en htpps:www.inei.gob.pe

responsabilidad según el Artículo 166° de la constitución Política del Perú recae directamente en los miembros de la Policía Nacional del Perú, quienes para cumplir esta misión se forman y capacitan profesionalmente en las Escuelas de Policía.

TABLA 01: "DENUNCIAS POR COMISIÓN DE DELITOS".

Delito Genérico	2012	2013	2014	2015	2016
Total	271,813	299,474	326,578	349,323	362,210
Delitos contra la vida, el cuerpo y la salud	39,744	33,613	36,643	37,057	38,006
Delitos contra la familia	3,684	4,755	3,354	2,013	2,560
Delitos contra la libertad	17,848	18,459	19,379	18,730	18,947
Delitos contra el Patrimonio	185,357	204,935	224,753	242,697	251,683
Delitos contra la seguridad pública	14,839	28,175	30,388	40,150	41,212
Delitos contra la administración pública	2,071	2,970	3,307	3,966	4,106
Delitos contra la fe pública	3,329	3,361	2,680	1,794	1,698
Otros delitos	4,941	3,206	6,074	2,916	3,998

Fuente: (INSTITUTO NACIONAL DE ESTADISTICA E INFORMÁTICA, 2016)

TABLA 02: "DENUNCIAS POR COMISIÓN DE DELITOS, SEGÚN DEPARTAMENTO".

Departamento	2012	2013	2014	2015	2016
Total	271,813	299,474	326,578	349,323	352,102
Amazonas	4,037	4,806	3,178	2,395	3,110
Ancash	7,097	7,618	8,783	9,862	8,553
Apurímac	2,412	2,993	2,533	1,601	2,533
Arequipa	13,556	14,167	16,576	18017	17,576
Ayacucho	3,625	3,989	4,786	4,395	4,986
Cajamarca	5,223	6,820	6,100	5,847	6,120
Prov. Const. del Callao	13,233	14,631	15,765	19,328	19,631
Cusco	8,542	9,830	14,328	9,271	9,830
Huancavelica	962	1,045	1,917	1,223	979
Huánuco	2,601	3,157	3,275	3,126	1,931

Ica	7,835	9,288	10,107	10,869	11,308
Junín	8,337	9,433	8,791	7,632	7,123
La libertad	13,413	13,504	18,712	15,628	9,221
Lambayeque	11,356	12,260	13,740	15,757	10,300
Lima	135,777	147,119	151,256	180,409	196,494
Loreto	2,825	3,240	3,054	2,670	2,825
Madre de Dios	1,549	2,256	2,118	1427	1,549
Moquegua	1,568	1,791	1,804	1,713	1,568
Pasco	1,183	1,314	1,987	1,054	1,183
Piura	11,511	12,178	16,200	16,099	16,911
Puno	2,099	2,445	4,114	3,314	2,099
San Martin	4,730	4,665	5,597	5,545	4,930
Tacna	3,391	3,850	3,892	2,975	3,391
Tumbes	2,935	3,437	3,883	3,163	2,935
Ucayali	2,016	3,638	4,082	6,003	5,016

Fuente: (INSTITUTO NACIONAL DE ESTADISTICA E INFORMÁTICA, 2016)

Actualmente la Policía Nacional cuenta con 25 Escuelas de Formación Técnica Policial distribuidas a nivel nacional, donde según cifras de la Dirección de Educación y Doctrina Policial[3] existen actualmente un promedio de 10000 alumnos internados en los diferentes centros de formación Policial, siendo la Escuela de Policía "Alférez PNP. Alipio Ponce Vásquez" de la ciudad de Lima la que alberga el mayor número con un promedio de 3000 Alumnos, quienes reciben una formación Técnico Profesional enmarcado en un diseño educativo Policial de internado durante una etapa de tres años, sobre la base de criterios académicos vinculados a un perfil que permita responder a la demanda, con contenidos y evidencias de desempeño que garanticen un eficiente accionar en la función Policial del egresado.

Cabe mencionar que cada centro de formación Policial es un órgano ejecutivo, encargado de "organizar, impartir, evaluar y certificar la formación técnica de los

[3] Dirección de Educación y Doctrina PNP: Órgano Policial encargado de la formación, capacitación y perfeccionamiento del potencial humano.

estudiantes y miembros de la Policía Nacional del Perú[4]" dentro de su estructura funcional cuenta con una unidad académica de pregrado la cual está encargada de programar, coordinar, controlar, supervisar y evaluar las actividades académicas, así como la gestión de los grados académicos y títulos profesionales; de mantener el registro y matrícula de los estudiantes, la gestión de los servicios bibliotecarios y recopilar, centralizar y analizar la información estadística sobre sus actividad académica para su publicación en el portal institucional y para toma de decisiones por parte del comando Policial; pero actualmente esta unidad académica de pregrado cuentan con la siguiente problemática:

- No ha documentado e identificado sus vulnerabilidades y esto se ha visto evidenciado cuando ha tenido problemas en el funcionamiento de sus sistemas informáticos ocasionados tanto por factores humanos como por factores tecnológicos no ha sabido establecer claramente las medidas preventivas y correctivas más viables para certificar la seguridad de su data y así mismo la continuidad de sus procesos.

- Personal Policial que labora en dicha unidad no cuentan con la capacitación para el sostenimiento de los sistemas informáticos que son utilizados, así mismo no se tiene identificados las funciones críticas de sus procesos formativos.

- Carece de un plan de respuesta y recuperación que le permita realizar con normalidad sus Procesos formativos, ya que actualmente soporta constantes interrupciones en el acceso a los sistemas informáticos institucionales; sobre

[4] Los centros de formación policial, son órganos ejecutivos, tienen limitada autonomía en cuanto a la administración de recursos, dependen decisional mente de la ENFPP.

todo en las en las escuelas de provincias donde se han tenido paralizado sus procesos por espacios muy prolongados de tiempo, generando con ello que el Director de la institución y a su vez el comando de la Policía Nacional no pueda saber de manera real respecto a la formación Policial que reciben los Alumnos debido a la dilación en la entrega de los reportes.

Es así que debido a las constantes interrupciones en el funcionamiento de los sistemas, no contar con un plan de respuesta y recuperación y sumado a ello la falta de capacitación y deficiencia en las labores propias del personal policial encargado, el comando Institucional no pueden acceder a una buena calidad de información, generando que en muchos casos se dictan órdenes locales o nacionales fuera del contexto real o con datos inexactos, todo ello se ve expresado en el trabajo profesional de sus miembros, ya que según las estadísticas de la "Inspectoría General de la PNP"[5] a setiembre del 2017, el 65% de los Efectivos Policiales de reciente egreso en su primer año de servicio policial registran un alto índice de sanciones administrativas disciplinarias debido a su accionar policial y desconocimiento de los procedimientos actuales en materia de intervención enmarcados dentro de la normatividad vigente, también se debe acotar que la Inspectoría General de la PNP recibe constantes quejas y denuncias por parte de los ciudadanos quienes indican que fueron tratados inadecuadamente por personal policial ; todo esto conlleva a que la ciudadanía tenga una percepción negativa del accionar policial en su conjunto, y a su vez un serio cuestionamiento sobre la formación Profesional Policial que reciben durante su periodo de internamiento y capacitación.

[5] Inspectoría General PNP: Órgano Policial encargado de fortalecer y salvaguardar los bienes jurídicos (Disciplina, Imagen Institucional, Servicio Policial y la Ética Policial) de la Policía.

En síntesis este estudio tiene como finalidad la de brindar un modelo de continuidad de negocio y buenas prácticas para la Unidad Académica de Pregrado de las Escuela Técnica de Policía, a través de la identificación y análisis de las posibles amenazas y funciones críticas de los servicios de TI. Actualmente ninguna Escuela de Educación Superior Policial y/o Militar cuenta con un Plan de Continuidad para su Unidad Académica. Esto sin duda alguna permitirá optimizar la formación de los Alumnos Policías y así poder hacer frente de manera más eficiente a la problemática social que actualmente vive nuestro país con la delincuencia e inseguridad ciudadana.

1.2 FORMULACIÓN DEL PROBLEMA.

- **PROBLEMA GENERAL.**

¿En qué medida la carencia de un modelo de continuidad de negocio y Buenas Prácticas genera una deficiencia en los procesos formativos de las Unidades Académicas de Pregrado de las Escuelas Técnicas de Policía?

- **PROBLEMAS ESPECÍFICOS.**

¿Cómo la identificación y análisis de las posibles amenazas optimizará los Procesos formativos de las Unidades Académicas de las Escuelas Técnicas de Policía. ?

¿Cómo la identificación y análisis de las funciones críticas y servicios de TI optimizará los Procesos formativos de las Unidades Académicas de las Escuelas Técnicas de Policía. ?

¿Cómo el proponer un plan de respuesta y recuperación para las funciones críticas optimizará los Procesos formativos de las Unidades Académicas de las Escuelas Técnicas de Policía. ?

1.3 JUTIFICACIÓN E IMPORTANCIA DE LA INVESTIGACIÓN

1.3.1 JUSTIFICACIÓN.

- **INSTITUCIONAL.**

  La propuesta de este modelo práctico y personalizado ha permitido proporcionar un marco de trabajo apropiado para dar una respuesta práctica y un servicio de calidad, permitiendo así proteger los intereses, imagen y valor de los procesos críticos y operativos realizados por la unidad Académica de Pregrado dentro de un tiempo predeterminado después de una interrupción o siniestro manteniendo así el prestigio y credibilidad de la institución Policial, a su vez ser el primer centro de formación Policial del País en contar con este modelo de continuidad y buenas prácticas.

  Esto conllevará a que la ciudadanía en su conjunto tenga una percepción positiva sobre la labor desempeñada por los efectivos Policiales graduados.

- **TECNOLÓGICA.**

  Este proyecto de investigación ha sido desarrollado bajo los estándares internacionales que brindan las normas internacionales.

  Así mismo al implementar un marco de trabajo de buenas prácticas para los servicios académicos ha permitido tener una mayor integración con la institución Policial al proporcionarle seguridad, precisión, velocidad y disponibilidad de los servicios que administra.

  El resultado de la interacción de éste marco de trabajo de continuidad y buenas prácticas dará como resultado un modelo alineado y personalizado para la institución Policial.

- **INVESTIGACIÓN.**

  Debido a que este modelo ha sido desarrollado bajo estándares internacionales y alineado a una institución que no contaba con antecedentes del mismo, ha permitido tener una mayor experiencia en este tipo de estudios. Así también la presente investigación es marco de referencia para el planteamiento de estudio de otros Centros de Formación Policial y/o Militares del país.

1.3.2 IMPORTANCIA.

La Formación Profesional Policial constituye el proceso educativo que tiene como finalidad la preparación, integración, actualización, especialización y perfeccionamiento Policial en el nivel superior del

sistema educativo, y cuya finalidad pública es "certificar la idoneidad y eficacia de la Policía para el acatamiento de sus funciones, garantizando así la prestación de un servicio y un derecho fundamental para la sociedad", por lo cual el comando Policial de la Unidad Académica de Pregrado de la Escuela Técnica de Policía "Capitán PNP Alipio Ponce Vásquez" realiza constantes esfuerzos por realizar una mejora constante e integral en la formación de los Alumnos Policial para cumplir cabalmente con la finalidad antes mencionada.

La importancia de la investigación radica en que se ha pretendido conocer detalladamente cuales son las funciones críticas y posibles amenazas que tendría la Unidad Académica de la Escuela Técnica de Policía que generarían interrupción o un inadecuado funcionamiento de sus procesos académicos y si estos se optimizan al brindar una propuesta de un modelo de continuidad y buenas prácticas.

Así mismo este modelo podrá ser replicado en las 25 Escuelas de Formación Técnica Policial distribuidas a nivel nacional, de esta manera, esta investigación abrirá nuevos caminos para estudios que presenten situaciones similares a las aquí planteadas, sirviendo como marco de referencia.

1.4 LIMITACIONES DE LA INVESTIGACIÓN.

Tiene límite temporal, debido a que su realización y los resultados del estudio se limitan al año 2017 y 2018.

Existe delimitación bibliográfica en cuanto a la existencia de investigaciones realizadas en el Perú, son pocas las investigaciones que puedan ser tomadas por antecedentes sobre todo en el ámbito policial y/o militar para la presente investigación.

Existe así mismo delimitación económica por lo que se ha tenido que buscar fuentes de financiamiento que apoyen la presente investigación.

Además cuenta con delimitación operativa debido a que el acceso a la información y políticas de confidencialidad propias del área del dominio del problema, y las implicaciones reglamentarias del sector público sobre todo del ministerio del interior en lo concernientes a instalaciones Policiales en cuanto al acceso a datos e información.

1.5 OBJETIVOS.

1.5.1 OBJETIVO GENERAL.

"Optimizar los Procesos formativos de las Unidades Académicas de Pregrado de las Escuelas Técnicas de Policía mediante la propuesta de un modelo de continuidad del negocio y buenas prácticas".

1.5.2 OBJETIVOS ESPECIFICOS.

- Realizar la identificación y análisis de las posibles amenazas de los Procesos formativos de las Unidades Académicas de Pregrado de las Escuelas Técnicas de Policía.

- Realizar la identificación y análisis de las funciones críticas y servicios de TI de los Procesos formativos de las Unidades Académicas de Pregrado de las Escuelas Técnicas de Policía.

- Realizar la propuesta de un plan de respuesta y recuperación para las funciones críticas de los Procesos formativos de las Unidades Académicas de Pregrado de las Escuelas Técnicas de Policía.

CAPITULO II. MARCO TEÓRICO

2.2 ANTECEDENTES

- **Antecedentes Internacionales.**

Sarabia Zapata (2015) en su tesis de maestría titulada: "Modelo de Gestión de Continuidad de Infraestructura Tecnológica para la Operación de Servicios de TI en Empresas Financieras sobre la Base de las Normas ISO 22301 e ISO 27001. Aplicación a un caso de estudio" (p. 1).

Tiene por objetivo facilitar un estándar de gestión que permita afrontar incidentes disruptivos de forma eficaz y oportuna, integrando normativas legales y técnicas (SARABIA ZAPATA, 2015).

Entre sus conclusiones se estableció que : Respecto al modelo de gestión se identificó que es necesario discriminar entre el Proceso de Continuidad de Negocio total de la corporación y la continuidad estratégica de la Infraestructura Tecnológica, así como esquemas de alta disponibilidad, la estrategia de continuidad de Infraestructura Tecnológica está propuesta a nivel de áreas y aplicativos que soportan los servicios de TI operacionales, lo cual permiten cubrir todos los servicios tecnológicos brindados para la organización, el modelo que el investigador presento permite garantizar los servicios tecnológicos de TI en cualquier institución financiera nacional, y pretende concientizar y socializar la importancia fundamental de la Infraestructura Tecnológica en las empresas (SARABIA ZAPATA, 2015).

Peña Castro (2015) en su tesis de maestría titulada: “Guía metodológica para elaborar un BCP en entidades del estado” (p. 1). Tiene por objetivo: “Diseñar y desarrollar una metodología general para que las entidades estatales de orden nacional y territorial, elaboren sus procedimientos de continuidad de negocio de la gestión en tecnologías de información y telecomunicaciones, procesos y personas, basándose en buenas prácticas internacionales, pero ajustada a la infraestructura local de las entidades del estado en Colombia” (PEÑA CASTRO, 2015, p.19).

El método utilizado “fue de tipo aplicada”, donde el objetivo era “obtener un conocimiento técnico para la aplicación utilitaria”, se planteó para satisfacer necesidades de información que conducen a la aplicación inmediata en la solución de problemáticas apremiantes (PEÑA CASTRO, 2015).

Entre sus conclusiones se estableció que el proyecto permitió ajustar metodologías y estándares a la empresa Colombiana, para la implementación de un Plan de continuidad de las Operaciones y de los Sistemas de Información críticos, definiendo guías y paso a paso para definir estrategias, tiempos de respuesta y posibles planes de contingencia, así también la implementación de cualquier estándar de seguridad o de continuidad de negocio, depende directamente de la cultura organizacional y del nivel de compromiso de la dirección, es necesario que sea visualizado como estrategia de la compañía, de tal forma que se unan esfuerzos de talento humano, tecnología y financiero en pro de la consecución del plan de continuidad (PEÑA CASTRO, 2015).

- **Antecedentes Nacionales.**

Cueva Murillo (2015), en su estudio: “Diseño de un Sistema de Gestión de Continuidad de Negocios para una entidad estatal de salud bajo la óptica de la ISO/IEC 22301:2012” (p. 01).

Tiene por objetivo diseñar un sistema de gestión de continuidad de negocios el cual le permita proteger los servicios críticos que brinda dicha institución, realizando un análisis concreto de las amenazas que puedan afectar su operatividad y estableciendo los planes de prevención y recuperación a seguir en caso se manifieste la materialización de alguno de los riesgos considerados en la presente investigación (CUEVA MURILLO, 2015).

Entre sus conclusiones se estableció que se debe tener el apoyo de la Alta Gerencia y la disponibilidad del personal para la realización del Sistema de Gestión de Continuidad de Negocio (SGCN), es sumamente importante tener debidamente documentos y actualizados los procesos de negocio – en especial los procesos críticos – ya que dan un mejor conocimiento de la gestión de los mismos, el no haberlos tenido documentados, le implico al investigador un mayor tiempo de entrevistas, visitas para realizar el modelado, lo cual produjo un retraso en el inicio del desarrollo del SGCN (CUEVA MURILLO, 2015).

Delgado Concha (2015), en su tesis titulada: “Diseño y Propuesta de una Metodología para la Implementación de un Sistema de gestión de Continuidad del Negocio, Basado en la Norma ISO/IEC 22301:2012” (p. 01).

Tiene por objetivo permitir la viabilidad de un modelo práctico basado en la norma ISO/IEC 22301, el modelo propone su actualización y mejora constante, en función al crecimiento operativo y estratégico de la organización a lo largo del tiempo, a fin de lograr su operatividad y efectividad bajo cualquier circunstancia (DELGADO CONCHA, 2015).

Utilizó una metodología de tipo "aplicada", basada en la utilización de los conocimientos en la práctica, para aplicarlos, siempre como principal objetivo brindar u ofrecer un beneficio a las pequeñas y medianas empresas (PYMES), elabora su diseño metodológico realizando un análisis acerca de la implementación de Planes de Continuidad del negocio en el sector escogido, posteriormente realiza el levantamiento de información de procesos críticos con el fin de identificar posible vulnerabilidades y riesgos, después y de acuerdo a la información recaudada de la muestra escogida realiza el Análisis de Impacto de Negocios (BIA), en seguida y con base en dicho análisis hace la evaluación de riesgos para finalmente diseñar las estrategias que conforman BCP (DELGADO CONCHA, 2015).

Entre sus conclusiones, se estableció que el hecho de que no se presenten fallas constantemente, no es excusa para no implementar un BCP, ya que es necesario tener en cuenta la probabilidad de ocurrencia como el impacto al negocio, a su vez la causa más común de la falta de implementación de un plan de continuidad del negocio es la ausencia de recursos monetarios que apoyen este tipo de desarrollos en dichas entidades, además del desconocimiento del tema (DELGADO CONCHA, 2015).

2.3 MARCO CONCEPTUAL

Metodologías y estándares para elaborar un Modelo de Continuidad de Negocio.

2.3.1 COBIT 5.0

La Asociación para la Auditoria y Control de Sistemas de Información, ISACA (INFORMATION SYSTEM AUDIT AND CONTROL ASSOCIATION) y su IT GOVERNANCE INTITUTE, ITGI, desarrollaron los Objetivos de Control para la Información y Tecnologías relacionadas, COBIT (CONTROL OBJETIVES FOR INFORMATION AND RELATED TECHNOLOGY) **(ASSOCIATION, 2014)**.

COBIT es el único marco de negocio para el gobierno y la gestión de Tecnología de la empresa, proporciona principios globalmente aceptados, prácticas, herramientas analíticas y modelos para ayudar a aumentar la confianza en el valor de los sistemas de información **(ASSOCIATION, 2014)**.

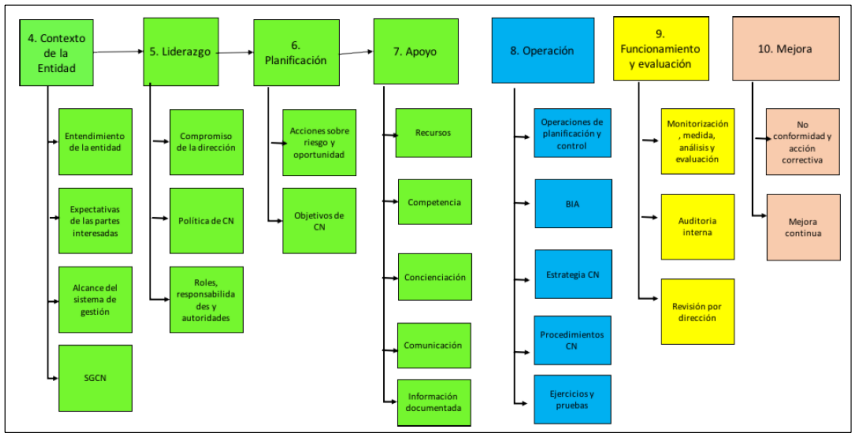
2.3.2 ISO 22301

Cuenta con una reconocida reputación de independencia en la realización de estándares e información de productos que promueven las mejores prácticas, entre estos productos se encuentra la BS ISO 22301:2012, es la norma internacional para la gestión de la continuidad del negocio, y se basa en éxito de la norma Británica BS 25999 y otras normas regionales, está diseñada para proteger la entidad de una interrupción potencial, incluyendo las condiciones meteorológicas extremas, incendios, inundaciones, desastres

naturales, robos, corte de Información y Tecnología, enfermedad general del personal o ataque terrorista **(INSTITUTION, 2014)**.

La continuidad del negocio contribuye al desarrollo de una sociedad más resiliente. Organizaciones sin un BCMS eficaz en la gestión y prevención de vulnerabilidades a las que son expuestas, podría llegar a generar impactos negativos en sus empleados, usuarios, clientes y proveedores **(INSTITUTION, 2014)**.

FIGURA. 03. "ESTRUCTURA DE ALTO NIVEL – ISO 22301"



FUENTE: **(INSTITUTION, 2014)**

2.3.3 ISO 27001.

Modelo internacional reconocida para la Gestión de "Seguridad de la Información (SGSI)", la gestión de la seguridad de la información se realiza mediante un proceso sistemático, documentado y conocido por toda la organización **(NORMA ISO 27001, 2005).**

Mediante ésta norma se establece la necesidad de crear un SGSI, constituyendo un eje vital para preservar la Continuidad del Negocio **(NORMA ISO 27001, 2005)**.

La seguridad de la información consiste "en la preservación de su confidencialidad, integridad y disponibilidad, incluyendo todos los sistemas manejados dentro de las empresas. La base de la norma lo conforman 3 términos sobre los cuales se edifica la seguridad de la información" **(NORMA ISO 27001, 2005)**.

- **Confidencialidad:** La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados **(NORMA ISO 27001, 2005)**.

- **Integridad:** Mantenimiento de la exactitud y complejidad de la información y sus métodos de proceso **(NORMA ISO 27001, 2005)**.

- **Disponibilidad:** Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran **(NORMA ISO 27001, 2005).**

2.3.4 ISO/IEC 27035:2012 "GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN".

La ISO/IEC 27035 es la Guía Técnica Colombiana, de Tecnologías de la Información. Técnicas de Seguridad. Gestión de Incidentes de Seguridad de la Información **(INCONTEC ISO 22301:2012, 2012)**.

2.3.5 BS 25777.

En muchas organizaciones, la realización de los procesos más importantes tiene como dependencia los servicios de información y tecnología de comunicaciones, definido en el BS 25777 como ICT (INFORMATION AND COMMUNICATIONS TECHNOLOGY) **(GROUP, 2008)**.

La finalidad del BS 25777 es soportar a las empresas a realizar una correcta estrategia para los servicios de información y tecnología de comunicaciones **(GROUP, 2008)**.

2.3.6 ¿QUÉ ES EL "PLAN DE CONTINUIDAD"?

Es un plan logístico para la práctica de cómo una organización debe recuperar y restaurar sus funciones críticas parcial o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción no deseada o desastre **(FUNDACIÓN WIKIMEDIA, 2018).**

En lenguaje sencillo, BCP es cómo una organización se prepara para futuros incidentes que puedan poner en peligro a ésta y a su misión básica a largo plazo, las situaciones posibles incluyen desde incidentes locales (como incendios, terremotos, inundaciones, etc.), incidentes de carácter regional, nacional o internacional hasta incidentes como pandemias, apocalipsis zombi, ataques extraterrestres **(FUNDACIÓN WIKIMEDIA, 2018).**

2.3.7 ¿PARA QUE UN "PLAN DE CONTINUIDAD"?.

El principal propósito de la planificación de la continuidad del negocio consiste en ayudar a las organizaciones a reiniciar las operaciones críticas

dentro de un marco de tiempo aceptable después de una interrupción, esta intenta reparar dificultades de gran envergadura (ya sean producidas por el hombre o por la naturaleza) que tienen un impacto sobre la efectiva ejecución de los procesos críticos de una organización, todas las áreas críticas del negocio y las funciones de apoyo están incluidas en el proceso de planificación **(LEON LOPEZ, 2008).**

En la era de la información la disponibilidad ininterrumpida de la misma es esencial, puede suceder que un desastre natural, una catástrofe o una acción fraudulenta interrumpan la posibilidad de acceso a la información afectando desfavorablemente los procesos clave del negocio, asimismo, las exigencias del mercado, junto con un mayor nivel de dependencia de la tecnología para ejecutar los procesos del negocio evidencian la necesidad de una planificación de continuidad eficiente **(LEON LOPEZ, 2008).**

2.3.8 NORMA ISO 22301.

La normativa ISO 22301 es un estándar publicado por la ISO en 2012, con el fin de brindar un documento que ofrezca soporte a las organizaciones para protegerse, mitigar o recuperarse de cualquier evento disruptivo a las operaciones **(ZAWADA, 2014)**.

2.3.9 CONTINUIDAD DE NEGOCIO.

Capacidad de la Organización para continuar con la entrega de productos o servicios a los niveles predefinidos aceptables después de un evento perjudicial **(INCONTEC ISO 22301:2012, 2012)**.

2.3.10 GESTIÓN DE LA CONTINUIDAD DE NEGOCIO.

Proceso de gestión integral que identifica las amenazas potenciales para la organización y los impactos que dichas amenazas podrían causar a las operaciones del negocio en caso de Guía para Elaborar un BCP en Entidades del Estado materializarse, las cuales proporcionan un marco para la construcción de la resiliencia de la organización con la capacidad de una nueva respuesta efectiva que salvaguarde los intereses de sus partes interesadas clave, su reputación, marca y las actividades que crean valor **(INCONTEC ISO 22301:2012, 2012)**.

2.3.11 PLAN DE CONTINUIDAD DE NEGOCIO.

Procedimientos documentados que guían a las organizaciones para responder, recuperar, reanudar y restaurar a un nivel pre-definido de operación debido a la interrupción **(INCONTEC ISO 22301:2012, 2012)**.

