



UNIVERSIDAD CÉSAR VALLEJO

**FACULTAD DE INGENIERÍA Y ARQUITECTURA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS**

**“IMPLEMENTACIÓN DE ISO 27001 Y 27002 ADAPTADAS PARA
GESTIÓN DE SEGURIDAD DE INFORMACIÓN EN SECRETARÍA
EJECUTIVA DE POLICÍA NACIONAL DEL PERÚ”**

**TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:
INGENIERO DE SISTEMAS**

AUTOR:

CHÁVARRY BONILLA, SLEEM NÉSTOR FRANCISCO (ORCID: 0000-0003-0112-5545)

ASESOR:

Mgtr. JOHNSON ROMERO, GUILLERMO MIGUEL (ORCID: 0000-0003-0352-1971)

LÍNEA DE INVESTIGACIÓN:

SISTEMAS DE INFORMACIÓN Y COMUNICACIONES

LIMA – PERÚ

2021

Dedicatoria

Este trabajo va dedicado en memoria de mi abuelita, quien por su apoyo constante me impulso a terminar la carrera; y a mis padres, esposa, hija y hermana quienes estuvieron en todo momento de mi carrera. Además, dedico este trabajo a todos los efectivos policiales que fueron víctimas del coronavirus y que teniendo familia arriesgaron su vida para hacer cumplir la ley.

Agradecimientos

Agradezco a cada profesor que a lo largo de mi carrera me han brindado sus conocimientos para poder plasmarlo en mi trabajo.

ÍNDICE DE CONTENIDOS

DEDICATORIA.....	ii
AGRADECIMIENTO.....	iii
ÍNDICE DE TABLAS.....	vii
ÍNDICE DE FIGURAS.....	viii
ÍNDICE DE ANEXOS.....	ix
RESUMEN.....	xi
ABSTRACT.....	xii
I. INTRODUCCIÓN.....	01
II. MARCO TEÓRICO.....	08
III. METODOLOGÍA.....	20
3.1. Tipo y diseño de investigación.....	21
3.2. Variables y operacionalización.....	23
3.2.1 Definición conceptual.....	23
3.3.1 Variable Independiente (VI).....	23
3.3.2 Variable Dependiente (VD).....	24
3.2.2 Definición Operacional.....	24
3.2.3 Operacionalización de variables.....	25
3.3. Población, Muestra y Muestreo.....	25
3.3.1 Población.....	25
3.3.2 Muestra.....	25
3.3.3 Muestreo.....	26
3.4. Técnicas e instrumentos de recolección de datos.....	26
3.4.1 Técnica: Observación.....	27

3.4.2 Validez.....	27
3.4.3 Confiabilidad.....	28
3.4.4 Técnicas de recolección de datos:	28
3.5. Procedimientos.....	29
3.6. Método de análisis de datos.....	29
3.7. Aspectos éticos	29
IV. IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD	
DE LA INFORMACIÓN	30
4.1. Fase 0: Estudio de factibilidad.....	31
4.2. Fase 1: Contexto de la organización	31
4.3. Fase 2: Liderazgo.....	33
4.4. Fase 3: Planificación.....	34
4.5. Fase 4: Soporte	34
V. RESULTADOS.....	35
5.1. Análisis e interpretación de resultados	36
5.1.1. Resultados generales	36
5.1.2. Resultados específicos	36
5.1.3. Análisis e interpretación de resultados	37
5.1.4. Cuadro de implementación final de la ISO 27001 y 27002	44
5.1.5. Gráfico del estado de implementación final de la ISO 27001	
y 27002	44
5.1.6. Gráfico del estado de implementación final de los controles de la	
ISO 27001 y 27002	45
5.2. Nivel de confianza y grado de significancia.....	46

5.3. Contrastación de hipótesis	47
VI DISCUSIÓN	53
VII CONCLUSIONES	55
VIII. RECOMENDACIONES	57
IX. REFERENCIAS	59

ÍNDICE DE TABLAS

Tabla 1: Validez de cuestionario: Seguridad de Información	27
Tabla 2: Validez de entrevista: Seguridad de Información	28
Tabla 3: Estructura de la NTP/ISO 27001:2013	36
Tabla 4: Resultados del pre test y post test	36
Tabla 5: Medias de los KPIs para el pre test y post test	37
Tabla 6: Prueba de normalidad del indicador 1	47
Tabla 7: Prueba de normalidad del indicador 2	48
Tabla 8: Prueba de normalidad del indicador 3	49
Tabla 9: Prueba de Wilcoxon del indicador 3	50
Tabla 10: Prueba de normalidad del indicador 4	51
Tabla 11: Prueba de Wilcoxon del indicador 4	52

