Universidad Nacional José Faustino Sánchez Carrión

Facultad de Ingeniería Industrial, Sistemas e Informática

Escuela Profesional de Ingeniería de Sistemas

Implementación de plan de contingencia de tecnologías de información en el parque informático de la Diresa Lima Huacho – 2022

Tesis

Para optar el Título Profesional de Ingeniero de Sistemas

Autor

Luis Angel Torres Quevedo

Asesor

Ing. Erlo Wilfredo Lino Escobar

Huacho – Perú

2024

UNIVERSIDAD NACIONAL
JOSÉ FAUSTINO SÁNCHEZ CARRIÓN

LICENCIADA

(Resolución de Consejo Directivo N° 012-2020-SUNEDU/CD de fecha 27/01/2020

"Año de la unidad, la paz y el desarrollo"

Facultad de Ingeniería Industrial, Sistemas e Informática

Escuela Profesional de Ingeniería de Sistemas

INFORMACIÓN DE METADATOS

DATOS DEL AUTOR (ES):		
NOMBRES Y APELLIDOS	**DNI**	**FECHA DE SUSTENTACIÓN**
Luis Angel Torres Quevedo	72654483	28/12/2023
DATOS DEL ASESOR	**DNI**	**CÓDIGO DE ORCID**
Erlo Wilfredo Lino Escobar	15608475	0000-0003-4889-6646
DATOS DE LOS MIEMBROS DE JURADOS – PREGRADO/POSTGRADO-MAESTRÍA-DOCTORADO:		
NOMBRES Y APELLIDOS	**DNI**	**CÓDIGO DE ORCID**
Luis Arsenio Rivera Morales	15611049	0000-0002-8070-8724
Ronald Eimer Alcántara Paredes	17925220	0000-0002-8016-1474
Josue Joel Rios Herrera	41997989	0000-0002-1157-0194

IMPLEMENTACIÓN DE PLAN DE CONTINGENCIA DE TECNOLOGÍAS DE INFORMACIÓN EN EL PARQUE INFORMÁTICO DE LA DIRESA LIMA, HUACHO - 2022

INFORME DE ORIGINALIDAD

20%	19%	2%	9%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	repositorio.unjfsc.edu.pe Fuente de Internet	4%
2	repositorio.udl.edu.pe Fuente de Internet	2%
3	hdl.handle.net Fuente de Internet	2%
4	repositorio.unesum.edu.ec Fuente de Internet	2%
5	repositorio.espe.edu.ec Fuente de Internet	<1%
6	dspace.ucuenca.edu.ec Fuente de Internet	<1%
7	repositorio.ug.edu.ec Fuente de Internet	<1%
8	repositorio.ucv.edu.pe Fuente de Internet	<1%

“IMPLEMENTACIÓN DE PLAN DE CONTINGENCIA DE TECNOLOGÍAS DE INFORMACIÓN EN EL PARQUE INFORMÁTICO DE LA DIRESA LIMA HUACHO – 2022”.

Autor

Bach. Torres Quevedo, Luis Angel

TESIS DE PREGRADO

Asesor

Ing. Lino Escobar, Erlo Wilfredo

UNIVERSIDAD NACIONAL JOSÉ FAUSTINO SANCHEZ CARRIÓN

FACULTAD DE INGENIERÍA INDUSTRIAL, SISTEMAS E INFORMÁTICA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

HUACHO – PERÚ

2024

IMPLEMENTACIÓN DE PLAN DE CONTINGENCIA DE TECNOLOGÍAS DE INFORMACIÓN EN EL PARQUE INFORMÁTICO DE LA DIRESA LIMA, HUACHO - 2022

ASESOR

ING. LINO ESCOBAR ERLO WILFREDO

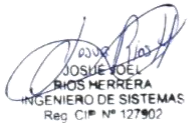
JURADOS EVALUADORES

PRESIDENTE

ING. LUIS ARSENIO RIVERA MORALES

SECRETARIO

ING. RONALD EIMER ALCANTARA PAREDES



VOCAL

ING.JOSUE JOEL RIOS HERRERA

.

DEDICATORIA

A Dios, por guiarme en mi camino y bendecirme siempre, por haber llegado hasta este preciso momento.

A mi hermosa familia que es mi razón de seguir luchando, esforzándome, dando muchas ganas de salir adelante, a mi madre Gloria, que siempre me apoya incondicionalmente, me da aliento para seguir adelante y no darme por vencido; a mi progenitor Arturo que me enseña con su fuerza y perseverancia para poder cumplir mis metas.

A mis hermanas Mery y Francesca que son mi motivación a diario.

A mis abuelos, quienes han sido los pilares de mi vida, ya que, con su trabajo duro y determinación, son a quienes admiro mucho.

A mi pareja Claudia, que nunca dejo de darme su ayuda idónea, la persona que me tuvo mucho paciencia y entrega, apoyándome en cada decisión que tomaba, la razón de no rendirme ni retroceder ante la vida.

AGRADECIMIENTO

Deseo agradecer al jurado por su dedicación al evaluar mi tesis y también a la Universidad por darme la oportunidad de obtener mi título profesional. Agradezco a mi familia y amigos cercanos por brindarme apoyo y confianza en mí mismo durante esta investigación.

INDICE

ÍNDICE DE TABLAS

ÍNDICE DE ANEXOS

RESUMEN

El presente trabajo de investigación titulado “Implementación de Plan de Contingencia de Tecnologías de Información en el Parque Informático de la DIRESA Lima, Huacho - 2022” tuvo como objetivo determinar la implementación de un Plan de Contingencia de Tecnologías de Información mejora el parque Informático de la DIRESA Lima. El estudio se llevó a cabo siguiendo una metodología no experimental en un nivel de investigación descriptivo. Además, tuvo un diseño no experimental y transversal con un enfoque cuantitativo. En este trabajo de investigación de metodología descriptiva las hipótesis se formulan, más no se demuestran, esto es por su metodología de investigación. Los estudios descriptivos se centran en medir variables de forma independiente.

Del total de trabajadores evaluados 100% (44) con respecto al plan de contingencia de tecnologías de la información, el 56.8% manifiesta que está indeciso, el 22.7% que si mejora y el 20.5% que no mejora. Sobre la dimensión de calidad se puede observar que del 100% (44) de los encuestados con respecto al plan de contingencia de tecnologías de la información, el 40.9% manifiesta que está indeciso, el 36.4% que si mejora y el 22.7% que no mejora. Sobre la dimensión de eficiencia se puede observar que del 100% (44) de los encuestados con respecto al plan de contingencia de tecnologías de la información, el 61.4% manifiesta que está indeciso, el 29.5% que si mejora y el 9.1% que no mejora. También podemos observar con respecto a la dimensión de continuidad que del 100% (44) de los encuestados con respecto al plan de contingencia de tecnologías de la información, el 59.1% manifiesta que está indeciso, el 29.5% que si mejora y el 11.4% que no mejora.

Se concluye que la DIRESA no está apta para hacer frente a eventos que puedan amenazar la seguridad de la información de sus activos. Es necesario realizar evaluaciones periódicas, ya sea cada semana o todos los días, que permitan conocer los riesgos y su impacto en los activos de información y en aquellos que los respaldan.

Palabras claves: plan de contingencia, tecnologías de información, calidad

ABSTRACT

The objective of this research work entitled "Implementation of the Information Technology Contingency Plan in the Information Technology Park of DIRESA Lima, Huacho - 2022" was to determine the implementation of an Information Technology Contingency Plan to improve the Information Technology Park of the DIRESA Lima. Methodology: the study was non-experimental, descriptive research level, non-experimental-transversal design and quantitative approach. In this descriptive methodology research work, the hypotheses are formulated, but not demonstrated, this is due to its research methodology, since descriptive studies measure variables independently.

Of the total number of workers evaluated 100% (44) with respect to the information technology contingency plan, 56.8% state that they are undecided, 22.7% that if it improves and 20.5% that it does not improve. Regarding the quality dimension, it can be observed that of 100% (44) of those surveyed regarding the information technology contingency plan, 40.9% state that they are undecided, 36.4% that it does improve and 22.7% that it does not. improvement. Regarding the dimension of efficiency, it can be observed that of 100% (44) of the respondents regarding the information technology contingency plan, 61.4% state that they are undecided, 29.5% that it does improve and 9.1% that it does not. improvement. We can also observe with respect to the continuity dimension that of 100% (44) of those surveyed regarding the information technology contingency plan, 59.1% state that they are undecided, 29.5% that if it improves and 11.4% that does not improve

It is concluded that the DIRESA is not prepared for any event that puts the security of the information of its assets at risk. There is a lack of weekly or daily assessments of risks and their impact on information assets, and those that support them.

Keywords: contingency plan, information technologies, quality.

INTRODUCCIÓN

Este trabajo de investigación titulado: “Implementación de Plan de Contingencia de Tecnologías de Información en el Parque Informático de la DIRESA Lima, Huacho - 2022”. Gonzales (2019) señala que: “La aprobación del presente Plan de Contingencias debe ser autorizada por el gobierno regional de Lambayeque y la UGEL para poder llevar a cabo las pruebas y aplicaciones correspondientes.”.

En una autoridad sanitaria como la DIRESA el respaldo de la información es de suma importancia, siendo una necesidad y obligación. Hoy en día, los Planes de Contingencia se refieren a protocolos preestablecidos que permiten alertar, movilizar y responder de manera efectiva ante la posibilidad de un evento específico extremadamente perjudicial. Estos planes incluyen escenarios definidos con claridad.

El Plan de Contingencia debe ser diseñado de acuerdo a las emergencias, para proporcionar una acción oportuna y efectiva con la probabilidad de minimizar sus efectos sobre la información de la institución.

Este Plan de Contingencia constituye un documento imprescindible de estar en constante actualización por parte de los encargados del área de DEIT, ya sea periodicamente un año siendo lo más factible y beneficioso para la organización; Con el objetivo de preservar la información, se busca detectar y reportar una emergencia lo más rápido posible, controlan, y minimizando el peligro de los equipos de trabajo como también la información.

En el capítulo I: Se planteó la situación de investigar un problema, se establecieron los propósitos generales y específicos, y se justificó la relevancia de llevar a cabo la investigación, así como la restricción y posibilidad de realizar el estudio.

En el capítulo II: Se tomaron en cuenta los contextos internacionales y nacionales, así como las teorías fundamentales del estudio, las definiciones conceptuales y la formulación de las suposiciones.

En el capítulo III: Se explica el enfoque y los métodos utilizados en la investigación, como la selección de la población y muestra, los criterios para incluir o excluir participantes, y cómo se

definieron y midieron las variables. También se detalla la técnica utilizada para recopilar los datos y cómo se procesaron los resultados obtenidos.

En el capítulo IV: Se presentan los datos, los hallazgos o los resultados obtenidos a partir de la investigación o el estudio realizado.

En el capítulo V: Se mencionan los análisis de los resultados obtenidos, las conclusiones alcanzadas y se ofrecen algunas recomendaciones basadas en el estudio.

En el capítulo VI: Se mencionan los recursos empleados para recopilar información en el estudio y, por último, se agregan los apéndices correspondientes.

Capítulo I: PLANTEAMIENTO DEL PROBLEMA

1.1. Descripción de la Problemática

Según DIRESA (2008), la Dirección Regional de Salud Lima es una entidad subordinada del Gobierno Regional Lima encargada de supervisar y aplicar la política, misión, visión, objetivos y regulaciones en el ámbito de la salud.(Artículo N°1. Naturaleza Jurídica); donde el respaldo de la información es una necesidad de vital importancia y una obligación.

En el Artículo N°6 del Título II. Estrucutura Orgánica del Reglamento de Organización y Funciones de la Dirección Regional de Salud, el apartado 6 presenta a los Órganos en Línea donde se encuentran las Direcciones Ejecutivas, encargadas de dirigir y supervisar el adecuado funcionamiento de la DIRESA, siendo de estas la Dirección Ejecutiva de Inteligencia Sanitaria una de las más importantes por tener a su cargo la Dirección de Estadística, Informática y Telecomunicaciones. (p. 5).

Las distintas direcciones que tiene la DIRESA Lima donde se encuentra la Oficina de Dirección de Estadística, Informática y Telecomunicaciones tiene como función básica conducir, planear, organizar, supervisar y coordinar, disponer de la información sanitaria para la toma de decisiones a todo nivel, así como también integrar, promover y desarrollar actividades formativas y de desarrollo que impulsen la mejora de los procesos estadísticos y de tecnologías de la información. Tiene a su cargo el Área de Desarrollo tecnológico, el Área de Estadística, y el Área de Informática y Telecomunicaciones siendo el último de estas, el área encargada de apoyar en estructurar la base de datos en coordinación con el responsable del Área de Informática y Telecomunicaciones; participar en el desarrollo de aplicativos que puedan optimizar, en la calidad y generación de reportes, de la

información requerida por la institución; apoyar en la programación e implementación de software administrativo y asistencial; brindar apoyo en las capacitaciones a los usuarios sobre los diversos software y aplicativos desarrollados en las diferentes áreas; brindar soporte técnico a los usuarios internos de la DIRESA Lima y externos (Direcciones de Redes de Salud y Hospitales); colabora en las tareas de prevención y solución de problemas en los equipos informáticos de la DIRESA Lima.

Los Planes de Contingencia son los protocolos previamente establecidos para coordinar y responder de manera rápida ante un evento en particular. Estos planes incluyen escenarios definidos y se utilizan para anticiparse y reaccionar eficientemente ante situaciones de emergencia o potenciales problemas, cabe recalcar que la mayoría de empresas e instituciones por no decir la mayoría de cualquier tipo de rubro no son ajenas a fallos o caídas de su sistema, evidenciando así el riesgo que corre sus diversas, funcionamientos o actividades diarias; ralentizando, retrasando los servicios internos que realiza la institución o empresa.

En lo que respecta a los datos de una empresa, el Plan de Contingencia se enfocará en una serie de medidas coordinadas y completas aplicadas con el fin de evitar, regular, resguardar y respaldar la información que se encuentra o es propiedad de la Dirección Regional de Salud Región Lima.

La creación del Plan de Contingencia tiene como objetivo principal lograr una respuesta rápida, oportuna y eficiente ante las situaciones de emergencia más probables, con el fin de reducir al mínimo los impactos negativos en la información.

La dirección de Estadística, Informática y Telecomunicaciones es la encargada de administrar, diseñar e implementar proyectos de desarrollo de software que permitan la optimización de los procesos que dan soporte a la DIRESA.