Según la norma ISO 22301:2012, propone que los planes de continuidad de negocio deben contener colectivamente:

- Un proceso para la activación de la respuesta **(INCONTEC ISO 22301:2012, 2012)**.

- Los detalles para gestionar las consecuencias inmediatas de un incidente perjudicial **(INCONTEC ISO 22301:2012, 2012)**.

- Cómo la organización va a continuar o recuperar sus actividades prioritarias dentro de los plazos determinados **(INCONTEC ISO 22301:2012, 2012)**.

2.3.12 PROGRAMA DE CONTINUIDAD DE NEGOCIO.

"Proceso continuo de gestión y la gobernabilidad con el apoyo de la alta dirección y los recursos adecuados para implementar y mantener la gestión de la Continuidad de Negocio" **(INCONTEC ISO 22301:2012, 2012)**.

2.3.13 AMENAZA.

"Una amenaza es la posibilidad de que un evento – causado o no – ponga en peligro a una persona, grupo, empresa si es que no se toman las medidas adecuadas" **(ISACA, CISM Review Manual 2013, 2012)**.

Se define como: Cualquier circunstancia o hecho que pueda afectar negativamente a las operaciones de la organización, sus activos de información o individuos a través del acceso no autorizado, destrucción, acceso, modificación de la información, y/o negación de servicio, además, la posibilidad de una amenaza de fuente de explotar con éxito una vulnerabilidad de la información del sistema en particular, en otra acepción, son todas las actividades, eventos o circunstancias que pueden afectar el buen uso de un activo de información dañando el soporte a un proceso, perjudicando el logro de los objetivos de negocio **(TUPIA ANTICONA, 2011)**.

2.3.14 VULNERABILIDAD.

"La vulnerabilidad es la capacidad que tiene un evento de ser susceptible ante una amenaza, que impacte negativamente sobre algo" **(ISACA, CRISC Review Manual 2014, 2013)**.

Según el BCI: Las vulnerabilidades en el negocio y en el modelo de operación de una organización pueden considerarse en siete áreas (reputación, cadena de suministro, información y comunicaciones, sedes e instalaciones, personas, finanzas y clientes) **(BUSINESS CONTINUITY INSTITUTE, 2010)**.

2.3.15 RIESGO.

"Un riesgo es la probabilidad de que una amenaza se aproveche de la vulnerabilidad para materializarse e impactar positiva o negativamente sobre algún evento o proceso" **(ISACA, CRISC Review Manual 2014, 2013)**.

Tratamiento de riesgo:

- **Aceptar:** Cuando el riesgo no tiene un fuerte impacto, o no se tiene el presupuesto adecuado para combatirlo, lo cual dependerá del apetito de riesgo de la empresa, es decir, de cuanto riesgo está dispuesto a aceptar y manejar **(ISACA, CISM Review Manual 2013, 2012)**.

- **Mitigar o Evitar:** Cuando se reduce el riesgo mediante medidas y controles **(ISACA, CISM Review Manual 2013, 2012).**

- **Transferir:** Cuando se riesgo terceriza el riesgo para que ellos se encarguen de su tratamiento, típicamente se transfiere el riesgo a una aseguradora **(ISACA, CISM Review Manual 2013, 2012)**.

- **Eliminar:** Este tratamiento es extremo, pues no se puede eliminar el riesgo, pero sí su origen o fuente **(ISACA, CISM Review Manual 2013, 2012)**.

2.3.16 IMPACTO.

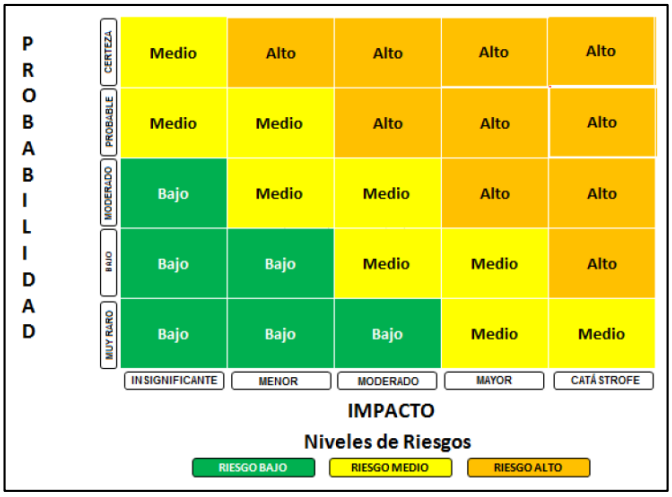
Se define como: Evento que tiene la capacidad de provocar la pérdida de o la interrupción de las operaciones, servicios o funciones de la organización, el cual, si no se administra, puede escalar y convertirse en una emergencia, crisis o desastre **(BUSINESS CONTINUITY INSTITUTE, 2010)**.

La interrupción se puede evitar teniendo un procedimiento que, o bien proporciona alguna forma alternativa de la continuidad del negocio o corrige el problema dentro de un tiempo aceptable **(SANCHEZ SILVA, 2005)**.

El impacto no siempre se produce inmediatamente después de una interrupción y la mayoría de las empresas pueden sobrevivir durante algún tiempo antes de que las pérdidas comiencen, este período es vital para el negocio y varía entre empresas y líneas de negocio, si se realiza un análisis de riesgos basado de tipo cuantitativo de impacto y las probabilidades, las escalas cualitativas del impacto son: catastrófico o extremo, grave, medio, moderado o bajo e insignificante probable **(SANCHEZ SILVA, 2005)**.

En la Figura 01 se muestra la matriz 5x5 conocida para la cuantificación de riesgos **(SANCHEZ SILVA, 2005)**.

FIGURA 01. MATRIZ DE RIESGOS BASADO.



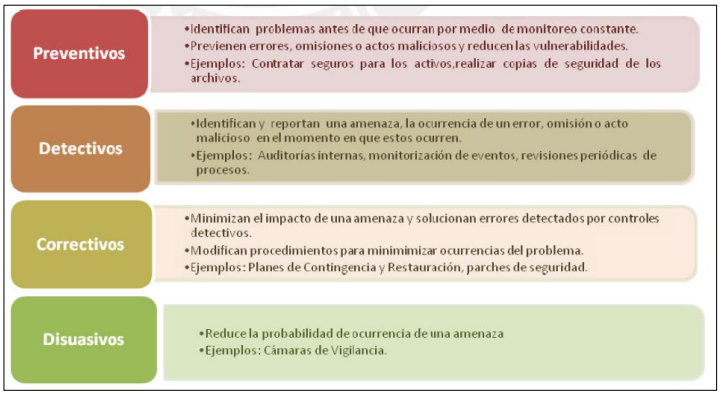
FUENTE: (SANCHEZ SILVA, 2005)

2.3.17 CONTROLES.

"Son políticas, prácticas, procedimientos y lineamientos para asegurar que los riesgos son reducidos a un nivel aceptable de tal forma que no afecten el cumplimiento de los objetivos de la empresa" **(ISACA, CISM Review Manual 2013, 2012)**.

Son las políticas, medidas de seguridad, procedimientos y prácticas para reducir riesgos y que proveen cierto grado de certeza de que se lograrán los objetivos del negocio **(TUPIA ANTICONA, 2011)**.

FIGURA 02. "TIPO DE CONTROLES"



FUENTE: (TUPIA ANTICONA, 2011)

2.3.18 COBIT:

Es un instrumento para la administración de las tecnologías de información, desarrollada por ISACA como un estándar para la seguridad de la tecnología de información y buenas prácticas de control, Constituye un marco unificador internacionalmente aceptado como una buena práctica para la gestión, el control de la información, de la tecnología de información y de los riesgos que estas sufren **(ISACA, CISM Review Manual 2013, 2012)**.

2.4 ASPECTOS DE RESPONSABILIDAD SOCIAL Y MEDIO AMBIENTAL

Esta Investigación ha permitido en la práctica agilizar los procesos Académicos y con ello poder brindar un mejor servicio educativo tanto a los Alumnos internados, docentes que son parte de la plana educativa de la Institución y al mismo personal administrativo, que en muchos casos tiene retraso en la entrega de sus reportes. Esto propicia un Clima institucional favorable entre las personas que interactúan en la ejecución de los procesos académicos, cumpliendo con objetivos trazados respecto a la formación Policial de los alumnos, debido a que éstos reciben una mejor preparación durante su tiempo de internamiento, con la finalidad de que puedan ejercer eficientemente su función Policial al servicio de la sociedad.

2.4.1 MARCO REGULATORIO / LEGAL.

- **NORMA TÉCNICA PERUANA (NTP) ISO/IEC 17799:2007.**

  "Aprobada mediante la Resolución Ministerial N° 246-2007-PCM en agosto del año 2007 en calidad de uso obligatorio para todas las

entidades que integran el Sistema Nacional de Informática", establece una serie de recomendaciones generales – sin enfocarse en algún giro de negocio específico – para llevar una correcta gestión de la seguridad de la información en dichas organizaciones **(CRTC - INDECOPI, 2007)**.

Tiene como objetivo poder reaccionar a la interrupción de actividades del negocio y proteger sus procesos críticos frente a grandes fallos de los sistemas de información o desastres **(CRTC - INDECOPI, 2007)**.

- **NORMA TÉCNICA PERUANA (NTP) ISO/IEC 27001_2008.**

  "Es una norma que nació como iniciativa del Gobierno Peruano para asegurarse que todas las empresas del estado tengan un Sistema de Gestión de Seguridad de la Información (SGSI) y cuente con los lineamientos generales para realizar el proceso de implementación" **(CNB - INDECOPI, 2008)**.

  Esta norma indica que se debe: "Conocer los procesos, Cumplir con la documentación obligatoria como Business Case, metodologías de riesgos y activos, etc., Controles para establecer la declaración de aplicabilidad" **(CNB - INDECOPI, 2008)**.

  Tiene como objetivo neutralizar las interrupciones a las actividades del negocio y proteger los procesos críticos del negocio de los efectos de fallas mayores o desastres en los sistemas de información y asegurar su reanudación oportuna **(CNB - INDECOPI, 2008)**.

- **LEY N° 28551 – "LEY QUE ESTABLECE LA OBLIGACIÓN DE ELABORAR Y PRESENTAR PLANES DE CONTINGENCIA".**

  Esta ley indica que "los planes de contingencia son instrumentos de gestión que definen los objetivos, estrategias y programas que orientan las actividades institucionales para la prevención, la reducción de riesgos, la atención de emergencias y la rehabilitación en casos de desastres permitiendo disminuir o minimizar los daños, víctimas y pérdidas que podrían ocurrir a consecuencia de fenómenos naturales, tecnológicos o de la producción industrial, potencialmente dañinos." **(CONGRESO DE LA REPÚBLICA, 2005)**.

  También indica que:

  Capacitar a todo el personal de la entidad, y realizar los simulacros necesarios para la correcta aplicación de los procedimientos contenidos en los Planes de Contingencia y de Prevención y Atención de Desastres **(CONGRESO DE LA REPÚBLICA, 2005)**.

CAPITULO III. MÉTODO

3.1 TIPO DE INVESTIGACIÓN

La investigación aplicada se caracteriza porque busca la aplicación o utilización de los conocimientos adquiridos, a la vez que se adquieren otros, después de implementar y sistematizar la práctica basada en investigación, el uso del conocimiento y los resultados de investigación que da como resultado una forma rigurosa, organizada y sistemática de conocer la realidad **(VARGAS CORDERO, 2009).**

Según el objeto de estudio, el tipo de investigación es ***"Aplicada"*** por qué parte de una situación problemática concreta e identificable, de los procesos de la "Unidad Académica de Pregrado de la Escuela de Policía", que requieren ser optimizados, para ello la propuesta de solución debe tener integrado los conocimientos del investigador para poder resolver la problemática identificada elaborando así un modelo de continuidad de negocio y buenas prácticas de acuerdo a los requerimientos de la Institución Policial.

3.2 POBLACIÓN Y MUESTRA

- **POBLACIÓN**

  La investigación se realizará en la Escuela Técnica de la Policía "Capitán PNP Alipio Ponce Vásquez", Ubicada en el Departamento de Lima, Perú. La población objetivo está conformada por 22 personas, la cual se detalla a continuación:

Tabla 04: POBLACIÓN

ESCUELA TÉCNICA DE LA PNP "CAPITÁN PNP ALIPIO PONCE VÁSQUEZ"		
N°	**UNIDADES ADMINISTRATIVAS**	**CANTIDAD PERSONAL PNP**
1	DIRECCIÓN	01
2	UNIDAD DE ORDENES	03
3	UNIDAD ACADÉMICA	
	DEP. PLANEAMIENTO EDUCATIVO	04
	DEP. DE EVALUACIÓN Y SUPERVISION ACADÉMICA	04
	DEP. DE MÉDIOS Y MATERIALES EDUCATIVOS.	04
	DEP. DE PROYECCIÓN EDUCATIVA.	03
	DEP. PSICOPEDAGOGICA	03
	POBLACIÓN TOTAL	**22**

Fuente : Unidad Administración de la PNP

- **MUESTRA**

La muestra es censal, porque se trabajará con toda la población.

3.3 HIPÓTESIS.

3.3.1 HIPOTESIS GENERAL.

"La Propuesta de un Modelo de Continuidad de negocio y Buenas Prácticas, optimiza los procesos formativos de las Unidades Académicas de Pregrado de la Escuela de Policía."

3.3.2 HIPOTESIS ESPECÌFICAS.

- El Realizar la identificación y análisis de las posibles amenazas optimiza los Procesos formativos de las Unidades Académicas de Pregrado de las Escuelas Técnicas de Policía.

- El realizar la identificación y análisis de las funciones críticas y servicios de TI optimiza los Procesos formativos de las Unidades Académicas de Pregrado de las Escuelas Técnicas de Policía.

- El Realizar la propuesta de un plan de respuesta y recuperación para las funciones críticas optimiza los Procesos formativos de las Unidades Académicas de Pregrado de las Escuelas Técnicas de Policía.

3.4 OPERACIONALIZACIÓN DE LAS VARIABLES

- **Variable Independiente.**

  Modelo de Continuidad de negocio y Buenas Prácticas.

- **Variable Dependiente.**

  Los procesos formativos de las Unidades Académicas de Pregrado de la Escuela Técnica de la Policía.

TABLA 03: OPERACIONALIZACIÓN DE LAS VARIABLES.

VARIABLE	INDICADOR	DESCRIPCION	FORMULA Y ELEMENTOS	PERIODO
Modelo de Continuidad de negocio y Buenas Prácticas.	Registro de matrícula de los Alumnos	Registro de matrícula en el sistema académico de los alumnos, el cual se realiza a la apertura de cada período de estudio. Su unidad de medida está dada en cantidad.	**CAMD = TTD / TPMA** **CAMD =** Cantidad de Alumnos Matriculados por día. **TTD** = Tiempo de trabajo diario destinado para matricular alumnos. **TPMA** = Tiempo promedio para matricular a un Alumno.	**CUATRIMESTRAL**
	Registro de notas de los Alumnos.	Es la digitalización de los registros de notas que los docentes entregan a mitad del ciclo académico y posteriormente al término del mismo respecto a las notas de los alumnos. Su unidad de medida está dada en cantidad.	**CRDD = TTD / TPDRN** **CRDD** = Cantidad de Registros de notas digitalizadas por día. **TTD** = Tiempo de trabajo diario destinado para registrar de notas. **TPDRN** = Tiempo promedio para digitalizar y verificar un registro de notas.	**BIMESTRAL**
	Registro de datos del Personal de Alumnos.	Registro o Actualización de los datos personales de cada alumno internado en ésta Institución, este proceso se da cada semestre conforme a disposiciones emitidas por la superioridad. Su unidad de medida está dada en horas.	**TRDPA = TENC + TDI** TRDPA = Tiempo de registro de los datos del Personal de alumnos. **TENC** = Tiempo en la entrega de la información solicitada **TDI** = Tiempo de digitalizar la información	**SEMESTRAL**

	Número de reportes emitidos por semana	**Es el número total de reportes que han sido solicitados por la superioridad y que éstos fueron emitidos dentro de los plazos establecidos.** **Dichos reportes son contabilizados por cantidad.**	NRE = NRED * DLS **NRE = Número de reportes emitidos por semana.** **NRED = Número de reportes emitidos por día.** **DLS = Días laborados en la semana.**	**DIARIAMENTE**
Procesos formativos de las Unidades Académicas de Pregrado de la Escuela Técnica de Policía.	Tiempo de entregar de reportes.	Es el tiempo empleado en la entrega de los reportes emitidos por la unidad Académica, los cuales son derivados a la dirección de la institución, esto se realiza diariamente. Su unidad de medida está dada en horas.	**TER = TPR + TER** TER = Tiempo Empleado en la entrega de reporte. TPR = Tiempo de elaboración del reporte. TER = Tiempo de elevación del reporte.	DIARIAMENTE
	Tiempo de entrega de solicitudes de información	Es el tiempo empleado en la entrega de requerimientos de información académica a los alumnos, profesores o padres de familia, respecto a las actividades académicas. Su unidad de medida está dada en horas.	**TESI = TPR + TER** TESI = Tiempo Empleado en la entrega de solicitudes de información. TEIS = Tiempo de elaboración de la información solicitada. TEEIS = Tiempo empleado en la entrega de la información al solicitante.	DIARIAMENTE

FUENTE: Elaboración Propia.

3.5 INSTRUMENTOS

Los Instrumentos que serán utilizados en la recolección de información son:

Entrevistas.- La entrevista se realizará al director de la institución, al personal de la Unidad de Ordenes y de la unidad académica en su totalidad; formulando una serie de preguntas puntuales de las cuales se procedió a evaluar la situación en lo que se encontraban las áreas involucradas. Con estas entrevistas se obtendrá la problemática de dichas áreas.

Análisis documental.- Recopilación de la Información a través de documentos ya existentes en la Institución como son: Actas consolidadas de evaluación académica, nómina de matrícula, horarios de clase, lista de revista de presencia del personal Policial, relación nominal del personal Policial con mención de su área de trabajo y cargo y otros que se crea conveniente y alineados a la investigación.

La Guía de Observación que permitirá recoger la información directa respecto a las posibles amenazas, funciones críticas y los planes de respuesta en situaciones críticas relacionadas con los Procesos de la Unidad Académica.

Se utilizará una guía de observación con ítems de opción múltiple con escala de calificación de 5 alternativas.

La guía de observación será sometida a "validez de contenido a través de la técnica de juicio de expertos", para confirmar que el instrumento es válido y confiable.

3.6 PROCEDIMIENTO.

El procedimiento utilizado en esta investigación es ***"No Experimental"***.

"Se trata de un estudio donde no se hará variar en forma intencional la variable independiente para ver su efecto sobre la variable dependiente" **(HERNÁNDEZ, FERNÁNDEZ, & BAPTISTA, 2010)**.

Es ***"No Experimental, Transversal, Transeccional o Descriptivo",*** porque el investigador "recolecta datos en un solo momento, en un tiempo único, describe los hechos como son observados en la realidad actual de los procesos de la Unidad Académica de Pregrado de la Escuela Técnica de Policía".

El procedimiento es "observacional", que tal como se muestra adelante, se hizo la aplicación y análisis de todos los procesos formativos de la Unidad Académica de Pregrado de la Escuela Técnica de Policía, notándose que nuestro modelo de Continuidad de Negocio y Buenas Prácticas propuesto permite optimizar cada uno de ellos.

3.7 ANÁLISIS DE DATOS.

Para el análisis de datos se utilizó el software SPSS 2.0 para Windows.

El análisis estadístico de las datos se realizó mediante el programa SPSS, de los resultados obtenidos de la encuesta **(ANEXO N° 01)** dirigidos al Personal Administrativo y Docentes de la Escuela de Policía

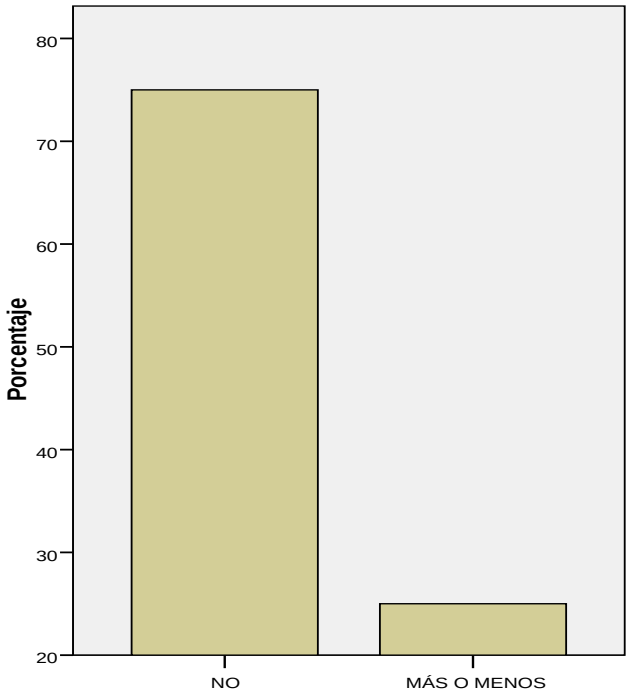
CAPITULO IV. RESULTADOS

4.1 CONTRASTACIÓN DE HIPÓTESIS

4.1.1 HIPÓTESIS GENERAL

La "Propuesta de un Modelo de Continuidad de negocio y Buenas Prácticas, optimiza los procesos formativos de las Unidades Académicas de Pregrado de la Escuela Técnica de la Policía".

FIGURA Nº 04: "El PLAN DE CONTINGENCIA ACTUAL DE LA INSTITUCIÓN LE HA PERMITIDO OPTIMIZAR LAS TAREAS COMUNMENTE REALIZADAS REFERENTE A LOS PROCESOS FORMATIVOS".



FUENTE: Elaboración propia

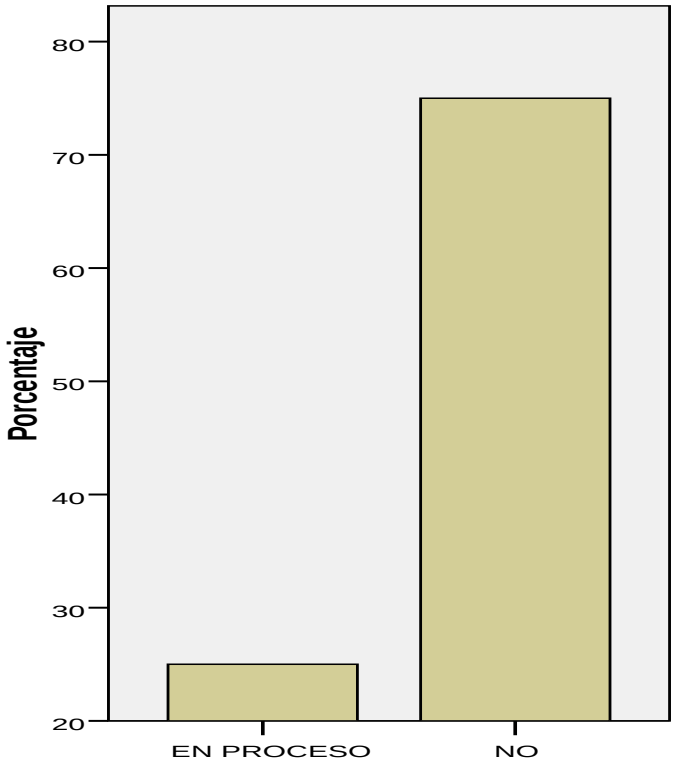
INDICADOR DE FRECUENCIA Nº 01

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
NO	3	75.0	75.0	75.0
MÁS O MENOS	1	25.0	25.0	100.0
Total	4	100.0	100.0	

FUENTE: Elaboración propia

El 75% sostiene que el actual plan de contingencia de la Institución "**NO"** le permite optimizar las tareas comúnmente realizadas referente a los procesos formativos el 25% menciona que "**MÁS O MENOS".**

FIGURA Nº 05: ACTUALMENTE LA UNIDAD ACADÉMICA CUENTA CON EQUIPAMIENTO TECNOLÓGICO ASIGNADO QUE LE PERMITE TENER SU BASE DATOS ACTUALIZADA



Fuente: Elaboración propia

INDICADOR DE FRECUENCIA Nº 02

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	EN PROCESO	1	25.0	25.0	25.0
	NO	3	75.0	75.0	100.0
	Total	4	100.0	100.0	

Fuente: Elaboración propia

El 75% sostiene que actualmente la base de datos de la Unidad Académica "**NO"** se encuentra actualizada y el otro 25% sustenta que se encuentra "**EN PROCESO".**

El resultado de la consulta realizada, ha evidenciado el requerimiento de implementar un "Modelo de Continuidad de Negocio y Buenas prácticas" ágil y adaptado a las necesidades de la Institución para poder optimizar los procesos formativos, en esta pregunta puntual poder tener actualizada la información de todos los procesos académicos elaborados por la Institución Educativa Policial así el Comando Policial pueda tomar acciones respecto a la información proporcionada.

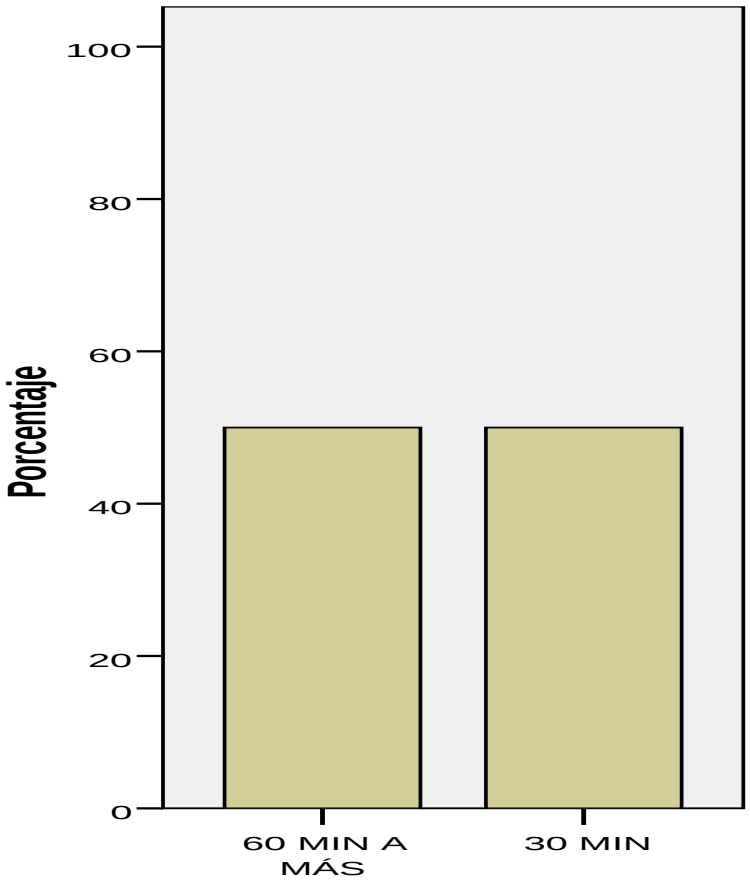
4.1.2 HIPOTESIS ESPECÌFICAS.