ÍNDICE DE FIGURAS

Figura 1: Estado inicial de implementación ISO 27001 – SECEJE PNP – Nov. 2020	03
Figura 2: Estado inicial de controles de acuerdo a ISO 27002 – SECEJE PNP- Nov. 2020	04
Figura 3: Modelo PHVA para ISO 27001	14
Figura 4: Diseño de comparación con dos grupos estáticos.....	22
Figura 5: Organigrama de la Secretaría Ejecutiva de la PNP.....	32
Figura 6: Ubicación de la Secretaría Ejecutiva de la PNP	33
Figura 7: Organigrama propuesto del comité de seguridad de información.....	34
Figura 8: Resultados de la Pre-Prueba y Post-Prueba para KPI 1	38
Figura 9: Media de resultados de Pre-Prueba y Post-Prueba para KPI 1	38
Figura 10: Resultados de la Pre-Prueba y Post-Prueba para KPI 2	39
Figura 11: Media de resultados de Pre-Prueba y Post-Prueba para KPI 2	39
Figura 12: Resultados de la Pre-Prueba y Post-Prueba para KPI 3	40
Figura 13: Media de resultados de Pre-Prueba y Post-Prueba para KPI 3	41
Figura 14: Resultados de la Pre-Prueba y Post-Prueba para KPI 4	42
Figura 15: Media de resultados de Pre-Prueba y Post-Prueba para KPI 4	42
Figura 16: Gráfico de resultados de Pre-Prueba para KPI 5	43
Figura 17: Gráfico de resultados de Post-Prueba para KPI 5	43
Figura 18: Estado de implementación del SGSI en la SECEJE PNP – Jul 2021...	44
Figura 19: Estado de implementación de controles en la SECEJE PNP – Jul 2021	45
Figura 20: Fórmula de test de Shapiro-Wilk	46

ÍNDICE DE ANEXOS

Anexo 01: Declaratoria de autenticidad del autor.	65
Anexo 02: Declaratoria de autenticidad del asesor.	66
Anexo 03: Cuadro Fase Inicial a la Implementación de ISO 27001 y 27002....	67
Anexo 04: Cuadro Fase Final a la Implementación de ISO 27001 y 27002.....	68
Anexo 05: Matriz de Operacionalización de Variables.....	69
Anexo 06: Matriz de Consistencia.....	70
Anexo 07: Validación de Instrumento Seguridad de Información: Experto 01...	72
Anexo 08: Validación de Instrumento Entrevista Seguridad de Información Experto 01.....	74
Anexo 09: Encuesta para determinar la Gestión de Seguridad de Información en la SECEJE PNP.....	76
Anexo 10: Formato de entrevista sobre Seguridad de Información - ISO 27001 en la SECEJE PNP.....	80
Anexo 11: Coeficiente Alfa de Cronbach.....	85
Anexo 12: Carta de aceptación de la empresa.....	86
Anexo 13: Autorización para la realización y difusión de resultados de la investigación.....	87
Anexo 14: Políticas de Seguridad de Información de la Secretaría Ejecutiva de la Policía Nacional del Perú.....	88
Anexo 15: Plan de Gestión de Riesgos	102
Anexo 16: Formato de Lista maestra de registros.....	119
Anexo 17: Instrucciones de llenado del Formato de Lista maestra de registros.....	120
Anexo 18: Formato de hoja de trabajo para desarrollar un planeamiento	

de seguridad.....	121
Anexo 19: Formato de hoja de trabajo para desarrollar un plan de auditoría interna.....	122
Anexo 20: Reporte de Turnitin.....	123

Resumen

El problema de la investigación fue en qué manera el implementar ISO 27001 y 27002 adaptadas para la seguridad de la información en la Secretaría Ejecutiva de la PNP tiene efecto en la seguridad de la información en la Unidad Policial. El objetivo de la investigación fue determinar el efecto de implementar las normas ISO 27001 y 27002 adaptadas para la seguridad de la información en la Secretaría Ejecutiva de la Policía Nacional del Perú. El tipo de investigación que se realizará será aplicada con diseño es cuasi experimental debido a que se realizarán estudios con dos grupos, el primer grupo en pre test y el segundo grupo en post test.

Palabras clave: ISO 27001, ISO 27002, Seguridad de la información, Aseguramiento de información, Controles de seguridad de información.