El área de Informática que está dentro de DEIT tiene a su cargo el mantenimiento de las aplicaciones software; realizar investigaciones en tecnologías de información, así como la planificación desarrollo e implementación de soluciones de Software; actualizar los procedimientos y dar mantenimiento al software desarrollado por la institución o sobre cuyo código fuente se tiene los derechos de propiedad.

Las debilidades que podemos encontrar en el área de Informática es el personal de Soporte Técnico insuficiente para atender la demanda de las áreas usuarias; fallo en las comunicaciones; la falta de capacitación a los trabajadores; infraestructura física acorde a las exigencias del área; problemas en los sistemas de información, como fallas en las redes, equipos y software; falta de implementación de un plan de capacitaciones al personal; falta de equipos de contingencia para la continuidad de servicios críticos; virus informáticos, troyanos, malware, etc; desastre por pandemia (COVID-19).

Para respaldar lo mencionado previamente, podemos resaltar algunos ejemplos de situaciones vividas en el campo de la tecnología de la información y el desarrollo DEIT en la DIRESA, como fue la pandemia de COVID-19 que se dio en el 2020 antes mencionada.

En el año 2020 en el mundo se da inicio a la pandemia de COVID-19, trayendo consigo desgracia e incontables perdidas a nivel mundial. El 15 de marzo de 2020, el Gobierno de Perú anunció un Estado de emergencia y una medida de aislamiento

social obligatorio en todo el país que duraría 15 días, lo cual se fue alargando así por varios meses; conllevando esa situación a que nadie pudiera ver o dar seguimiento a los equipos que se encontraban en mal estados, o los que necesitaban que un personal se encuentre viendolos para que no se den por obsoletos, pero por medidas de la pandemia no se podía trabajar; conllevando esto al descuido del parque informático de la DIRESA empeorando así los equipos. Los trabajadores de la institución regresaron en su mayoría a laborar, con fecha aproximada de agosto. Así mismo los directivos de cada área de oficina asistieron pero con el incoveniente de no utilizar con normalidad todos los equipos existentes hasta ese momento, poniendo así en duda la calidad que brinda el área de DEIT de las políticas que propone para soporte tecnológico. Dando en evidencia que no se a seguido con un monitoreo adecuado, no se llevo acabo una continuidad respecto a las evaluaciones de los equipos informáticos.

Estos problemas tienen como consecuencia la pérdida de la información recolectada y almacenada por la institución, lo cual puede ser muy difícil de recuperar, lo que a su vez afecta las funciones del área de DEIT y retrasa la eficiencia de los laboran dentr de la instituación. Por ende, se sugiere implementar un plan de contingencia para reducir y controlar los riesgos presentes o futuros.

Es importante considerar que el riesgo no se limita solo a los sistemas de información de TI, sino que también se aplica a los computadores utilizados en otras áreas, e incluso a los activos de toda la organización.

En tal sentido el trabajo de investigación tiene la finalidad de evaluar dicha implementación del Plan de Contingencia de Tecnologías de la Información en el Parque Informático de la Dirección Regional de Salud, que busca mitigar la mayoría

de riesgos existentes y/o posibles, mejorando la calidad demostrando que posee características unicas en la institución probando así que es seguro y confiable; mejorando la eficiencia para realizar su función adecuadamente argumentando que se encuentra actualizado y está bien adecuado; mejorando la continuidad en las capacitaciones para conformar un grupo de trabajadores eficacez en sus áreas respectivas.

1.2. Formulación del Problema

1.2.1. Problema General.

¿La implementación de un Plan de Contingencia de tecnologías de información mejora el parque informático de la DIRESA Lima, Huacho - 2022?

1.2.2. Problemas Específicos.

¿La implementación de Plan Contingencia de Tecnologías de Información mejora el nivel de calidad del parque informático de la DIRESA, Huacho-2022?

¿La implementación de Plan Contingencia de Tecnologías de Información mejora el nivel de eficiencia del parque informático de la DIRESA, Huacho-2022?

¿La implementación de Plan Contingencia de Tecnologías de Información mejora el nivel de continuidad del parque informático de la DIRESA, Huacho-2022?

1.3. Objetivos de la Investigación

1.3.1. Objetivo General.

Desarrollar la mejora de la implementación de un Plan de Contingencia de Tecnologías de información en el parque Informático de la DIRESA Lima, Huacho - 2022.

1.3.2. Objetivos Específicos.

Determinar si el Plan de Contingencia de Tecnologías de Información va a mejorar el nivel de calidad en el Parque Informático de la Dirección Regional de Salud, Huacho – 2022.

Determinar si el Plan de Contingencia de Tecnologías de Información en el Parque Informático va a mejorar el nivel de eficiencia de la Dirección Regional de Salud, Huacho – 2022.

Determinar si el Plan de Contingencia de Tecnologías de Información va a mejorar el nivel de continuidad en el Parque Informático de la Dirección Regional de Salud, Huacho – 2022.

1.4. Justificación de la Investigación

Conveniencia

Este estudio reveló ver el cambio que produce el plan de contingencia de Tecnologías de Información en el Parque Informático de la Dirección Regional de Salud, Huacho – 2022, a sabiendas de las incidencias que se presentan, las cuales afectan el desempeño y productividad de los servicios informáticos.

Relevancia social

Esta investigación permitió evidenciar los problemas en el parque informático, el desempeño del plan de contingencia de tecnologías de información en el parque informático de la Dirección Regional de Salud Lima, aportar soluciones a los problemas que se pueden presentar, porque busca mejoró el estado de la DIRESA, por tanto. Además, la realización de este estudio permitió a la DIRESA obtener información precisa y actualizada, lo que a su vez contribuyó a mejorar su desempeño mediante la implementación de medidas correctivas en colaboración con las autoridades correspondientes. Por lo tanto, se justifica plenamente la realización de esta investigación.

Implicaciones prácticas

El estudio llevado a cabo permitió la adopción de medidas que contribuyeron a solucionar en cierto grado el estado del parque informático de la Dirección Regional de Salud Lima, hecho que revirtió en lograr un mejor rendimiento en el desempeño de los trabajadores, implementando estrategias dirigidas a las autoridades de la DIRESA LIMA en la toma de decisiones para la mejora del plan de contingencia de tecnologías de información en el parque informática, y de qué manera influyen en varios aspectos de la calidad de los servicios informáticos.

Valor teórico

La información analizada proporcionó un mayor entendimiento sobre cómo utilizar a teoría de la contingencia señala que no hay nada definitivo en las organizaciones o en la teoría administrativa, ya que todo está sujeto a circunstancias específicas. Esto implica que existen vínculos funcionales entre las condiciones del entorno y las prácticas administrativas adecuadas para cumplir de manera exitosa los

objetivos de la organización. Ello permitió evaluar el nivel de aprobación del plan de contingencia de Tecnologías de Información en el parque informático de la Dirección Regional de Salud Lima.

Utilidad metodológica

Este estudio ha sido utilizado como una guía y una referencia para investigaciones futuras relacionadas con el problema identificado. Estas investigaciones han utilizado una delimitación espacial diferente y diferentes reactivos.

1.5. Delimitación del Estudio

1.5.1. Delimitación Espacial.

La investigación se llevará a cabo en el Parque Informático de la Dirección Regional de Salud, situado en la avenida Calle José Arámbulo La Rosa N° 134 de la ciudad de Huacho, departamento de Lima, Perú.

1.5.2. Delimitación Temporal

La investigación mencionada fue llevada a cabo en la Dirección Regional de Salud Lima - Huacho, durante los meses de Febrero – Julio del año 2022.

1.5.3. Delimitación Temática

El objetivo de este estudio es analizar la conexión entre el plan de emergencia y las tecnologías de la información.

1.6. Viabilidad del Estudio

1.6.1. Viabilidad Temática

Se pudo llevar a cabo la investigación debido a que se obtuvo suficiente información de diversas fuentes como la internet, revistas científicas, tesis académicas y otros documentos bibliográficas.

1.6.2. Viabilidad Administrativa

Se obtuvo el permiso del jefe del Parque Informático y también se contó con la autorización del director de DIRESA al firmar el consentimiento informado.

1.6.3. Viabilidad Económica

El responsable de esta investigación proporcionó los recursos humanos y económicos necesarios sin recibir financiamiento externo, asegurando así que la DIRESA no incurriera en gastos adicionales.

1.6.4. Viabilidad Técnica

El presente estudio cuenta con todas las herramientas adecuadas y necesarias para llevar a cabo la presente investigación: Metodología, Empresa de desarrollo la investigación, personal humano, internet, computadoras, etcétera.

Capítulo II: MARCO TEÓRICO

2.1. Antecedentes de la investigación

Los frecuentes problemas que se venían aquejando el parque informático, que pusieron en manifiesto la necesidad de Equipos de Cómputo y un gran déficit de Software que tiene la DIRESA Lima de equipos de cómputo para las diversas Oficinas de la Dirección Regional de Salud de Lima, en reemplazo de las computadoras que se encuentran No Operativas, y algunas que presentan fallas críticas.

Durante el periodo comprendido desde el año 2015 a la actualidad, el área de soporte técnico de la DIRESA ha venido reparando, repotenciando y dando mantenimiento preventivo y correctivo con mucha mayor frecuencia que en años anteriores a los equipos de cómputo dicha institución. A su vez el área de soporte técnico ha reportado equipos entre impresoras, laptops y computadoras de escritorio como dados de baja, debido a esto se ha podido observar que un alto número de ordenadores están llegando al límite de su funcionabilidad; estás cifras aumentaron aún más en pandemia, ya que no se estuvieron monitoreando ni dando seguimiento a los equipos.

2.1.1. Antecedentes Internacionales

Gonzabay (2022). En su estudio de investigación Avance de un plan de contingencia informático para central de datos y comunicación de la empresa AGUAPEN-EP por medio del uso de normas internacionales. Para obtener la titulación de Ingeniero en Tecnologías con respecto a la Información en la Universidad Estatal Península de Santa Elena, Ecuador.

Cuyo finalidad es Crear un plan de contingencia mediante la detección de posibles peligros y la implementación de protocolos de control basados en estándares internacionales para el departamento de Tecnologías de la Información de la empresa Aguapen EP. La metodología empleada fue de investigación de tipo exploratorio, según la investigación, se pudo determinar que se implementaron medidas y protecciones recomendadas por las normas ISO 27002 y proporcionadas por el instituto SANS, con el fin de garantizar una adecuada gestión de la seguridad de la información y proteger la confidencialidad, integridad y disponibilidad de los datos..

Llumiquinga (2015). Cuyo estudio de investigación analizaron el diseño de política de seguridad de la información y la creación de un plan de contingencias para el área de sistemas de la Cooperativa de Ahorro y Crédito Alianza del Valle, para la titulación de Ingeniero en Sistemas e Informática en la Universidad de las Fuerzas Armadas ESPE, Ecuador. Cuyo objetivo es promover o facilitar la oferta de servicios a los miembros mediante la utilización de ventanillas compartidas y la instalación de cajeros automáticos a través de BANRED. El enfoque utilizado para desarrollar las Políticas de Seguridad se basó en el análisis previo de las amenazas y riesgos a los que se enfrenta la COACAV, teniendo en cuenta el ciclo de vida de una Política de Seguridad. Según la investigación, actualmente, las instituciones dependen en gran medida de la informática para llevar a cabo sus actividades, especialmente en aquellas de carácter financiero que dependen en gran medida de la información para llevar a cabo sus operaciones y brindar un buen servicio a sus clientes. La COAC Alianza del Valle es un claro ejemplo de esto, ya que su funcionamiento se basa casi exclusivamente en los recursos

informáticos. En caso de que ocurra un desastre que interrumpa los servicios informáticos por un período prolongado, las consecuencias podrían ser tanto pérdidas financieras como un grave daño a la reputación de la institución, especialmente si la responsabilidad recae en el área de tecnología. Esto podría llegar a afectar la credibilidad del público y, en última instancia, llevar al fracaso total de la institución. Por esta razón, es fundamental considerar la información como un activo clave y prepararse para protegerla y estar listos para enfrentar distintos tipos de desastres tomando medidas de seguridad, ya sean de origen humano o natural, mediante un Plan de Contingencia y la implementación de políticas de seguridad adecuadas.

Granda (2011). En su estudio de investigación la creación de un plan de contingencia en el campo de las Tecnologías de la Información y las Comunicaciones (TICs) para la empresa Eléctrica Centrosur, como parte del proceso de obtención del título de Magíster en Gerencia de Sistemas de Información (MGSI). Cuyo objetivo es Desarrollar un Plan de Contingencia de TI para la Empresa Eléctrica Cento Sur. La metodología empleada fue Magerit en conjunto con los controles de seguridad norma ISO 27001. Según la investigación, se deduce que el propósito del plan no es evitar por completo los riesgos, sino minimizar al máximo el impacto que las incidencias puedan tener en la organización.

Llerena (2006). En su estudio de investigación Desarrollo del Manual de Seguridades Informáticas de la Armada del Ecuador, para la titulación de Ingeniero en Sistemas, Informática en la Universidad de las Fuerzas Armadas ESPE, Ecuador. El objetivo de este proyecto es crear un Manual de Seguridad

Informática específicamente para la Armada del Ecuador, con el objetivo de lograr una protección eficiente de los recursos informáticos.. La metodología empleada fue metodología de análisis de riesgos. La investigación llega a la siguiente conclusión Se realiza un análisis de la situación actual del entorno informático con el fin de identificar los posibles riesgos a los que se encuentran expuestos los activos y los factores que los ponen en dicha situación. Esto permite generar políticas que se ajusten a las normas institucionales, con el objetivo principal de lograr la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de los datos.

2.1.2. Antecedentes Nacionales

Gonzales (2019). En su investigación, se ha realizado un estudio sobre la creación de un Plan de Contingencia como una forma de gestionar los riesgos de seguridad de la información en el área del centro de Sistemas de Información de la UGEL-FERREÑAFE durante el año 2018. El objetivo principal del estudio es desarrollar este Plan de Contingencia con el propósito de abordar y mitigar los riesgos de seguridad de la información en dicha área durante el período mencionado. La metodología empleada es Magerit V3. Se ha determinado que la organización no está preparada para enfrentar situaciones que amenacen la seguridad de la información de sus recursos. Para resolver esta situación, es importante realizar evaluaciones periódicas, ya sea semanalmente o diariamente, con el objetivo de identificar y comprender los riesgos y su impacto en los activos de información y en los sistemas que los respaldan.