- *El Realizar la identificación y análisis de las posibles amenazas optimiza los Procesos formativos de las Unidades Académicas de Pregrado de las Escuelas Técnicas de Policía.*

- *El realizar la identificación y análisis de las funciones críticas y servicios de TI optimiza los Procesos formativos de las Unidades Académicas de Pregrado de las Escuelas Técnicas de Policía.*

- *El Realizar la propuesta de un plan de respuesta y recuperación para las funciones críticas optimiza los Procesos formativos de las Unidades Académicas de Pregrado de las Escuelas Técnicas de Policía.*

FIGURA Nº 06: CUAL ES EL TIEMPO APROXIMADO QUE EMPLEA PARA ATENDER UN REPORTE ACADÉMICO SOLICITADO POR LA SUPERIORIDAD.



FUENTE: Elaboración propia

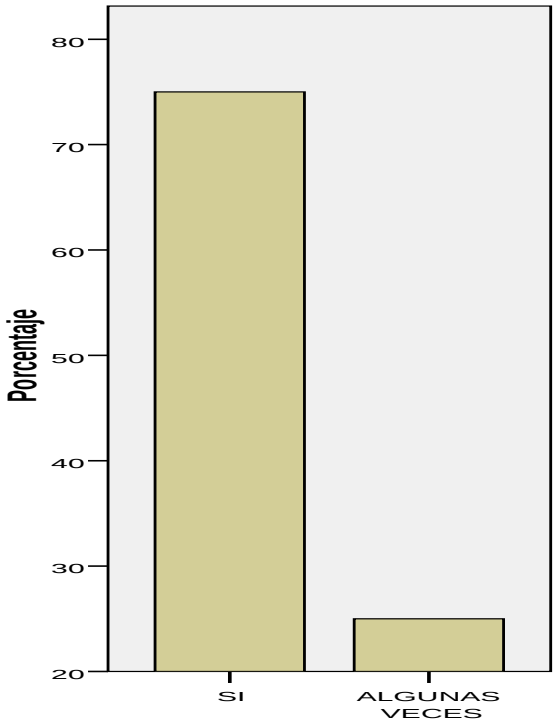
INDICADOR DE FRECUENCIA Nº 03

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	60 MIN A MÁS	2	50.0	50.0	50.0
	30 MIN	2	50.0	50.0	100.0
	Total	4	100.0	100.0	

Fuente: Elaboración propia

El 50% sostienes que el tiempo que tardan en atender un reporte académico es de "**60 min a Más"** y el otro 50% que el tiempo estimado es de "**30 min".**

FIGURA Nº 07: HA TENIDO CONSTANTEMENTE DIFICULTAD PARA EL INGRESO A LOS SISTEMAS POLICIALES ACADÉMICOS



FUENTE: Elaboración propia

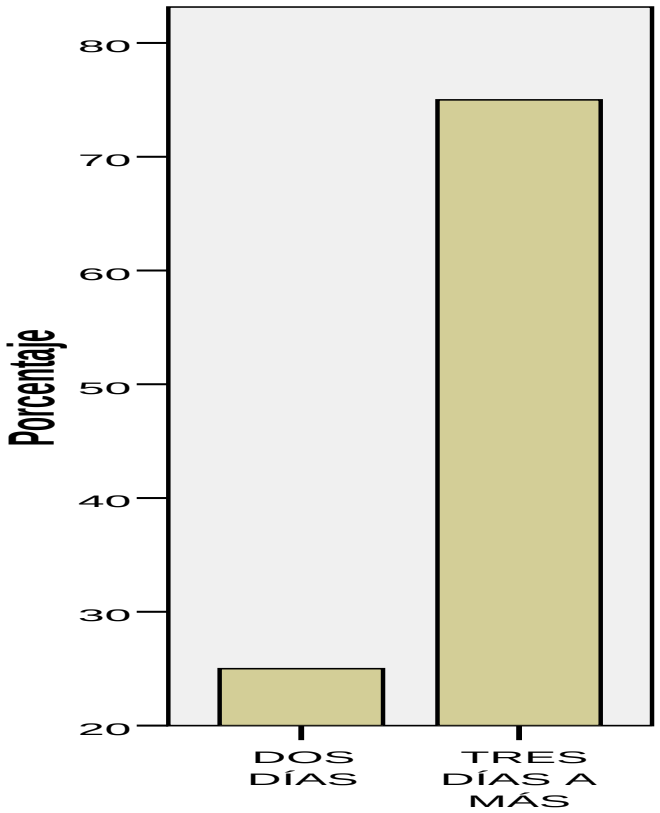
INDICADOR DE FRECUENCIA Nº 04

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	SI	3	75.0	75.0	75.0
	ALGUNAS VECES	1	25.0	25.0	100.0
	Total	4	100.0	100.0	

Fuente: Elaboración propia

El 75% sostiene que "**SI"** ha tenido dificultades en el sistema al momento de ingresar a los sistemas académicos y el otro 25% afirma que "**ALGUNAS VECES".**

FIGURA Nº 08: CUAL ES EL TIEMPO PROMEDIO ACTUAL PARA RECUPERAR EL NORMAL FUNCIONAMIENTO DE LOS SISTEMAS ACADÉMICOS ANTE SINIESTROS



Fuente: Elaboración propia

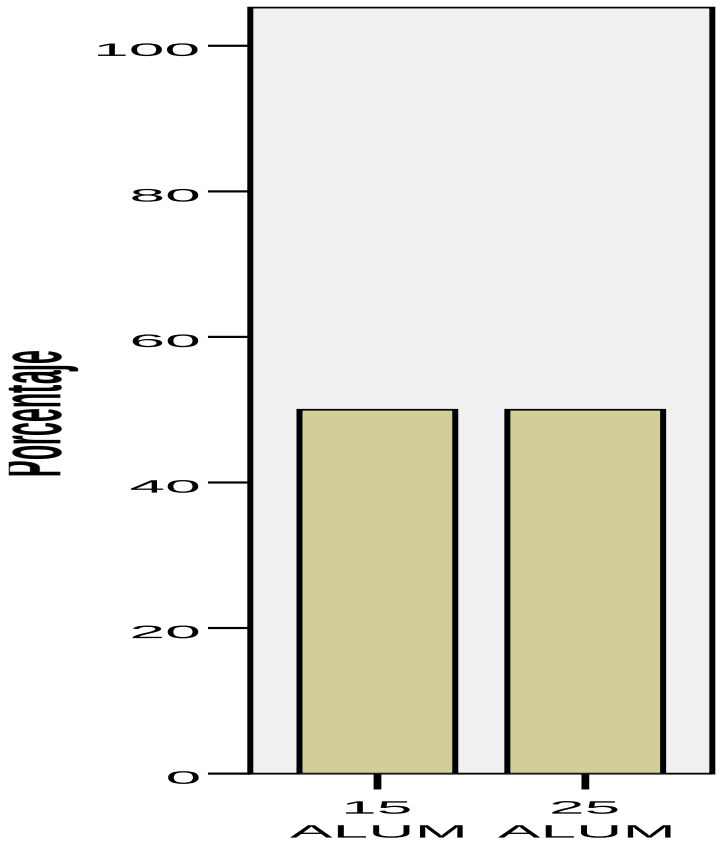
INDICADOR DE FRECUENCIA Nº 05

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	DOS DÍAS	1	25.0	25.0	25.0
	TRES DÍAS	3	75.0	75.0	100.0
	Total	4	100.0	100.0	

Fuente: Elaboración propia

El 25% sostiene que "**DOS DÍAS"** se demoran en recuperar el normal funcionamiento de los sistemas académicos ante siniestros y el otro 75% afirma que de "**TRES DÍAS A MÁS".**

FIGURA Nº 09: CUAL ES EL PROMEDIO DE ALUMNOS MATRICULADOS POR DIA, AL EMPEZAR UN NUEVO SEMESTRE ACADÉMICO



Fuente: Elaboración propia

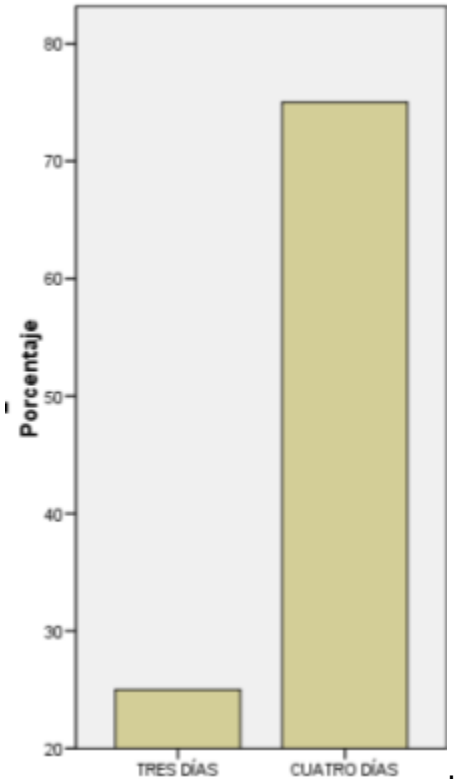
INDICADOR DE FRECUENCIA Nº 06

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	15 ALUM	2	50.0	50.0	50.0
	25 ALUM	2	50.0	50.0	100.0
	Total	4	100.0	100.0	

Fuente: Elaboración propia

El 50% sostiene que "**aprox. 15 ALUMNOS"** son matriculados por día y el otro 50% afirma que "**aprox. 25 ALUMNOS".**

FIGURA Nº 10: TIEMPO PROMEDIO EN CONSOLIDAR LAS NOTAS AL TÉRMINO DEL SEMESTRE



Fuente: Elaboración propia

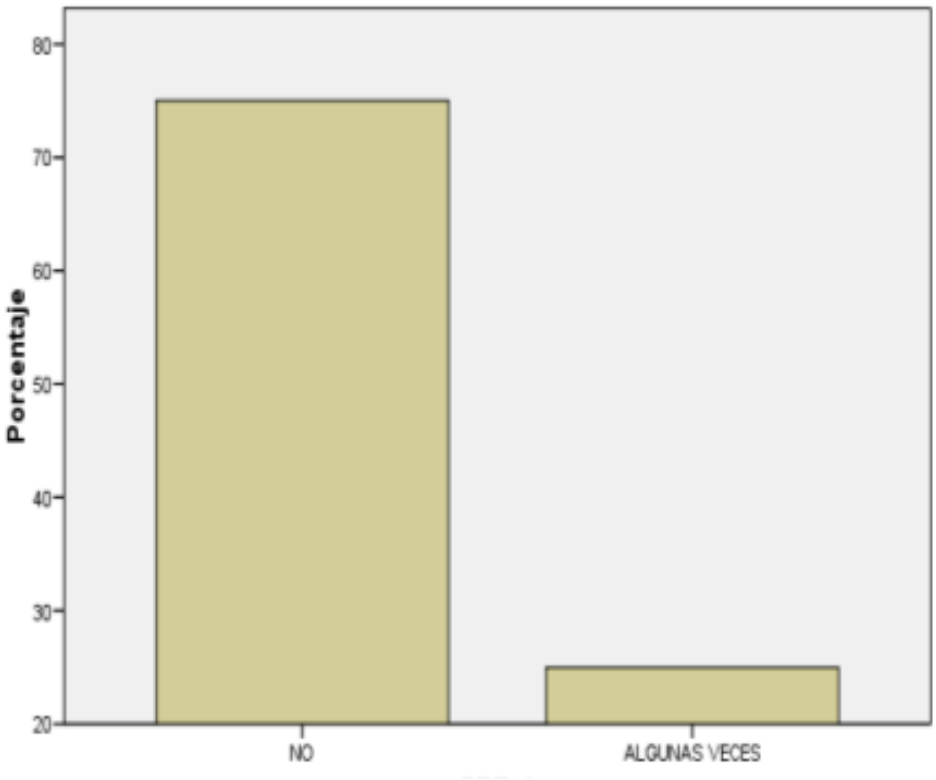
INDICADOR DE FRECUENCIA Nº 07

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	TRES DÍAS	1	25.0	25.0	25.0
	CUATRO DÍAS	3	75.0	75.0	100.0
	Total	4	100.0	100.0	

Fuente: Elaboración propia

El 75% sostiene que el tiempo promedio que se emplea en consolidar las notas es de "**CUATRO DÍAS"** y el otro 25% afirma que emplea "**TRES DÍAS".**

FIGURA Nº 11: RECIBE CAPACITACIÓN SOBRE EL PLAN DE CONTINGENCIA TECNOLÓGICO



Fuente: Elaboración propia

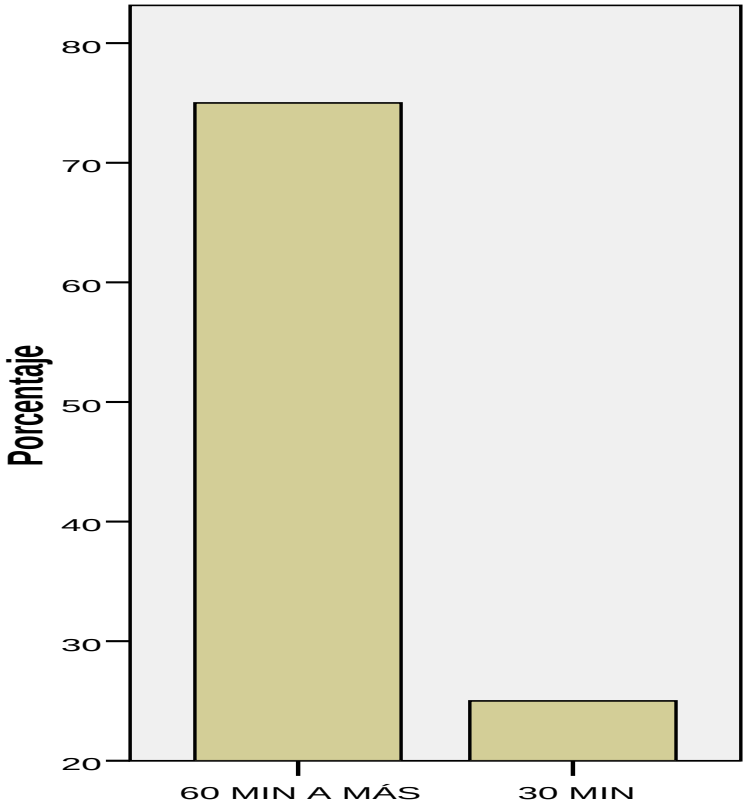
INDICADOR DE FRECUENCIA Nº 08

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	NO	3	75.0	75.0	75.0
	ALGUNAS VECES	1	25.0	25.0	100.0
	Total	4	100.0	100.0	

Fuente: Elaboración propia

El 75% sostiene que "**NO"** recibe capacitación sobre el plan de contingencia tecnológico y el otro 25% afirma sólo "**ALGUNAS VECES".**

FIGURA Nº 12: TIEMPO APROXIMADO PARA ATENDER UNA SOLICITUD DE REPORTE



Fuente: Elaboración propia

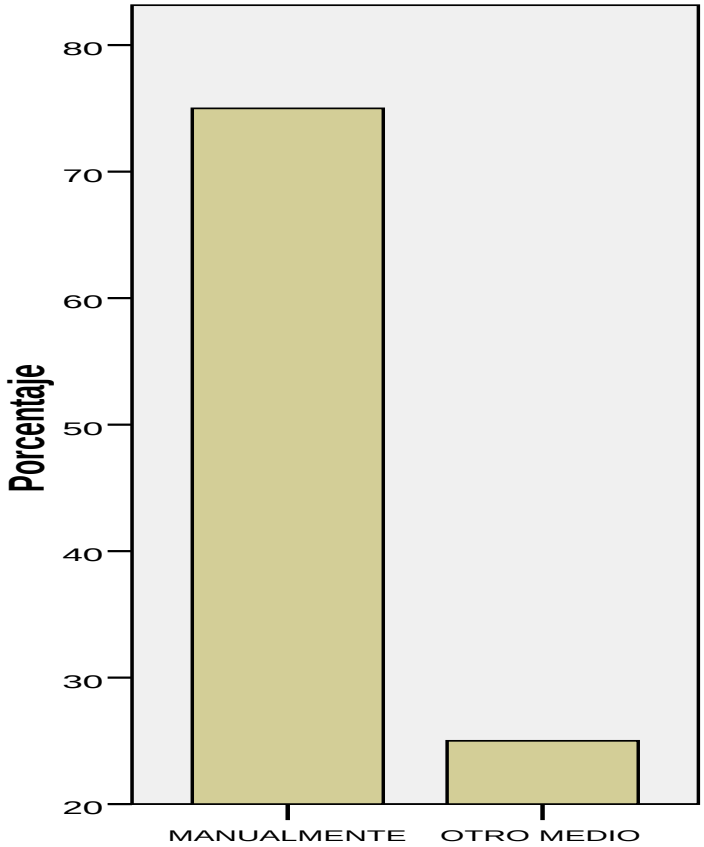
INDICADOR DE FRECUENCIA Nº 09

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	60 MIN A MÁS	3	75.0	75.0	75.0
	30 MIN	1	25.0	25.0	100.0
	Total	4	100.0	100.0	

Fuente: Elaboración propia

El 75% sostiene que el tiempo promedio que se emplea para atender un reporte es de "**60 MINUTOS A MÁS**" y el otro 25% afirma que demora "**30 MINUTOS"**.

FIGURA Nº 13: ANTE UN SINIESTRO MEDIANTE QUE MEDIO ATIENDE LAS SOLICITUDES DE REPORTE



Fuente: Elaboración propia

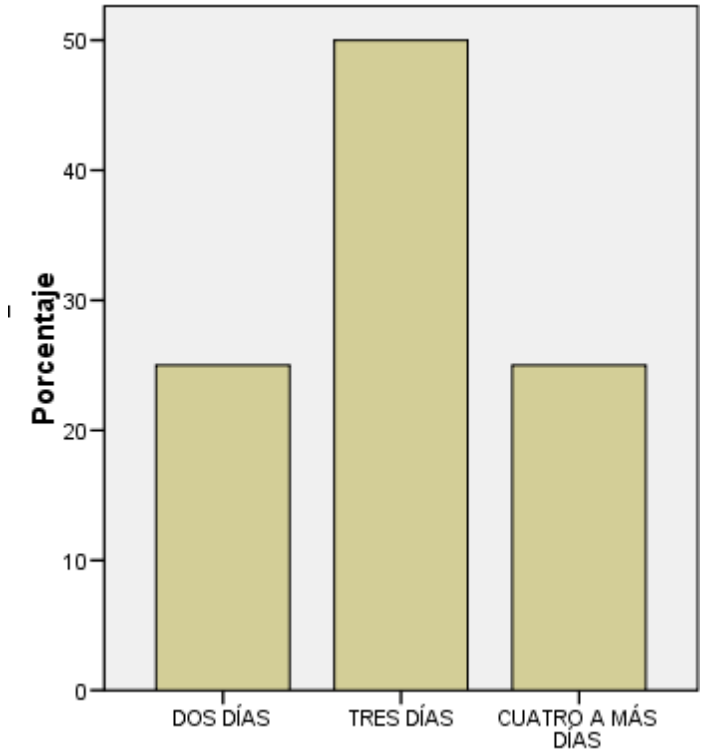
INDICADOR DE FRECUENCIA Nº 10

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	MANUALMENTE	3	75.0	75.0	75.0
	OTRO MEDIO	1	25.0	25.0	100.0
	Total	4	100.0	100.0	

Fuente: Elaboración propia

El 75% sostiene que ante un siniestro las solicitudes de reporte son atendidas "**MANUALMENTE"** y el otro 25% afirma que por "**OTRO MEDIO".**

FIGURA Nº 14: CUANTOS DIAS AL MES HA SUFRIDO EN PROMEDIO DE INTERRUPCIÓN DEL SERVICIO DE INTERNET



Fuente: Elaboración propia

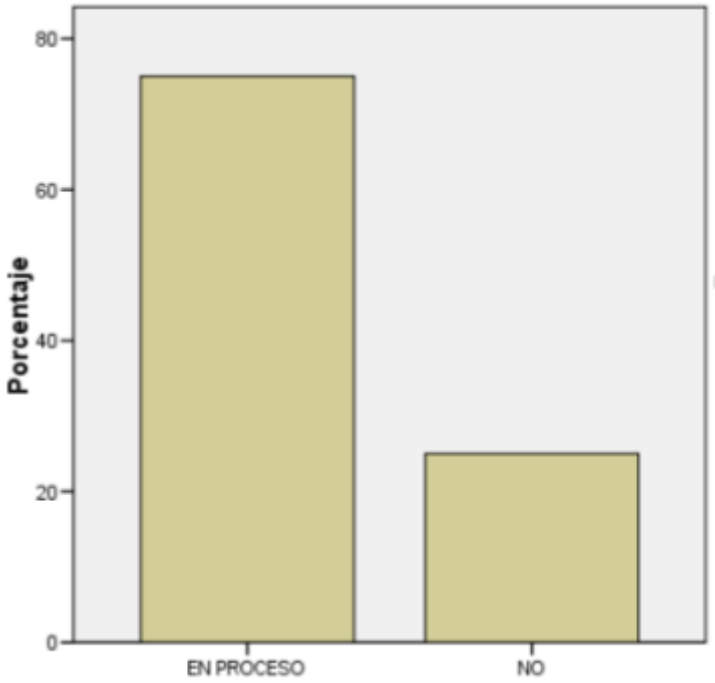
INDICADOR DE FRECUENCIA Nº 11

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
DOS DÍAS	1	25.0	25.0	25.0
TRES DÍAS	2	50.0	50.0	75.0
CUATRO A MÁS DÍAS	1	25.0	25.0	100.0
Total	4	100.0	100.0	

Fuente: Elaboración propia

El 50% sostiene que ha sufrido de interrupción del servicio de internet en promedio de "**DOS DÍAS"**, el otro 25% afirma que ha sufrido de dicha interrupción de **"TRES DÍAS"** y el otro 25% que de **"CUATRO A MÁS DÍAS**".

FIGURA Nº 15: ACTUALMENTE SE CUENTA CON "EL PLAN DE CONTINGENCIA ACTUALIZADO DE LA INSTITUCIÓN"



Fuente: Elaboración propia

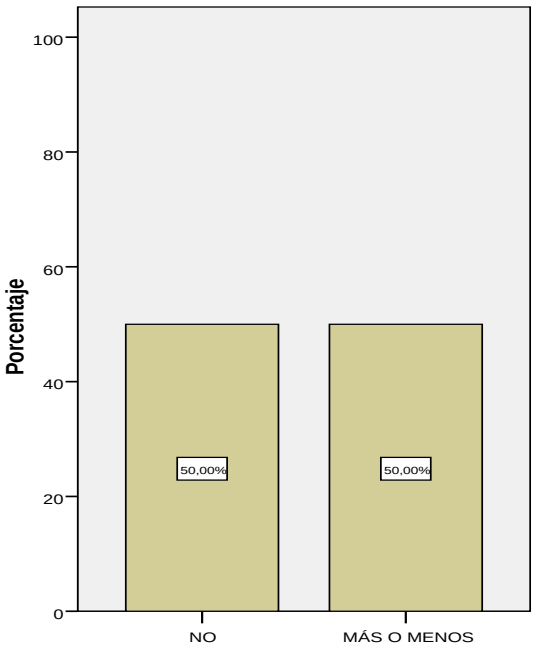
INDICADOR DE FRECUENCIA Nº 12

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	EN PROCESO	3	75.0	75.0	75.0
	NO	1	25.0	25.0	100.0
	Total	4	100.0	100.0	

Fuente: Elaboración propia

El 75% sostiene que actualmente el plan de Contingencia de la Institución se encuentra "**EN PROCESO"** de ser actualizada y el otro 25% afirma que "**NO"** está actualizada**.**

FIGURA Nº 16: ACTUALMENTE CUENTA CON EL APOYO DE LA INSTITUCION PARA OPTIMIZAR LOS PROCESOS ACADÉMICOS QUE REALIZA



Fuente: Elaboración propia

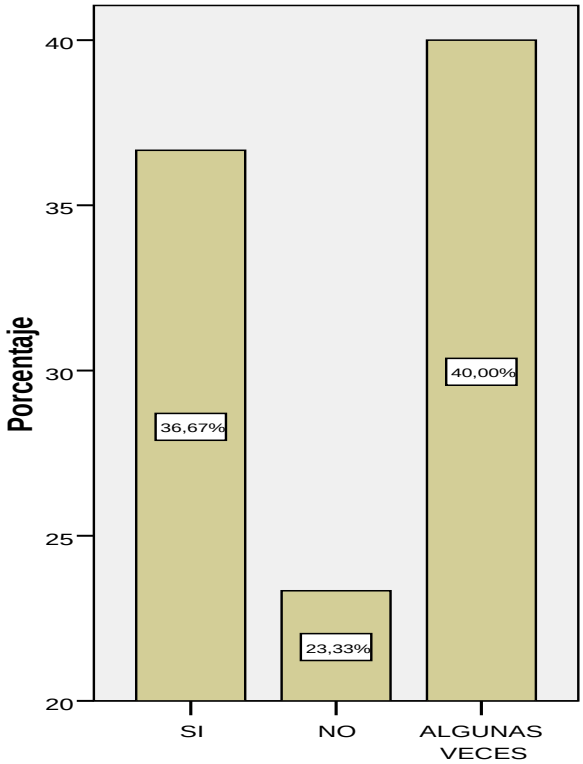
INDICADOR DE FRECUENCIA Nº 13

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	NO	15	46.9	50.0	50.0
	MÁS O MENOS	15	46.9	50.0	100.0
	Total	30	93.8	100.0	
Perdidos	Sistema	2	6.3		
Total		32	100.0		

Fuente: Elaboración propia

El 50% sostiene que actualmente la Escuela de Policía "**NO"** le brinda el apoyo tecnológico para poder optimizar los procesos académicos que le son asignados y el otro 50% afirma que "**algunas veces" (MÁS O MENOS)**.