Abstract

The problem of the investigation was how implementing the ISO 27001 and 27002 standard adapted for information security in the Executive Secretariat of the PNP has an effect on information security in the Police Unit. The objective of the investigation was to determine the effect of implementing the ISO 27001 and 27002 standard adapted for information security in the Secretaría Ejecutiva of the National Police of Peru. The type of research that will be carried out will be applied with a quasi-experimental design because studies will be carried out with two groups, the first group in pre-test and the second group in post-test.

Keywords: ISO 27001, ISO 27002, Security of the information, Information Assurance, Information security controls.

I. INTRODUCCIÓN

En la actualidad nos encontramos en un ambiente globalizado en el que la información es importante para la realización de trámites, transacciones, búsqueda de información, tener contacto con personas en diversas partes del orbe, entre otros; es de esta forma que la información puede encontrarse en diversos medios o formas, y no necesariamente en medios informáticos.

Para las personas y organizaciones, la seguridad de información posee un resultado significativo en relación a la privacidad, la que puede alcanzar diversas dimensiones dependiendo del ámbito social en el que se desempeñe.

La transformación digital llevada a cabo en las empresas soporta una cadena de desafíos; mientras que, algunos significarán una ventaja, habrá otros que representarán riesgos para la seguridad.

En la VIII Encuesta Latinoamericana de Seguridad de la Información: Nuevos horizontes para América Latina, informan que, de las 985 incidencias detectadas en organizaciones, el 13% son por Virus o Caballos de Troya, el 12% es por Instalación de software no autorizado y el 11% son incidencias dadas por Phishing.

En el ESET SECURITY REPORT: Latinoamérica 2019, México es el primer país en tener mayor porcentaje de incidentes de seguridad con 72%, seguido por Perú con 71%, Paraguay con 67%, Ecuador con 65%, mientras que Chile tiene 57% de incidentes de seguridad. En este mismo reporte identifican los niveles de implementación de controles básicos de seguridad en Perú, siendo el 84% los antivirus, el 70% firewall y 59% backups o copias de seguridad.

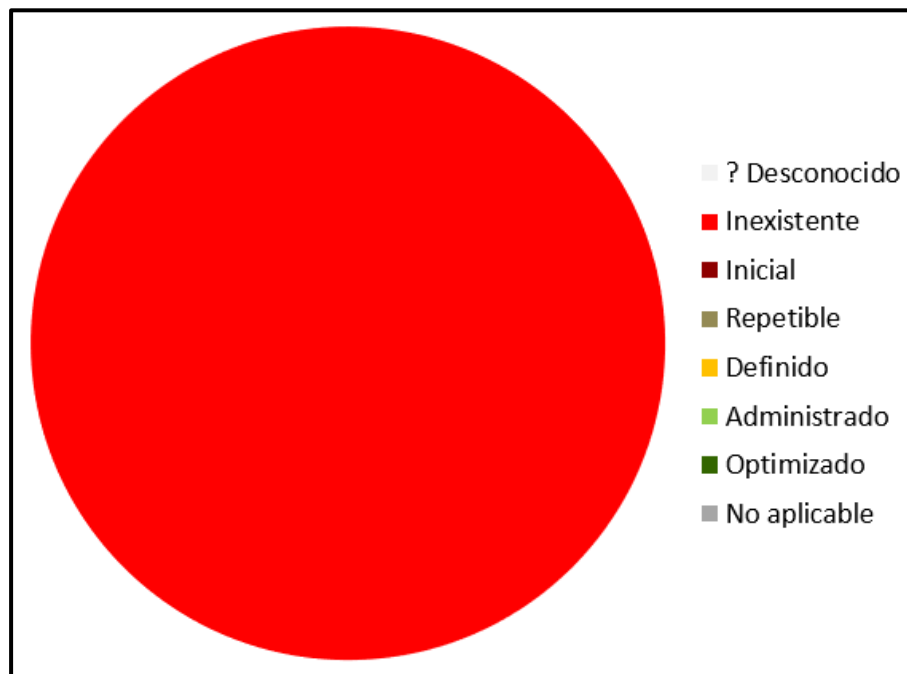
El 16 de diciembre del 2016, se crea la Secretaría Ejecutiva de la Policía Nacional del Perú, la cual posee a su cargo la dirección, organización, ejecución, evaluación, desarrollo, coordinación y supervisión de la gestión administrativa y documentaria de la Institución Policial, para la implementación de los sistemas

administrativos correspondientes, en el marco de las funciones que le competen a la Policía Nacional del Perú. Sin embargo, hoy en día se puede evidenciar que las empresas pueden sufrir filtraciones de su información si no poseen políticas adecuadas para asegurar su información, por causa de la delincuencia y de la escasa información por parte de los empleados sobre los riesgos en los que se vería comprometida la documentación.¹

En varias ocasiones, se han visto publicaciones en medios televisivos, en las que se muestran documentos con carácter confidencial que son entregados por efectivos policiales y/o empleados a cambio de una retribución monetaria.