Espinoza (2014). En su estudio titulad Diseño de un plan de contingencia de sistemas informáticos para la Universidad Peruana los Andes, con el propósito de obtener el título de Ingeniero de Sistemas y Computación, se propone el diseño de un plan para asegurar la continuidad de los sistemas informáticos en dicha institución. La metodología empleada es la Norma ISO 27001 y el ISO 27002. De acuerdo con la investigación, se propone una solución para abordar la problemática actual, la cual se basa en la metodología del ciclo de vida de sistemas.

Alfaro (2008). En su estudio de investigación metódica de la auditoría integral para la Gestión de la TI, para la titulación de Ingeniero Informático en la Pontífice Universidad Católica del Perú. Se busca crear una metodología (MAIGTI) que permita auditar de forma integral la gestión de la tecnología de información, utilizando un enfoque basado en estándares de calidad internacionales como: COBIT, ISO/IEC 12207, ISO/IEC 17799, ISO/IEC 20000 Y PMBOK. Esto ayudará a realizar evaluaciones más precisas y a contribuir al logro de los objetivos de la organización. Una metodología es un conjunto de métodos, procedimientos y estándares que se utilizan para desarrollar un producto mediante enfoques de ingeniería integrados. Sin embargo, investigaciones han demostrado que no se ha creado una metodología completa para auditar la gestión de la tecnología de la información. Actualmente, los enfoques existentes se basan en el proceso general de auditoría, pero no integran de manera adecuada los diferentes estándares internacionales de calidad y las normas vigentes para las entidades que se someten a una auditoría.

2.1.3. Antecedentes Locales

Vega (2015). Su estudio se titula Plan de Contingencia para OSI dentro de la Universidad Nacional José Faustino Sánchez Carrión , por el grado de Ingeniero Informático en la Universidad Nacional José Faustino Sánchez Carrión. El propósito de este estudio es determinar el grado de aceptación de un plan de emergencia por parte del departamento de Tecnología de la Información de la UNJFSC. La metodología empleada es el descriptivo. El estudio concluye que, para el Nivel de Seguridad del Plan de Contingencia dimensiones como calidad, eficiencia y continuidad, porque para toda organización la información es uno de los bienes más valiosos, y mantenerlo debe ser de mucho cuidado para que no sea vulnerable por algún delito informático. Se realizaron encuestas, aplicando como instrumento un cuestionario para determinar el Nivel de Seguridad del Plan de Contingencia de la Oficina de Servicios Informáticos validado mediante el juicio de expertos alcanzando 88,84 y con una fuerte confiabilidad obtenida mediante el Alpha de Cronbach 0.801. Se trabajo con la población total debido a que esta es pequeñaa, pero para darle el sustento estadístico se aplico la muestra probabilística al 99% de confiabilidad siendo esta muestra igual a la población de los trabajadores de la oficina de servicios informáticos.

2.2. Bases Teóricas

2.2.1. Plan de Contingencias

Para Aguilera (2010), sostiene que cualquier amenaza a los activos del sistema de información puede representar un riesgo para la supervivencia de una empresa. Por este motivo, el plan de contingencia se muestra como una herramienta de administración que incluye medidas tecnológicas, humanas y organizativas, con el objetivo de salvaguardar el sistema de información frente a las posibles amenazas o recuperarlo después de un incidente.

se divide en tres subplanes que funcionan de forma independiente, que se mencionan a continuación:

El plan de respaldo se implementa acciones de precaución con el objetivo de evitar posibles daños. Podemos tomar como ejemplo el acto de crear y guardar duplicados de la información en un lugar seguro para su protección y preservación, para así poder recuperarla en caso de sufrir un impacto negativo.

Plan de emergencia. incluye las medidas que se deben seguir cuando una amenaza se materializa o acaba de suceder, como agilizar la recuperación de las copias de seguridad o automatizar el sistema de extinción de incendios.

Plan de recuperación. Tiene como objetivo principal restaurar la normalidad después de un evento catastrófico. Esto implica implementar acciones diversas para minimizar los daños y restablecer las operaciones lo más rápido posible. Después de un desastre, se pone en marcha un plan cuyo propósito es evaluar el impacto y restablecer el funcionamiento normal del sistema y la

organización. Por ejemplo, si un lugar alternativo para seguir con las actividades habituales ha sido devastado, se buscará otro lugar para llevar a cabo estas actividades. Además, se sustituirá el material que se haya deteriorado, se reinstalarán aplicaciones y se restaurarán las copias de seguridad.

Es fundamental que, al desarrollar el plan de contingencias, no se descuide la preparación del personal de la organización. Es importante que estén informados sobre el plan y reciban entrenamiento para estar preparados y saber cómo actuar en caso de que ocurra una amenaza o un impacto.

Plan de Contingencia como Subconjunto de Seguridad de la Información

Kuong (1986), menciona que el coordinador de recuperación de desastres debe estar involucrado en áreas de seguridad, como la supervisión de acceso físico al centro de procesamiento de datos. Muchos desastres son causados intencionalmente o por accidente por empleados u otras personas que tienen acceso a los datos. La implementación de medidas efectivas de control de acceso puede reducir significativamente el riesgo de desastres causados por el hombre. Es importante que el grupo que tiene la responsabilidad de la creación del plan de contingencia comprenda los sistemas de seguridad instalados y qué están protegiendo, para determinar si deben permanecer en el sitio o ser guardados fuera. Además, puede ser necesario que el responsable de la seguridad sea parte de los equipos de recuperación para garantizar que se reinstalen los controles de seguridad cuando se reaccione o reconstruya el centro de cómputo. Estos ejemplos ilustran la importancia de la conexión entre la seguridad de la información y el plan de contingencia, ya que este

último es esencial para garantizar la continuidad de las operaciones empresariales.

Plan de Contingencia y de Seguridad de la Información

Según Stallings (1990), define que la seguridad de la información se comprende como un conjunto de herramientas creadas para proteger los datos. Los recursos o activos que deben ser salvaguardados son la información y el equipo, siendo la información la más importante. Por lo tanto, cuando hablamos de pérdidas de estos recursos, nos referimos a la divulgación no autorizada o accidental de información y a la pérdida de medios físicos. También hay otras causas de incidentes informáticos, como errores del operador, fallos en los componentes físicos del sistema, errores en el software utilizado, inexactitudes en los datos almacenados, problemas en las instalaciones y bajo rendimiento del sistema, entre otros.

La seguridad de la información también busca combatir el crimen informático, que se dirige al software y los datos de una computadora.

Los recursos computacionales que se deben proteger son los elementos físicos y la información que se almacena y procesa en las computadoras.

El hardware o hardware computacional abarca diferentes tipos de computadoras, como:

- Las grandes (mainframes) que se encuentran en los centros de datos.
- Las medianas (mid-range), así como también incluye las comunicaciones y redes, y distintos dispositivos de

almacenamiento como discos duros fijos, discos flexibles y otros medios de almacenamiento.

Se considera información computarizada a los programas de software y su documentación, así como a los datos almacenados o en proceso en computadoras, los datos transmitidos por líneas de comunicación y los datos en medios transportables como discos y cintas.

Seguridad Informática

> "La disciplina se dedica a desarrollar las normas, procedimientos, técnicas y métodos pertinentes para establecer un sistema financiero e informativo confiable." (Aguilera, 2010).

Tipo de Seguridad

En efecto Aguilera (2008), menciona lo siguiente:

a. La activa comprende las medidas de defensa que buscan prevenir o reducir los riesgos en el sistema, como impedir el acceso no autorizado mediante contraseñas, instalar antivirus para evitar la entrada de virus y encriptar mensajes para evitar que sean leídos sin autorización.
b. La pasiva comprende las acciones que se llevan a cabo después de que se produce un incidente de seguridad, con el propósito de reducir sus efectos y ayudar en la recuperación del sistema, tales como efectuar las copias periódicos de los datos.

Servicios de Seguridad

a. Integridad: La integridad de los datos y la autenticidad de los mensajes recibidos se aseguran.
b. Confidencialidad: Protección para evitar la revelación no autorizada de datos en una comunicación.
c. Disponibilidad: Asegurar la disponibilidad de la información para los entes autorizados.
d. Autentificación o identificación: Verificación de la identidad de los usuarios y entidades para permitir el acceso al sistema.
e. No repudio (o irrenunciabilidad): Generación de evidencias irrefutables de la auditoría de un hecho para evitar la negación de acciones realizadas.
f. Imposibilidad de negar la emisión o recepción de información ya realizada.
g. Control de acceso: Se implementa un control riguroso sobre quién puede acceder a los recursos del sistema, permitiendo el acceso solo a aquellos usuarios y personal autorizados.

Mecanismos de Seguridad

a. Las medidas de prevención son implementadas antes de que un ataque ocurra con el fin de evitarlo.

b. Los sistemas de detección se activan una vez que ha ocurrido un ataque, pero antes de que cause daño al sistema.
c. Las medidas correctivas se aplican después de que se ha producido un ataque y ha causado daños, con el objetivo de corregir las consecuencias del mismo.

La protección de la información digital se basa en la seguridad lógica, que utiliza herramientas y métodos para garantizar su integridad.

a. Control de Acceso: Para ingresar es necesario tener un nombre de usuario y una contraseña.
b. El Cifrado de Datos implica utilizar un algoritmo para encriptar la información, generando así una clave especial. Solo el emisor y el receptor están en conocimiento de esta clave.
c. Antivirus: El antivirus tiene la capacidad de identificar y detener la entrada de virus y otros programas dañinos, y si el sistema se infecta, puede eliminarlos y solucionar los problemas causados en el sistema.
d. Firewall: El cortafuegos es un dispositivo (puede ser software, hardware o una combinación de ambos) que controla el acceso al sistema, permitiendo, denegando o restringiendo dicho acceso.

e. Certificados Digitales: Los certificados digitales son documentos en formato digital que verifican la identidad de una persona o entidad y cuentan con el respaldo de la validación de su clave.

Seguridad Física: Se refiere a las medidas físicas y mecanismos implementados para salvaguardar el sistema y la información de posibles riesgos tanto físicos como lógicos.

a. Hacer una copia de seguridad de los datos implica obtener una duplicación de la información del sistema y guardarla en un lugar seguro para asegurar que esté disponible cuando se necesite.
b. Los dispositivos físicos de protección son herramientas como pararrayos, detectores de humo, extintores, cortafuegos físicos, alarmas contra intrusos, sistemas de alimentación ininterrumpida, y sistemas de acceso restringido para proteger contra intrusiones a las instalaciones.

Directrices de Seguridad

La política de seguridad de la información recoge los lineamientos y metas establecidas por una organización. Es una parte esencial de su política general y requiere la aprobación de la dirección.

La principal intención al redactar una política de seguridad es crear conciencia entre todo el personal, especialmente aquellos involucrados directamente en el sistema de información, sobre los

principios que las reglas y directrices que establecen la seguridad en la entidad y las normas que se deben seguir para alcanzar los objetivos de seguridad planificados son los principales responsables de la seguridad. Es por ello que la política de seguridad debe ser redactada de manera que todos los empleados de la organización la comprendan. Las políticas varían en función de la realidad y las necesidades particulares de la organización a la que se dirigen, lo que implica que no todas son idénticas.

También hay normas de políticas de seguridad que han sido establecidas por diferentes países.

Una política de seguridad tiene como objetivo establecer los planes y estrategias que la empresa utilizará para proteger su sistema de información. Estos objetivos se agrupan en cuatro áreas principales:

- Identificación de necesidades de seguridad y evaluación de riesgos para los sistemas de información, incluyendo la evaluación de posibles impactos de ataques.
- Identificar las reglas de seguridad apropiadas que se deben implementar para protegerse de los riesgos identificados en cada activo.
- Establecer reglas y procedimientos que deben seguirse en todos los departamentos de la organización para hacer frente a los riesgos identificados.

- Identificar vulnerabilidades en el sistema de información para monitorear cualquier falla que ocurra en los recursos, incluyendo las aplicaciones que hayan sido instaladas.

2.2.1.1. Calidad

Para Baca (2014) , la calidad se refiere a la medida en la que un dato cumple con los estándares, convenciones y regulaciones vigentes en relación con la calidad de los datos en un contexto particular de uso..

En la opinión de Aranda, et al. (2013) argumentan que evaluar la calidad de los datos implica medir el nivel de satisfacción de sus características y cómo cumplen con las necesidades establecidas. Por otro lado, el enfoque dependiente del sistema analiza la calidad de los datos considerando el ámbito tecnológico en el que se utilizan, incluyendo hardware, sistemas informáticos, planes de contingencia y otros programas.

2.2.1.1.1. Seguro

En la opinión de Arroyo (2016) es crucial garantizar seguridad de la infraestructura, la información almacenada o transmitida en una computadora o red de computadoras es de vital importancia. Esta disciplina se encarga de establecer reglas, estrategias, pautas, enfoques y prácticas para garantizar la seguridad. Su objetivo principal es asegurar que los recursos de software se empleen únicamente con los fines para los que fueron diseñados.

Por otro lado, Erb (2005) nos menciona que la seguridad está relacionada con los atributos y situaciones de los sistemas de tratamiento de información y su conservación, para asegurar la privacidad, exactitud y disponibilidad de dichos datos. Tomar aspectos de seguridad en cuenta implica tener conocimiento de los riesgos, clasificar y salvaguardarlos de los choques o perjuicios de la forma más eficiente.

2.2.1.1.1.1. Confiable

Según Castillo (2012) nos relata que la confiabilidad se relaciona con la posibilidad de que un sistema funcione de manera adecuada durante un periodo de tiempo específico y bajo condiciones específicas. Este concepto es esencial en los procesos de producción, ya que los sistemas están en constante cambio y modernización. El análisis de la confiabilidad se vuelve cada vez más importante y necesario al evaluar los procesos, con el objetivo de garantizar el buen desarrollo de los sistemas de producción. Por lo tanto, es crucial contar con literatura que sea fácil de entender y que proporcione una revisión exhaustiva del tema.

2.2.1.2. Eficiencia

Yepes (2013) se afirmó que el uso de recursos del sistema es apropiado. Estos recursos pueden abarcar otros programas de software con los cuales la aplicación debe interactuar en ciertos momentos, así como también la configuración de software y hardware necesaria para el sistema, y los materiales necesarios.