FIGURA Nº 17: RECIBE CAPACITACIÓN RESPECTO AL PLAN DE EMERGENCIA



Fuente: Elaboración propia

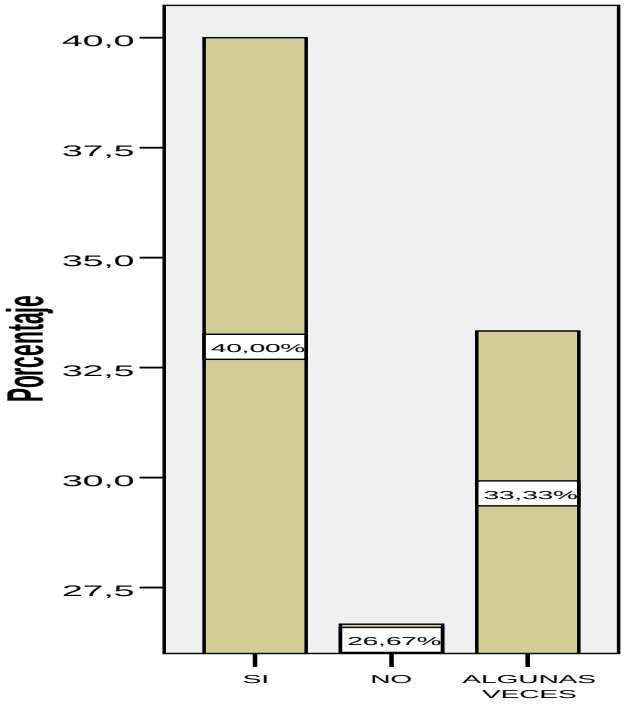
INDICADOR DE FRECUENCIA Nº 14

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	SI	11	34.4	36.7	36.7
	NO	7	21.9	23.3	60.0
	ALGUNAS VECES	12	37.5	40.0	100.0
	Total	30	93.8	100.0	
Perdidos	Sistema	2	6.3		
Total		32	100.0		

Fuente: Elaboración propia

El 40% sostiene que "**ALGUNAS VECES"** ha recibido capacitación respecto al PLAN DE EMERGENCIA, 36.67% que "**SIEMPRE"** recibe capacitación y el otro 23.33% que "**NUNCA"** ha recibido, ni tiene conocimiento que existe un Plan de Capacitación de Emergencia**.**

FIGURA Nº 18: HA TENIDO DIFICULTADES DE ÍNDOLE TECNOLÓGICO PARA REALIZAR EL REGISTRO DE INFORMACIÓN ACADÉMICA



Fuente: Elaboración propia

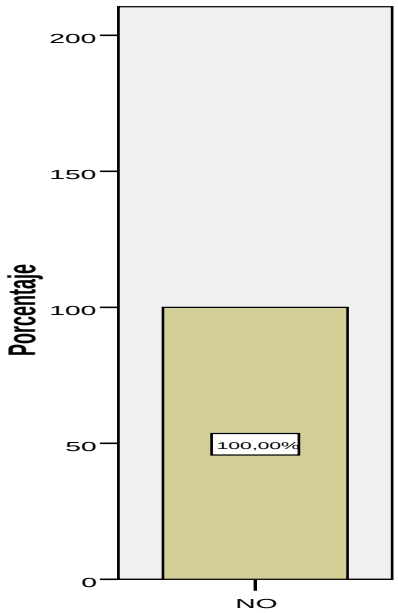
INDICADOR DE FRECUENCIA Nº 15

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
	SI	12	37.5	40.0	40.0
	NO	8	25.0	26.7	66.7
	ALGUNAS VECES	10	31.3	33.3	100.0
	Total	30	93.8	100.0	
Perdidos	Sistema	2	6.3		
Total		32	100.0		

Fuente: Elaboración propia

El 40% sostiene que "**SIEMPRE"** tienen dificultades de índole tecnológico para realizar el registro de información académica, el 33.33% que "**ALGUNAS VECES"** y el otro 26.67% afirma que "**NUNCA TIENE PROBLEMA".**

FIGURA Nº 19: EL SISTEMA ACADÉMICO ACTUAL LE HA PERMITIDO OPTIMIZAR LAS TAREAS COMÚNMENTE REALIZADAS.



Fuente: Elaboración propia

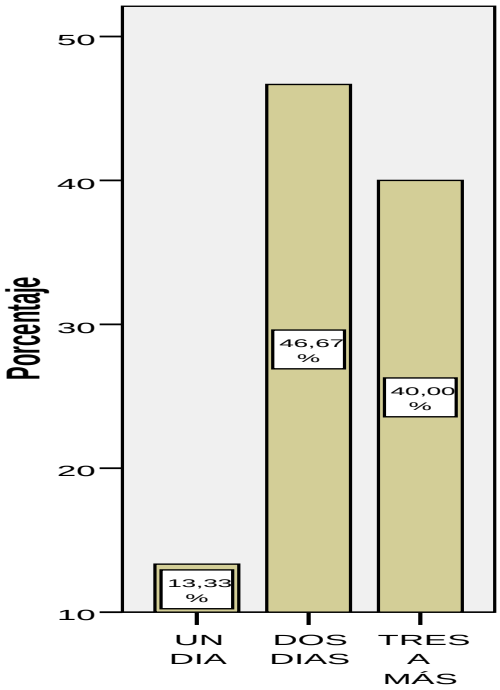
INDICADOR DE FRECUENCIA Nº 16

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	NO	30	93.8	100.0	100.0
Perdidos	Sistema	2	6.3		
Total		32	100.0		

Fuente: Elaboración propia

El 100% sostiene que actualmente el sistema académico "**NO"** les ha permitido optimizar las tareas comúnmente realizadas**.**

FIGURA Nº 20: CUAL ES EL TIEMPO PROMEDIO PARA EL RECOJO Y PROCESAMIENTO DE NOTAS AL FINALIZAR EL SEMESTRE ACADÉMICO.



Fuente: Elaboración propia

INDICADOR DE FRECUENCIA Nº 17

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	UN DIA	4	12.5	13.3	13.3
	DOS DIAS	14	43.8	46.7	60.0
	TRES A MÁS	12	37.5	40.0	100.0
	Total	30	93.8	100.0	
Perdidos	Sistema	2	6.3		
Total		32	100.0		

Fuente: Elaboración propia

El 46.67% sostiene que demora "**DOS DÍAS"** en el recojo y procesamiento de notas al finalizar el semestre académico, el 40% que "**TRES A MÁS DÍAS"** y sólo el 13.33% sostiene que después de "**UN DÍA"** de terminado el semestre.

4.2 ANÁLISIS E INTERPRETACIÓN

El análisis e interpretación de los datos responde a los Indicadores descritos en la Operacionalización de las Variables **(Tabla 03)** habiendo obtenido los siguientes resultados:

- **Este punto responde al Indicador *Registro de matrícula de los Alumnos,* para ello se analiza la siguiente tabla:**

Tabla 05. INDICADOR DE MATRICULA DE ALUMNOS POR DÍA

ACTIVIDAD	***Antes (cantidad)***	***Después (Cantidad)***	***Diferencia (Cantidad)***	***% de diferencia***
Cantidad de Alumnos matriculados por día.	36	50	14	38.9

Fuente: Elaboración propia

Los datos que se encuentran en la columna de ***"Antes"*** han sido obtenidos a través de las observaciones que se realizaron en la Institución Policial y de los datos del documentario académico encargado del registro de alumnos.

Los datos que se encuentran en la columna de **"Después"** han sido obtenidos a través de los reportes, luego de poner en práctica nuestro modelo de continuidad propuesto.

- **Este punto responde al Indicador *Registro de Notas de los Alumnos,* para ello se analiza la siguiente tabla:**

Tabla 06: INDICADOR DE REGISTRO DE NOTAS DE LOS ALUMNOS POR DÍA

ACTIVIDAD	*Antes (cantidad)*	*Después (Cantidad)*	*Diferencia (Cantidad)*	*% de diferencia*
Cantidad de Registros de notas digitalizados por día.	20	40	20	50.0

Fuente: Elaboración propia

Los datos que se encuentran en la columna de ***"Antes"*** han sido obtenidos a través de las observaciones que se realizaron en la Institución Policial y de la información del documentario académico encargado de la digitalización de los registro de notas de los alumnos.

Los datos que se encuentran en la columna de **"Después"** han sido obtenidos a través de los reportes, luego de poner en práctica nuestro modelo de continuidad propuesto.

- **Este punto responde al Indicador *Registro de datos del Personal*, para ello se analiza la siguiente tabla:**

Tabla Nº 07: INDICADOR DE REGISTRO DE DATOS DEL PERSONAL

ACTIVIDAD	*Antes (Horas)*	*Después (Horas)*	*Diferencia (Horas)*	*% de diferencia*
Tiempo empleado en el registro o actualización de los datos del Personal.	24	12	12	50.0

Fuente: Elaboración propia

Los datos que se encuentran en la columna de **"Antes"** han sido obtenidos a través de las observaciones que se realizaron en la Institución Policial y de la información del documentario de dicha área encargado del registro o actualización de los datos del Personal Policial tanto administrativos como Alumnos internados.

Los datos que se encuentran en la columna de **"Después"** han sido obtenidos a través de los reportes, luego de poner en práctica nuestro modelo de continuidad propuesto.

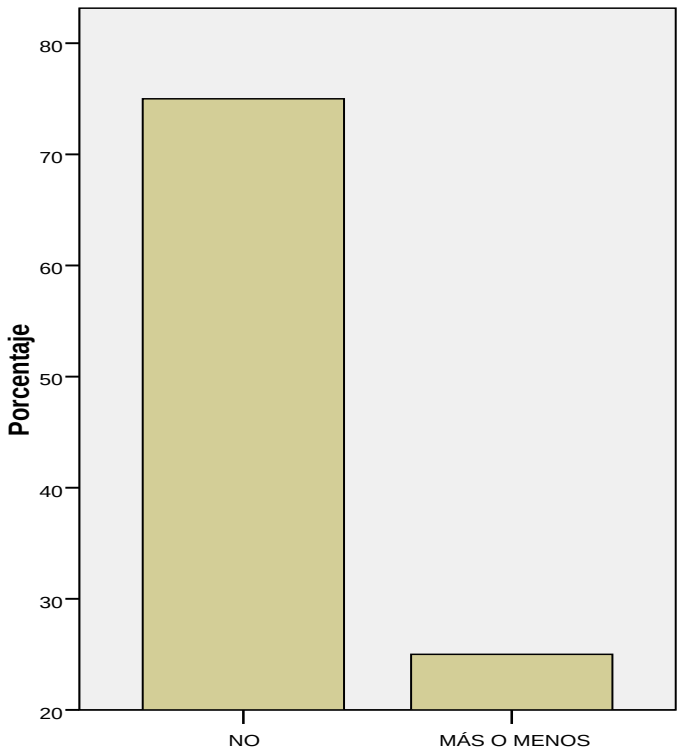
CAPITULO V. DISCUSIÓN DE RESULTADOS

5.1 DISCUSIÓN

5.1.1 EXISTENCIA E IMPORTANCIA DE UN MODELO DE CONTINUIDAD.

De acuerdo a los resultados de aplicación del instrumento de recolección de datos aplicados a la Población objetiva conformada por 22 Efectivos Policiales, el 75% de los encuestados sostiene que "NO" tiene conocimiento de algún Plan de Contingencia de la Institución Policial y el 25% menciona que MÁS O MENOS (Ver Figura N° 33).

FIGURA Nº 33: PREGUNTA ¿TIENE CONOCIMIENTO DE ALGÚN El PLAN DE CONTINGENCIA DE LA INSTITUCIÓN POLICIAL?



FUENTE: Elaboración propia

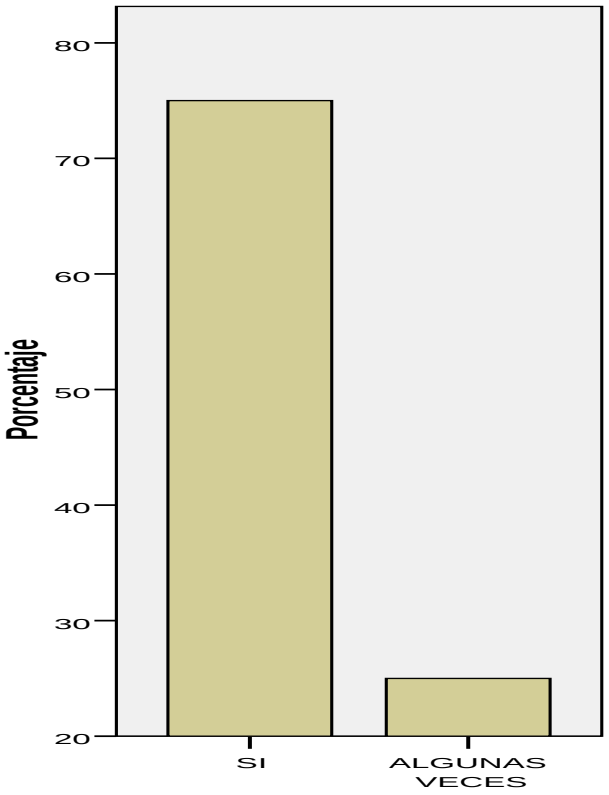
INDICADOR DE FRECUENCIA Nº 01

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
NO	3	75.0	75.0	75.0
MÁS O MENOS	1	25.0	25.0	100.0
Total	4	100.0	100.0	

FUENTE: Elaboración propia

El 75% de los encuestados sostiene que **"SI"** es muy importante que exista un Modelo de Continuidad en la Unidad Académica de Pregrado de la Escuela Técnica de Policía y el otro 25% afirma que sólo ALGUNAS VECES sería necesario (Ver Figura N° 34).

FIGURA Nº 34: DIFICULTAD EN EL REGISTRO DE LOS DATOS ACADÉMICOS



Fuente: Elaboración propia

INDICADOR DE FRECUENCIA Nº 04

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	SI	3	75.0	75.0	75.0
	ALGUNAS VECES	1	25.0	25.0	100.0
	Total	4	100.0	100.0	

Fuente: Elaboración propia

5.1.2 BENEFICIOS EN LA IMPLEMENTACIÓN DE LA PROPUESTA

Los beneficios que tendría esta propuesta, después de evaluar cada uno de los riesgos, se ven reflejados en el cuarto capítulo en la parte correspondiente al ***ANÁLISIS E INTERPRETACIÓN DE LOS DATOS***, donde la adopción de la propuesta por parte de la Institución Policial ayudaría a optimizar los procesos académicos realizados minimizando las pérdidas ante el impacto de un siniestro y sus consecuencias que este pudiese ocasionar.

En el factor operativo se podrían prevenir grandes pérdidas en cuanto a la paralización productiva, donde por cada paralización de un proceso se podrían generar pérdidas irreparables en cuanto a la imagen de la institución y de lo que representa para el bienestar social y satisfacción laboral por parte de los clientes (Alumnos PNP).

5.2 CONCLUSIONES

- Se realizó la personalización y análisis de los posibles peligros y vulnerabilidades que afectarían los Procesos formativos de las Unidades Académicas de Pregrado, basado en el análisis FODA, análisis de PESTEL y otros, adicional a esto se ha analizado la estructura de la empresa; los procesos y servicios que la Institución Policial ofrece, además de ello se ha realizado la identificación y análisis de las funciones críticas y servicios de TI, identificando su vulnerabilidades y las respuestas que se puede dar ante diversos escenarios propuestos.

- Se realizó un estudio pormenorizado de la problemática actual y se percibe que la Institución Policial, a pesar de contar con políticas establecidas se encuentra frágil en cuanto a recuperación tecnológica ante siniestros que pongan en peligro el normal desarrollo de sus procesos académicos.

- Del estudio desarrollado se ha determinado que los riesgos que podrían generar un mayor impacto en la continuidad de sus procesos en el caso que se suscitaran serían los un incendio, falla de la red informática y riesgos operacionales.

- Se ha tomado como base de estudio la norma ISO 22301, un estándar internacional que ha permitido establecer una propuesta robusta, ágil y practica adecuada a los riesgos y vulnerabilidades que se identificaron en la institución, así mismo se plasma el aporte que los integrantes de la institución proporcionan en el desarrollo de la propuesta de continuidad.

5.3 RECOMENDACIONES

- Para optimizar los procesos que actúan en la gestión Académica que se generan en la institución Policial se recomienda implementar el modelo de continuidad de negocio y buenas prácticas propuesto, ya que proporciona una visión global que puede ser replicada en las diferentes Escuelas de la Policía a nivel nacional.

- Se recomienda implementar como política de comando capacitaciones sobre la ejecución y difusión de los planes de contingencia vigentes y los que se puedan desarrollar a futuro.

- Se recomienda que el personal delegado de la dirección del Modelo de Continuidad establezca y defina las personas que conformarán el comité de crisis, así también establecer la ejecución de una política de comando Policial para la actualización del plan de continuidad y un cronograma de las pruebas del mismo.

REFERENCIAS

ASSOCIATION, I.-L. (12 de Enero de 2014). *ISACA.ORG*. Obtenido de ISACA.ORG: https://www.isaca.org

BUSINESS CONTINUITY INSTITUTE. (2010). *GOOD PRACTICE GUIDELINES 2010*. REINO UNIDO: BCI.

CASTRO MARQUINA, L. D. (2013). *DISEÑO DE UN SISTEMA DE GESTIÓN DE CONTINUIDAD DE NEGOCIOS (SGCN) PARA LA RENIEC BAJO LA ÓPTICA DE LA NORMA ISO/IEC 22301*. LIMA: PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ.

CNB - INDECOPI. (2008). *NTP-ISO/IEC 27001:2008. EDI TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN. REQUISITOS.* LIMA.

COMPUTERWORLD. (27 de DICIEMBRE de 2007). *COMPUTERWORLD FROM IDG*. Recuperado el 12 de OCTUBRE de 2018, de COMPUTERWORLD FROM IDG: http://www.computerworld.es/archive/citi-firma-con-ibm-espana-un-contrato-de-servicios-de-continuidad-y-recuperacion-de-negocio

CONGRESO DE LA REPÚBLICA. (2005). *LEY N° 28551 - LEY QUE ESTABLECE LA OBLIGACIÓN DE ELABORAR Y PRESENTAR PLANES DE CONTINGENCIA.* LIMA.

CRTC - INDECOPI. (2007). *NTP - ISO/IEC 17799:2007. EDI TECNOLOGÍA DE LA INFORMACIÓN. CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.* LIMA.

CUEVA MURILLO, M. F. (2015). *DISEÑO DE UN SISTEMA DE GESTIÓN DE CONTINUIDAD DE NEGOCIOS PARA UNA ENTIDAD ESTATAL DE SALUD BAJO LA ÓPTICA DE LA ISO/IEC 22301:2012*. LIMA: PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ.

DELGADO CONCHA, K. G. (2015). *DISEÑO Y PROPUESTA DE UNA METODOLOGÍA PARA LA IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE CONTINUIDAD DEL NEGOCIO, BASADO EN LA NORMA ISO/IEC 22301:2012.* AREQUIPA: UNIVERSIDAD CATÓLICA DE SANTA MARÍA.

FUNDACIÓN WIKIMEDIA, I. (20 de MARZO de 2018). *WIKIPEDIA*. Recuperado el 12 de OCTUBRE de 2018, de WIKIPEDIA: https://es.wikipedia.org/wiki/Plan_de_continuidad_del_negocio

GONZÁLES VILLALOBOS, J. A. (2015). *ELABORACIÓN DE UN PLAN DE AUDITORÍA PARA EVALUACIÓN DE CUMPLIMIENTO EN SISTEMAS*

PARA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO BASADO EN LA NORMATIVA ISO 22301. SAN JOSÉ: UNIVERSIDAD DE COSTA RICA.

GROUP, B. (2008). *Code of practice (BS 25777: 2008).* Information and communications technology continuity management.

HERNÁNDEZ, S. R., FERNÁNDEZ, C. C., & BAPTISTA, L. M. (2010). *METODOLOGÍA DE LA INVESTIGACIÓN* (QUINTA ed.). (J. MARES CHACON, Ed.) MEXICO: Mc. Graw-Hill Companies. Inc.

INCONTEC ISO 22301:2012, I. (2012). *ISO 22301:2012.* CONTINUIDAD DE NEGOCIO SISTEMAS DE GESTION DE CONTINUIDAD DE NEGOCIO. NORMAS TECNICAS Y CERTIFICACION INCONTEC.

INSTITUTION, B. T. (15 de FEBRERO de 2014). *BSIGROUP*. Obtenido de BSIGROUP: http://www.bsigroup.com/en-GB/iso-22301-business-continuity/

INSTITUTO NACIONAL DE ESTADISTICA E INFORMÁTICA. (01 de DICIEMBRE de 2016). *INEI*. Obtenido de INEI: www.inei.gob.pe

ISACA. (2012). *CISM Review Manual 2013.* Illinois, USA.

ISACA. (2013). *CRISC Review Manual 2014.* Illinois, USA.

LEON LOPEZ, D. (2008). PLAN DE CONTINGENCIA PARA EL ARCHIVO DE LA UNIVERSIDAD DE LA SALLE COMO PARTE DE LA IMPLANTACION DEL SISTEMA INTEGRADO DE CONSERVACIÓN. *INFORMATION SCIENCE, 4*(1), 85-90.

NORMA ISO 27001. (2005). *INTERNATIONAL STANDARD ISO/IEC 27001*. GINEBRA: Primera Edición.

PEÑA CASTRO, L. A. (2015). *GUIA METODOLÓGICA PARA ELABORAR UN BCP EN ENTIDADES DEL ESTADO.* BOGOTA: ESCUELA COLOMBIANA DE INGENIERÍA JULIO GARAVITO.

RODRIGUEZ LACHE, E. (2012). *Plan de Continuidad BS-25999.* TUNJA: Universidad de Boyacá, Facultad de Ingeniería de Sistemas.

SANCHEZ SILVA, M. (2005). *INTRODUCCIÓN A LA CONFIABILIDAD Y EVALUACIÓN DE RIESGOS. TEORIA Y APLICACIONES EN INGENIERÍA.* BOGOTA: UNIVERSIDAD DE LOS ANDES.

SARABIA ZAPATA, A. V. (2015). *MODELO DE GESTIÓN DE CONTINUIDAD DE INFRAESTRUCTURA TECNOLÓGICA PARA LA OPERACIÓN DE SERVICIOS DE TI EN EMPRESAS FINANCIERAS SOBRE LA BASE DE LAS NORMAS ISO 22301 E ISO 27001. (TESIS DE MAESTRÍA).* ECUADOR: UNIVERSIDAD DE LAS AMÉRICAS.

Serralde, J. (12 de ENERO de 2006). *TopManagement*. Recuperado el 16 de FEBRERO de 2015, de TopManagement: http://www.topmanagement.com.mx/modules.php?name=Noticias&file=show&clave=52643

TUPIA ANTICONA, M. F. (2011). *PRINCIPIOS DE AUDITORÍA Y CONTROL DE SISTEMAS DE INFORMACIÓN* (SEGUNDA ed.). LIMA, LIMA, PERÚ: TUPIA CONSULTORES Y AUDITORES.

VARGAS CORDERO, Z. R. (2009). LA INVESTIGACIÓN APLICADA: UNA FORMA DE CONOCER LAS REALIDADES CON EVIDENCIA CIENTÍFICA. *REVISTA EDUCACIÓN*, 165.

ZAWADA, B. (2014). The practical application of ISO 22301. *Journal of Business Continuity & Emergency Planning, 8*, 83-90.

ZIMMERMAN, A., & BAUERLEIN, V. (12 de SETIEMBRE de 2005). *TARINGA*. Recuperado el 12 de OCTUBRE de 2018, de TARINGA: https://www.taringa.net/posts/noticias/15610/EE-UU-estaria-mejor-gobernado-por-Wal-Mart.html

ANEXO N° 01

GUIA DE OBSERVACIÓN PARA APRECIACION DE LA REALIDAD ACTUAL DEL LA UNIDAD ACADÉMICA DE PREGRADO RESPECTO A LA CONTINUIDAD DE NEGOCIO Y BUENAS PRÁCTICAS.

Esta guía está dirigida al Personal Policial que labora en la Unidad Académica de la Escuela Técnica Superior de Policía – Sede Puente Piedra y tiene por finalidad la recolección de información para poder apreciar y evaluar la realidad actual de dicha institución respecto a su continuidad de negocio.

A. Datos Generales:

1. Efectivo Policial Evaluado
2. Cargo que ocupa
3. Fecha de Evaluación
4. Marcar:

Pretest ☐ Postest ☐

B. Indicadores:

De acuerdo a la escala de calificación, por favor asigne en el cuadro a la derecha de cada ítem la calificación que considere más adecuada.

- Escala de calificación es la siguiente:

1	=	Nunca
2	=	Ocasionalmente
3	=	Habitualmente
4	=	Casi siempre
5	=	Siempre

Ítem	Continuidad Negocio y Buenas Prácticas	1	2	3	4	5
1	Recibe capacitación sobre el Plan de contingencia documentado de la Institución.					
2	Realiza pruebas documentadas del Plan de Contingencia para garantizar su adecuado funcionamiento.					
3	Participa de las pruebas documentadas del Plan de contingencia para garantizar su adecuado funcionamiento					
4	Recibe capacitación sobre el Plan de contingencia tecnológico					
5	Recibe capacitación sobre el Plan de contingencias de traslado de la operación.					
6	Tiene conocimiento si existe un centro de cómputo alterno y las características.					
7	Utiliza enlaces de comunicación telefónicos alternos o redundantes					
8	Tiene conocimiento de los sitios alternos para operar ante fallas de infraestructura física o de cualquier otra índole.					
9	Ha tenido interrupción de la energía eléctrica últimamente.					
10	Ha tenido interrupción del servicio de internet.					
11	Ha tenido dificultades o interrupción para poder acceder al Sistema Académico online.					
12	Tiene conocimiento del Plan de Emergencias documentado.					
13	Recibe capacitación respecto al plan de Emergencia.					
14	Ha participado de simulacros y pruebas del plan de emergencias.					
15	Recibe capacitación o tiene conocimiento del esquema de retención y transferencia de conocimiento e información para continuar las operaciones académicas ante novedades del personal Policial respecto a retiros, incapacidad o similares.					
16	A su parecer el sistema académico actual le ha permitido optimizar las tareas comúnmente realizadas.					
17	Tiene dificultades tecnológicas para atender un reporte solicitado por la superioridad.					
18	El equipamiento tecnológico asignado le permite tener su base de datos académica referente a la información básica de los Alumnos internados y los docentes actualizada.					
19	Ha tenido dificultades de índole tecnológica para realizar el registro de información académica.					
20	Tiene dificultades tecnológicas para el recojo y procesamiento de notas al finalizar el semestre académico.					

ANEXO 02.

DESARROLLO DE LA PROPUESTA

1. DESCRIPCIÓN DE LA INSTITUCIÓN POLICIAL

La "Escuela Técnica de la Policía Nacional del Perú", tiene la misión de formar Suboficiales PNP a través de un proceso educativo exhaustivo de acuerdo al perfil académico y profesional; desarrollando competencias cognitivas, aptitudes, habilidades y destrezas que sustentadas en principios axiológicos humanistas, permitan poner a disposición de la sociedad a un profesional competente para cumplir la función policial.

Figura N° 21. ESCUELA TÉCNICA DE POLICIA – SEDE PUENTE PIEDRA

FUENTE: ESCUELA TÉCNICA DE POLICÍA

Figura N° 22. FORMACIÓN DE LA ESCUELA TÉCNICA DE POLICIA

FUENTE: ESCUELA TÉCNICA DE POLICÍA

a. VISIÓN

Ser en el año 2020 debe ser un centro de formación policial, eje de todos los centros de formación Policial a Nivel Nacional, que dependiendo de la Dirección de Instrucción y Doctrina Policial, imparta una eficiente formación profesional y humanística de los futuros suboficiales PNP, a fin de potenciar la seguridad y el orden interno en la región".

b. MISIÓN

Constituye el Primer Nivel del Sistema Educativo Policial, formar integralmente a los futuros Sub-Oficiales de Policía, de acuerdo al perfil educativo y técnico profesional diseñado".