La Unidad Policial no se encontraba alineada a las Políticas Generales en Seguridad de Información brindadas por la Dirección de Tecnologías de Información y Comunicaciones de la PNP, por lo que, se requiere un método de seguridad de información alineados a la ISO correspondiente.

Figura 1 Estado inicial de implementación ISO 27001 – SECEJE PNP – Nov. 2020

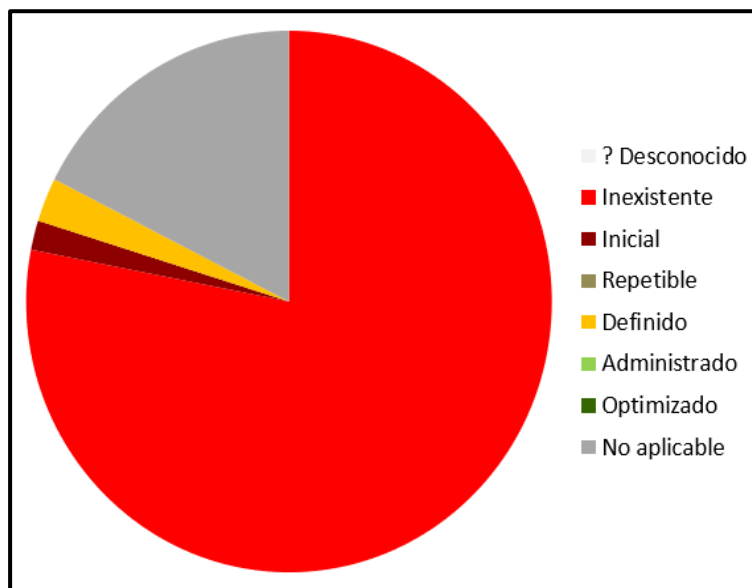


¹ Policía Nacional del Perú. 2016. Decreto Legislativo N° 1267 "Ley de la Policía Nacional del Perú". Lima : El Peruano, 2016.

Fuente: Elaboración Propia

De la misma manera, aplicando los controles de acuerdo a la norma ISO 27002, para verificar el estado del aseguramiento de los datos podemos verificar que los controles de seguridad en su mayoría son inexistentes, mientras que otros se encuentran en etapa inicial o definidos.

**Figura 2 Estado inicial de controles de acuerdo a ISO 27002 – SECEJE PNP –
Nov. 2020**



Fuente: Elaboración Propia

Se ha podido detectar que las computadoras del personal que labora en las oficinas no tienen ningún tipo de restricción para el acceso a los sitios web, lo cual puede originar una infección de virus o malware, además se pudo observar que los antivirus no están actualizados y en muchos ordenadores no existe un antivirus que detecte riesgos potenciales.

Además, se ha corroborado que no se aplican políticas de seguridad para el aseguramiento de los datos que se origina y la que se recibe en la Institución Policial, es por eso que los trabajadores no se encuentran debidamente

capacitados en temas de vulneración de la información y peligros que puedan conllevar a un mal manejo de la data que manejan. Lo que puede acarrear delitos sea dolosos o culposos por la pérdida, sustracción y/o alteración de la información. Ver Anexo 03.

Bajo los argumentos antes mencionados, se identifica como problema principal, ¿De qué manera el implementar las ISO 27001 y 27002 adaptadas para el aseguramiento de los datos en la Secretaría Ejecutiva de la PNP tiene efecto en el aseguramiento de los datos en la Unidad Policial? Los problemas específicos de la investigación fueron los siguientes:

- PE1: ¿De qué manera el implementar las ISO 27001 y 27002 adaptadas para el aseguramiento de los datos en la Secretaría Ejecutiva de la PNP tiene efecto en la confidencialidad de la información en la Secretaría Ejecutiva de la Policía Nacional del Perú?
- PE2: ¿De qué manera el implementar las ISO 27001 y 27002 adaptadas para el aseguramiento de los datos en la Secretaría Ejecutiva de la PNP tiene efecto en la integridad de la información en la Secretaría Ejecutiva de la Policía Nacional del Perú?
- PE3: ¿De qué manera el implementar las ISO 27001 y 27002 adaptadas para el aseguramiento de los datos en la Secretaría Ejecutiva de la PNP tiene efecto en la disponibilidad de la información en la Secretaría Ejecutiva de la Policía Nacional del Perú?