2.2.1.2.1. Actualizado

Bellido (2013) nos relata que las actualizaciones de planes de contingencia, software y normativas consisten en que las mencionadas se encuentren en continua actualización para mejorar o corregir falencias dentro de la empresa, institución u organismo gubernamental.

2.2.1.3. Continuidad

En la opinión de Martínez, (2020) la continuidad comprende un conjunto de acciones orientadas a alcanzar la excelencia en los productos, servicios y procedimientos de una organización. Muchas empresas grandes cuentan con un departamento dedicado específicamente a la mejora constante de sus procesos de fabricación.

Para Bessant (1993), citado en Carrascosa (2012) afirma que la continuidad es un concepto fácil de aplicar para diversos aspectos en la producción, tales como la flexibilidad, los costos, la productividad y por último la calidad.

2.2.1.3.1. Capacitación

IICA (2020) nos explica que la capacitación se refiere a actividades de enseñanza y aprendizaje que permiten a las personas adquirir nuevos conocimientos y habilidades, así como cambiar su actitud en relación con las necesidades de un campo ocupacional específico. Estas actividades suelen ser de corta duración y se

consideran parte de la educación no formal, especialmente en el caso de la educación de adultos.

2.2.1.3.2. Respaldo

Cardador (2015) analiza que, dado que un proceso de respaldo, backup o copia de seguridad nunca se puede interrumpir, en este caso lo ideal sería esperarnos en torno a los 10-15 min a que a los usuarios de la red les diera tiempo de volver a la normalidad de trabajo con sus equipos y lanzar de nuevo el proceso de respaldo que estábamos realizando. Además, deberíamos tener en cuenta que si ha producido un corte en el suministro eléctrico inesperado puede ser que algún equipo haya reusltado dañado.

2.2.2. Tecnologías de Información (TI)

Para Baca (2014), se refiere a un conjunto de teorías y técnicas que se utilizan para aplicar el conocimiento científico de manera práctica. De acuerdo con Manuel Castells, las tecnologías de la Información engloban varias tecnologías relacionadas con la microelectrónica, la informática, las telecomunicaciones y la ingeniería genética, la cual se enfoca en decodificar, manipular y reprogramar los códigos de materia viva. En la década de los 90, se produjo una convergencia entre la biología, la electrónica y la informática, lo que permitió su interacción en diferentes áreas como aplicaciones, materiales y conceptos de planificación. La incorporación de las Tecnologías de la Información (TI) ha sido de gran relevancia en el mundo empresarial, ya que ha posibilitado acelerar de forma coordinada los flujos de información y logística, algo que no sucedía por completo en las empresas tradicionales.

La tecnología de la información se refiere a las funciones de información necesarias para las actividades de un proceso de negocios. Estas actividades están vinculadas a estas funciones y la TI realiza funciones operativas para respaldarlas. Las operaciones son consideradas como funciones de información activas y forman parte del soporte que la tecnología de la información proporciona a los procesos. Esto establece el fundamento conceptual para reconocer los elementos, los cuales deben incluirse en los tipos de procesos de negocios que explícitamente consideren una relación con la TI.

Por su parte Fernández (2014), la Tecnología de Información se refiere a las herramientas y medios que permiten a las personas interactuar utilizando tecnología como base. Esta interacción requiere la participación de un emisor, un receptor y un canal de comunicación, por lo que algunas veces se las denomina TI y Comunicaciones.

La TI brinda el cimiento necesario para que una empresa pueda construir sus sistemas de información específicos. Anteriormente, cada departamento contaba con un autónomo sistema de información y tecnología propia. Similar ocurre con el área de producción, e incluso dentro de cada departamento, existían sistemas libres los cuales no se comunicaban entre ellos. Esto generaba ineficiencias en el trabajo y aumentaba la posibilidad de cometer errores al momento de compartir información, ya que se requería integrar ambos sistemas.

En la opinión de Corona (2015), se entiende por tecnología el conjunto de técnicas utilizados en procesos productivos, sistemas operativos. Esta

puntualización incluye tanto la tecnología visible o tangible, como la tecnología invisible o intangible, que engloba conocimientos y técnicas. Por otro lado, la Información se define como un conjunto organizado de datos que transmiten un mensaje sobre un ente o fenómeno específico. En consecuencia, la Tecnología de la Información hace referencia a las herramientas específicas, sistemas y programas informáticos utilizados para transferir información entre las partes interesadas.

Desde la posición de De Pablos Heredero (2011), se entiende como un sistema de información empresarial a un grupo de bienes técnicos, económicos e individuos que se relacionan entre sí de manera dinámica al objetivo de responder las necesidades de información de una organización empresarial para la toma de decisiones. Los elementos esenciales de un sistema de información empresarial moderno son:

- La información, capturada, almacenada, procesada y distribuida por el sistema.
- Los individuos que ingresan para emplear la información.
- Los grupos de tratamiento de la información y conectarse con los usuarios, como hardware, software y redes de comunicaciones.
- Las normas de trabajo, que son los métodos utilizados para las tecnologías que llevan a cabo sus tareas.

En resumen, un SI eficaz es aquel que proporciona la información requerida al ente del momento adecuado, mientras que un sistema eficiente lo hace utilizando los recursos tecnológicos, humanos, temporales y económicos mínimos. El sistema de una entidad es un componente adentro

del sistema de información y está compuesto por los recursos necesarios para el procesamiento automático y la comunicación de la información, es decir, las TI y las comunicaciones.

Definición de Información

Según Daler (1988), señala que el término información se utiliza de diversas formas, pero en el contexto del procesamiento electrónico de datos (EDP), se refiere a la recopilación y presentación de datos con un significado. En la actualidad, un sistema de información basado en EDP eficiente que pueda generar información relevante de manera oportuna para apoyar la toma de decisiones correcta se ha convertido en uno de los factores de competitividad más relevantes.

Gestión de información

Los datos y los sistemas de datos son extremadamente valiosos, por lo tanto, deben ser considerados como recursos estratégicos (al igual que el capital o el espacio físico) y deben recibir la misma protección. Es crucial asegurar la protección de toda la información para garantizar la credibilidad, calidad y precisión para los usuarios. El responsable de la seguridad de la información es la persona o entidad que posee dicha información

Componentes de las Tic's.

Según Hernández (2013), cuyos componentes fundamentales de las tic’s incluyen:

1. Software: Se categorizan en tres aspectos importantes:
    - ✓ Lenguajes de programación: Son software utilizados para comunicarse con una computadora. Funcionan como lenguajes artificiales para dar instrucciones al equipo y permitir que realice diferentes tareas. Tanto los sistemas operativos como los paquetes de software, como Word. A lo largo del tiempo, los lenguajes de programación han evolucionado para ser más seguro y robustos. También se han ajustado a los entornos tecnológicos actuales, como la evolución en Internet. Incluso, a partir de un lenguaje de programación pueden originarse nuevos idiomas. Algunos ejemplos de lenguajes de programación son Cobol, C#, Java, Visual Basic, PHP y HTML.
    - ✓ Sistemas operativos: son esenciales para el funcionamiento de cualquier dispositivo electrónico que realice múltiples tareas. Por ejemplo, un teléfono celular necesita controlar cada una de sus funciones para asegurarse de que todas las acciones se ejecuten correctamente, sin conflictos y de acuerdo a las instrucciones del usuario. Lo mismo ocurre con las computadoras, donde el sistema operativo se encarga de determinar qué acción se realiza primero y

consecuente. Es como el control de tráfico en un cruce de dos avenidas principales, donde cada automóvil representa una instrucción, como imprimir, abrir un archivo o mover el cursor del mouse. Sin un sistema operativo para regular ese tráfico, habría un caos y nadie podría avanzar. En resumen, sin un sistema operativo, una computadora no podría funcionar.

- ✓ Paquetes computacionales y aplicaciones: se refieren a los programas que se ejecutan en un sistema operativo para llevar a cabo tareas específicas en la vida cotidiana. Estos programas pueden dividirse en categorías como automatización de oficinas, diseño, música, videojuegos y bases de datos.

2. Componentes físicos: se refiere a todos los elementos físicos de una computadora, tanto internos como externos, que ayudan a procesar y obtener información. Antiguamente, se consideraba hardware solo a los dispositivos enlazados de primera al equipo, sin embargo en la actualidad, se han creado nuevas categorías como las tablets, gadgets y smartphones, que también se consideran hardware. Una forma de clasificarlo es:

   - ✓ Los periféricos de entrada son los dispositivos físicos utilizados para ingresar información en una

computadora de escritorio. Algunos ejemplos de periféricos de entrada son el teclado, el mouse, el escáner, los monitores táctiles, las memorias USB, las cámaras de video y los lectores ópticos.

- ✓ Periféricos de salida son dispositivos físicos que extraen datos de una PC, por ejemplo, el monitor, la impresora, USB, los altavoces, entre otros.

Hay varios tipos de ordenadores, y aunque todos ellos realizan tareas similares, su rendimiento puede variar significativamente. Estos se pueden categorizar como:

- o De escritorio: Las computadoras de escritorio constan de un despacho, una pantalla, un teclado y un ratón.
- o Portátiles: son muy convenientes, ya que se pueden llevar a cualquier lugar y trabajar con ellas debido a su tamaño y batería integrada. Incluso existen modelos que pueden recibir internet a través de la telefonía celular. Estos dispositivos son cada vez más populares y es muy probable que reemplacen a las computadoras de escritorio en el futuro.
- o Servidores: son equipos informáticos más potentes que proporcionan diversos servicios, como impresión, conectividad, comunicación y aplicaciones, a otros equipos informáticos.

- Súper computadoras: son equipos utilizados en grandes organizaciones, instituciones educativas o centros de investigación para llevar a cabo una amplia gama de tareas que no pueden ser realizadas por computadoras de escritorio o servidores convencionales.

Los robots son dispositivos electrónicos y mecánicos que realizan tareas repetitivas o peligrosas para los seres humanos, sin tener una apariencia o diseño específico. En el ámbito de la fabricación en serie, los robots son de gran importancia, ya que, con un mantenimiento adecuado y una programación eficiente, pueden trabajar durante largos períodos sin cometer errores y reducir los costos de producción.

3. Las comunicaciones entre dispositivos han evolucionado y se han adaptado a las nuevas tecnologías. La existencia de diversas formas de internet, como intranet y extranet, han ayudado a fortalecer las distintas clases de redes, como las LAN, las WA) y las intercontinentales IAN. Para que estas redes puedan comunicarse, se utilizan diferentes dispositivos de hardware de comunicación, como switches, hubs, ruteadores, microonda, cables UTP o de fibra óptica, etc.

   Las redes pueden ser clasificadas en diferentes categorías:

- ✓ LAN: Conocida como Red de Área Local, es utilizada por organizaciones que vinculan sus equipos y distribuir archivos, impresoras y servicios de aplicaciones o bases de datos. Si bien no existe una definición precisa sobre la distancia entre los dispositivos conectados en una red LAN, generalmente se refiere a redes que se encuentran en un mismo edificio o en varios edificios dentro de una misma empresa.
- ✓ Una Red de Área Metropolitana (MAN) permite a una empresa enlazar dos ubicaciones diferentes en la misma ciudad a través de una misma red. La conexión puede realizarse mediante diferentes medios, como teléfono, microondas, enlaces dedicados digitales o Internet. Por ejemplo, una empresa con su sede corporativa en el norte de la ciudad y un punto de venta en el sur puede establecer una conexión para que ambos formen parte de la misma red.
- ✓ WAN: es un tipo de red que conecta 2 o más redes LAN ubicadas en distintos puntos geográficos. Por ejemplo, una empresa que tiene una sede principal y una sucursal en otra ciudad. La conexión entre estas redes puede realizarse a través de diferentes medios, como microondas, enlaces de fibra óptica

o incluso a través de Internet. No existe una definición precisa que determine cuántos kilómetros son necesarios para que una red sea considerada WAN en lugar de una red MAN.

- ✓ IAN: conectan 2 redes ubicadas en continentes distintos, ya sea a través de satélites o mediante cables de fibra óptica. Estas redes son menos conocidas debido a su conexión mediante Internet.

4. Redes web:
    - ✓ Internet es un sistema global de servidores interconectados que permite compartir información y comunicarse entre sí. También es conocido como la red de redes, este medio permite realizar transacciones como también puede conseguir información en vivo. El internet ha revolucionado el trabajo en equipo, ya que ha eliminado las limitaciones de tiempo, distancia y espacio.
    - ✓ La intranet se refiere al empleo de las tecnologías de internet en el seno de una entidad específica. Esto abarca servidores de aplicaciones, correo electrónico y páginas web, pero su alcance se limita a la red local o LAN de la organización.
    - ✓ La extranet es una ampliación de la intranet que permite a clientes, usuarios externos o socios acceder a servicios tales como aplicaciones, correos

y servicios en línea. A diferencia de la intranet, la extranet tiene un alcance más amplio que la red local, pero el acceso puede estar restringido.

- ✓ Internet 2 es un proyecto en desarrollo que cuenta con el involucramiento de entidades universidades por todo el mundo y cuenta con el respaldo financiero de importantes empresas. El objetivo de esta nueva red es poder ofrecer velocidades de transmisión aún más rápidas que las actuales en internet. Se espera que los usuarios particulares puedan disfrutar de velocidades de hasta 50 Mbps, mientras que los miembros de Internet 2 podrán alcanzar velocidades de hasta 622 Mbps. Entre las propuestas que se están considerando para Internet 2 se encuentra la implementación de un nuevo protocolo de comunicación llamado IPv6.

5. Las bases de datos: son una parte especial del software que merece una atención particular. Se trata de un conjunto de datos e información que se almacena, organiza y se divide en categorías, y que puede ser administrado y consultado para aprovecharse y ayudar en las decisiones. Los bancos de datos están compuestos por tablas, que forman la estructura básica de la información. Todas las empresas hacen uso de bases de datos las cuales están compuestas por campos de datos que forman registros. Hay diferentes

formas de utilizar la información almacenada en una base de datos:

- ✓ Data warehouse: almacenamiento de bases de datos en el cual se recopila información generada por diferentes sistemas y se guarda en una base de datos propia. Si una organización dispone de diversos sistemas o bases de datos sin conexión entre sí, puede resultar complejo aprovechar la información de manera eficiente. Data Warehouse es crucial, puesto que actúa como un punto de unión para las bases de datos de todos los sistemas corporativos, lo cual posibilita la extracción de información según los criterios o variables requeridos por parte del usuario. El término "Data Warehouse" se utiliza cuando una empresa maneja una gran cantidad de información proveniente de una amplia variedad de información, y los administradores necesitan tomar decisiones de forma confiables como también rápidas. Según Bill H Inmon, un DW es un sistema que combina diferentes bases de datos para brindar un soporte eficiente a la toma de decisiones de los altos y medios directivos. Este conjunto de información está enfocado en un tema específico y cada dato almacenado es relevante en algún momento determinado.