"La nueva concepción filosófica de la educación policial, releva una formación humanista, científica y tecnológica, sustentada en principios y valores, donde se enfatiza el acatamiento irrestricto de los Derechos Humanos, que coadyuve al desarrollo integral de la persona humana".

c. OBJETIVO

Formar Profesionales – Suboficiales 3ra íntegros, dinámicos e inteligentes con sólidos principios éticos e integridad moral, Respeto por las personas e instituciones, Capacidad para influir positivamente en la comunidad.

d. OBJETIVOS ESTRATEGICOS

Tabla N° 08. OBEJTIVOS ESTRATEGICOS

NIVEL ESTRATÉGICO	DESCRIPCIÓN
Financiero	Mantener una sólida capacidad financiera con el propósito de aumentar la rentabilidad de la institución.
Comercial y Ventas	Mejorar la experiencia del cliente. Mejorar el servicio de atención al cliente.
Infraestructura, Organización, Procesos	Cumplir con los estándares de seguridad y asegurar la disponibilidad y continuidad de negocio. Lograr eficiencia y excelencia operativa.
Personal	Gestionar el capital humano, desarrollando competencias en nuestros colaboradores. Fortalecer las competencias del capital humano

FUENTE: ELABORACIÓN PROPIA

e. IDENTIFICACIÓN DEL "CORE BUSSINESS DE LA INSTITUCIÓN POLICIAL".

Si bien cada proceso de la institución Policial es fundamental para el cumplimiento de su objetivo principal, pero se ha tenido a bien elegir para la presente investigación los procesos formativos de la Unidades Académicas de Pregrado.

f. CLIENTES

La Escuela Técnica de la Policía tiene clientes que están orientados a todos los sectores de la población, que logren obtener una vacante en el proceso de admisión y cumplan con los siguientes requisitos

- Estar soltero(a), y no tener hijos.

- Ser peruano por nacimiento.

- Estudios de educación secundaria concluidos.

- Cumplir con la talla mínima y peso establecido para cada proceso de admisión.

- Tener entre 18 y 24 años de edad.

g. PROBLEMAS

La Escuela Técnica de Policía registra la siguiente problemática:

- **No cuenta con políticas definidas de continuidad de negocios :**

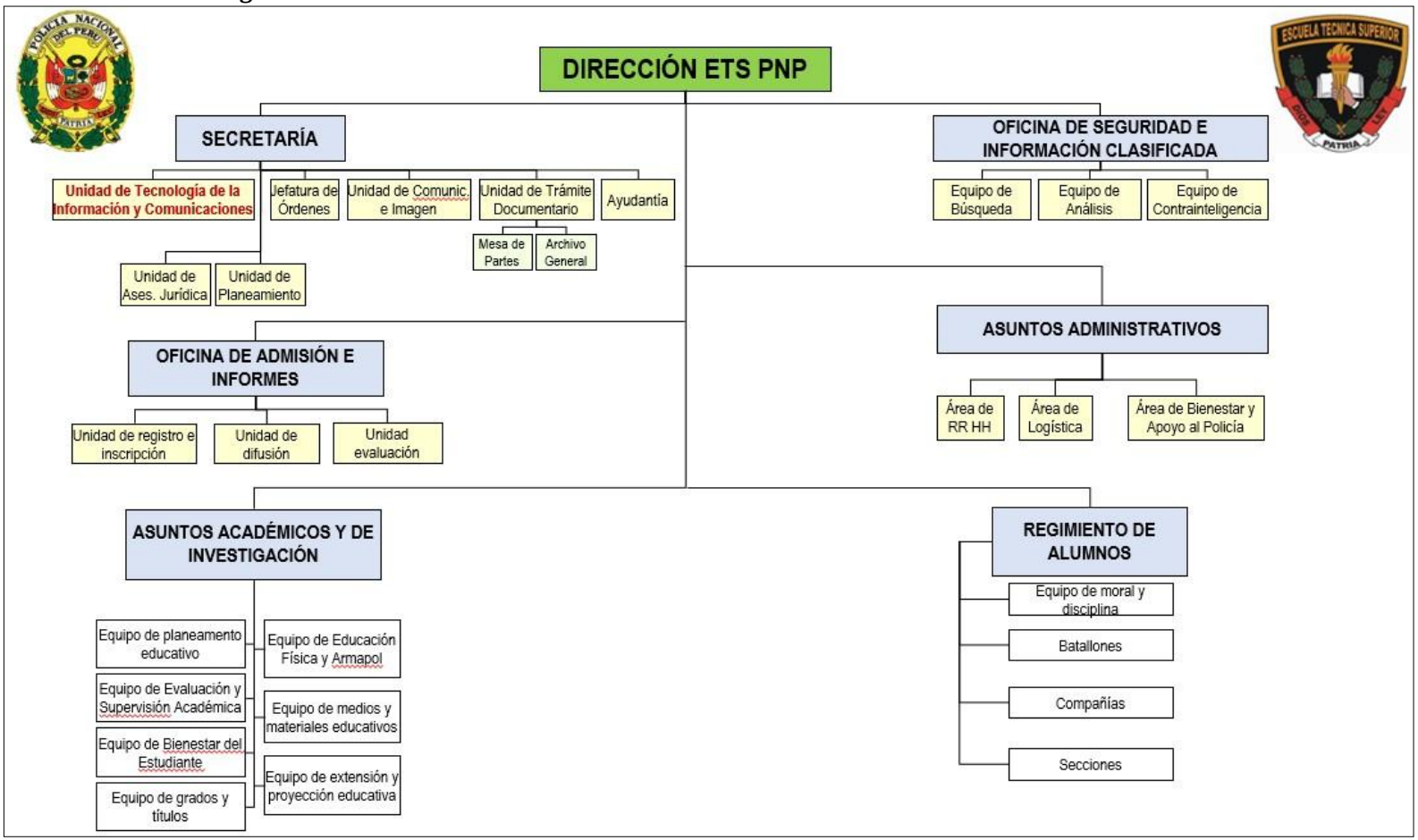
  En la Unidad Académica de Pregrado de la Escuela Técnica de la Policía, se debe implantar un Modelo de Continuidad, incorporando "estrategias, planes de recuperación, planes de continuidad y plan de gestión de crisis y emergencia", para lo cual es vital conseguir el apoyo del Comando de la Institución.

- **No cuenta con medios de control:**

  La Escuela de Policía se halla frágil ante una calamidad o incidencia, es por ello que, un "modelo de continuidad" están liadas a la gestión de seguridad de información y uno de sus principales objetivos es el de asegurar la disponibilidad de los procesos críticos y la información según lo requiera la Unidad Académica de Pregrado de la Escuela Técnica de la Policía.

h. ESTRUCTURA ORGANIZACIONAL

Figura N° 23. ESCUELA TECNICA SUPERIOR POLICIA – SEDE PUENTE PIEDRA



Fuente : Escuela Técnica de Policía

i. ANÁLISIS FODA

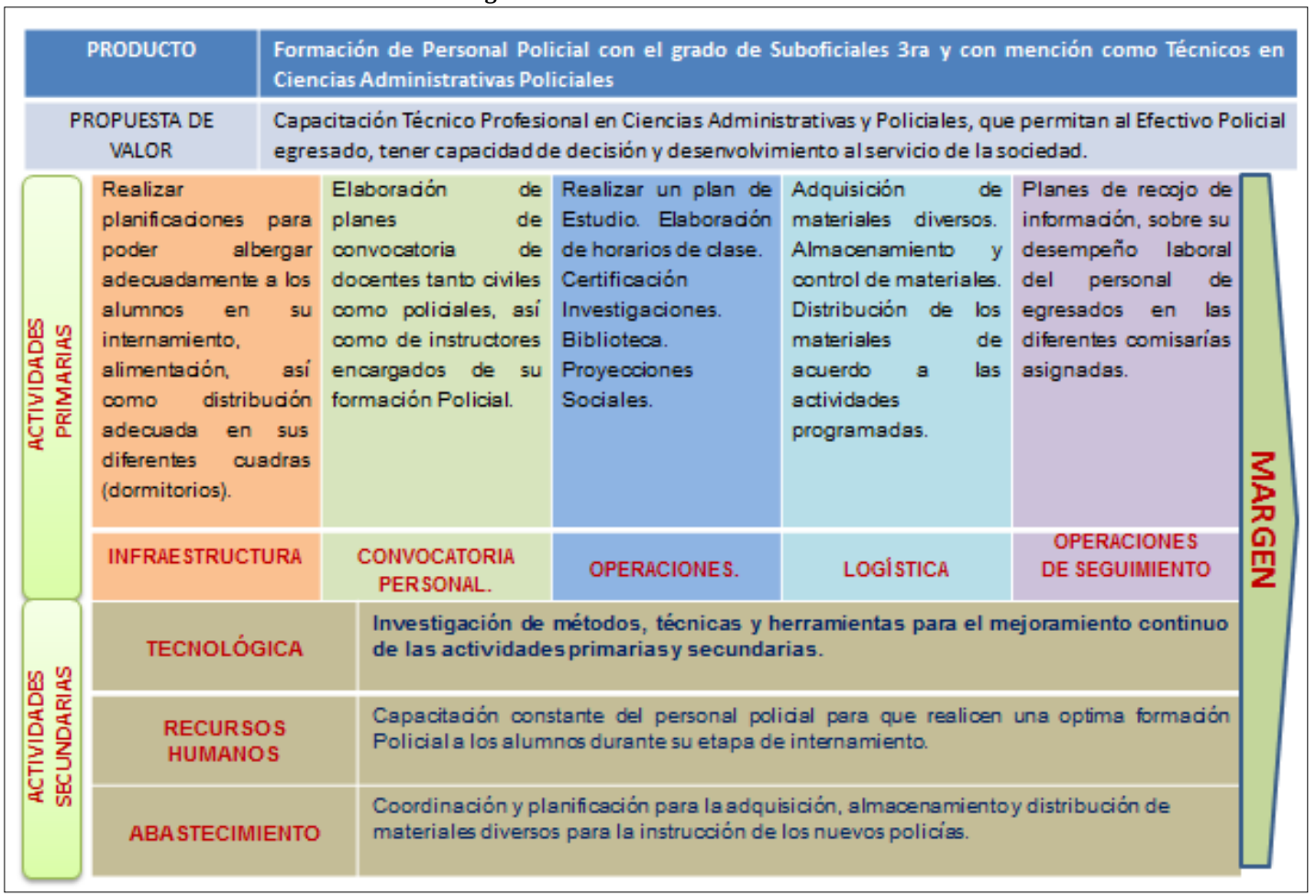
Figura N° 24 ANÁLISIS FODA

ANÁLISIS FODA		FORTALEZAS	DEBILIDADES
		F1. Contar con nuevas tecnologías dentro del campo educativo. F2. Contar con Instructores capacitados en la formación Policial. F3. Ser la única escuela de formación Técnica Policial (varones) dentro de la región. F4. Brindar estabilidad laboral y título a nombre de la nación dentro de la carrera ciencias administrativas. F5. Contar con personal técnico para el manejo de las nuevas tecnologías. F6. Egresados con capacidades y habilidades acorde con las necesidades de la población actual.	D1 Limitado presupuesto económico para mejoras continuas. D2 Deficiente marketing respecto a la forma de ingreso y beneficios que brinda la Escuela Técnica de Policía. D3 Falta de comunicación entre las diferentes áreas de trabajo en tiempo real. D4 Limitada infraestructura para cumplir las necesidades de vivienda, alimentación y educación. D5 Falta de políticas de seguridad respecto al tratamiento de la información. D6 No cuenta con un software para la administración de la información. D7 Conflicto entre el personal por desconocimiento del organigrama funcional. D8 No cumplir con el pago a proveedores en los plazos establecidos.
OPORTUNIDAD	O1 El apoyo del gobierno regional y/o Local. O2 Creciente demanda por personal Policial O3 Apoyo del gobierno central. O4 Demanda de estabilidad laboral. O5 Apoyo de entidades privadas.	FO FO1 Apoyo del gobierno Central y de las entidades privadas para realizar cursos de capacitación en el exterior para instructores de la Escuela de Policía. FO2 Apoyo del gobierno regional y/o local para realizar cursos de perfeccionamiento para el personal técnico de la Escuela de Policía. **FO3** Apoyo del gobierno central y regional para realizar convenios para convalidación de cursos en universidades de la región. FO4 Apoyo de las entidades privadas adquirir nuevas tecnologías para todas las necesidades dentro de las funciones de la organización.	DO DO1 Lograr convenios de cooperación con entidades privadas para el financiamiento de mejoras continuas. DO2 Con el apoyo del gobierno regional y local realizar una estrategia de marketing dentro de toda la región Lima. DO3 Con el apoyo de las entidades privadas gestionar cursos de capacitación en administración de personal dirigido a jefes y trabajadores de la Escuela. DO4 Con el apoyo del gobierno regional y empresa privada realizar convenios para adquirir personal calificado y tecnología adecuada para el diseño e implementación de un sistema de información gerencial.
AMENAZAS	A1 Clausura de las Escuelas de Formación Policial por falta de presupuesto. A2 Privatización de la institución Policial. A3 Desconfianza de los padres sobre el trato y formación policial de sus hijos. A4 Aumento del número de instituciones que brindan servicio de educación. A5 Ausencia de proveedores por incumplimiento en los pagos.	FA FA1 Desarrollar estrategias de publicidad para mostrar a la población los beneficios que brinda la institución (Estabilidad laboral al término de la formación policial), la calidad de enseñanza durante su formación y el personal altamente calificado para la formación de los alumnos. FA2 Ser la única escuela de formación Técnico Policial (Varones) dentro de la Región Lima por tanto cerrarla provocaría escases de efectivos policiales y aumento de la delincuencia, además de ser una opción de trabajo estable dentro de la región. FA3 Los egresados de la Escuela de policía durante su desenvolvimiento laboral muestran a la población la buena formación policial que han recibido durante su etapa de internamiento.	DA DA1 Implementar un área de marketing, con la finalidad de realizar estrategias continuas de publicidad para aumentar el número de postulantes y el ingreso económico que esto genera, para así contar con un mayor presupuesto económico. DA2 Implementar reuniones periódicas informativas entre padres de familia, estudiantes e institución. DA3 Realizar cronograma de pagos a los proveedores por prioridad

Fuente : Escuela Técnica de Policía

j. CADENA DE VALOR

Figura N° 25. CADENA DE VALOR



Fuente: Escuela Técnica de Policía.

2. DESCRIPCIÓN DE LA "UNIDAD DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIONES" (UNITIC) DE LA ESCUELA TÉCNICA DE POLICIA (ETS-PNP) – SEDE PUENTE PIEDRA.

a. Ubicación de la UNITIC de la ETS-PNP sede puente piedra.

La UNITIC está ubicada en el interior de las instalaciones de la Escuela Técnica de Policial, sito Auxiliar Panamericana Norte Km 26 en Distrito de Puente Piedra – Lima, desde donde tiene bajo su mando al Departamento de Administración de Centros de Datos y el Departamento de Ingeniería de Soporte Técnico, los cuales tienen el siguiente esquema:

Departamento de administración de centros de datos.

- Sección de Administración redes y base datos.
- Sección de operaciones.
- Sección de Ciberseguridad.
- Sección Administración de usuarios y transferencia de datos.

Departamento de ingeniería de soporte técnico.

- Sección mantenimiento de redes
- Sección laboratorio1. Mantenimiento y reparación de PC's
- Sección laboratorio 2. Mantenimiento y reparación impresoras y monitores.

Entre los servicios que brinda a la Institución Policial la UNITIC tenemos:

- Intranet.
- Mantenimiento de equipos (Hardware y Software)

- Administración de base datos.
- Soporte a usuarios.
- Asignación y administración de usuarios para el acceso a sistemas Policiales.
- Soporte en los sistemas de información utilizados en la formación académica.

b. Objetivos y Funciones

La UNITIC órgano de apoyo técnico, administra los sistemas informáticos y brinda apoyo técnico especializado a todas las áreas operativas y administrativas de la Escuela Técnica de Policía.

Sus Funciones son las siguientes:

- Mantener actualizados y operativos los sistemas y aplicativos usados en la Escuela Técnica de Policía.
- Brindar mantenimiento y soporte informático a los sistemas de información, aplicativos y el portal web a su cargo.
- Administrar, garantizar y mantener los servicios de correo electrónico y Intranet.
- Establecer, implementar y activar mecanismos de auditoría y control y otros.

c. Estructura Funcional de la UNITIC.

En la Figura N° 27 se muestra la Estructura Funcional Actual de la UNITIC PNP que está contenida en la Estructura Organizacional de la Escuela Técnica de Policía.

FIGURA N° 26. "ESTRUCTURA FUNCIONAL DE LA UNITIC"

Fuente: Escuela Técnica de Policía

3. DESCRIPCIÓN DEL PROBLEMA Y NECESIDAD DE CONTINUIDAD.

a. Descripción del Problema.

La Escuela Técnica Superior de Policía – Sede Puente Piedra es una institución educativa, tiene como objeto la de formar Sub Oficiales de Policía, los mismos que luego de un periodo de internamiento egresan para ejercer la función Policial al servicio de la sociedad; por lo tanto al tratarse de una Institución en la cual la reserva y protección de la información procesada y almacenada respecto a los Procesos formativos de los Alumnos y egresados obtenidas durante su periodo de formación es vital para una apropiada toma de disposiciones por parte del Comando de la Institución Policial, motivo por el cual dicha información no puede ser perdida, modificada o alterada por terceros y tampoco existir demora excesiva en su procesamiento, es aquí donde radica el problema considerando la infraestructura que posee la Institución actualmente.

La Escuela Técnica de Policía cuenta con un centro de datos a cargo de la UNITIC dentro de las instalaciones del complejo Policial antes mencionado donde se encuentra alojados los servidores, actualmente no se cuenta con una contingencia tecnológica que permita continuar con la normal operación de los servicios y a su vez permita obtener la información procesada y almacenada en los servidores de archivo en caso de ocurrencia de incidentes o catástrofes que inhabiliten el del actual centro de datos.

b. Necesidad de Continuidad.

La Escuela Técnica de Policía tiene la necesidad de continuar con sus labores aun presentándose alguna catástrofe teniendo en cuenta que la imagen que presta como una institución de formación Policial debe mantenerse y esta se vería seriamente afectada si sus actividades se suspenden con algún evento desafortunado que ocurra a unidad de tecnología considerando que es el lugar donde radican los servidores donde es almacenada la información de los alumnos, docentes, egresados, personal administrativo y otros, y si la información es alterada o se pierde se asumirá deficiencias en los procesos formativos de los alumnos internados y con ellos que éstos tengas falencias en su formación y accionar policial al egresar los cual traerá como consecuencia que la ciudadanía tenga una percepción negativa sobre los miembros de la Policía en su conjunto, y a su vez un serio cuestionamiento sobre la formación Profesional Policial que reciben durante su periodo de internamiento y capacitación.

Como toda institución, la Escuela Técnica de Policía, aun en medio de una catástrofe debe reanudar sus procesos formativos académicos lo ante posible y es ahí donde entra la "**Propuesta de un Modelo de Continuidad",** determinando los procedimientos claves para seguir brindando una óptima formación profesional Policial.

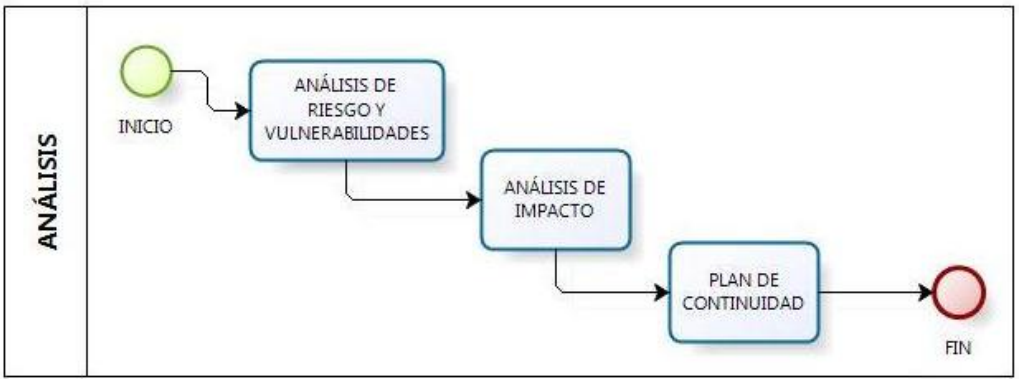
4. PROPUESTA DEL PLAN DE CONTINUIDAD.

En este capítulo se describirá propiamente la propuesta, analizando el impacto del daño que pueden causar los puntos mencionados en la matriz de riesgos que se

detallará enfatizando el grado de afectación mediante un valor determinado por la multiplicación de los valores de severidad y de vulnerabilidad de cada uno de ellos.

Se detallara el plan describiendo los planes para salvaguardar la institución como tal de dichos riesgos; el plan completo se conformará de todos los proyectos / planes pequeños que se enfocan en cubrir los procesos formativos relevantes de la unidad académica de pregrado, enunciando proveedores que pueden facilitar cumplir con los objetivos de la propuesta. En la Figura N° 27 se muestra los procesos a seguir durante el desarrollo de la propuesta.

Figura N° 27. DIAGRAMA DEL DESARROLLO DEL PLAN DE CONTINUIDAD



Elaboración: Propia

a. Liderazgo

El "Plan de continuidad" se encuentra liderado por el Director de la Escuela de Policía y el Jefe de la UNITIC.

Actualmente la Escuela de Policía cuenta con brigadas en el caso de tener que evacuar el edificio, estas brigadas se encuentran capacitadas en cómo proceder en caso de enfrentar algún desastre natural o un conato de

incendio. Las brigadas entran en acción al momento de presentarse alguno de estos incidentes, o al ser prevenidos por las alarmas sonoras que se encuentran ubicadas en cada uno de los ambientes estratégicamente distribuidos del recinto Policial.

Así mismo la Escuela de Policía no ha establecido un Comité de Riesgos ni ha designado el personal que conformará el mismo. Este comité será el encargado de gestionar las acciones a tomarse en caso de enfrentarse a alguno de los percances o siniestros inminentes a los que se puede enfrentar la institución.

b. Política de Continuidad del Negocio.

El objetivo clave de realizar el "plan de continuidad de negocio", es de seguir con las diligencias programadas sin interrupción de cualquier índole o en su defecto que exista un mínimo tiempo de recuperación de tal manera que no afecte a gran escala, esto es realizar planes y preparativos para enfrentar el incidente que se suscite y que atente contra las actividades académicas normales de la institución.

c. Objetivo

La premisa de crear la propuesta para la protección y seguridad tanto de los activos de la institución como de los recursos humanos.

d. Respaldo de Información

El personal Policial y/o civil que labora en la institución, deben realizar los respaldos de información de manera frecuente, sea de manera automática o

manual. Esto se definirá por áreas, o en su defecto con soporte del personal tecnológico.

e. Roles y Responsabilidades

Las tareas por cada acción de recuperación deberán estar segregadas asignando los roles correspondientes al personal idóneo para cumplir con las responsabilidades del cargo a él/ella impuestos para salvaguardar sea un activo o el recurso humano.

Cada rol debe tener relación con su capacidad de respuesta ante el evento y/o incidente y de acuerdo a los conocimientos que pueda tener respecto a una respuesta ante las situaciones de emergencia.

f. Pruebas.

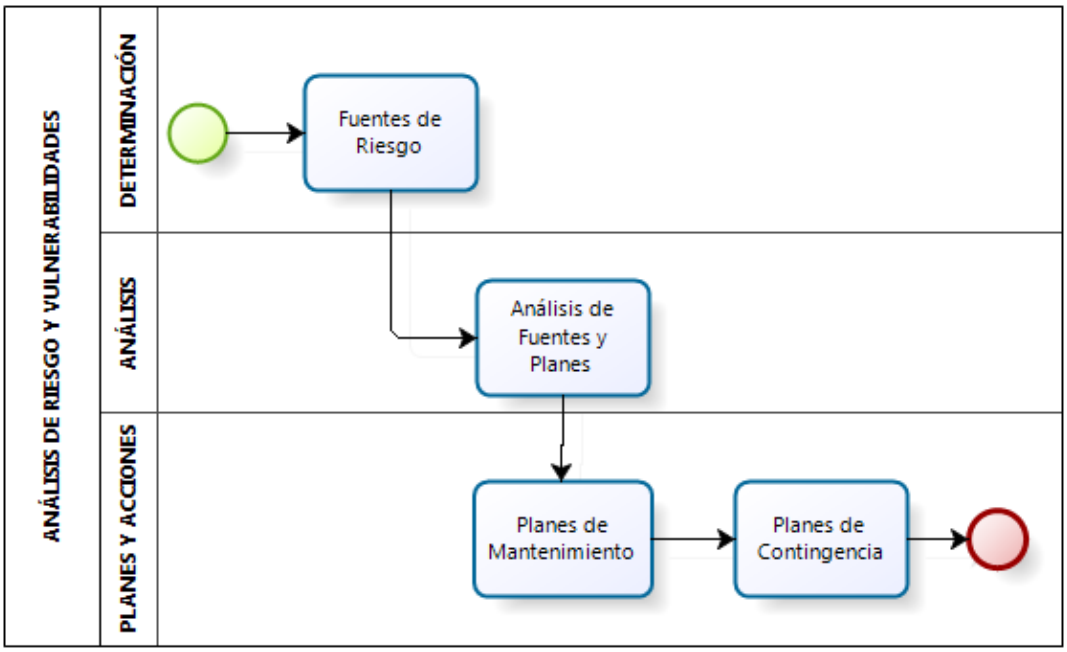
Se debe probar continuamente el plan de continuidad de negocio, dejando documentado sea en actas o bitácoras con los resultados obtenidos de dichas pruebas.

Se debe probar el plan de manera integral, para poder definir tareas, situaciones, características, sub planes que ayuden a mejorar el plan en función de los resultados obtenidos anteriormente y así poder cubrir todas las brechas correspondientes.

5. ANÁLISIS DE RIESGO Y VULNERABILIDADES.

En las figuras N° 28 y 29 se describen los procesos a seguir para realizar el análisis de riesgos y vulnerabilidades, y como se van a obtener las fuentes de riesgo.

Figura N° 28. ANÁLISIS DE RIESGO Y VULNERABILIDADES

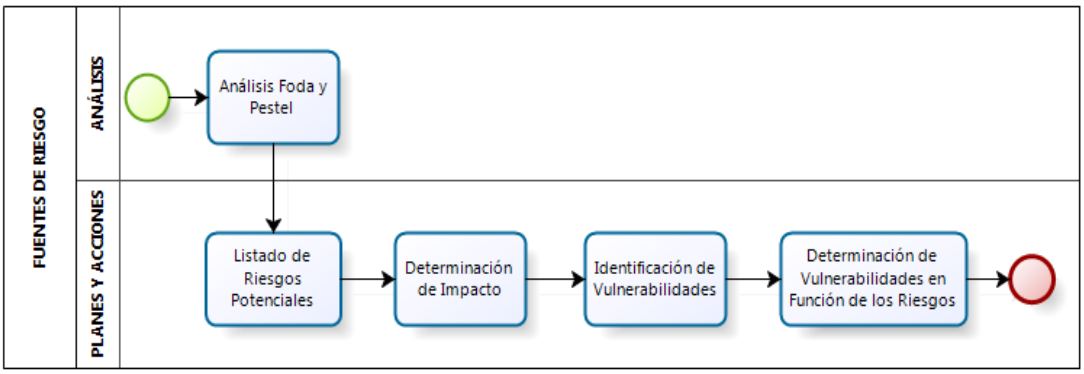


Elaboración: Propia

a. Identificación de Riesgos

Al analizar los riesgos es importante cuantificar las medidas de impacto de los parámetros cualitativos de dichos riesgos por lo que para calcular la incidencia o gravedad de los riesgos, se puede tener varias escalas dependiendo el tipo de uso que se le puede dar, por lo general es recomendable usar escalas simples que permitan a cualquier persona independientemente de su cultura profesional entender el cálculo para determinar la severidad de los riesgos encontrados tendremos 2 escalas que usaremos para valorar el riesgo las mismas que se encuentran en la Tabla N° 9.