El presente trabajo de investigación se apoya en las siguientes justificaciones:

- a) En cuanto al aspecto teórico, el personal que labora en la Secretaría Ejecutiva de la Policía Nacional del Perú adquirirá los conocimientos necesarios para contrarrestar la vulneración de la información, además de conocer los diversos ataques informáticos que se pueden presentar en el trabajo cotidiano; así como, conocer las sanciones que se puedan dar por cometer actos que afecten la reserva de la información de la

Institución Policial, de acuerdo a la Ley N° 30096 – Ley de Delitos Informáticos². Además, al implementar las ISO 27001 y 27002³ adaptadas para la Secretaría Ejecutiva de la Policía Nacional del Perú, la cual contribuirá al aseguramiento de los datos, así como, tener de una forma adecuada y más ordenada la información que se elabora y manipula en dicha institución policial.

- b) En tanto al aspecto institucional, la Ley de la PNP⁴, nos dice que la Secretaría Ejecutiva como ente rector de la parte administrativa de la Institución Policial, debe garantizar las buenas prácticas en los procesos que se manejan en la mencionada institución y los diversos riesgos que pueda conllevar el uso de la información.
- c) En el aspecto tecnológico, en la Ley N° 27658 – Ley Marco de Modernización de la Gestión del Estado en el artículo 5, inciso f⁵. nos menciona que la “institucionalización de la evaluación de la gestión por resultados, a través del uso de modernos recursos tecnológicos, planificación estratégica y concertada ...”, debido a que en una época en la que la tecnología es imprescindible en el manejo de la información, las amenazas informáticas también van evolucionando, por lo que, es recomendable que se apliquen medidas para mitigar los riesgos ante vulneraciones o sustracción de información en las áreas de la Unidad Policial. Además de capacitar al personal policial y civil sobre las amenazas que pueda conllevar el desconocimiento en el manejo de la información.; en este sentido, resulta de importancia la aplicación del aseguramiento de los datos, puesto que, al realizar la gestión por resultados con recursos tecnológicos se necesita que la información sea confidencial, íntegra y disponible, capacitando al

² Congreso de la República del Perú. 2002. *Ley 27658 - Ley Marco de Modernización de la Gestión del Estado*. Lima : El Peruano, 2002

³ Organización Internacional de Normalización. 2013. ISO 27001. 2013

⁴ Policía Nacional del Perú. 2016. Decreto Legislativo N° 1267 "Ley de la Policía Nacional del Perú". Lima : El Peruano, 2016.

⁵ Congreso de la República del Perú. 2002. *Ley 27658 - Ley Marco de Modernización de la Gestión del Estado*. Lima : El Peruano, 2002

personal en las nuevas tecnologías y los peligros inminentes para un buen uso de la información.

- d) En cuanto a justificación económica, con un buen plan de seguridad de información en la institución reducirá los costos ocasionados debido al mal uso de los equipos tecnológicos y de la vulneración de la información.
- e) Para la justificación legal, se puede acotar que la información que maneja la Secretaría Ejecutiva de la Policía Nacional del Perú es de carácter “RESTRINGIDO” y “CONFIDENCIAL”, su uso por parte de personas ajenas o no autorizadas es ilegal, por lo tanto, se debe resguardar dicha información para que no sea filtrada.
- f) En el aspecto operacional, la gestión del aseguramiento de los datos en la Secretaría Ejecutiva de la Institución Policial se verá controlada por un sistema informático que permitirá llevar un mejor manejo y monitoreo en el soporte de las métricas para el aseguramiento de los datos.

El objetivo de la presente investigación, es el determinar el efecto de implementar las ISO 27001 y 27002 adaptadas para el aseguramiento de los datos en la Secretaría Ejecutiva de la Policía Nacional del Perú, teniendo como objetivos específicos determinar el efecto en la confidencialidad, integridad y disponibilidad de la información al implementar las ISO 27001 y 27002 adaptadas para el aseguramiento de los datos en la Secretaría Ejecutiva de la Policía Nacional del Perú.

La hipótesis general de esta investigación es, implementar la norma ISO 27001:2013 adaptada para el aseguramiento de los datos en la Secretaría Ejecutiva de la Policía Nacional del Perú tiene un efecto positivo en el aseguramiento de los datos que se maneja en la Unidad Policial, mientras que las hipótesis específicas se basan en, implementar las ISO 27001 y 27002 adaptadas para el aseguramiento de los datos en la Secretaría Ejecutiva de la Policía Nacional del Perú tiene un efecto positivo en la confidencialidad,

integridad y disponibilidad de la información en la Secretaría Ejecutiva de la Policía Nacional del Perú.