- ✓ Datamart: Es un tipo de repositorio de datos que se especializa en un solo tema o departamento y recibe información de una o pocas fuentes. Tanto un data warehouse como un datamart tienen una estructura de datos eficiente que permite analizar información detallada y abarcar todos los procesos importantes para un departamento. Ambos pueden emplearse para desarrollar sistemas expertos y sistemas de apoyo a la toma de decisiones, como DSS y también ESS.
- ✓ Minería de Datos: Podemos inferir que en una base de datos extensa con muchas tablas, campos y registros, la mayoría de la información no es importante para tomar decisiones. Por lo tanto, es necesario filtrar la información, lo cual puede ser complicado si la información necesaria no es explícita. El uso de la minería de datos se asemeja a buscar piedras preciosas en una mina, ya que se sabe que lo que se busca está entre la tierra y la piedra, pero es necesario excavar, picar, remover y luego filtrar para llegar a él. La minería de datos se utiliza en diversos ámbitos: IA, árboles de decisión, redes neuronales, etc.

6. Sistemas de BD de vanguardia: Existen varios sistemas de última generación disponibles. Hay diversas alternativas para elegir, tanto gratuitas como de pago, para elegir. Entre las opciones gratuitas más populares y actuales se encuentran MySQL, SQLite, entre otros. Por otro lado, entre los sistemas de BD de pago más populares se encuentran Microsoft Access, Microsoft SQL y Oracle. Aunque también existen sistemas más antiguos como dBase, Fox Pro, Sybase, entre otros por mencionar; aún se utilizan debido a su estabilidad y funcionalidad. Es relevante mencionar que los softwares de código abierto no siempre son gratis, aunque suelen ser mucho más económicos en comparación con los sistemas con licencia. Los pros y contras de utilizar software de código abierto o con licenciamiento podrían ser discutidas en detalle. Es destacable mencionar que al optar por sistemas libres, es necesario considerar el coste del proyecto se encuentra en la manutención de la BD y no habrá ningún respaldo o responsabilidad por parte de una compañía en la gestión de la misma. En contraste, es importante planificar de manera adecuada cuando se adquiere software privativo, ya que su costo puede ser elevado en función del número de licencias necesarias.
7. Tecnología de negocios: En la era actual, la tecnología ha generado transformaciones en los esquemas comerciales,

siendo el internet un protagonista crucial en este proceso. Estos términos, como E-commerce, E-business por nombrar algunos, han cambiado la forma en que se llevan a cabo transacciones y trámites:

- ✓ E-commerce: El comercio electrónico se refiere a la venta de bienes y servicios a través de internet, lo que permite hacer transacciones de compra de manera fácil y rápida. Con solo tener una computadora en casa o incluso un teléfono celular se pueden realizar compras desde cualquier lugar. Cada vez más empresas adaptan sus productos y servicios para ser vendidos en línea.
- ✓ E-business: se diferencia del ecommerce en que no se limita a intercambios comerciales, sino que implica procesos operativos y de colaboración entre empresas, clientes y proveedores. Algunas empresas realizan todas sus operaciones a través de plataformas web, permitiendo un acceso seguro desde cualquier parte del mundo a su CRM, ERP, etc. Adicionalmente, el comercio electrónico utiliza otros términos como el negocio entre empresas (B2B) y el negocio entre empresa y cliente (B2C). (p. 22).
- ✓ E-government: El gobierno ha implementado una forma de facilitar los trámites para el pago a los

residentes o colaboradores Ahora es posible realizar estas actividades a través de internet, como, por ejemplo, pagar la tenencia o impuestos personales, así como solicitar documentación como actas de nacimiento, licencias o permisos.

2.3. Definición de términos básicos

a) Plan de Contingencia

Para Capra (2013). la continuidad operativa consiste en un plan estratégico con diferentes pasos que nos guían para encontrar una solución alternativa que nos ayude a recuperar los servicios de la organización de manera rápida, en caso de que se presenten eventos que afecten los servicios de forma parcial o total.

b) Contingencia

Nos dice Nauca (2019). Un evento o suceso es algo que ocurre de manera imprevista y genera cambios en el funcionamiento habitual de una organización.

c) Información

Según Lapiedra (2011). Un conjunto de datos organizados de manera sistemática y estructurada destinados a generar conocimiento en uno o varios temas para el lector.

d) Calidad

Para Baca (2014), la calidad se refiere al nivel en el que los datos cumplen con normativas, convenciones o regulaciones actuales y reglas similares, relacionadas con la calidad de los datos en un contexto de uso específico.

e) Seguro

En la opinión de Arroyo (2016) la protección de la infraestructura, la computación y la información en un ordenador o red de ordenadores es de suma importancia. Este autor sostiene que la disciplina encargada de diseñar las reglas, estrategias, procesos, técnicas y metodologías para mantener la

seguridad y confiabilidad de un sistema de información es fundamental. En resumen, su objetivo es garantizar que los materiales y recursos de software se utilicen exclusivamente para los fines para los que fueron creados.

f) Confiable

Según Castillo (2012) explica que la confiabilidad, entendida como la probabilidad de que un sistema funcione correctamente durante un periodo de tiempo determinado bajo condiciones específicas, es un concepto esencial en la producción. A medida que los sistemas de producción evolucionan y se modernizan constantemente, el análisis de confiabilidad se vuelve cada vez más relevante e imprescindible en la evaluación de los procesos, con el fin de asegurar un buen desarrollo de dichos sistemas. En consecuencia, es necesario contar con literatura de fácil comprensión y que abarque exhaustivamente el tema.

g) Eficiencia

Yepes (2013) se considera apropiado utilizar los recursos del sistema, los cuales pueden abarcar otros productos de software con los que la aplicación necesita interactuar, así como la configuración del software y hardware necesarios para el funcionamiento del sistema, así como los materiales que se requieren.

h) Actualizado

Bellido (2013) nos relata que las actualizaciones de planes de contingencia, software y normativas consisten en que las mencionadas se encuentren en continua actualización para mejorar o corregir falencias dentro de la empresa, institución u organismo gubernamental.

i) Continuidad

En la opinión de Martínez, (2020) la continuidad se refiere a todas las acciones que se realizan con el fin de garantizar la calidad óptima de los productos, servicios y procesos de una empresa. Muchas empresas importantes cuentan con un departamento encargado de mejorar de manera constante sus procesos de producción.

j) Capacitación

IICA (2020) nos menciona lo siguiente, la capacitación se refiere a actividades educativas que tienen como objetivo que los participantes adquieran nuevos conocimientos y habilidades, y también cambien su actitud hacia las necesidades de un campo de trabajo específico. Estas actividades suelen ser de corta duración y se consideran dentro de la educación "no formal" y, en este caso, dentro de la "educación de adultos".

k) Respaldo

Cardador (2015) analiza que, dado que un proceso de respaldo, backup o copia de seguridad nunca se puede interrumpir, en este caso lo ideal sería esperarnos en torno a los 10-15 min a que a los usuarios de la red les diera tiempo de volver a la normalidad de trabajo con sus equipos y lanzar de nuevo el proceso de respaldo que estábamos realizando. Además, deberíamos tener en cuenta que si ha producido un corte en el suministro eléctrico inesperado puede ser que algún equipo haya reusltado dañado.

2.4. Hipótesis de investigación

2.4.1. Hipótesis General.

La implementación de un Plan de Contingencia mejora las tecnologías de información en el Parque Informático de la DIRESA Lima, Huacho – 2022.

2.4.2. Hipótesis Específicos.

La implementación de un Plan de Contingencia de Tecnología de Información mejora el nivel de calidad en el Parque Informático de la DIRESA Lima, Huacho - 2022.

La implementación de un Plan de Contingencia de Tecnología de Información mejora el nivel de eficiencia en el Parque Informático de la DIRESA Lima, Huacho - 2022.

La implementación de un Plan de Contingencia de Tecnología de Información mejora el nivel de continuidad en el Parque Informático de la DIRESA Lima, Huacho - 2022.

2.5. Operacionalización de las variables

Variable		Definición Conceptual	Definición Operacional	Dimensiones	Indicadores	Ítems	Escala de medición	Instrumento
Variable Independiente	**Plan de Contingencia**	Se trata de una herramienta de gestión para asegurar el buen funcionamiento de las Tecnologías de la Información y las Comunicaciones en relación con el apoyo y el rendimiento de los empleados. (Verdú, 2015)	Mi variable Plan de Contingencia tiene las siguientes dimensiones: ➢ Calidad ➢ Eficiencia ➢ Continuidad	**Calidad:** El Plan de contingencia cumpla con los requisitos que se deben adoptar con el objetivo de reducir los daños**.**	**Seguro:** Existencia de normas, manuales, políticas o documentación de soporte tecnológico. **Confiable:** Dispone de una historia demostrando buenos resultados, además de ser fiable y da seguridad.	1,2,3,4,5,6	**Escala de Likert** (5) Totalmente de acuerdo (4) De acuerdo (3) Indiferente (2) En desacuerdo (1) Totalmente en Desacuerdo	Cuestionario
				Eficiencia: El Plan obtiene el mejor resultado empleando la menor cantidad de recursos.	**Actualizado:** Consigue estar al día en normas y políticas que van surgiendo.	7,8,9,10,11		
				Continuidad: Supervisión y análisis de los procedimientos de contingencia y recuperación	**Capacitación:** Enseñanzas acerca del plan de contingencia y asuntos relacionados. **Respaldo:** Protege y garantiza el impacto del problema.	11,12,13,14, 15		

Fuente: Elaboración propia: Operacionalización de Variables

Capítulo III: METODOLOGÍA

3.1. Diseño Metodológico

Tipo de investigación

El tipo de estudio es no experimental porque según Velázquez (2023) el estudio en cuestión es no experimental ya que no se basa en la realización de acciones y reacciones reproducibles en un entorno controlado para obtener resultados interpretables, como lo haría un estudio experimental. En este tipo de investigación, las conclusiones finales y los datos de trabajo no se extraen mediante experimentos.

Nivel de investigación

De acuerdo con Gay (1996) la investigación descriptiva implica recopilar datos para verificar hipótesis o responder preguntas sobre la situación actual de los sujetos del estudio. Un estudio descriptivo revela y reporta las características de los objetos.

Diseño

Según Dzul (2008), se afirma que el estudio no es experimental ya que no se manipularon ni modificaron ninguna variable.

Según su amplitud en el tiempo

La toma de información se llevó a cabo durante un período de tiempo en relación a la muestra, por lo tanto, es una investigación transversal.

Enfoque

Según Hernández (2014) , sostiene que el enfoque cuantitativo defiende la idea de que el conocimiento debe ser imparcial y que se obtiene mediante un proceso de

razonamiento deductivo. Para esto, es necesario utilizar mediciones numéricas y análisis estadísticos para probar hipótesis que han sido previamente formuladas.

3.2. Población y muestra

La población de la investigación estará constituida por 44 trabajadores de la DIRESA.

3.2.1. Población

Según la definición dada por Espinoza (2016) un conjunto es un grupo de elementos que puede ser finito o infinito y que comparten una o más características. Este conjunto se representa con la letra N.

La población de la investigación estará constituida por los 44 trabajadores de la Dirección Regional de Salud en este año laboral 2022.

De las siguientes áreas:

Tabla 1

Tamaño de la Población

Personal de DIRESA	**N de Muestra**
Adquisiciones	2
Asesoría Legal	2
Oficina de Estadística, Informática y Telecomunicaciones	3
Logística	3
Calidad	2
Educación para la Salud	2

Epidemiología y Salud	2
Dirección de Prevención y Control de Emergencias y Desastres.	2
Registro	2
Economía	2
Oficina Promoción de Vida Sana y Participación Comunitaria en Salud-DESI	2
Recursos Humanos	2
DPCED	2
Tramite Documentario	2
Samu	2
Salud Ambiental	2
Salud Mental	2
Salud en tu Casa	2
OCI	2
Patrimonio	2
Promsa	2
N° Total	44

Fuente: Elaboración Propia: Tamaño de la población

Áreas donde las personas fueron encuestadas.

3.2.2. Muestra

De acuerdo con Díaz (2016), una muestra representa una porción de la población total. La muestra se puede describir como un subconjunto o grupo más pequeño que forma parte de una población o universo. Para seleccionar una muestra, es necesario primero establecer y delimitar las características de la población. (p. 5).

Criterios de inclusión

- Trabajadores cuyas edades están entre 18 a más años

Criterios de exclusión

- Trabajadores cuyas edades son menores de 18 años.
- Personas que no trabajen en la institución.

3.3. Técnicas de recolección de datos

Para llevar a cabo la investigación y recopilación de datos, se proporciona a los trabajadores un cuestionario adjunto (anexo 1). Por lo tanto, para nuestra primera variable, Plan de Contingencia, hemos elegido utilizar una ficha de recolección de datos como instrumento para obtener la información necesaria.

3.4. Técnicas para el procedimiento de la información

Después de recopilar los datos, se utilizará Microsoft Excel para codificarlos y luego serán analizados en el software estadístico SPSS 25.0 para crear y analizar las tablas estadísticas.

Capítulo IV: RESULTADOS

4.1. Análisis de resultados

Tabla 2

Plan de Contingencia de Técnologías de Información

Plan de Contingencia	n	%
No mejora	9	20,5
Indeciso	25	56,8
Si mejora	10	22,7
Total	44	100,0

FUENTE: PARQUE INFORMATICO DE LA DIRESA LIMA, HUACHO – 2022

En la tabla 2 se puede observar que del 100% (44) de los encuestados con respecto al plan de contingencia de tecnologías de la información, el 56.8% manifiesta que está indeciso, el 22.7% que si mejora y el 20.5% que no mejora.