Figura N° 29. DIAGRAMA DE FUENTES DE RIESGO



Elaboración: Propia

En esta escala de severidad de Riesgo en la que se lo califica acorde la probabilidad de ocurrencia de un incidente y adicionalmente acorde al impacto o severidad del mismo.

Tabla N° 09. ESCALA DE SEVERIDAD DE RIESGO

Probabilidad de Ocurrencia (P)	Valor Referencial	Impacto (I)	Valor Referencial
Improbable	1	Muy bajo	2
Poco probable	2	Bajo	4
Posible	3	Medio	6
Probable	4	Alto	8
Altamente Probable	5	Muy Alto	10

Elaboración: Propia

Para evaluar el Riesgo (R) utilizamos la siguiente fórmula: **R = P * I**

El valor obtenido en este cálculo comparado con la siguiente tabla (Tabla N° 10) nos dará la calificación del riesgo identificado.

Tabla N° 10. CALIFICACIÓN DEL RIESGO

Riesgo	Valor Referencial
Muy Alto	40 – 50
Alto	30 – 39
Medio	20 – 29
Bajo	10 – 19
Muy bajo	0 - 9

Elaboración: Propia

b. Análisis FODA

Tabla N° 11. ANÁLISIS FODA

FORTALEZAS	OPORTUNIDADES
F1. Contar con nuevas metodologías dentro del campo educativo Policial.	O1. Apoyo del Gobierno Regional y/o Local
F2. Contar con Instructores Capacitados en la Formación Técnico Policial.	O2. Creciente demanda por Personal Policial
F3. Ser la única Escuela de Formación Técnica Policial (Varones) dentro de la Región.	O3. Apoyo del Gobierno Central
F4. Brindar Estabilidad laboral y título dentro de la carrera de "ciencias administrativas Policiales".	O4. Demanda de Estabilidad Laboral
F5. Contar con personal técnico especializado para el manejo de las nuevas tecnologías.	O5. Apoyo de entidades privadas
F6. Egresados con capacidades y habilidades acorde con las necesidades de la población actual.	
F7. Personal Policial dedicado, responsable y trabajador.	
F8. Personal con conocimientos en varios ámbitos (Core del negocio).	
DEBILIDADES	**AMENAZAS**
D1. Limitado presupuesto económico para mejoras continuas.	A1. Clausura de las Escuelas de Formación Policial por falta de presupuesto
D2. Limitado marketing respecto a la forma de ingreso y beneficios que brinda la Escuela Técnica de Policía.	A2. Privatización de la institución Policial.
D3. Políticas de respaldos de información no aplicadas.	A3. Desconfianza de los padres sobre el trato y formación policial de sus hijos.
D4. Limitada Infraestructura para cumplir las necesidades de vivienda, alimentación y educación.	A4. Aumento del número de instituciones que brindan servicio de educación.
D5. Falta de políticas de continuidad respecto a los procesos importantes de la institución.	A5. Ausencia de proveedores por incumplimiento en los pagos.

D6. Carencia de un sistema de Información integral para la administración de la información.	
D7. Incumplimiento de pagos a los proveedores en los plazos establecidos.	
D8. Equipamiento Tecnológico desfasado	
D9. Carencia de Personal Profesional calificado en TIC.	

Elaboración: Propia

c. Análisis PESTEL.

Tabla N° 12 ANÁLISIS PESTEL

POLITICOS	ECONÓMICOS
- Políticas de gobierno central respecto al ámbito Policial.	- Crecimiento del índice de desempleo en el país.
- Leyes emitidas por el Ministerio de Educación sobre reestructuración Educativa.	- Costo para el acceso al proceso de admisión.
- Políticas del Ministerio del Interior	- Inestabilidad del cambio de políticas de impuestos y aranceles.
- Manual de Régimen Disciplinario para las Escuelas de Formación Policial.	- Costo al ocupar una vacante del proceso de admisión
- Ley del "Régimen Disciplinario de la Policía Nacional".	- Costo de pagos por conceptos educativos y de indumentaria Policial.
- Ley de la "Policía Nacional".	
SOCIALES Y DEMOGRÁFICOS	**TECNOLÓGICOS**
- Demanda por estabilidad laboral.	- Costo en el desarrollo e implementación de propuestas tecnológicas.
- Densidad poblacional de sectores	- Fallos de energía.

populares.	
- Trabajo estable, seguro médico integral y familiar.	- Fallos en el sistema de Red Informática.
- Demanda de seguridad ciudadana.	- Ataques a los sistemas computacionales.
- Aceptación de la población por una creciente afluencia policial.	
- Aumento del índice de delincuencia.	
- Población: Egresados 5to secundaria, personal premilitar.	
- Población migratoria.	
ECOLÓGICOS O AMBIENTALES	
- Incendios	
- Terremotos	

Elaboración: Propia

d. Matriz de Riesgos.

Se ha determinado objetivamente la "Matriz de Riesgos" en la Tabla N° 13, para la Escuela de policía, el mismo que está enmarcado dentro del tipo de Amenazas siguientes: "Provocadas por la mano del hombre, Técnicas y Organizacional".

Tabla N° 13 MATRIZ DE RIESGO

TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	RIESGO	IMPACTO
AMENAZAS PROVOCADAS POR LA MANO DEL HOMBRE.	Delito Informático	Líneas de comunicación no protegidas	Información Institucional poca y/o nada protegida.	Difusión de Información Confidencial.
		Arquitectura de Red insegura.		
		Conexiones de Red públicas sin protección		
		Transferencia de contraseñas no autorizadas.		
		Tráfico sensible sin protección.		
		No existen controles para asegurar la confidencialidad e Integridad de la Información.		
		No contar con una unidad de seguridad informática.		
		Políticas de Seguridad Inadecuadas o no difundidas.		
		Falta de controles de Autenticación para el acceso a los sistemas informáticos Policiales.		
	Terrorismo / Vandalismo	Ausencia de cámaras de video vigilancia en los diferentes ambientes de la institución.	Falta de control de seguridad interna	La seguridad y funcionamiento de los equipos podrían verse gravemente comprometidos.
		Limitada vigilancia por todos los diferentes ambientes de la institución.		
	Personal y Usuarios Internos (Descontentos, Negligencia, etc.)	Procedimientos inadecuados de rotación de personal PNP.	Personal con falta de experiencia y/o descontentos.	Ejecución de Operaciones ficticias o alteradas en los sistemas de información.
		Falta de una continua capacitación al personal PNP con respecto a la seguridad informática.		
		Falta de concientización con respecto a la		

		seguridad informática		
		Trabajo no supervisado de personal externo o de mantenimiento.		
		Falta de Mecanismos de monitorización		
	Alta rotación del Personal Policial**.**	No existen controles para asegurar la confidencialidad e integridad de la información.	Falta de control en la continuidad de las actividades del cargo del personal Policial que rota.	Pérdida de la continuidad de las operaciones del área de Centro de Datos.
		Falta de gestión de conocimiento ante la ausencia de un efectivo Policial.		
		Falta de dispositivos de vigilancia como cámaras para detectar cualquier evento inusual.		
		Falta de capacitación sobre valores y ética profesional.		
	Incorrecta Administración del Sistema Informático y de los Derechos de Acceso.	Gestión deficiente de contraseñas	Personal con acceso no autorizado a información clasificada.	Registro de Transacciones no permitidas o alteradas en los sistemas de información.
		Habilitación de servicios innecesarios		
		Falta de control eficaz del cambio		
		No existen documentados los servicios que presta la red informática a los usuarios.		
		Mejoramiento de las políticas que regulen el uso de los sistemas informáticos de acuerdo al perfil de usuario.		
		Configuración de seguridad inadecuada en los sistemas de información.		
	Robo	Falta de controles de acceso y seguridad implantadas en la institución Policial.	Pérdida de Información.	Interrupción en los servicios internos

		Ausencia de control permanente a los activos de información.		prestados por la institución.
TIPO DE AMENAZA	**AMENAZA**	**VULNERABILIDAD**	**RIESGO**	**IMPACTO**
AMENAZAS TÉCNICAS.	Falla de Componentes electrónicos.	No haber establecido políticas de reemplazo de piezas sensibles en el funcionamiento de los dispositivos electrónicos.	Poca / nula Funcionalidad de las herramientas	Suspensión temporal o definitiva de los equipos informáticos o comunicaciones con los que dispone la institución.
		No se realiza pruebas periódicas tanto de hardware como de software antes de su uso o puesta en funcionamiento.		
		Controles de cambios de configuración deficientes.		
		No se han identificado componentes críticos de los dispositivos.		
		No contar con personal calificado para la operación de los equipos informáticos con los que cuenta la institución.		
	Falla en el Servidor de Proveedores (Internet, etc.)	No se cuenta con un procedimiento en el que se indique la forma de proceder en caso de fallos del servicio de internet.	**Baja productividad.**	**Pérdida de los servicios en línea y las comunicaciones con el exterior.**
		No se cuenta con un enlace de back up para continuar con la continuidad de las operaciones críticas de la institución.		
	Mala Implementación	Implementación de controles deficientes.	**Poco control sobre la seguridad.**	Pérdida de Información o daños
		Implementación de controles que no se		

	de controles o incumplimiento de los mismos.	encuentran acordes a la realidad de la institución (negocio).		en los equipos de usuario final.
		No se han monitoreado o no se ha evaluado el cumplimiento de los controles de seguridad.		
	Falta / Falla de Software Empresarial (Antivirus, Gestor de base Datos, etc.)	Configuración incorrecta de parámetros.	Baja funcionalidad de las herramientas disponibles.	Afectación de los servicios prestados. Se podría comprometer la disponibilidad, integridad y confidencialidad de la información almacenada tanto en servidores como en equipos de usuario final.
		Cambios de configuración no documentados.		
		Falta de auditoria de software (Servidores, Equipos, etc.)		
		Deficiencia en los procedimientos de respaldo periódico de Información.		
		Uso de Software desactualizado o ilegal.		
	Falla / Mal Funcionamiento de los equipos Informáticos (Electrónicos).	Falta de implementación de esquemas de reemplazo de equipos.	Retraso en las tareas de los colaboradores con equipos informáticos defectuosos.	El funcionamiento del equipo informático podría ser gravemente afectado, al igual que se vería interrumpido el servicio de respaldo diario que se ejecuten.
		Sensibilidad a radiación electromagnética.		
		Susceptibilidad ante variaciones de tensión.		
		Susceptibilidad ante variaciones de temperatura.		
		Falta de capacitación del Uso de los equipos a los usuarios.		
		Gestión inadecuada de la Red Informática (Capacidad de recuperación de enrutamiento.)	Fallas en la correcta funcionalidad de la red Informática de la Institución.	Fallos en la comunicación tanto en la red informática interna como la salida al servicio de internet
		Falta de políticas de uso de recursos de red como el buen uso del servicio de internet.		
		Deficiente diseño de la red Informática.		

	Saturación de la Red Informática	Falta de monitorización de tráfico de la red informática.		por parte de los funcionarios de la institución.
		Líneas de comunicación sin protección.		
		Conexiones deficientes de cables.		
		Punto de red informática con fallas.		
		Puntos de acceso a la red informática sin protección y vulnerables a ataques informáticos.		
TIPO DE AMENAZA	**AMENAZA**	**VULNERABILIDAD**	**RIESGO**	**IMPACTO**
AMENAZAS ORGANIZACIONALES	Inexistencia de Planes, Políticas y Procedimientos organizacionales y de administración de Usuarios y Proyectos.	No se ha elaborado un plan de contingencia.	Baja gestión y poco control sobre el cumplimiento de las políticas internas.	Daños en equipos de procesamiento de datos y de información así como la pérdida de la información almacenada.
		Falta del procedimiento formal para el registro y bloqueo o eliminación de usuarios.		
		Inexistencia de procedimientos de revisión de los derechos de acceso otorgados a los usuarios.		
		Falta de procedimientos de monitoreo de los recursos de procesamiento y almacenamiento de información.		
		Falta de auditorías regulares.		
		Inexistencia de políticas que exijan la documentación de cambios de configuración en los sistemas y recursos existentes.		
		Inexistencia de Estándares para la Documentación.		
	Falta o Insuficiente Gestión de la	Incumplimiento de las Políticas de Seguridad Informática.	Bajo control sobre normas operativas	Daños en equipos de procesamiento de

	Seguridad de la Información (Monitorear, Procedimientos, etc.)	Falta de asignación adecuada de responsabilidades en la seguridad de la información.	institucionales.	datos y de información así como la pérdida de la información almacenada.
		Falta de registros en las bitácoras tanto de administradores como de usuarios finales (operarios).		
		Falta de responsabilidades en la seguridad de la información.		
		Falta de mecanismos de monitoreo		
	Falta de licencias de software propietario o violaciones de derecho de autor.	Falta de procedimientos para el cumplimiento de las disposiciones con respecto a los derechos intelectuales.	Baja funcionalidad de las aplicaciones	Incurrir en problemas legales con entidades de control por la falta de licenciamiento.

Elaboración: Propia

6. ANÁLISIS DE “IMPACTO DEL NEGOCIO”.

Identificados los peligros se debe analizar el impacto que generará en el negocio para realizar una propuesta para disminución de la afectación a la continuidad y las transacciones que proporciona la Escuela de Policía no se interrumpan vean afectados por largo tiempo y las actividades de los colaboradores (Efectivos Policiales) no se interrumpan.

a. Descripción del Impacto.

En función de los riesgos identificados se debe analizar el impacto que generará en el negocio para realizar una propuesta para disminución de la afectación a la continuidad y las transacciones que brinda la Escuela de Policía no se interrumpan.

Es importante tener en cuenta las actividades a las que se remite la institución y sus procesos dando valoraciones o cuantificando la prioridad de dichas actividades para considerar el impacto al ser dañadas o en última instancia completamente pérdidas.

Una vez que se han identificado todas las amenazas con la fórmula de cálculo de Riesgo vamos a identificar las amenazas con mayor valoración como se muestra en la Tabla N° 14. Las amenazas con riesgo Medio, Alto y Muy alto van a ser consideradas para nuestro análisis de riesgos.

Tabla N° 14. VALORACIÓN DE RIESGO

AMENAZAS	PROBABILIDAD DE OCURRENCIA	VALORACIÓN	IMPACTO	VALORACION	RIESGO	VALORACIÓN DEL RIESGO
Riesgo Operacional	Altamente probable	5	Muy Alto	10	Muy Alto	50
Terremoto	Probable	4	Muy Alto	10	Muy Alto	40
Incendio	Posible	3	Alto	10	Alto	30
Robo	Posible	3	Alto	8	Medio	24
Falla de energía	Posible	3	Alto	8	Medio	24
Falla de Red Informática	Probable	4	Medio	6	Medio	24
Ataques al sistema de información computacional	Posible	3	Alto	8	Medio	24
Daños ocasionados por personal interno	Posible	3	Medio	6	Bajo	18
Competencia de otras instituciones	Probable	4	Bajo	4	Bajo	16
Alta rotación de personal	Probable	4	Bajo	4	Bajo	16
Saturación de la red informática	Probable	4	Bajo	4	Bajo	16
Falta o insuficiente Gestión de la Seguridad de la Información	Poco probable	2	Alto	8	Bajo	16
Inestabilidad Política	Posible	3	Bajo	4	Bajo	12
Reformas Institucionales Educativas	Posibles	3	Bajo	4	Bajo	12
Cambios en políticas del Sector Interior	Poco probable	2	Medio	6	Bajo	12
Terrorismo/ Vandalismo	Poco probable	2	Medio	6	Bajo	12

Errores en la administración de derechos de acceso de los sistemas informáticos.	Poco probable	2	Medio	6	Bajo	12
Falla en el servicio de proveedores	Poco probable	2	Medio	6	Bajo	12
Inexistencia de Documentación de control (Planes, políticas y procedimientos de administración de usuarios)	Poco probable	2	Medio	6	Bajo	12
Falta de licencias de software propietarios o violaciones de derechos de autor.	Poco probable	2	Medio	6	Bajo	12
Incumplimiento con los proveedores	Poco probable	2	Bajo	4	Muy Bajo	8
Crimen informático.	Improbable	1	Alto	8	Bajo	8
Falta de componentes electrónicos.	Poco probable	2	Bajo	4	Muy Bajo	8
Mala implementación de controles e incumplimiento de los mismos.	Poco probable	2	Bajo	4	Muy Bajo	8
Falla de software Empresarial.	Poco probable	2	Bajo	4	Muy Bajo	8
Mal funcionamiento de los equipos informáticos.	Poco probable	2	Bajo	4	Muy Bajo	8

Fuente: Elaboración Propia

Una vez que se han determinado los riesgos es necesario establecer una descripción los escenarios, afectación, etc., categorizando de manera más amplia los riesgos y dando características esenciales.

De las Tablas 15 a la 21 se muestran la probabilidad, el impacto, el escenario, la afectación, la acción y los responsables.

Tabla N° 15. ESCENARIO – INCENDIO.

Riesgo	**Incendio**
Probabilidad	Posible
Impacto	Alto
Escenario	Un incendio puede provocar la devastación total de las diferentes oficinas administrativas, perdiendo no solo los equipos informáticos sino las vidas que en ese momento estén presentes, considerando que las alfombras y también el techo cielo raso son de grado combustible (inflamable). La institución debe tener en cuenta que las toma de corrientes están cerca de las alfombras lo cual haría más fácil la propagación del fuego a las áreas por donde la misma cruza.
Afectación	El grado de afectación es severo al tener pérdidas humanas y en adición los equipos informáticos que ofrecen el servicio para cumplir las labores diarias (Data Center).
Acción	Implementar extintores de espuma para inhibir la combustión de las alfombras y techo cielo raso, así mismo en el data center tener como mínimo DOS (02) extintores de anhídrido carbónico los cuales contrarresten la combustión de las alfombras y protegen los equipos electrónicos.
Responsable	Brigadista.

Fuente: Elaboración Propia

Tabla N° 16. ESCENARIO – TERREMOTO.

Riesgo	Terremoto
Probabilidad	Probable
Impacto	Muy Alto
Escenario	Un terremoto puede provocar la destrucción total no solo de las Oficinas Administrativas sino de todo el complejo Policial; dependiendo de la magnitud puede destruir apenas solo parte de las oficinas administrativas o completamente todo el Complejo Educativo Policial.
Afectación	Dependiendo el grado de magnitud del terremoto puede causar que se cuarteen o caigan las paredes con bajo nivel de destrucción (recuperables sin incidencia catastrófica) o puede ser una destrucción completa de las oficinas administrativas residentes.
Acción	Independientemente del grado o magnitud del terremoto la acción por parte del brigadista encargado es de ayudar a otros a evacuar el complejo evitando primordialmente pérdidas humanas y de ser posible los equipos informáticos (anteponer la vida antes que los equipos).
Responsable	Brigadista.

Fuente: Elaboración Propia

Tabla N° 17 . ESCENARIO – FALLA DE ENERGÍA.

Riesgo	**Falla de energía**
Probabilidad	Posible
Impacto	Alto
Escenario	El complejo Policial puede presentar fallas eléctricas por lo general por antigüedad en sus conexiones lo cual puede producir un cortocircuito que origine DOS (02) posibles escenarios: 1. Corte total de la energía eléctrica. 2. Incendio.
Afectación	La Afectación puede ser leve o severa dependiendo del escenario, en el caso de CORTE TOTAL DE ENERGÍA puede

	quedar solamente en la discontinuidad de los servicios, por otro lado también pueden quemarse los equipos electrónicos no solo las UPS sino los servidores y otros. En caso de que se ocasione un incendio la afectación se vuelve severa y caeríamos en el caso de RIESGO POR INCENDIO.
Acción	Implementar UPS especiales que soporten grandes cargas de energía eléctrica de modo que no se produzca un apagón de los servidores y estos no resulten afectados; en adición tener en cuenta la acción del riesgo del incendio.
Responsable	Departamento de Tecnología.

Fuente: Elaboración Propia

Tabla N° 18. ESCENARIO – ROBO.

Riesgo	**Robo**
Probabilidad	Posible
Impacto	Alto
Escenario	Existen DOS (02) escenarios: 1. Robo Interno: Robo de equipos informáticos y otros que se produzcan dentro de las instalaciones por lo general en horas que las oficinas están prácticamente vacías. 2. Robo externo: Robo de equipos al personal mientras están fuera de las instalaciones de la institución Policial.
Afectación	El robo de los equipos informáticos a los efectivos Policiales de la Institución, en este caso la afectación recae severamente por la información de "el/los" clientes (alumnos, docentes, padres de familia y otros) que posee el efectivo policial en el computador a su cargo.
Acción	En el caso de robo interno, se debe tener alarmas además de las cámaras de seguridad y tener cuidado con el ingreso de personal ajeno a la institución para estar pendientes que se trate de un agente de confianza. En el caso de robo externo, es importante que los efectivos Policiales consideren el hecho de ir en unidades policiales de las

	comisarías de la zona al movilizarse con equipos computacionales.
Responsable	Todo el Personal.

Fuente: Elaboración Propia

Tabla N° 19. ESCENARIO – FALLA DE RED INFORMÁTICA.

Riesgo	Falla de la Red Informática
Probabilidad	Probable
Impacto	Medio
Escenario	Existen varios tipos de causas por las cuales puede suscitarse fallas en la red informática de comunicaciones, como son: 1. Cruce entre hilos (mala conexión). 2. Ruptura de los cables. 3. Exceso de ruido y/o estática.
Afectación	El efecto que causa las fallas en la red informática es netamente con los sistemas de información, ya que si los servidores están haciendo rutinas automáticas de respaldo o incluso el personal está haciendo sus respaldos propios puede generar conflicto o fallas al generar la información respaldada, además de errores en la comunicación.
Acción	Proteger y resguardar el Data Center, cambiando el cableado estructurado periódicamente conforme a los protocolos de instalación y mantenimiento que exigen las normas internacionales, así mismo hacer mantenimiento de los equipos informáticos para reducir el impacto al suscitarse dicho problema.
Responsable	Unidad de UNITIC.

Fuente: Elaboración Propia

Tabla N° 20. ESCENARIO – ATAQUES AL SISTEMA INFORMACIÓN

Riesgo	**Ataques al sistema de información computacional**
Probabilidad	Posible
Impacto	Alto
Escenario	Al contar con información crítica de los clientes (Alumnos PNP, Docentes, Personal PNP y otros) es necesario que la resguardemos de manera confidencial, aunque los piratas informáticos atacarían la red organizacional para obtener dicha información.
Afectación	Al tener plagio de información propia de la institución o información de otras instituciones de Educación Policial a nivel nacional ponemos en riesgo no solo a dichas instituciones sino a la misma Policía como tal por el factor de desconfianza que generaría dicho plagio lo que terminaría en pérdida de credibilidad y de clientes.
Acción	Implementar el "Sistema de Detección de Intrusos (IDS)" y otros sistemas para prevenir y detectar ataques de piratas informáticos.
Responsable	Unidad de UNITIC.

Fuente: Elaboración Propia

Tabla N° 21. ESCENARIO – RIESGO OPERACIONAL.

Riesgo	**Riesgo Operacional**
Probabilidad	Altamente probable
Impacto	Muy Alto
Escenario	Al momento de realizar los procesos formativos de la unidad académica en sí se corre el riesgo de incumplir tiempos estipulados para entrega de informas resultantes, utilizar un lenguaje no adecuado con el cliente (alumnos PNP, Docentes, y otros) o dar juicios que provoquen inconvenientes dentro de la institución Policial.
Afectación	La severidad de impacto es la más alta considerando que si se produce el riesgo, lo posible es que se pierda prestigio de la

	imagen propia de la institución y por ende se perdería clientes a gran escala por lo cual la afectación de darse este riesgo es inminentemente catastrófico.
Acción	Planificar bien la realización de los procesos formativos de la unidad académica para mejorar tiempos de desarrollo de la misma teniendo en cuenta que se debe tener un lenguaje cordial sin emitir juicios anticipados respecto a matrículas, pase a retiro de alumnos, sanciones administrativas, admisión, contratación de docentes y otros.
Responsable	Unidad Académica.

Fuente: Elaboración Propia

El impacto se debe analizar en función de los procesos críticos que posee la institución.

7. ESTRATEGIAS DE RECUPERACIÓN.

Al analizar las necesidades de recuperación de los sistemas desde la vista del negocio, es necesario establecer el Tiempo de tolerancia (RPO) a la interrupción que poseen los procesos de Negocios y los Tiempos de Recuperación (RTO) que poseen los sistemas tecnológicos que soportan al mismo. Por ello es importante establecer los Objetivos de Tiempo de Recuperación y Tiempo de Tolerancia.

En la tabla 22 se muestra el tiempo en el que se deben reestablecer las operaciones dependiendo de la institución y las políticas establecidas en las mismas. Para marcar las opciones seleccionadas en las tablas utilizadas en este capítulo se utilizará una “X”.

Tabla N° 22. TIEMPO DE RESTABLACIMIENTO DE LAS OPERACIONES.

RTO RPO	0–30 Min.	30 Min. – 2 Horas	2–6 Horas	6–12 Horas	12–24 Horas	24–48 Horas	48< X Horas
Recuperación de correo electrónico.		X					
Recuperación de Información digital de clientes.			X				
Recuperación de servidores.	X						
Recuperación de equipos operativos para personal Administrativos.			X				
Recuperación de equipos operativos para personal de seguridad.							X

Fuente: Elaboración Propia

a. Recuperación de Correo Electrónico.

El impacto que genera la perdida de correo electrónico es alto, considerando que se puede perder la comunicación con los órganos de comando Policial, con el cliente y perjudica la imagen y de igual manera la interrelación con el mismo se verá afectada.

El servicio de correo estará activo en un 99,99% considerando que se maneja correo institucional (@policia.gob.pe) por lo que las comunicaciones e información que se tenga en el correo está prácticamente a salvo en caso de producirse algún incidente en la institución, aunque no queda exenta de perdida pero prácticamente el riesgo es mínimo.

b. Recuperación de Información digital de clientes.

Es vital para poder proseguir con las actividades académicas de pre grado al mismo, sin ella se pierde no solamente el esfuerzo realizado en el tiempo

que se llevó a cabo el procesamiento de dicha información sino también la confianza del cliente lo que genera un gran impacto a la imagen de la institución Policial.

c. Recuperación de Servidores.

La recuperación de los servidores debe ser inmediata para poder seguir con las actividades, teniendo en cuenta esto debemos tener un lugar donde poder levantar los servidores, de manera que los servicios con los que cuenta la institución sean levantados uno por uno de manera correcta y seguir obteniendo los servicios correspondientes.