II. MARCO TEÓRICO

La gestión es hacerse cargo de administrar, organizar y poner en funcionamiento una organización, actividad económica o institución ⁶. Mientras que, la WebFinance Inc. (2020) textualmente define gestión como: *“Las actividades de un negocio se organizan y coordina con la finalidad de cumplir objetivos determinados. A menudo, el gestionar se incluye como factor para la elaboración adyacente a maquinarias, materia prima y capital. Peter Drucker (1909-2005) – Gurú en gestión, nos dice que la gestión tiene tareas básicas que incluyen mercadeo e innovación. El origen de la gestión moderna nace en el estudio del siglo 16 del vendedor inglés Sir Thomas More (1478-1535) acerca de una eficiencia baja y el fracaso de algunas empresas. Al entrelazar funciones en la elaboración de políticas corporativas y la organización, planeación, control, y dirección de los recursos en una institución con la finalidad de alcanzar los objetivos para la mencionada política se estará realizando la gestión de la empresa”*.

En cuanto a seguridad, INSPQ (2020) nos indica textualmente que: *“La seguridad es la fase por la que riesgos y circunstancias que suelen ocasionar perjuicios psicológicos, físicos o materiales se controlan con el fin de resguardar el bienestar y la salud para las personas y la comunidad. Resulta primordial en la vida cotidiana, pues consiente que la persona y la sociedad realicen sus aspiraciones.*

Para alcanzar un grado óptimo de seguridad es necesario que las personas, sociedades, los países y otros intermediarios realicen y conserven las sucesivas circunstancias, y esto, cualquiera que exista como grado estimado de vida:

- *Un clima de paz social y cohesión, así como de justicia, que ayude a proteger los derechos y las libertades en el entorno familiar, local, nacional como internacional.*

⁶ Real Academia Española. 2020. Real Academia Española. [En línea] 03 de Octubre de 2020. [Citado el: 03 de Octubre de 2020.] <https://dle.rae.es/gestionar>.

- *Prevenir y controlar los daños y efectos ocasionados por incidentes.*
- *Respetar la valoración e integridad tanto en el entorno físico, psicológico o material de los individuos.*
- *El camino a mecanismos eficaces para prevenir, controlar y rehabilitar para el aseguramiento de las circunstancias antes nombradas.*

Dichas circunstancias pueden avalarse con acciones en relación al medio ambiente (política, física, psicológica, económica, organizacional, social, etc.) y las conductas.”

Para García Marco (2011), la palabra información puede significar “acción y efecto de informar o informarse” cuando indica un proceso, y “noticia o conjunto de noticias resultantes de esa acción o efecto” cuando indica un producto.

“La comunicación o captación de conocimientos que sirven para ampliar o especificar los que se poseen sobre alguna materia en particular”. (Real Academia Española, 2020).

Para Chiavenato (2007): *“Información. Es un grupo determinado de data con un resultado, o sea, que aminora la indecisión o incrementa la comprensión de algo. La información es un recado con un conocimiento específico de acuerdo al contexto en que se dé, y que se encuentra disponible para ser usado en forma inmediata y que suministra orientación a las acciones para que se pueda reducir el nivel de incertidumbre con relación a las decisiones adoptadas”.*

Se deduce que información es la agrupación de datos organizados que otorgan un valor añadido a una institución, dicha información se puede obtener en forma impresa, escrita, oral y se utiliza de acuerdo a los requerimientos de la institución.

Según ISOTools Excellence (2015) dice que: La norma ISO 27001 para el aseguramiento de los datos posee como objetivos proteger la data y procedimientos para el tratamiento de los datos.

Las terminologías referidas a seguridad informática y seguridad de la información son generalmente utilizadas. Sus significados difieren, pero todas tienen como finalidad la seguridad de los ejes fundamentales para el aseguramiento de los datos (disponibilidad, confidencialidad e integridad) en la organización. Las diferencias entre los términos dependen de la orientación que se les dé, los métodos utilizados y las franjas de reunión.

Las organizaciones públicas y privadas poseen grandes cantidades de información confidencial sobre recursos humanos, logísticos, de investigación, proveedores, clientes, etc. Gran parte de esta información es reunida, tratada, almacenada y disponible para las personas que deseen revisarla.

En caso que la data confidencial de la empresa, de su clientela, de las disposiciones adoptadas, de su contabilidad, entre otros. se filtre a sus contrincantes, esta se hará pública de manera no acreditada y puede tener peligrosos resultados, debido a la afectación de la credibilidad ante los clientes, probables negocios no concluirán, pueden originarse denuncias e inclusive originar el desplomo financiero de la empresa.