Figura 1

Plan de Contingencia de Tecnologías de Información

FUENTE: PARQUE INFORMATICO DE LA DIRESA LIMA, HUACHO – 2022

Tabla 3

Plan de Contingencia de Tecnologías de Información en la Dimension Calidad

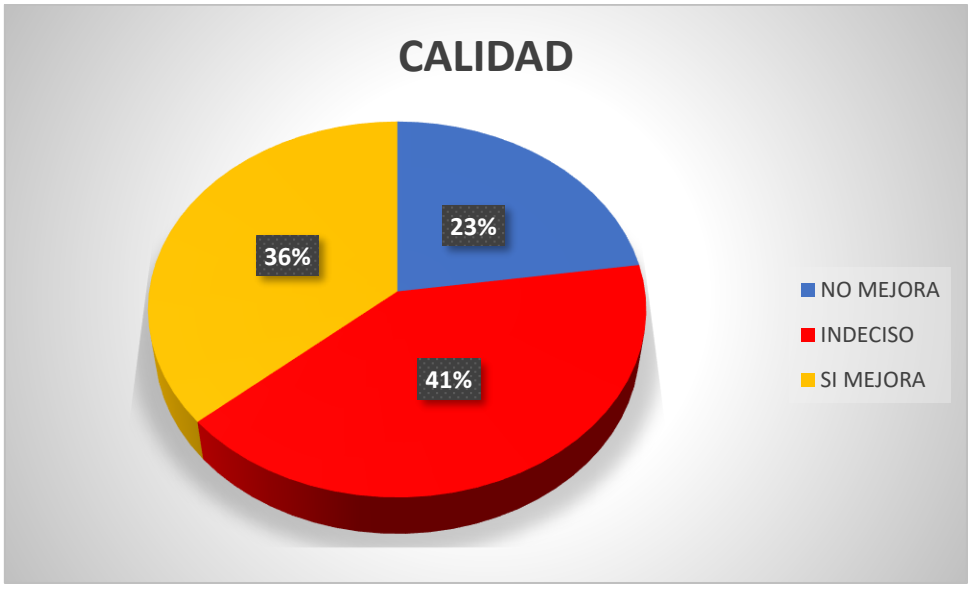
Plan de Contingencia	n	%
No mejora	10	22,7
Indeciso	18	40,9
Si mejora	16	36,4
Total	44	100,0

FUENTE: PARQUE INFORMATICO DE LA DIRESA LIMA, HUACHO – 2022

En la tabla 3 se puede observar que del 100% (44) de los encuestados con respecto al plan de contingencia de tecnologías de la información en la dimensión calidad, el 40.9% manifiesta que está indeciso, el 36.4% que si mejora y el 22.7% que no mejora.

Figura 2

Dimensión Calidad



FUENTE: PARQUE INFORMATICO DE LA DIRESA LIMA, HUACHO – 2022

Tabla 4

Plan de Contingencia de Tecnologías de Información en la Dimensión Eficiencia

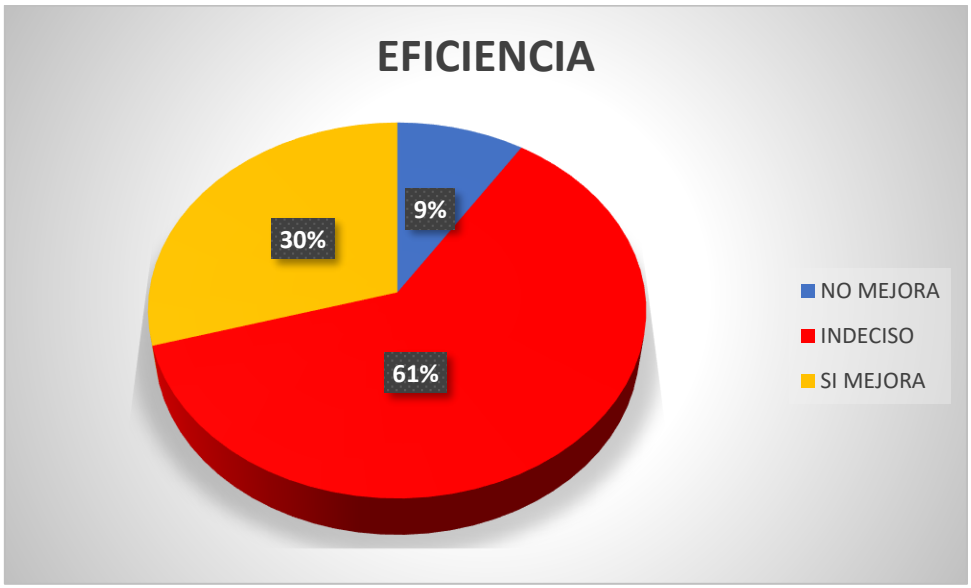
Plan de Contingencia	n	%
No mejora	4	9,1
Indeciso	27	61,4
Si mejora	13	29,5
Total	44	100,0

FUENTE: PARQUE INFORMATICO DE LA DIRESA LIMA, HUACHO – 2022

En la tabla 4 se puede observar que del 100% (44) de los encuestados con respecto al plan de contingencia de tecnologías de la información en la dimensión eficiencia, el 61.4% manifiesta que está indeciso, el 29.5% que si mejora y el 9.1% que no mejora.

Figura 3

Dimensión Eficiencia



FUENTE: PARQUE INFORMATICO DE LA DIRESA LIMA, HUACHO – 2022

Tabla 5

Plan de Contingencia de Tecnologías de Información en la Dimensión Continuidad

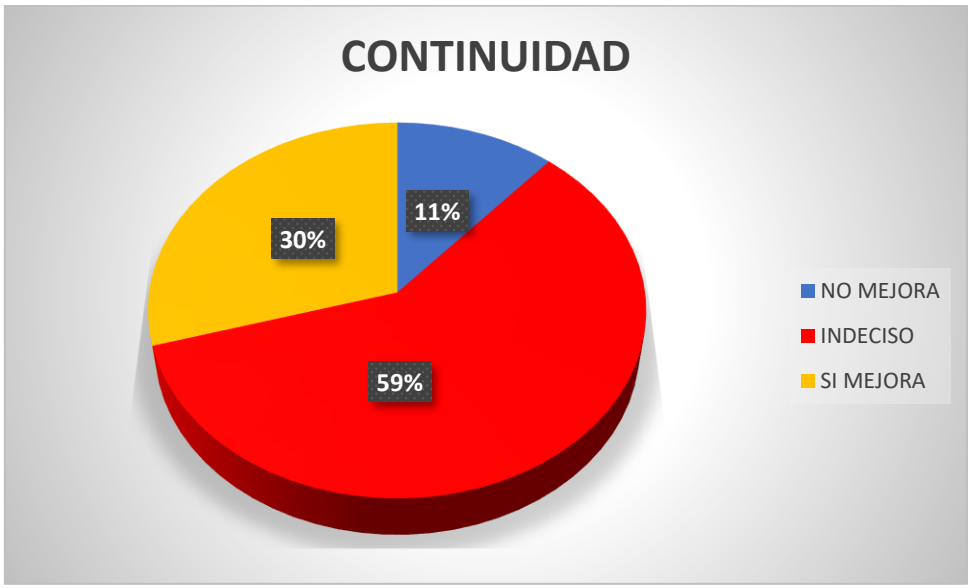
Plan de Contingencia	n	%
No mejora	5	11.4
Indeciso	26	59.1
Si mejora	13	29,5
Total	44	100,0

FUENTE: PARQUE INFORMATICO DE LA DIRESA LIMA, HUACHO – 2022

En la tabla 5 se puede observar que del 100% (44) de los encuestados con respecto al plan de contingencia de tecnologías de la información en la dimensión continuidad, el 59.1% manifiesta que está indeciso, el 29.5% que si mejora y el 11.4% que no mejora.

Figura 4

Dimensión Continuidad



FUENTE: PARQUE INFORMATICO DE LA DIRESA LIMA, HUACHO – 2022

Tabla 6

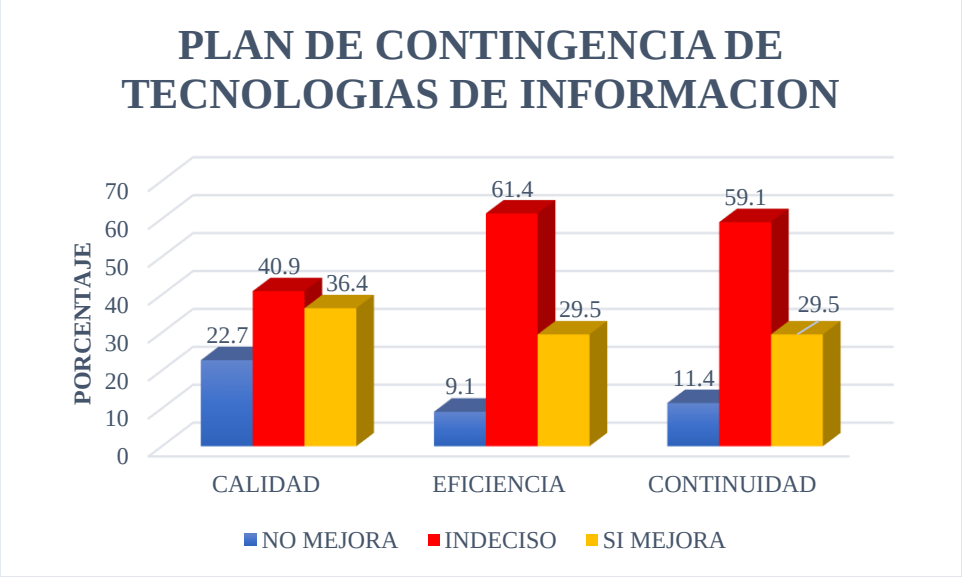
Plan de Contingencia de Tecnologías de Información a Nivel de Dimensiones

DIMENSIONES	PLAN DE CONTINGENCIA						TOTAL	
	NO MEJORA		INDECISO		SI MEJORA			
	n	%	n	%	n	%	n	%
CALIDAD	10	22.7	18	40.9	16	36.4	44	100.0
EFICIENCIA	4	9.1	27	61.4	13	29.5	44	100.0
CONTINUIDAD	5	11.4	26	59.1	13	29.5	44	100.0

FUENTE: PARQUE INFORMATICO DE LA DIRESA LIMA, HUACHO – 2022

Figura 5

Nivel de Dimensiones



FUENTE: PARQUE INFORMATICO DE LA DIRESA LIMA, HUACHO – 2022

Tabla 7

Distribución de Frecuencias del Plan de Contingencia de Tecnologías de Información

ITEM	TD		D		I		A		TA	
	n	**%**	**n**	**%**	**n**	**%**	**n**	**%**	**n**	**%**
ITEM 1	5	11.36%	8	18.18%	9	20.45%	20	45.45%	2	4.55%
ITEM2	12	27.27%	23	52.27%	4	9.09%	5	11.36%	0	0.00%
ITEM3	11	25.00%	20	45.45%	3	6.82%	5	11.36%	5	11.36%
ITEM4	7	15.91%	11	25.00%	11	25.00%	14	31.82%	1	2.27%
ITEM5	8	18.18%	9	20.45%	5	11.36%	20	45.45%	2	4.55%
ITEM6	4	9.09%	18	40.91%	8	18.18%	10	22.73%	4	9.09%
ITEM7	5	11.36%	11	25.00%	4	9.09%	16	36.36%	8	18.18%
ITEM8	17	38.64%	20	45.45%	4	9.09%	2	4.55%	1	2.27%
ITEM9	6	13.64%	14	31.82%	1	2.27%	20	45.45%	3	6.82%
ITEM10	5	11.36%	16	36.36%	6	13.64%	12	27.27%	5	11.36%
ITEM11	15	34.09%	26	59.09%	2	4.55%	1	2.27%	0	0.00%
ITEM12	10	22.73%	19	43.18%	6	13.64%	7	15.91%	2	4.55%
ITEM13	6	13.64%	9	20.45%	6	13.64%	20	45.45%	3	6.82%
ITEM14	11	25.00%	13	29.55%	11	25.00%	6	13.64%	3	6.82%
ITEM15	8	18.18%	24	54.55%	8	18.18%	2	4.55%	2	4.55%

FUENTE: PARQUE INFORMATICO DE LA DIRESA LIMA, HUACHO – 2022

PUNTOS DE CORTE DE LA VARIABLE PLAN DE CONTINGENCIA

15 – 31 NO MEJORA

32 – 45 INDECISO

46 – 75 SI MEJORA

PUNTOS DE CORTE DE LA VARIABLE CALIDAD

6 – 12 NO MEJORA

13 – 18 INDECISO

19 – 30 SI MEJORA

PUNTOS DE CORTE DE LA VARIABLE EFICIENCIA

5 – 9 NO MEJORA

10 – 14 INDECISO

15 – 25 SI MEJORA

PUNTOS DE CORTE DE LA VARIABLE PLAN DE CONTINUIDAD

4 – 7 NO MEJORA

8 – 11 INDECISO

12 – 20 SI MEJORA

PUNTOS DE CORTE DETERMINADOS SEGÚN LA ESCALA DE ESTANINOS

Capítulo V: DISCUSIÓN

5.1. Discusión de resultados

A partir de los hallazgos encontrados con respecto al objetivo general y específicos planteados, se determinó que la implementación de un Plan de Contingencia de Tecnologías de información si mejora el parque Informático de la DIRESA Lima.

En contraste con el objetivo 4 planteado por Gonzales (2019), que busca elegir una táctica de respaldo para garantizar la seguridad de la información en el departamento de sistemas de información; se pudo evidenciar que existe similitud en su investigación titulada Diseño del Plan de Contingencia como Herramienta para Gestionar Riesgos de la Seguridad de la Información en el Área del Centro de Sistemas de Información de la UGEL-FERREÑAFE en el Periodo 2018, según los resultados de la encuesta y el análisis llevados a cabo en el centro de sistema de la información, se está desarrollando un plan de contingencia para garantizar la seguridad de la información. Este plan se diseñará con el objetivo de brindar apoyo en la toma de decisiones y proteger los activos de la información. El estudio realizado concluyó que la metodología utilizada actualmente en el área para tratar los riesgos de la información no es efectiva.