Para tener en cuenta el tipo de recuperación de medios físicos es importante tener en cuenta la magnitud del impacto que se tendrá al producirse el incidente, por lo que es necesario considerar los escenarios de recuperación que se encuentran establecidos en la Tabla N° 23.

Tabla N° 23. ESCENARIOS DE RECUPERACIÓN.

Sitio	Costo	Hardware	Telecomunicaciones	Tiempo	Localización
Sitio en frío	Bajo	No	Ninguno	Largo	Fijo
Sitio semi-preparado	Medio	Parcial	Parcial	Medio	Fijo
Sitio preparado (hot site)	Alto	Completo	Parcial	Corto	Fijo
Sitio Móvil.	Alto	Variable	Variable	Variable	No Fijo
Espejo (Mirror)	Muy Alto	Completo	Completo	Mínimo	Fijo
Sitio Reciproco.	Bajo	Parcial	Parcial	Medio	Fijo

Fuente: Elaboración Propia.

- **Sitio en frío (ColdSites).**

Este sitio no comprende ni sistemas de comunicación, ni hardware necesario para levantar inmediatamente un centro de Datos necesario para que al menos las labores principales se reanuden; es decir solo tenemos el arrendamiento o compra de un espacio físico (No recomendado en empresas Medianas y Superiores).

- **Sitios semi-preparados (WarmSites).**

En este tipo de sitios tenemos el sistema de comunicaciones y equipos de servidores y ordenadores parcialmente instalados en el espacio físico arrendado, es decir se cubre los procesos más críticos a levantar para que el negocio retome sus actividades casi inmediatamente después del incidente ocurrido.

- **Sitios preparados (Hot Sites).**

El sitio preparado, es en el que tenemos una réplica del Centro de Datos, principal; es decir que tiene el sistema de comunicaciones en su mayor parte instalado y arreglo de servidores ya implantado similar al original que al suscitarse un incidente está listo para que los servicios se levanten en un máximo de 3 horas.

- **Sitio espejo (Mirror Site)**

Este tipo de contingencia es uno de los más elevados en costo por su nivel de cobertura considerando que al igual que el sistema de arreglo de servidores y el de telecomunicaciones es completo, por lo que el tiempo de recuperación es mínimo, tan solo depende del tiempo de movilización del

personal para el sitio y completar el levantamiento de servicios de acuerdo a las funciones de los colaboradores aunque los servicios en línea estarían funcionales prácticamente al instante.

Al ser un sitio espejo, es esencial que tenga la misma infraestructura del sitio principal, es decir que tanto los servidores, ordenadores e incluso el software que tenga sea idéntico al principal para que no exista problemas de compatibilidad.

d. Recuperación de equipos operativos para personal Administrativos.

La recuperación de las labores depende del trabajo a realizar por lo que hay que tener en cuenta que los desastres deben ser totalmente o en gran parte transparentes al cliente final, por lo que es importante que se adquiera equipos informáticos para que estén disponibles al menos para los efectivos Policiales de la Unidad Académica encargados y seguir con el proceso formativos y no perder la buena imagen y credibilidad ante el cliente y la sociedad.

e. Recuperación de equipos operativos para personal de Seguridad.

La recuperación de equipos para personal de seguridad no tiene mayor incidencia como recuperar equipos para encargados de la unidad académica administrativa pero aun así se tendría impacto al perder equipos computacionales teniendo en cuenta que también tienen información valiosa que sustente parte de algunos procesos académicos sobre todo durante el proceso de postulación.

8. DESCRIPCIÓN DEL PLAN DE "RECUPERACIÓN DE DESASTRES (DISASTER RECOVERY PLAN – DRP)".

Se escogió dicha norma ya que engloba los parámetros de gestión como un sistema lo cual permite enfocarse en la revisión de riesgos para posteriormente poder estar preparados ante cualquier desastre y el impacto sea mínimo sin que la interrupción de las actividades normales sea a largo plazo o en gran medida.

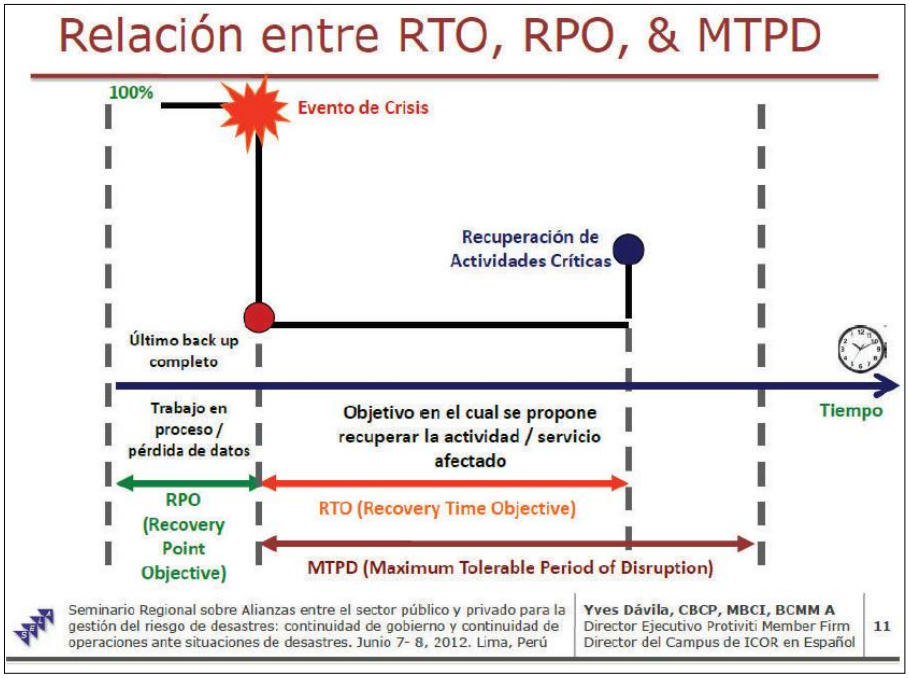
Figura N° 30. CICLO "PDCA APLICADO AL PROCESO DE LA CONTINUIDAD DEL NEGOCIO".

Fuente: ISO 22301

En la Figura N° 31. Se puede ver como la norma se enfoca en realizar una mejora continua para un proceso propio de continuidad de negocio donde se pueda responder ante cualquier eventualidad negativa que pueda afectar la normalidad de las actividades.

Como muestra la Figura 31.se puede observar que la norma también describe casos de recuperación y tiempos del mismo proyectándose en las actividades críticas a recuperar y el tiempo mínimo que debe demorarse por cada una de ellas para que el impacto sea casi imperceptible y se puede volver a la normalidad lo antes posible.

Figura N° 31. RELACIÓN ENTRE EL RTO, RPO Y MRPD



Fuente: ISO 22301

El plan de recuperación ante desastres es aquel capaz de responder ante sucesos improvistos que interrumpen o afectan de alguna manera las actividades normales de una empresa y los servicios que presta interna o externamente.

a. Objetivos del Plan DRP.

- El objetivo más importante de este documento es definir los procedimientos de recuperación ante la interrupción de la operación de los principales servidores y la red de comunicaciones.

- Se ofrece una mayor atención y énfasis en una recuperación ordenada y a la reanudación de las operaciones de negocio críticas para la empresa.

- Los elementos que conciernen a las computadoras están contempladas, sin embargo las funciones relacionadas con los

servicios prestados al cliente final por parte del equipo de Tecnología no se abordan.

- La invocación de este plan implica que la operación de recuperación ha comenzado y continuará con la máxima prioridad de viabilizar el servicio y restablecer las operaciones informáticas de la empresa.

b. Servicios Críticos a Salvaguardar.

Para la preservación de servidores es importante para tener continuidad en cuanto a los servicios que posee la empresa a nivel interno, en términos generales los principales servidores y servicios que deben resguardarse son los siguientes:

- Comunicaciones de red/conectividad, Internet.
- DNS y DHCP.
- Servicio de Correo.
- Controlador de Dominio.
- Servicio de Archivos.
- Servicio de Aplicaciones.
- PCs individuales.
- Servicio de Respaldos de información.

c. Incidente y Contingencia

Este plan de recuperación de desastres se invocará bajo una de estas Circunstancias:

- Un incidente que puede parcial o completamente paralizar las operaciones del centro de cómputo por un período de 24 horas.

- Un incidente, que ha afectado la utilización de las computadoras y redes administradas por Tecnología, debido a circunstancias que están más allá del normal procesamiento de las operaciones del día a día. Esto incluye todos los procedimientos administrativos del Departamento de Tecnología.

Situaciones generales que pueden destruir o interrumpir usualmente un Computador ocurren bajo las principales categorías:

- Interrupción de energía/ variación/ fluctuación
- Fuego
- Agua
- Fenómenos naturales y climáticos
- Sabotaje/vandalismo
- Robo
- Virus

Hay diferentes niveles de severidad las cuales necesitan diferentes estrategias de contingencia y diferentes tipos y niveles de recuperación. Este plan cubre estrategias para:

- Recuperación parcial: operación en un sitio alterno y/o en áreas de clientes de la compañía.

d. Seguridad Física.

Por norma y control se debe tener instalados sensores de temperatura, humedad y humo, además que los servidores, tienen que estar protegidos por UPS's que los tengan activos por aproximadamente 15 minutos después de cortes de energía o hasta levantar la corriente con otro medio alterno de energía.

e. Energía Eléctrica y Controles Ambientales.

Se debe considerar el flujo de corriente eléctrica y ambiente en el sitio donde se aloja la empresa como tal y donde se alojan los servidores de la misma, siendo un edificio es necesario contar con diferentes medios para no interrumpir la carga en los equipos pues pueden sufrir daños como pueden ser generadores dedicados y auxiliares con conexión a UPS's que resguarden la integridad en carga a los servidores.

f. Protección ante software mal intencionado.

La empresa debe tener un software licenciado y especializado de acuerdo a las necesidades para la protección de virus y cualquier tipo de software mal intencionado que quiera atacar la red y los equipos de la empresa; debe existir una política donde quede por escrito que todos los equipos pertenecientes a la empresa obligatoriamente deben tener instalado el antivirus empresarial.

g. Planes de recuperación.

Se formula el plan de recuperación con los sub planes auxiliares que aportan a la recuperación integra ante el incidente producido.

“Plan de Recuperación de los Servicios del Centro de Cómputo”.

Como tal debe iniciar inmediatamente de la ocurrencia del incidente al ser necesario el uso del sitio alternativo y/o cuando el incidente haya afectado parte del sitio principal y puedan reanudarse las operaciones en un tiempo razonable.

En cualquiera de los 2 casos se debe determinar lo siguiente:

- Determinar el alcance de el/los incidente/s.
- Determinar gastos implícitos para recuperación.

En el caso de necesitar el sitio alternativo se debe considerar ciertos aspectos:

- Informar al responsable externo del sitio alternativo para poner en marcha la utilización del mismo.
- Organizar el movimiento de los equipos de apoyo al sitio alternativo.
- Establecer operaciones de servicios en el sitio alternativo.
- Organizarlos planes a largo plazo y apoyo de soporte.

9. GUÍA DE PROCEDIMIENTOS DEL PLAN.

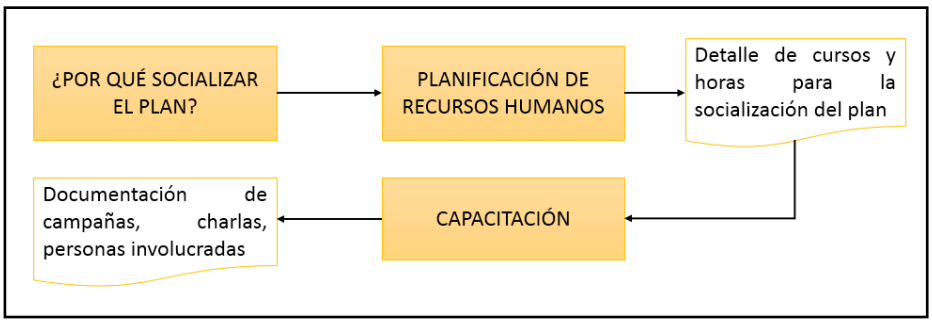
Se debe determinar los componentes, facilidades, herramientas y demás características actuales de la institución para en función de ella describir los procesos críticos a levantar y con ellos describir las áreas y/o dispositivos primarios a levantar.

a. Descripción de los procesos levantados.

Se debe detallar los procesos enlistados y los dispositivos asociados a poner en marcha para la continuidad, se debe considerar tanto los servidores como los equipos para el personal correspondiente que lo utiliza identificando el personal más crítico que deba obtener los equipos en primera instancia.

b. Socialización Del Plan.

Figura N° 32. SOCIALIZACIÓN DEL PLAN



Fuente: Elaboración Propia.

- **¿Por qué socializar el plan?**

Un plan de continuidad de negocio no tiene sentido ni valor al solo mantenerlo documentado si el personal de la institución no tiene un conocimiento adecuado de los procedimientos que se detallan en el mismo para están preparados ante eventualidades que puedan suscitarse y afecten la continuidad del negocio; es decir, si el personal no tiene una capacitación adecuada de lo que es la propuesta no existirá una gestión adecuada en un caso contingente lo cual puede afectar potencialmente a la institución.

- **Planeación de RR.HH.**

Se debe tener un plan para la capacitación al personal que labora en la institución tanto los colabores nuevos como los que ya tienen tiempo trabajando en la organización, describiendo los riesgos potenciales que incurren al no tener conciencia clara de lo que es un "Procedimiento de Continuidad" y lo importante que es cada colaborador para la eficiencia y eficacia del mismo y éste pueda cumplirse a cabalidad minimizando el riesgo potencial en la institución.

- **Capacitación.**

Se debe implementar campañas continuas donde se detallen aspectos de los procedimientos de la Propuesta de manera que los colaboradores vayan continuamente familiarizándose y empoderándose del tema siendo ellos la parte fundamental para que el plan se lleve a cabo.

Se debe dar charlas prácticas donde se enuncien escenarios de contingencia y dar las respuestas a eventos críticos de tal manera que el personal pueda estar preparado ante cualquier eventualidad.

Se debe establecer brigadas y capacitar a los miembros para los casos de contingencia, donde se pueda determinar personas idóneas con actitud y aptitud de poder responsablemente en caso de que se produzca un incidente.

c. Validación del Plan.

Una vez realizado el plan de continuidad se procede a validar el plan en un caso de estudio escogido para realizar las pruebas correspondientes, adaptando el plan a la institución para determinar los puntos críticos a proteger y se puedan continuar con las labores y actividades normales sin interrumpir propiamente a los colaboradores siguiendo con el Core del negocio.

El caso de estudio al que se aplicará el plan de continuidad será la Unidad Académica de Pregrado de la Escuela Técnica de la Policía.

Donde enfocaremos los planes y actividades a realizar para salvaguardar la integridad del negocio y no se pierda continuidad en las labores de los procesos formativos que realizan los colaboradores.

d. Preparación de Casos de Continuidad.

- **Identificación de Procesos a Respaldar.**

  La Escuela Técnica de Policía como tal es una institución del Estado encargada de formar SubOficiales de Policía donde sus procesos académicos de Gestión principales son: "Matrícula, notas, Horarios, procesos disciplinarios, Proceso de Admisión, Seguridad". Como se muestra en la Tabla N° 24 se han Priorizado las actividades a desarrollarse.

Tabla N° 24. PRIORIZACIÓN DE LAS ACTIVIDADES

Actividades	Prioridad		
	1	2	3
Gestión de Matrícula	X		
Gestión de notas	X		
Gestión de horarios	X		
Gestión de Procesos disciplinarios	X		
Gestión del Proceso de admisión		X	
Gestión de seguridad		X	

Fuente: Elaboración propia.

Los procesos que tienen relación directa son los que se encuentran listados en la Tabla 25.

Tabla N° 25. "PERSONAL NECESARIO PARA ESTABLECER LA CONTINUIDAD DE LAS OPERACIONES".

Personal	Actividades que deben cumplir	Prioridad		
		1	2	3
Jefe del área académica	Jefe del área académica y sus procesos.	X		
Documentario Académico	Encargado del registro de los procesos académicos	X		
Jede del área de moral y disciplina	Jefe del área de moral y disciplina y sus procesos	X		
Documentario de disciplina	Encargado del registro de los procesos disciplinarios.	X		
Jefe de Admisión	Jefe del proceso de admisión y sus diferentes actividades	X		
Documentario de Admisión	Encargado del registro de los postulantes y sus actividades	X		
Jefe de Seguridad	Jefe de la seguridad externa e interna de la institución		X	
Documentario de Seguridad	Encargado del registro de los procesos de seguridad.		X	

Fuente: Elaboración Propia.

Los procesos de Gestión: “Matrícula, notas, horarios, servicio de permanencia (seguridad)” son importantes porque son servicios fundamentales que posee la institución para cumplir con el objetivo de formar óptimamente suboficiales Policías, los mismos que son definidos en las siguientes tablas:

Tabla N° 26. Gestionar Matrícula

Gestionar Matrícula	
Definición	Proceso académico, mediante el cual el estudiante ingresa al sistema educativo, en el semestre y aula correspondiente.
Metas	Realizar con eficiencia “el proceso de matrícula en sus diferentes modalidades, alcanzando un consolidado de matrículas por semestres, especialidades, ciclos y turnos, esto permitirá realizar estadísticas de alumnado y además permitirá la elaboración y remisión de documentos”.
Actores	Jefe del Área Académica, Documentario y Alumno.
Riesgos	Al realizar un inadecuado proceso de matrículas, perjudicará la elaboración de documentos como fichas y nóminas de matrículas, además de los procesos de notas y sus respectivos documentos.

Fuente: Elaboración Propia.

Tabla N° 27. Gestionar Notas

Gestionar Notas	
Definición	Es un proceso académico, mediante el cual se registran las notas correspondientes a cada alumno, tomando en cuenta el semestre, ciclo, turno y cursos, donde se encuentra matriculado.

Metas	Al realizar eficientemente el proceso de notas por estudiante, se consigue la elaboración de documentos correspondientes, además de permitir la publicación inmediata de las notas de los alumnos y su cuadro de mérito.
Actores	Documentario, Jefe del Área Académica, Docentes, Alumnos
Riesgos	Al realizar un inadecuado proceso de registro de notas: "perjudicará la elaboración de documentos como cuadro de méritos, fichas y nóminas de matrículas, además de los procesos de notas y sus respectivos documentos".

Fuente: Elaboración propia

Tabla N° 28. Gestionar Horarios

Gestionar Horarios	
Definición del Caso de Uso	"Proceso Académico", en el cual se asignan los respectivos horarios correspondientes a cada docente, tomando en cuenta el semestre, especialidad, ciclo, turno y cursos, donde dictará la cátedra respectiva.
Metas	Al realizar eficientemente el proceso de asignación de horarios a los docentes, se consigue la elaboración de documentos correspondientes, además de permitir la publicación inmediata de los horarios para cada semestre académico.
Actores	Documentario, Jefe del Área Académica, Docentes.
Riesgos	Al realizar un inadecuado proceso de asignación de horarios, perjudicará la elaboración de documentos como los horarios de cada sección del respectivo semestre a iniciar, distribución de los laboratorios de cómputo para las asignaturas de computación y la asignación de los equipos multimedia.

Fuente: Elaboración propia

Tabla N° 29. Gestionar Servicio de Permanencia (Seguridad)

Gestionar Servicio de Permanencia	
Definición del Caso de Uso	Es un proceso Administrativo, mediante el cual se nombra al Personal Policial de servicio diario que será responsable del cuidado de la institución, durante las 24 horas del día que son designados según Rol de servicio.
Metas	Al realizar eficientemente el Rol de Servicio para el Personal Policial, se consigue la correcta distribución del servicio de Permanencia diario, lo cual permitirá que la seguridad interna de las instalaciones este protegida, así mismo nombrar diariamente a un responsable para el trámite de la documentación de urgencia que se tenga que realizar fuera del horario de trabajo administrativo.
Actores	Documentario, Jefe del Área de Recursos Humanos.
Riesgos	Al realizar un inadecuado Rol de Servicio de Permanencia, creará confusión dentro del personal Policial quien no sabrá exactamente cuándo es su día de servicio, creando malestar en el personal debido a que podrían repetir su día de servicio en los días que no les corresponde, así mismo podría generarse retraso en los plazos que se estipulan para el trámite de los documentos que se tengan que realizar fuera del horario administrativo (07:45 a 15:00 horas) al no contar con el personal de servicio encargado.

Fuente: Elaboración propia

Lista el personal operativo con el que se debería contar para reanudar las operaciones en tema de desastre natural se encuentra listada en la Tabla N° 30.

Establece las prioridades de los servicios proporcionados por los sistemas utilizados dentro de la institución. A continuación en la Tabla N° 30. Se detalla información relevante de los sistemas más importantes.

Tabla N° 30. SISTEMA DE INFORMACIÓN REQUERIDOS PARA LA CONTINUIDAD DE OPERACIONES.

Sistemas / Aplicaciones			Prioridad		
NOMBRE	SIGLAS	DIRECCIÓN ELECTRÓNICA	1	2	3
Sistema de "Gestión Educativa PNP".	SIGA PNP	http://www.sigadiredu.pnp.edu.pe/	X		
Sistema "Integrado de Gestión de la Carrera".	AGUILA 6 PNP	https://aguila6.pnp.gob.pe	X		
Sistema "Integrado de Gestión de Expedientes".	SIGE MININTER	https://aplicaciones.mininter.gob.pe		X	
Sistema de "Administración de Recursos Humanos".	SIWARH PNP	https://siwarh.pnp.gob.pe	X		
Sistema de "Registro y Control de denuncias".	SIDPOL PNP	https://denuncias.pnp.gob.pe		X	
Sistema de "Información Policial".	E-SINPOL PNP	https://sinpol.pnp.gob.pe		X	
Correo Electrónico Institucional PNP	@-PNP	https://correo.pnp.gob.pe		X	

Fuente: Elaboración Propia

- **Sistema de "Gestión Educativa PNP".**

Es un sistema integrado de la Policía que contiene todo los datos de los Alumnos PNP de las distintas promociones de sus respectivas escuelas técnicas a nivel nacional, la cual permite la interconexión de todas las Escuelas Técnicas de Educación Policial.

- **Sistema "Integrado de Gestión de la Carrera PNP".**

Es un sistema integrado de la Policía que contiene todo los datos del personal Policial de las distintas unidades policiales a nivel nacional, lo cual permite hacer un seguimiento a cualquier efectivo a nivel nacional, así mismo cada uno de estos poder verificar su hoja electrónica de reporte personal durante toda su permanencia en la institución Policial.

- **Sistema "Integrado de Gestión de Expedientes MININTER".**

Sistema informático administrativo documentario que asigna a todos los documentos de los órganos policiales y no policiales un único código o número de identificación mediante la Hoja de Trámite y nos permite realizar procedimientos de derivación, respuesta, archivo, consultas, reportes, entre otros, en el diligenciamiento de los expedientes.

- **Sistema de "Administración de Recursos Humanos PNP".**

Es un sistema integral que dentro de su alcance se usa para el registro y administración de sanciones administrativas disciplinarias al personal de Alumnos, así mismo al personal Policial en situación de actividad.

- **Sistema de "Registro y Control de denuncias PNP".**

Es un sistema que automatiza funciones y procesos relacionados al registro de denuncias policiales; asimismo, determina información que será de mucha ayuda en establecer decisiones a nivel Policial.

- **Sistema de Información Policial PNP.**

Sistema que permite el registro y consultas de las Requisitorias de Personas, Requisitorias de vehículos, antecedentes policiales y la emisión de certificados de antecedentes Policiales a nivel nacional.

- **Correo Electrónico Institucional.**

Correo institucional (@policia.gob.pe) permite tener una comunicación oficial entre los efectivos Policiales y las distintas unidades policiales a nivel nacional, es de uso obligatorio para las distintas comunicaciones oficiales.

La Tabla N° 31 contiene un detalle de los activos tecnológicos precisos para la puesta en marcha de las operaciones de la institución.

Tabla N° 31. "DESCRIPCIÓN DE LOS ACTIVOS TECNOLÓGICOS".

Activos Tecnológicos	Prioridad		
	1	2	3
Computadoras de Escritorio	X		
Computadoras Portátiles		X	
Teléfono	X		
Impresora		X	

Scanner		X	

Fuente: Elaboración propia

En la Tabla N° 32 y 33 se establece un detalle del mobiliario básico y los artículos de oficina con el que se debe contar para reanudar las operaciones.

Tabla N° 32. "MATERIAL MOBILIARIO".

Mobiliario	Prioridad		
	1	2	3
Estación de recepción			X
Sillas			X
Escritorio / Mesas			X

Fuente: Elaboración propia

Tabla N° 33. "MATERIAL DE OFICINA".

Material de Oficina	Prioridad		
	1	2	3
Hojas de papel bond	X		
Bolígrafos			X
Toners color negro	X		

Fuente: Elaboración propia

En la Tabla N° 34 se detalla el material de referencia a ser usado en caso de la ocurrencia de un incidente.

Tabla N° 34. MATERIAL DE REFERENCIA

Material	Prioridad		
	1	2	3
Listado de Alumnos PNP	X		
Listado de Docentes	X		
Listado del Personal PNP		X	
Listado de Proveedores			X
Nóminas de matrículas impresas	X		
Horarios impresos		X	
Listado de sanciones impuestas	X		
Listado de cursos impresas			X

Fuente: Elaboración propia

10. IDENTIFICACIÓN DE ESCENARIOS.

Se han tomado los principales escenarios que pueden perturbar la continuidad de los servicios académicos ofrecidos por la Escuela Técnica de Policía y estableciendo los posibles riesgos asociados a estos escenarios.

Casos:

Tabla N° 35. ESCENARIO IDENTIFICADO – INCENDIO.

Riesgo	**Incendio**
Probabilidad	Posible
Impacto	Alto
Escenario	En el caso de incendio que se suscite en las instalaciones del complejo Policial de la Escuela Técnica de Policía – Sede Puente Piedra – Lima; las pérdidas que se generan para la institución serían: humanas, información, servicios

	y activos, ya que existe personal administrativo policial que se encuentra laborando en las áreas administrativas, las cuales se afectarían en primera instancia. Además en caso de presentarse un connato de incendio provocaría pérdidas del centro de datos que está ubicado en el segundo nivel del pabellón central en un cuarto pequeño el cual se destruiría completamente con el incendio provocando la pérdida de información y los servicios prestados pues los servidores centrales se arruinarían y con ellos todo su contenido dando como resultado una pérdida total de la información. El complejo policial no cuenta con escaleras de emergencia para casos de incendio, siendo las escaleras internas la única vía de evacuación.
Afectación	El riesgo de incendio encontrado en la Escuela de Policía es alto ya que las oficinas administrativas están aprovisionadas con alfombras y techo cielo raso de material inflamable, las mismas que en caso de suscitarse un connato de incendio servirían para la propagación de fuego de manera más rápida devastando completamente el lugar. Otro factor de riesgo en el caso de incendio son las divisiones de las áreas administrativas las mismas que en algunos casos son de madera y vidrio las cuales no solo ayudan a la propagación del fuego si no que representan un peligro para las personas en el interior de las instalaciones debido a las explosiones de los vidrios causando lesiones graves al personal. Adicional a esto se debe considerar el almacenaje de la documentación de años anteriores que son apilados en el área académica.
Acción	Implementar extintores de espuma para inhibir la combustión de las alfombras y techo cielo raso, así mismo en el data center tener como mínimo DOS (02) extintores de anhídrido carbónico los cuales contrarresten la combustión de las alfombras y protegen los equipos electrónicos.
Responsable	Brigadista.