Por las razones expuestas, la protección de la información confidencial se convierte en una necesidad, debido al requerimiento de la organización, y en la mayoría de asuntos se convierte en algo ético y una obligación legal.

Para un ciudadano común, el aseguramiento de los datos puede ocasionar un resultado muy característico debido a que el quebrantamiento de su privacidad tendría diferentes consecuencias que dependen de la cultura.

En su artículo, Carbajal (2019) tuvo como objetivo la presentación de la aplicación de un caso sobre gestionar el aseguramiento de los datos en un organismo público, usando previa verificación de literatura, cuatro estándares internacionales para la seguridad de información (ISO/IEC 27001:2013, ISO/IEC

27002:2013, ISO/IEC 27003:2010 e ISO/IEC 27005:2008) y la contextualización en Colombia, partiendo de las directrices dadas por el Ministerio de Tecnologías de Información. Los resultados en dicha investigación fueron desarrollar una metodología orientada a las necesidades del organismo público con medidas e indicadores para una adecuada gestión sobre el peligro y controles correspondientes para contrarrestar la perplejidad para gestionar en forma adecuada la información.

En tanto, la Universidad de Hashemita (2014) mediante un caso de estudio tuvo como objetivo evaluar los niveles de seguridad en la información sobre universidades jordanas. El caso estuvo centrado en el análisis de riesgos a los que ven amenazados los sistemas de información de la HU desde perspectivas organizativas y técnicas mediante aplicación de evaluación de vulnerabilidades y pentesting, finalmente organizadas en un plan de evaluación de riesgos. Durante el estudio de caso, se ha elaborado un SGSI ISO/IEC 27001:2005 para aminorar los peligros a los que se ven asediados los sistemas informáticos en la HU. El Sistema para gestionar el aseguramiento de los datos proporciona las políticas y los mecanismos adecuados para minimizar posibles peligros identificados y facilitar un examen, además de la mejora de experiencia en el aseguramiento de los datos de HU.

En su artículo ISO/IEC 27001 Information Systems Security Management Standard: Exploring the Reason for Low Adoption (2015), se buscaron las razones de la baja adopción en la normativa internacional ISO/IEC 27000 que implica una gestión para el aseguramiento de los datos. Además, se comparó la citada norma con otras dos normas para la gestión comúnmente aplicadas: ISO 9001 para gestionar la calidad y la ISO 14001 para gestionar en materia ambiental. La investigación tuvo como resultado la demostración no solamente de las bajas tasas de adopción, sino que, la norma ISO/IEC 27001 ha recibido poco interés por parte del mundo académico, según lo medido por el número de publicaciones académicas sobre el tema. El estudio sugirió una hoja de ruta para futuras investigaciones sobre el tema.

En su investigación, Ortiz Morales (2018) tuvo como objetivo implementar de manera gradual la Norma Internacional ISO/IEC 27002:2013 con el que se busca gestionar el aseguramiento de los datos en la Universidad Nacional Agraria de la Selva. Dicha investigación fue Aplicada con un diseño cuasi - experimental debido a que realizaron controles al mismo conjunto de estudio. Se pudo afirmar con un 95% de nivel de confianza que al implementar mecanismos en el aseguramiento según la normativa ISO/IEC 27002:2013 la cual permitió un mejoramiento al gestionar el aseguramiento de los datos de la Universidad Nacional Agraria de la Selva.

Mientras que, en su investigación Salsavilca Ramos (2017) tuvo como objetivo establecer el efecto de gestionar de acuerdo a la normativa ISO 27001 el aseguramiento de los datos en la institución privada Atento del Perú en el año 2017. Para su diseño en la investigación se utilizó el sistema de representación universal. La muestra aplicada se dio en una base promediable de 20 padrones en un rango de un mes, con un ensayo que permite la medición en los niveles para gestionar y disponer medidas aplicadas al aseguramiento de los datos diarios en el sitio web de la sede Callao de acuerdo a los padrones conseguidos por los involucrados en cada área. Se concluyó que aplicando la norma ISO 27001 se obtuvo una reducción significativa de 21,70 en grado de información la cual podría accesarse sin autorización.

Para NQA (s.f.) la ISO 27001 se fundamenta mediante el ciclo PHVA o ciclo de Deming, éste puede aplicarse no solo al sistema de gestión, sino también a cada elemento individual para proporcionar un enfoque en el ciclo de mejora continua.

Figura 3 Modelo PHVA para ISO 27001



Fuente: NQA – ISO 27001.

En la fase Planificar, se establecen los objetivos, recursos, requisitos, política organizativa e identificación de riesgos y oportunidades.

En la fase Hacer, se implementa lo planificado.