En el trabajo de investigación se pudo observar que la tabla 1 muestra que al 100% (44) de los encuestados con respecto al plan de contingencia de tecnologías de la información, el 56.8% manifiesta que está indeciso, porqué si bien al contar con un plan de contingencia no se evidencia que este cumpliendose con las normas legales actuales, ya sea por la disconformidad de los trabajadores al no ver una buena calidad, o también al no ver continuidad por parte de la DIRESA, si bien ya se evidenciaba las fallas del parque informático con la pandemia de coronavirus muchas instituciones no recibieron tanto impacto en contra de su entidad, pero la DIRESA si ya venía en mal estado, evidencio más las carencias, retrasando así la producitvidad del personal; manifestando que las altas entidades de DIRESA quieran alivianar un poco este efecto nefasto. Por esa razón los trabajadores al no ver un progreso en las inmediaciones creen que no hay un plan de contigencia.

Según el objetivo 3, consiste en llevar a cabo una evaluación y manejo de los riesgos relacionados con la seguridad de la información en el departamento de sistemas de información, se verifico que se realizó una evaluación de los activos tomando en cuenta la seguridad, identificando los activos más importantes. Luego, se llevó a cabo un proceso de juicio de expertos en el que el encargado del área de CSI completó un formulario para evaluar las amenazas a los activos. Se determinó que los activos estaban expuestos a condiciones inadecuadas de temperatura o humedad y a cortes en el suministro eléctrico, los cuales se consideraron como los más críticos.

Los cuales guardan similitud con la tabla 2 donde se puede observar que del 100% (44) de los encuestados con respecto al plan de contingencia de tecnologías de la información en la dimensión calidad, el 40.9% manifiesta que está indeciso, debido a que algunas áreas se encontraban expuestas a condiciones inadecuadas, ya sea por mal cableado, temperatura, corte de suministro, siendo estos los más críticos. Además de lo antes mencionado, agregarle que algunos equipos tecnologícos se encuentran en pesimo estado, desfasados, no operativos, ya sean ordenadores, impresoras, servidores de red. Con estos factores los trabajadores de la institución teniendo un impacto negativo en su entorno laboral produce un bajo rendimiento y disminuye la productividad, también en ciertas ocasiones puede llegar a generar estrés para algunos trabajadores. Por estas razones algunas áreas respondieron con estar indecisos al no recibir calidad por parte de la DIRESA.

Observando el objetivo 1, realizar una evaluación inicial sobre la seguridad de la información en el área del centro de sistemas de información, se encontró que el 48% de los encuestados manifestaron sentirse insatisfechos o neutrales respecto al método utilizado para tratar los riesgos de seguridad de la información. Se recomienda que este indicador se mantenga en un 10%.

En el indicador estudiado de la tabla 3 se puede observar que del 100% (44) de los encuestados con respecto al plan de contingencia de tecnologías de la información en la dimensión eficiencia, el 61.4% manifiesta que está indeciso, porqué si bien la eficiencia del trabajador se ve en es lograr la mayor productividad sin exigir su máxima capacidad, cumpliendo con los objetivos propuestos; esto va de la mano con el punto antes mencionado que es la calidad, al no poseer unos

ordenadores capacitados, retrasa está productividad y por ende limita la capacidad de algunos de los trabajadores por no decir en su mayoría de ciertas áreas que se ven afectadas por esta problemática. Eso también no quiere decir que no entreguen un buen trabajo ya que la calidad depende también cargos, y tareas específicas que desempeñan diferentes áreas. Sin embargo, se ve el porcentaje del trabajo rechazado que realizan todas las áreas y eso es un indicador para medir la eficiencia de la DIRESA.

A su vez el objetivo 1, se llevó a cabo una evaluación inicial de la seguridad de la información en el departamento de sistemas de información. En relación al hallazgo relacionado con el personal y los métodos de divulgación del plan de contingencia, se observó que los encuestados no están al tanto de la existencia de personal y métodos para difundir los planes de contingencia. Además, el 83% de ellos nunca recibió estos documentos, lo cual resulta preocupante. Se recomienda que este indicador alcance el 100%.

Así mismo los resultados reportados en el estudio de investigación arrojaron que la tabla 4 se puede observar que del 100% (44) de los encuestados con respecto al plan de contingencia de tecnologías de la información en la dimensión continuidad, el 59.1% manifiesta que está indeciso, debido a no cumplir con los seguimientos, no exigir atención y los recursos necesarios ante los imprevistos, el personal del área de Informática, no a sido capacitado sobre los temas de seguridad de la información, pero lo más alarmante de esto es resaltar la carencia del personal ya que al contar con solo 2 personas para cubrir las incidencias o imprevistos, no pueden dar seguimiento a la mayoría de infortunios presentados en la empresa, retrasando aún más la corrección de los problemas, atrasando la productividad y generando más problemas por resolver dentro de la DIRESA.

Capítulo VI: CONCLUSIONES Y RECOMENDACIONES

6.1. Conclusiones

- En este trabajo de investigación de metodología descriptiva simple las hipótesis se formulan, más no se demuestran, esto es por su metodología de investigación, ya que los estudios descriptivos miden variables de manera independiente. Aunque pueden integrar las mediciones de cada una de las variables para decir cómo son y se manifiesta la problemática, su objetivo no es indicar como relacionan las variables medidas. Por ende, como las hipótesis no se demuestran no se emplea ningún test o prueba estadística.
- Se llega a la conclusión de que la DIRESA no está adecuadamente preparada para enfrentar cualquier evento que represente un peligro para la seguridad de la información de sus recursos. Es necesario realizar evaluaciones periódicas, ya sea semanales o diarias, para identificar y analizar los riesgos y su posible impacto en los activos de información y los sistemas que los respaldan.
- Se evidencia que en la DIRESA existen políticas o normativas para proteger la información, pero estás se encuentran desfazadas, no cumplen los requisitos de hoy en día de la mayoría de instituciones para poder responder ante alguna incidencia.
- Así mismo, se concluye que la institución por falta de presupuesto y gestión no se toma la mayor importancia con respectos las medidas acordes a lo que debería regir para la estructura del parque informático.
- Se evidencia que la demanda de incidencias va en incremento, al no contar con suficiente personal las actividades se retrasan y los procesos se detienen. De esta manera provoca una baja productividad del personal que está laborando causando grandes pérdidas de información.

6.2. Recomendaciones

- Al observar el indeciso nivel de calidad del Plan de Contingencia de Tecnologías de Información, se recomienda proporcionar una responsabilidad más comprometida al personal y las autoridades de la DIRESA, dedicando así compromiso de mantenimiento y servicio al cuidado de la información.

- Realizar un plan continuo de evaluaciones semanales midiendo la eficiencia del personal con respecto a cada área con la finalidad de prevenir fallos y proteger la información valiosa.

- Efectuar capacitaciones e inducciones a todas las áreas prevaleciendo el índice de continuidad, con respecto a asuntos relacionados con la administración de riesgos y la seguridad de la información de forma general, para así prevenir robo de perfiles y programas maliciosos.

- Pedir a las entidades estatales superiores el monto presupuestario requerido, teniendo en cuenta los indicadores planteados en esta investigación para poder desarrollar el Plan de Contingencia de Sistema de Información, buscando equipos de alta gama o capacidad que cumplan los estándares de calidad.

- Se recomienda reestructurar las instalaciones eléctricas, y redes de comunicación, evitando así accidentes laborales y perdidas de datos, priorizando así la seguridad y salud dentro de la institución.

- Se sugiere trasladar el servidor a un entorno apropiado y restringido únicamente al personal autorizado.

- Se sugiere la compra de un nuevo servidor para el área de DEIT priorizando el indicador de respaldo, se requiere crear copias de seguridad de los sistemas operativos, programas y sitios web, así como de toda la información, ya que no se cambia de servidor desde el 2007.

Capítulo VII: REFERENCIAS

7.1. Fuentes Bibliografía

(IICA), I. I. (2020). Elementos para Programar, Ejectuar y Evaluar Actividades de Capacitacion. En *Elementos para programar, ejecutar y evaluar actividades de capacitación* (pág. 122). Instituto Interamericano de Cooperación para la Agricultura (IICA). Obtenido de https://repositorio.iica.int/handle/11324/11114

Agudelo, G., Aigneren, M., & Ruiz, J. (2010). *La Sociologia En Sus Escenarios.* Medellin, Colombia: Centro De Estudios De Opinion. Obtenido de https://revistas.udea.edu.co/index.php/ceo/article/view/6545/5996

Aguilera López, P. (2010). *Seguridad Informática.* Madrid, España: Editorial Editex, S. A. Obtenido de https://books.google.com.pe/books?id=Mgvm3AYIT64C&lpg=PP1&dq=seguridad%20inform%C3%A1tica%20aguilera%20lopez&hl=es&pg=PP1#v=onepage&q=seguridad%20inform%C3%A1tica%20aguilera%20lopez&f=false

Aguilera López, P., & Morante Fernández, M. (2008). *Informática 4º ESO.* Madrid, España: Editex S. A. Obtenido de https://books.google.com.cu/books?id=qOX_SBdDjsEC&lpg=PP1&hl=es&pg=PP1#v=onepage&q&f=false

Alfaro, E. (2008). Metodología para la Auditoría Integral de la Gestión de la Tecnología de Información. *(Tesis para optar por el título de Ingeniero Informático).* Pontificia Universidad Católica del Perú, Lima, Perú. Obtenido de http://hdl.handle.net/20.500.12404/1048

Aranda, G., Martínez, N., Faraci, P., & Cechich, A. (2013). Hacia un framework de evaluación de calidad de Información en foros de discusión ténicos. *14*. Obtenido de http://sedici.unlp.edu.ar/bitstream/handle/10915/76364/Documento_completo.pdf-PDFA.pdf?sequence=1&isAllowed=y

Arroyo Fuentes, A. C. (2016). *Conocimiento Digital*. Obtenido de Conocimiento Digital: https://grupo4herramientasinformatica.blogspot.pe/2016/03/la-seguridad-informatica.html

Baca Urbina, G., Solares Soto, P. F., & Acosta Gonzaga, E. (2014). *Administración Informática I: Análisis y Evaluación de Tecnologías de Información.* Azcapotzalco, México.

Bellido Quintero, E. (2013). Instalación y actualización de Sistemas Operativos. En *Instalación y actualización de Sistemas Operativos.* IC EDITORIAL.

Capra, G., Chaves, R., Leiton, L., & Soto, E. (2013). *Plan de contingencia y recuperación en caso de suspensión de TI / Big Data.* Instituto Tecnologico de Costa Rica. Obtenido de https://sites.google.com/site/afig402013s26/home/plan-de-contingencia-y-recuperacin-en-caso-de-suspensin-de-ti--big-data

Cardador Cabello, A. L. (2015). Dimensionar, instalar y optimizar el hardware. En *Dimensionar, instalar y optimizar el hardware.* IC Editorial.

Carrascosa López, C. (2012). Mejora continua, innovación y compromiso medioambiental de la gerencia, un estudio empírico. *Tec. Empresaria*, 9-23.

Castillo Tzec, Y. M., & Soriano Montero, M. (2012). Confiabilidad de Sistemas. En *Confiabilidad de Sistemas* (pág. 232). Editorial Academica Espanola.

Corona Cabrera, A., Reyes Echeagaray, D., Bribiesca Correa, G., Ramírez Chavero, M., Cruz Quiroz, R., Torres Garibay, R., . . . Ramírez Munive, Y. (2015). *Tecnologías de información y comunicación en las organizaciones.* Coyoacán, México.

De Pablos Heredero, C., López Hermoso Agius, J. J., Romo Romero, S. M., & Medina Salgado, S. (2011). *Organización y Transformación de los sistemas de información en la empresa.* Madrid, España.

DIRESA. (2008). *Reglamento de Organización y Funciones.* Dirección Regional de Salud Lima, Lima. Obtenido de https://www.peru.gob.pe/docs/PLANES/14185/PLAN_14185__2012.pdf

Dzul Escamilla, M. (2008). *Aplicación básia de los métodos científicos.* Estado de Hidalgo. Obtenido de https://www.uaeh.edu.mx/docencia/VI_Presentaciones/licenciatura_en_mercadotecnia/fundamentos_de_metodologia_investigacion/PRES38.pdf

Erb. (2005). *Gestión de Riesgo en la Seguridad Informática*. Obtenido de https://protejete.wordpress.com/gdr_principal/seguridad_informacion_proteccion/

Espinoza Asto, S. C. (2014). *Diseño de un plan de contingencia de sistemas informáticos para la Universidad Peruana los Andes.* Universidad Peruana los Andes, Huancayo, Perú. Obtenido de http://www.repositorio.upla.edu.pe/bitstream/handle/20.500.12848/942/SHERLY%20CLERY%20ESPINOZA%20ASTO.pdf?sequence=1&isAllowed=y

Espinoza, E. (2016). Obtenido de chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/http://www.bvs.hn/Honduras/UICFCM/SaludMental/UNIVERSO.MUESTRA.Y.MUESTREO.pdf

Esteban Nieto, N. T. (2018). *Tipos de Investigación.* Universidad Santo Domingo de Guzmán. Obtenido de http://repositorio.usdg.edu.pe/handle/USDG/34

Férnandez , P. (27 de 5 de 2002). *Metodología de la Investigación.* 2002: Unidad de Epidemiología Clínica y Bioestadística . Obtenido de https://www.fisterra.com/formacion/metodologia-investigacion/investigacion-cuantitativa-cualitativa/

Fernández Collado, C., Baptista Lucio, P., & Hernández Sampieri, R. (2014). *Metodología de la Investigación.* México.

Gay, L. R. (1996). *Educational Research.* New Jersey, Estados Unidos: Prentice Hall Inc.

Gonzabay Tomalá, R. R. (2022). *Desarrollo de un plan de contingencias informático para el centro de datos y comunicaciones de la empresa AGUAPEN-EP mediante el uso de normas internacionales.* La Libertad: Universidad Estatal Península de Santa Elena. Obtenido de https://repositorio.upse.edu.ec/handle/46000/7724

Gonzales Sosa, H., & Delgado Flores, I. (2019). Diseño del Plan de Contingencia como herramienta para gestionar riesgos de la seguridad de la información en el área del centro de sistemas de información de la UGEL-FERREÑAFE en el periodo 2018. *DISEÑO DEL PLAN DE CONTINGENCIA COMO HERRAMIENTA PARA GESTIONAR RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN EN EL ÁREA DEL CENTRO DE SISTEMAS DE INFORMACIÓN DE LA UGEL-FERREÑAFE EN EL PERIODO 2018.* Universidad de Lambayeque. Obtenido de https://repositorio.udl.edu.pe/handle/UDL/235

Granda Juca, A. (2011). Diseño de un plan de contingencias del TICs para la Empresa Eléctrica Centrosur. *Diseño de un plan de contingencias del TICs para la Empresa Eléctrica Centrosur.* Universidad de Cuenca, Cuenca, España. Obtenido de http://dspace.ucuenca.edu.ec/handle/123456789/2556

Hernández Ayala, N. J. (2013). *Tecnologías de información para los negocios en la era del conocimiento.* Instituto Tecnológico de Estudios Superiores Monterrey, México.