Fuente: Elaboración propia

Tabla N° 36. ESCENARIO IDENTIFICADO – TERREMOTO.

Riesgo	**Terremoto**
Probabilidad	Probable
Impacto	Muy Alto
Escenario	Las instalaciones de la Escuela, está ubicada en el complejo policial sede puente piedra en la ciudad de lima, el mismo que tiene 38 años de construcción, por lo cual en caso de producirse un terremoto, dependiendo de la magnitud podría producir la pérdida parcial o total de las instalaciones. Una vez determinando el impacto que puede generar en la Escuela Técnica de Policía y al evaluar la magnitud de los daños provocados, podemos decir que riesgo asociado es alto ya que al destruirse las edificaciones y por ende los accesos al piso en el que se encuentran las oficinas administrativas se puede presentar pérdida de bienes materiales así como de vidas humanas, y la pérdida inminente de los servicios ya que el Centro de Datos se verá afectado a gran escala ya que los equipos en donde se aloja la información y los servicios pueden presentar daños provocando así la perdida de continuidad de los mismos.
Afectación	Dependiendo el grado de magnitud del terremoto puede causar que se cuarteen o caigan las paredes con bajo nivel de destrucción (recuperables sin incidencia catastrófica) o puede ser una destrucción completa de las oficinas administrativas residentes.
Acción	Independientemente del grado o magnitud del terremoto la acción por parte del brigadista encargado es de ayudar a otros a evacuar el complejo evitando primordialmente pérdidas humanas y de ser posible los equipos informáticos (anteponer la vida antes que los equipos).
Responsable	Brigadista.

Fuente: Elaboración propia

Tabla N° 37. ESCENARIO IDENTIFICADO - FALLA DE ENERGÍA.

Riesgo	**Falla de energía**
Probabilidad	Posible
Impacto	Media
Escenario	El complejo policial existe generador de energía eléctrica que es utilizada como contingencia en caso de la suspensión normal del servicio eléctrico. Al evaluar el riesgo relacionado a los eventos de fallas en el servicio eléctrico, encontramos que se pueden presentar problemas en los equipos alternos como UPS's, bypass o generador de energía eléctrica. Al fallar los UPS's se puede tener un fallo global de todos los equipos electrónicos conectados a los mismos lo cual genera una pérdida sustancial en la parte de activos, además de la información contenida en los equipos informáticos. La configuración del bypass en caso de que no se encuentre bien realizada puede provocar que no encienda el generador de energía de manera automática. Esto puede provocar la suspensión de los servicios y la no operatividad normal de la institución por un periodo considerable de tiempo. Las fallas de energía afectan directamente a los equipos electrónicos, pueden ocurrir fallas que provoquen corto circuito y generar incendios, o en su defecto afectar directamente a un colaborador pudiendo ser electrocutado por descarga eléctrica.
Afectación	La Afectación puede ser leve o severa dependiendo del escenario, en el caso de CORTE TOTAL DE ENERGÍA puede quedar solamente en la discontinuidad de los servicios, por otro lado también pueden quemarse los equipos electrónicos no solo las UPS sino los servidores y otros. En caso de un incendio la afectación se vuelve severa y caeríamos en el caso de RIESGO POR INCENDIO.

Acción	Implementar UPS especiales que soporten grandes cargas de energía eléctrica de modo que no se produzca un apagón de los servidores y estos no resulten afectados; en adición tener en cuenta la acción del riesgo del incendio.
Responsable	Departamento de Tecnología.

Fuente: Elaboración propia

Tabla N° 38. ESCENARIO IDENTIFICADO – ROBO.

Riesgo	**Robo**
Probabilidad	Posible
Impacto	Alto
Escenario	La afectación que se produce directamente a los activos de la institución de los insumos que los colaboradores Policiales utilizan para el trabajo diario como las portátiles, módems y demás insumos; lo cual perjudica económicamente a la institución, los datos almacenados en medios electrónicos: portátiles, memorias USB, discos duros y cualquier otro medio que contenga información de los procesos académicos dela Escuela Técnica de Policía. Existen DOS (02) escenarios: 1. Robo Interno: Robo de equipos informáticos y otros que se produzcan dentro de las instalaciones por lo general en horas que las oficinas están prácticamente vacías. 2. Robo externo: Robo de equipos al personal mientras están fuera de las instalaciones de la institución Policial.
Afectación	El robo de los equipos informáticos a los efectivos Policiales de la Institución, en este caso la afectación recae severamente por la información de “el/los” clientes (alumnos, docentes, padres de familia y otros) que posee el efectivo policial en el computador a su cargo.
Acción	En el caso de robo interno, se debe tener alarmas además de las cámaras de seguridad y tener cuidado con el ingreso de personal ajeno a la institución para estar pendientes que se trate de un agente de confianza.

	En el caso de robo externo, es importante que los efectivos Policiales consideren el hecho de ir en unidades policiales de las comisarías de la zona al movilizarse con equipos computacionales.
Responsable	Todo el Personal.

Fuente: Elaboración propia

Tabla N° 39. ESCENARIO IDENTIFICADO– FALLO DE RED.

Riesgo	**Falla de la Red Informática**
Probabilidad	Probable
Impacto	Medio
Escenario	La Escuela Técnica cuenta con un enlace de Datos de su sede en puente piedra a Chorrillos (Dirección De Educación de la PNP), por lo que un fallo de red no debería ocurrir, en caso de ser lo contrario se pierden los servicios que la sede en Chorrillos como central provee a sede Puente Piedra además de que los colaboradores tienen sus carpetas en red con la información de los alumnos y los procesos académicos a los cuales acceden vía FTP. Una falla de red, aunque no es crítica se la considera importante puesto que los colaboradores que acceden a las carpetas en red para ver su información y los colaboradores que están en oficina. Existen varios tipos de causas por las cuales puede suscitarse fallas en la red informática de comunicaciones, como son: 1. Cruce entre hilos (mala conexión). 2. Ruptura de los cables. 3. Exceso de ruido y/o estática.
Afectación	El efecto que causa las fallas en la red informática es netamente con los sistemas de información, ya que si los servidores están haciendo rutinas automáticas de respaldo o incluso el personal está haciendo sus respaldos propios puede generar conflicto o fallas al generar la información respaldada, además de errores en la comunicación.

Acción	Proteger y resguardar el Data Center, cambiando el cableado estructurado periódicamente conforme a los protocolos de instalación y mantenimiento que exigen las normas internacionales, así mismo hacer mantenimiento de los equipos informáticos para reducir el impacto al suscitarse dicho problema.
Responsable	UNITIC.

Fuente: Elaboración propia

Tabla N° 40. ESCENARIO IDENTIFICADO– ATAQUES AL SISTEMA DE INFORMACIÓN COMPUTACIONAL.

Riesgo	**Ataques al sistema de información computacional**
Probabilidad	Posible
Impacto	Alto
Escenario	Al contar con información crítica de los clientes (Alumnos PNP, Docentes, Personal PNP y otros) es necesario que la resguardemos de manera confidencial, aunque los piratas informáticos atacarían la red organizacional para obtener dicha información. La institución Policial no se puede dar el lujo de que los datos almacenados sean alterados o substraídos por gente o ciber delincuentes que quieran desestabilizar a la institución y utilizando dicha información para crear inestabilidad social debido a que se forman Sub Oficiales Policías.
Afectación	Al tener plagio de información propia de la institución o información de otras instituciones de Educación Policial a nivel nacional ponemos en riesgo no solo a dichas instituciones sino a la misma Policía como tal por el factor de desconfianza que generaría dicho plagio lo que terminaría en pérdida de credibilidad y de clientes.
Acción	Implementar el “Sistema de Detección de Intrusos (IDS)” y otros sistemas para prevenir y detectar ataques de piratas informáticos.
Responsable	UNITIC.

Fuente: Elaboración propia

Tabla N° 41. ESCENARIO IDENTIFICADO – RIESGO OPERACIONAL.

Riesgo	**Riesgo Operacional**
Probabilidad	Altamente probable
Impacto	Muy Alto
Escenario	Este tipo de riesgo se relaciona directamente con el giro del negocio en este caso con el objetivo de la institución Policial, el riesgo operacional se encuentra ligado a los eventos fortuitos que pueden presentarse en el lapso de tiempo durante el internamiento de los Alumnos PNP y el proceso formativo que realizan, estos problemas pueden presentarse por: Al momento de realizar los procesos formativos de la unidad académica en sí se corre el riesgo de incumplir tiempos estipulados para entrega de informas resultantes, utilizar un lenguaje no adecuado con el cliente (alumnos PNP, Docentes, y otros) o dar juicios que provoquen inconvenientes dentro de la institución Policial.
Afectación	La severidad de impacto es la más alta considerando que si se produce el riesgo, lo posible es que se pierda prestigio de la imagen propia de la institución y por ende se perdería clientes a gran escala por lo cual la afectación de darse este riesgo es inminentemente catastrófico.
Acción	Planificar bien la realización de los procesos formativos de la unidad académica para mejorar tiempos de desarrollo de la misma teniendo en cuenta que se debe tener un lenguaje cordial sin emitir juicios anticipados respecto a matrículas, pase a retiro de alumnos, sanciones administrativas, admisión, contratación de docentes y otros.
Responsable	Unidad Académica.

Fuente: Elaboración propia

11. SERVICIOS CRÍTICOS A SALVAGUARDAR.

Es esencial definir los servicios que se debe preservar para la continuidad, lo siguientes son los servicios de tecnología críticos de La Escuela Técnica de Policía sede Puente Piedra (Lima) y están dispuestos en orden de prioridad de recuperación:

- Comunicaciones de red/conectividad, Internet.
- DNS y DHCP.
- Servicio de Correo (Servicio actualmente externalizado para alta disponibilidad y continuidad, infraestructura fuera de oficinas).
- Controlador de Dominio.
- Servicio de Archivos.
- Servicio de Aplicaciones.
- PCs individuales.
- Servicio de Respaldos de información.

a. Incidente y contingencia.

Este plan de recuperación de desastres se invocará bajo una de estas circunstancias:

- Un incidente que puede parcial o completamente paralizar las operaciones del centro de cómputo de La Escuela Técnica de Policía por un período de 24 horas.
- Un incidente, que ha afectado la utilización de las computadoras y redes administradas por Tecnología, debido a circunstancias que están más allá

del normal procesamiento de las operaciones del día a día. Esto incluye todos los procedimientos administrativos de la Unidad de Tecnología.

b. Seguridad Física.

- El centro de cómputo tiene una puerta con una cerradura de una sola llave, sólo personal de Tecnología tiene esta llave para ingresar a este sitio.

- Se ha colocado un sistema de detección remota de apertura de puertas en el rack de servidores con el fin de que envíe alertas vía email.

- Existe una cámara de seguridad externa que registra el movimiento del personal en el acceso al centro de cómputo.

- Ambos centros de cómputo albergan racks, servidores y equipos de comunicaciones. Estos llegan a ser los centros de las redes de datos de las oficinas administrativas de la Escuela Técnica de Policía.

- Tienen instalados sensores de temperatura, humedad y humo, dichos sensores están colocados extintores de incendio para equipos electrónicos en la parte externa del centro de cómputo.

- Los cuartos de servidores, tienen equipos UPS; ambos protegen los servidores y principales computadores por aproximadamente 15 minutos después de cortes de energía.

- Los servicios de aire acondicionado y la iluminación en los cuartos de servidores no están conectados al UPS.

c. Energía eléctrica y controles ambientales.

La Escuela de Policía cuenta con una central generadora de energía eléctrica autónoma en caso de ocurrir un prolongado corte de energía del sistema eléctrico público. Esta fuente de energía alterna alimenta a todo el sistema eléctrico de las oficinas administrativas incluyendo a las unidades de Aire Acondicionado, pero en caso de que las centrales sufran algún desperfecto y se interrumpa el flujo eléctrico a continuación se contemplan las siguientes acciones:

- Los métodos alternativos de refrigeración serían mediante la apertura del rack y la puerta del cuarto, así como la puesta en marcha de los ventiladores alternos existentes en el rack y como alternativa se debe abrir la puerta y colocar los ventiladores móviles de confort. De esto se encargaría el personal del Departamento de Tecnología.

- Los procedimientos anteriores ayudarían a mantener la temperatura ambiente de los cuartos en un clima relativamente frío, pero en el caso en que el cuarto de cómputo podría alcanzar un estado muy caliente y se debería apagar los servidores para precautelar su integridad como último recurso.

- Los Tecnología de aire acondicionado han sido probados para su normal funcionamiento. Los UPS no ofrecen servicio de energía

eléctrica a las unidades de aire acondicionado en caso de interrupción de energía.

- La empresa proveedora de las unidades de aire acondicionado es la encargada de ofrecer soporte y mantenimiento en caso de darse un desperfecto, la misma situación es para las unidades UPS. Se tiene un contrato de mantenimiento anual con cada proveedor para recibir asistencia preventiva y asistencia de emergencia si es del caso.

d. Protección ante software mal intencionado.

El software utilizado para protección contra virus es Symantec EndPoint Protection el cual provee seguridad virtual del equipo de computación optimizando el tiempo y rendimiento del ordenador, siendo que se actualiza constantemente para cubrir la protección en contra de amenazas nuevas y/o desconocidas además de las ya presentes.

El antivirus se encuentra localizado/alojado actualmente en un servidor que provee la seguridad a toda la red empresarial de tal manera que un equipo perteneciente al dominio y que tengan instalado el producto tendrá actualizado su antivirus contra las amenazas locales o externas (por política todo el personal de la Escuela de Policía debe tener instalado el antivirus).

12. PERSONAL DEL EQUIPO DE RECUPERACIÓN, COMITÉ DE CRISIS, COMITÉ DE EMERGENCIA.

a. Personal del Equipo de Recuperación.

En caso de producirse una falla con los equipos mencionados, la lista para llamadas de emergencia tendrá que ser utilizada. Las obligaciones generales del coordinador de recuperación de desastres deben ser discutidas. Los encargados del equipo de recuperación están asignados en cada oficina administrativa y las obligaciones generales dadas. El líder del equipo hará la asignación de personal en las oficinas, así como de las tareas específicas durante la etapa de recuperación.

Las únicas personas autorizadas a declarar el estado de desastre y por ende a inicializar el plan de recuperación son el Jefe de Tecnología o el Jefe de Informática. Un ejemplo de la referencia con las personas a ser llamadas en caso de daños se encuentra detallada en la Tabla N° 42.

b. Personal del Comité De Crisis (CC).

En caso de producirse un desastre, los encargados del comité de crisis están asignados en cada oficina administrativa y las obligaciones generales dadas. El líder del comité hará la asignación de personal en las oficinas, así como de las tareas específicas durante la etapa de la crisis suscitada.

Las únicas personas autorizadas a declarar el estado de desastre y por ende a inicializar el plan de recuperación se encuentran detalladas en la Tabla N° 43 y Tabla N° 44.

Tabla N° 42. Comité de Emergencia (CE)

Nro.	Grado Policial	Cargo Policial	Rol	Siglas	Ubicación
1	Coronel	Director de la Unidad	Directivo del Comité de crisis	DCC	ETP- P.P
2	Comandante	Sub Director de la Unidad	Gestor de Continuidad	GC	ETP-P.P
3	Comandante	Jefe Asesoría Legal	Miembro consultor de asuntos legales	MCAL	ETP-P.P
4	Comandante	Jefe de la unidad de Tecnologías	Coordinador de Tecnologías	CT	ETS-P.P
5	Mayor	Jefe de Logística	Coordinador de Logística y Seguridad	CLS	ETS-P.P
6	Mayor	Jefe de Recursos Humanos	Coordinador de Recursos Humanos	CRH	ETS-P.P

Fuente: Elaboración propia

Tabla N° 43. Comité de Emergencia Detallado (CE)

MIEMBROS DEL COMITÉ DE CRISIS	
ROL	**DESCRIPCIÓN**
Directivo del Comité de Crisis (DCC)	- Liderar, activar y desactivar el Comité de Crisis. Además cumple la función de proveer de recursos económicos al Comité y Grupos de recuperación.
Gestor de Continuidad (GC)	- Asesorar a los miembros del Comité en lo referido a los planes de continuidad de negocio.
Miembro consultor de asuntos legales (MCAL)	- Asesorar a los miembros del comité en lo referente a asuntos legales.

Fuente: Elaboración propia

Tabla N° 44. Comité de Emergencia Detallado (CE)

COORDINADORES OPERATIVOS DE APOYO AL COMITÉ DE CRISIS	
ROL	**DESCRIPCIÓN**
Coordinador de Tecnología (CT)	- Coordinar las actividades de evaluación / reparación de daños al centro de cómputo y las telecomunicaciones. Coordinar la activación del DRP (Disaster Recovery Plan) de ser necesario.
Coordinador de Logística y Seguridad (CLS)	- Coordinar las actividades de evaluación / reparación de daños al sitio afectado, así como coordinar la seguridad física.
Coordinador de RR.HH (CRH)	- Coordinar y supervisar las actividades relacionadas a la protección y bienestar del personal.

Fuente: Elaboración propia

c. Personal del Comité de Emergencia (CE).

Las únicas personas autorizadas para una efectiva y oportuna respuesta a Emergencia de la Institución Policial se han establecido y detallado en la Tabla N° 45 y los roles de éstos se detallan en la Tabla N° 46.

Tabla N° 45. Comité de Emergencia (CE)

Nro.	Grado Policial	Cargo Policial	Rol	Siglas	Ubicación
1	Comandante	Jefe de Unidad Académ ica	Coordinador General de Emergencia	CGE	ETP- P.P
2	Comandante	Jefe de Administración	Coordinador de Seguridad Ocupacional	SSO	ETP-P.P
3	Comandante	Jefe de Regimiento	Coordinador de Brigada de Evacuación	CBE	ETP-P.P

4	Mayor	Jefe de Personal	Coordinador de Brigada de primeros Auxilios	CBPA	ETS-P.P
5	Mayor	Jefe de Seguridad 01	Líder de Emergencia del Local	LEL	ETS-P.P
6	Mayor	Jefe de Seguridad 02	Brigadista de Emergencia del Local	BP	ETS-P.P
7	Capitán	Jefe de Grados y títulos	Brigadista de Emergencia del local de: Primeros Auxilios		ETS-P.P
8	Capitán	Jefe de Almacén	Brigadista de Emergencia del local de: Evacuación		ETS-P.P
9	Mayor	Jefe de Disciplina	Coordinador de Evaluación y Control de Daños	CECD	ETS-P.P
10	Capitán	Secretario	Coordinador de Mantenimiento	CM	ETS-P.P

Fuente: Elaboración propia

Tabla N°46. Roles del Comité de Emergencia (CE)

ROL	DESCRIPCIÓN
Coordinador General de Emergencia (CGE)	- Responsable general del Comité de Emergencia (CE) y del manejo de la situación de emergencia. - Responsable de coordinar directamente con el Comité de Crisis a fin de controlar los imprevistos y buscar las soluciones según sean necesarios. - Responsable de asegurar los recursos necesarios para la atención de emergencias. - Responsable de coordinar el despliegue de las actividades con el Coordinador de Seguridad y Salud Ocupacional (SSO) y el Coordinador de Evaluación y Control de Daños (CECD).
Coordinador de	- Responsable de la coordinación con los roles

Seguridad Ocupacional (SSO)	Coordinadores de Brigadas (CBE, CBCI, CBPA) - Responsable de la capacitación a los coordinadores y líderes brigadistas - Responsable de obtener los tiempos de evacuación - Responsable de gestionar la estrategia en caso de emergencia con los brigadistas de primeros auxilios.
Coordinador de brigada de Evacuación (CBE)	- Responsable de gestionar sus requerimientos para las evacuaciones. - Responsable de programar y dirigir los simulacros de evacuación para todo el personal, incluyendo terceros, según el programa anual de simulacros establecido. - Responsable de ejecutar, conjuntamente con el Líder de Emergencia por Local (LEL), las rutas de evacuación y las zonas seguras en caso de sismos, así como las zonas de reunión externas. - Responsable de medir los tiempos de evacuación y sugerir las acciones correctivas o de mejora al Coordinador de Seguridad y Salud Ocupacional (SSO).
Coordinador de Brigada de Primeros Auxilios (CBPA).	- Responsable de definir el requerimiento para la atención de primeros auxilios. - Responsable de implementar un área de atención exclusiva de primeros auxilios para todo el personal afectado. - Responsable de coordinar el despliegue de las actividades de los Líderes de Emergencia del Local (LEL).
Líder de Emergencia del Local (LEL).	- Responsable de definir el requerimiento para la atención para la emergencia. - Responsable de dirigir a los Brigadistas de Emergencia de su local en las diferentes fases de la gestión de emergencias. - Responsable de coordinar con los brigadistas la evacuación inmediata del local. - Responsable del cuidado del personal del local.
Brigadista de Emergencia del Local (BP).	- Responsable de definir el requerimiento para la atención para la emergencia. - Responsable del cuidado del personal del local. - Su principal función es asistir, al Líder de

	Emergencia del Local (LEL) a quien reporta, en las actividades de gestión de emergencia. Este rol está conformado principalmente por las siguientes funciones del **Brigadista de Primeros Auxilios** y **Brigadista de Evacuación.**
Brigadista de Emergencia del local de: Primeros Auxilios.	- Coordina sus acciones con el Líder de Emergencia del Local (LEL) - Responsable de realizar el mantenimiento y abastecimiento de los botiquines y equipos de primeros auxilios y velar por su libre acceso de acuerdo a inspección programada.
Brigadista de Emergencia del local de: Evacuación.	- Coordina sus acciones con el Líder de Emergencia por Local (LEL). - Responsable de realizar el mantenimiento a las señalizaciones, rutas de evacuación, zonas seguras, así como asegurar el libre acceso a las escaleras de emergencia en caso sea oportuno evacuar.
Coordinador de Evaluación y Control de Daños (CECD).	- Responsable del Centro de Control (CC) tiene a su cargo al operador del CC, y además, interactúa permanentemente con el Coordinador General de Emergencias (CGE). - Responsable del cumplimiento de las Inspecciones Técnicas de Seguridad a cargo del Instituto Nacional de Defensa Civil (cada 2 años). - Responsable de mantener la vigencia y coherencia de los procedimientos de evaluación y control de daños de la infraestructura física.
Coordinador de Mantenimiento (CM).	- Responsable de proponer el Programa de Mantenimiento preventivo, correctivo e inspección de los componentes de seguridad y protección ante emergencias, el cual involucra principalmente equipos e infraestructura. - Participar en las acciones de control, seguridad y rehabilitación de las instalaciones. - Participar en la evaluación de daños de la infraestructura afectada. - Participa en la reparación y/o reconstrucción de la infraestructura afectada. - Apoyar al Coordinador de Evaluación y Control

	de Daños en el abastecimiento de materiales en general, repuestos o insumos, equipos, así como de recursos de prevención y protección para las actividades de respuesta y control que eventualmente serán requeridos en la emergencias. - Responsable de las comunicaciones del Centro de Control (CC) debe proveer diferentes medios para habilitar las comunicaciones en caso de emergencia.

Fuente: Elaboración propia

13. PREPARACIÓN ANTE UN DESASTRE.

a. Procedimiento General.

Las responsabilidades se han dado para garantizar que cada una de las siguientes acciones se ejecute y para que su actualización sea continúa.

Mantenimiento y actualización semestral del plan de recuperación ante desastres, garantizar que todo el personal sea consciente de sus responsabilidades en caso de un desastre.

Asegurar que las rotaciones programadas de las copias de seguridad periódicas se están ejecutando, sobre todo para las unidades de almacenamiento localizadas en sitios externos.

El sostenimiento y la actualización periódica de los materiales de recuperación de desastres, específicamente la documentación de

información almacenada en sitios de seguridad externos a las oficinas administrativas.

El mantenimiento del estado actual de los equipos en los cuartos principales de servidores.

Informar a todo el personal de tecnología sobre una emergencia y los procedimientos adecuados de evacuación del centro de cómputo y de la Unidad de Tecnología.

Garantizar que los dispositivos UPS están funcionando correctamente y que están siendo revisados periódicamente.

Velar por que se mantenga la temperatura adecuada del centro de cómputo.

b. Cronograma General.

Sobre la base de la notificación de que un incidente se ha producido en cualquiera de los servicios informáticos de la institución Policial, el Coordinador de Recuperación ante Desastres o el encargado deben notificar a todos los demás responsables de la Unidad de Tecnología. La comunicación entre estos miembros es fundamental para el éxito de la recuperación y restauración ante un desastre.

Si los procedimientos de emergencia no se han invocado, con el indicador de cuatro horas después de la notificación inicial de un incidente, en

cualquiera de los servicios informáticos, el Plan de Recuperación ante Desastres entrará en vigor y debe seguir el siguiente cronograma:

Fase 1 - Dentro de 6 horas de la notificación inicial:

- Asegurarse de que todos los efectivos Policiales han sido evacuados del lugar y que sean tomados lista.
- Asegurarse de que el sitio principal centro de cómputo ha sido asegurado.
- Asegurarse de que las autoridades de seguridad y anti-incendios han sido notificadas.
- Decidir si se va a reabrir las oficinas administrativas principales o se trasladarán a un sitio Policial alternativo.
- Notificar a todo el personal de Tecnología de un desastre.
- El personal de Tecnología ya debe conocer de sus responsabilidades de recuperación primaria y el envío de un informe.

Fase 2 - Dentro de las 12 horas de la notificación inicial

- Confirmar el financiamiento disponible para los requisitos del plan de recuperación.
- Notificar a los proveedores de apoyo para recuperación de la catástrofe y el orden de sustitución del hardware preliminar.
- Iniciar el transporte de suministros y equipos al sitio de recuperación.
- Iniciar el transporte de los medios/Tecnología de recuperación y el hardware para el nuevo sitio.

Fase 3 - Dentro de las 24 horas de la notificación inicial

- Restauración de las copias de seguridad del sistema y pruebas de integridad.
- Garantizar la existencia de suficientes suministros en el sitio de recuperación.
- Llevar todos los dispositivos de recuperación.
- Establecer planes de copia de seguridad de todos los dispositivos recuperados.
- Notificar a todo el personal de Tecnología y de administración del sitio de recuperación.
- Inventariar los materiales recuperados del sitio primario.
- Volver a evaluar los daños y las pérdidas en el sitio primario.

Fase 4 - Dentro de las 48 horas de la notificación inicial

- Discutir entre los miembros de la Unidad de Tecnología sobre las causas y resultados.
- Decidir sobre permanecer o trasladarse al sitio de recuperación.
- Preparación para desastres en el sitio de recuperación.

Fase 5 – Dentro de los 7 días de la notificación inicial

- Limpieza del sitio primario
- Re - establecimiento del sitio primario