Hernández, R. F. (2014). *Metodología de la investigación (6ª ed.).* México: McGrwall Hill Education. Obtenido de https://recursos.ucol.mx/tesis/investigacion.php

Kuong, J., & Isaacson, G. (1986). *How to prepare an EDP Contingency Plan for Business continuity.* Wellesley Hills, MA.

Lapiedra, R. D. (2011). *Introducción a la gestión de sistemas de información en la empresa.* Universitat Jaume I.

Llerena, M., & Saá, J. (2006). Desarrollo del manual de seguridades informáticas de la Armada del Ecuador. *(Tesis para optar por el título de Ingeniero de Sistemas e Informática).* Escuela Politécnica del Ejército, Ecuador. Obtenido de http://repositorio.espe.edu.ec/handle/21000/617

Llumiquinga, C., & Vallejo, P. (2015). Diseño de las políticas de seguridad de la información y desarrollo del plan de contingencia. *(Tesis para optar por el título de Ingeniero de Sistemas e Informática).* Universidad de las Fuerzas Armadas, Sangolqui. Obtenido de http://repositorio.espe.edu.ec/xmlui/bitstream/handle/21000/733/T-ESPE-012634.pdf?sequence=1&isAllowed=y

Martínez, J. (2020). Ingeniería de Gestión de Calidad de Procesos y la Mejora Continua aplicada a los sistemas de Producción de las Organizaciones Empresariales Complejas. Obtenido de https://www.redalyc.org/journal/6517/651769122005/651769122005.pdf

Mercado, I. d. (2022). *Question pro*. Obtenido de questionpro.com/blog/es/investigacion-correlacional/#:~:text=La%20investigación%20correlacional%20es%20un,un%20investigador%20mide%20dos%20variables.&text=Esto%20es%20precisamente%20lo%20que,en%20este%20ejemplo%20en%20particular).

Stallings, W. (1990). *Data and Computer Communications.* (P. d. Hall, Ed.)

Velázquez, A. (2023). *Questionpro*. Obtenido de https://www.questionpro.com/blog/es/investigacion-no-experimental/

Yepes, J. F. (2013). *Prezi.* Obtenido de Norma ISO 9126 - Eficiencia: https://prezi.com/xpg0h7trtnjg/norma-iso-9126-eficiencia/

ANEXOS

ANEXO 01 MATRIZ DE CONSISTENCIA

PROBLEMAS	OBJETIVOS	HIPÓTESIS	Variables			
Problema General	**Objetivo General**	**Hipótesis General**		**Dimensiones**	**Indicadores**	**Metodología**
¿La implementación de un Plan de Contingencia de tecnologías de información mejora el parque informático de la DIRESA Lima, Huacho-2022?	Desarrollar la mejora de la implementación de un Plan de Contingencia de Tecnologías de información en el parque Informático de la DIRESA Lima, Huacho - 2022.	La implementación de un Plan de Contingencia mejora las tecnologías de información en el Parque Informático de la DIRESA Lima, Huacho - 2022.		Calidad	Seguro Confiable	El presente trabajo es una investigación de: -Tipo: Investigación No Experimental. -Nivel: Descriptivo Simple -Enfoque: -Enfoque Cuantitativo -Diseño: no-experimental y transversal. Población: Trabajadores de la Dirección Regional de Salud Muestra: Se tomará una muestra de 44 de trabajadores de la Dirección Regional de Salud.
Problemas Específicos	**Objetivos Específicos**	**Hipótesis Específicas**				
¿La implementación de Plan Contingencia de Tecnologías de Información mejora el nivel de calidad en el Parque Informático de la DIRESA, Huacho-2022?	Determinar si el Plan de Contingencia de Tecnologías de Información va a mejorar el nivel de calidad en el Parque Informático de la DIRESA Lima, Huacho - 2022.	La implementación de un Plan de Contingencia mejora el nivel de calidad en el Parque Informático de la DIRESA Lima, Huacho - 2022.	Variable X: Plan de Contingencia	Eficiencia	Actualizado	
¿La implementación de Plan Contingencia de Tecnologías de Información mejora el nivel de eficiencia en el Parque Informático de la DIRESA, Huacho-2022?	Determinar si el Plan de Contingencia de Tecnologías de Información va a mejorar el nivel de eficiencia en el Parque Informático de la DIRESA Lima, Huacho - 2022.	La implementación de un Plan de Contingencia mejora el nivel de eficiencia en el Parque Informático de la DIRESA Lima, Huacho - 2022.		Continuidad	Capacitación Respaldo	
¿La implementación de Plan Contingencia de Tecnologías de Información mejora el nivel de continuidad en el Parque Informático de la DIRESA, Huacho-2022?	Determinar si el Plan de Contingencia de Tecnologías de Información va a mejorar nivel de continuidad en el Parque Informático de la DIRESA Lima, Huacho - 2022.	La implementación de un Plan de Contingencia mejora el nivel de continuidad en el Parque Informático de la DIRESA Lima, Huacho - 2022.				

ANEXO 02 INSTRUMENTO PARA LA TOMA DE DATOS

Presentación

El tesista Luis Angel Torres Quevedo, de la Escuela Profesional de Ingeniería de Sistemas de la Universidad Nacional José Faustino Sánchez Carrión - Huacho.

Se va a trabajar en el desarrollo de la tesis: **"PLAN DE CONTINGENCIA DE TECNOLOGÍAS DE INFORMACIÓN EN EL PARQUE INFORMÁTICO DE LA DIRESA LIMA, HUACHO - 2022".** Las opiniones que ustedes compartan serán muy valiosas para el estudio, ya que las utilizaremos para recopilar información de manera estadística.

Escala de calificación				
1	**2**	**3**	**4**	**5**
Totalmente en desacuerdo	**En desacuerdo**	**Ni de acuerdo ni en desacuerdo**	**De acuerdo**	**Totalmente de acuerdo**

Lee atentamente y marca con una "x" tu respuesta…

Sexo
- ◯ Hombre
- ◯ Mujer

Edad
- ◯ De 18 a 28 años
- ◯ De 29 a 39 años
- ◯ De 40 a 50 años
- ◯ De 50 años a más

Experiencia como trabajador
- ◯ De 1 año
- ◯ De 1 a 5 años
- ◯ De 5 años a más

Plan de Contingencia						
Ítem	**Calidad**	**1**	**2**	**3**	**4**	**5**
1	¿Tiene usted en cuenta del riesgo que corre la información dentro del Parque Informático de la DIRESA?					
2	¿Considera usted que las áreas están seguras donde se encuentran ubicados los equipos de cómputo? (accidente, desastre, etc.)					
3	¿Considera que es conveniente el estado de protección de los equipos de cómputo en el acontecimiento de una catástrofe?					
4	¿Cree óptimos los procedimientos a utilizar para realizar back up en el caso de una emergencia?					
5	¿Considera adecuados los métodos o protocolos utilizados para la seguridad de la red?					
6	¿Son confiables y/o seguros los controles de acceso a los servicios que se encuentran conectados a la red?					
Ítem	**Eficiencia**	**1**	**2**	**3**	**4**	**5**

7	¿Cree recomendable la protección ante el riesgo de un programa maligno (virus, malware, software malicioso, software dañino) que su equipo de cómputo puede contraer?					
8	¿Cree que los equipos de cómputo utilizado se encuentran actualizados constantemente según los requerimientos tecnológicos?					
9	¿Considera adecuado el acceso al servidor para interactuar con las aplicaciones?					
10	¿Cree que a cantidad de personal técnico es suficiente para actuar ante un incidente?					
11	¿Cree que a cantidad de personal técnico es suficiente para actuar ante un incidente?					
Ítem	**Continuidad**	**1**	**2**	**3**	**4**	**5**
12	Ante un incidente con el servidor, ¿Cree que las acciones que se toman para la restauración de procesos operativos del mismo, es inmediata?					
13	¿Considera usted que la cuenta del administrador se encuentra bien administrada o gestionada?					
14	¿Cree usted que el respaldo de la información es adecuado dentro del Parque Informático?					
15	¿Considera usted que el tiempo que se tiene planificado para el mantenimiento del parque informático es el apropiado?					

ANEXO 03 TABLA DE DATOS

N	Sexo	Edad	Experiencia como trabajador	1.-¿Tiene usted en cuenta el riesgo de la información del Parque Informático en la que se encuentra asegurada? [Respuesta]	2.- ¿Considera usted que las áreas están seguras donde se encuentran ubicados los equipos de cómputo ? (accidente, desastre, etc.) [Respuesta]	3.- ¿Considera que es conveniente el estado de protección de los equipos de cómputo en el acontecimiento de una catástrofe? [Respuesta]	4.-¿Cree óptimos los procedimientos a utilizar para realizar back up en el caso de una emergencia? [Respuesta]	5.- ¿Considera adecuados los métodos o protocolos utilizados para la seguridad de la red? [Respuesta]	6.-¿Son confiables y/o seguros los controles de acceso a los servicios que se encuentran conectados a la red? [Respuesta]	7.- ¿Cree recomendable la protección ante el riesgo de un programa maligno (virus, malware, software malicioso, software dañino) que su equipo de cómputo puede contraer? [Respuesta]	8.-¿Cree que los equipos de cómputo utilizado se encuentran actualizados constantemente según los requerimientos tecnológicos? [Respuesta]	9.- ¿Considera adecuado el acceso al servidor para interactuar con las aplicaciones? [Respuesta]	10.- ¿Considera adecuado el acceso a la consola del servidor? [Respuesta]	11.-¿Cree usted que la cantidad de personal técnico es suficiente para actuar ante un incidente? [Respuesta]	12.- Ante un incidente con el servidor, ¿Cree que las acciones que se toman para la restauración de procesos operativos del mismo, es inmediata? [Respuesta]	13.- ¿Considera usted que la cuenta del administrador se encuentra bien administrada o gestionada? [Respuesta]	14.- ¿Cree usted que el respaldo de la información es adecuado? [Respuesta]	15.- ¿Considera usted que el tiempo que se tiene planificado para el mantenimiento del parque informático es el apropiado? [Respuesta]
1	2	1	2	2	2	2	1	2	3	3	2	2	1	2	2	3	1	2
2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
3	2	1	2	1	2	2	2	1	2	1	2	1	1	1	1	2	1	1
4	1	1	1	3	2	2	4	4	3	3	1	2	3	3	2	2	3	3
5	1	1	1	2	3	4	4	4	3	2	2	2	3	2	3	3	2	3
6	1	1	2	4	4	5	4	2	4	5	3	4	5	2	5	4	2	3
7	1	1	2	3	2	2	2	2	2	2	2	2	2	2	2	2	2	2
8	1	1	2	3	4	4	1	4	4	4	4	4	4	4	4	4	5	5
9	2	1	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
10	2	1	1	4	2	2	2	2	2	2	2	2	2	2	2	2	2	2
11	1	1	1	3	2	2	2	2	2	2	2	2	2	2	2	2	2	2
12	2	2	2	4	2	3	2	1	2	1	2	1	2	1	2	1	1	2
13	2	1	3	2	1	5	5	5	5	5	5	1	5	2	5	5	5	5
14	2	2	2	5	1	5	1	1	1	5	1	5	1	1	1	1	5	1
15	2	1	2	3	2	5	4	4	3	5	2	2	2	1	2	2	3	2
16	2	1	1	2	1	2	1	1	2	1	1	2	1	2	1	1	1	2
17	1	2	2	4	4	5	4	4	2	5	3	4	2	2	4	2	4	2

18	2	3	2	2	2	2	2	1	1	5	1	2	2	1	2	1	1	1
19	1	4	3	4	3	4	4	3	4	2	4	4	4	3	4	4	3	4
20	2	4	3	4	4	4	3	3	2	3	2	2	2	2	4	4	4	2
21	1	4	3	4	2	2	3	4	5	4	3	4	3	2	1	3	3	2
22	1	3	3	4	4	1	1	4	4	2	1	4	3	1	1	4	3	2
23	2	3	3	5	1	1	2	5	3	3	1	4	4	1	4	1	2	2
24	2	3	3	4	1	2	3	4	2	1	1	4	4	1	4	4	3	3
25	2	3	3	2	3	2	2	4	3	4	2	4	4	1	1	3	3	2
26	2	4	3	2	1	1	2	4	2	2	2	5	2	2	2	4	2	3
27	1	4	3	1	2	1	1	2	2	2	2	3	3	2	1	4	2	4
28	1	2	3	4	2	2	4	4	2	2	1	4	4	1	1	4	3	2
29	1	2	3	4	1	3	3	1	3	4	1	1	4	2	4	2	1	2
30	2	4	3	1	1	1	2	4	1	2	1	1	4	2	1	5	3	3
31	2	2	2	4	2	1	3	1	4	5	2	4	2	2	2	5	2	2
32	1	4	3	1	1	1	3	4	2	5	1	4	4	1	3	4	1	1
33	1	4	3	3	1	1	3	3	3	4	1	2	5	1	3	4	1	1
34	1	2	3	3	2	1	4	4	5	4	1	5	5	2	3	3	3	2
35	1	2	3	4	3	3	3	4	5	4	3	4	5	2	3	4	3	3
36	1	4	3	3	2	1	3	3	2	4	1	4	4	1	2	4	2	3
37	1	4	3	3	2	2	4	4	4	4	1	4	4	2	2	4	1	1
38	1	3	3	4	2	2	3	3	2	4	2	4	4	1	3	4	1	2
39	2	3	3	4	2	2	3	2	2	4	2	2	3	2	2	3	2	2
40	2	4	3	4	1	2	4	2	2	4	2	2	2	2	2	4	2	1
41	1	4	3	4	2	2	4	4	4	4	1	4	2	2	2	4	4	2
42	2	3	3	4	2	2	4	4	4	4	2	4	2	2	2	4	4	2
43	1	2	3	4	2	2	4	4	4	4	2	4	2	2	2	4	4	2
44	1	4	3	4	2	4	4	4	4	4	2	4	2	2	2	4	4	2