En la fase Verificar, se controlan y miden los procesos para establecer el rendimiento de las políticas, objetivos, requisitos y actividades planificadas y se deben informar los resultados.

En la fase Actuar, se toman las acciones para mejorar el rendimiento, en la medida de lo necesario.

En los últimos años, el aseguramiento de la data ha ido aumentando, además de evolucionar considerablemente. Esta continua evolución ha permitido que se convierta en una carrera acreditada mundialmente, en la que se brindan diversas

especialidades que se consiguen al realizar una auditoría del Sistema de Gestión de Seguridad de la Información ISO-27001, como se muestra a continuación:

- Planificación de la continuidad de negocio: Es un plan en la cual una empresa debe rescatar y reintegrar funcionalidades críticas en forma parcial o que hayan sido detenidas en forma total, en un determinado tiempo luego de una interrupción no planificada o algún desastre.

Las posibles situaciones contienen ocurrencias locales (incendios, inundaciones, desastres naturales, etc), acontecimientos de representación en regiones, nacional o internacionalmente hasta eventualidades como epidemias, entre otros.

Las acciones dadas para planificar y prevenir se encontraban direccionadas para operaciones informáticas, que mayormente se encontraban concentradas en el Departamento de Informática e inclusive en un lugar físico concreto. Pero con el transcurrir de los años y la distribución informática, soportada en dispositivos informáticos y telemáticos desarrollados en las áreas de la empresa, esa diligencia modificó su alcance y se llamó Business Continuity Planning, que puede traducirse como Planificación de Continuidad del Negocio. Wikipedia (2020).

- Ciencia forense digital: Sirve para estudiar los dispositivos informáticos de manera que ayude a solucionar los delitos. También podría incluir dispositivos móviles. Aquellos versados que realizan dicha labor son llamados “analistas” o “investigadores”. En ocasiones las investigaciones son usadas en la disputa entre las organizaciones y/o personas. Estos no deberían implicar un crimen. En vez de esto, se solicita a un profesional que investigue información sobre de un individuo u organización observando su computadora. Existe un vocablo específico usado para referirse a este tipo de indagación, es “eDiscovery”.

Alguna utilización de la ciencia forense digital la conocemos como “detección de intrusos”. Luego de que un cibercriminal invade un conjunto de ordenadores. Luego de la pausa de un profesional muy seguido se le

solicita que observe a los ordenadores en red para conocer cómo sucedió. Wikipedia (2020).

- Administración de Sistemas de Gestión de Seguridad: Es aquel grupo de Políticas de Administración de la Información. Dicho término se utiliza especialmente por la ISO/IEC 27001, no obstante, no es la única norma que usa este término o concepto.

Realizar en forma adecuada la Gestión del aseguramiento de la data requiere formar y conservar los programas, revisiones y políticas de seguridad que se encuentran obligados en preservar la confidencialidad, integridad y disponibilidad de la data en una organización.

- Confidencialidad: Según (ISOTools Excellence, 2018), la confidencialidad demanda que la información sea de acceso exclusivamente por personas autorizadas. Resulta importante que la información sea accedida con autorización y control; puesto que, parte de la información y/o recursos se encuentran restringidos o se pretende mantener en secreto.

- Integridad: Según ISOTools Excellence (2018), la integridad tiene como objetivo que la información se conserve intacta ante incidentes o tentativas maliciosas. Únicamente se podrá alterar la información mediante autorización.

De acuerdo a Tecnologias-informacion.com (2018), la integridad de datos es utilizado para describir la exactitud y fiabilidad de los datos. Los datos deben estar completos, sin alteraciones con respecto al original, que se piensa confiable y exacto. Los compromisos con la integridad de la información pueden ocurrir de diversas formas.

En organizaciones donde la información es alterada, identificada y abordada, las probables fuentes de daño a los datos son un aspecto importante de la seguridad de los datos. Una fuente humana puede ser el inicio de los problemas de integridad de los datos, debido a que, los

individuos que ingresan para verificar los registros pueden cometer errores, lo que conllevará a alteraciones entre los datos originales y los almacenados en un sistema.

De igual forma, las personas suelen ocasionar errores involuntarios durante la transferencia o la copia electrónica de datos, permitiendo la disparidad entre las diversas versiones o referencias a un archivo.

- Disponibilidad: Para Universidad de Alicante (2018), la información poder ser accesada por personas, procesos y/o aplicativos en el instante que se requiera. Se habla de alta disponibilidad cuando un sistema está implementado o diseñado de forma que garantiza la continuidad operacional absoluta durante un periodo de tiempo dado, es decir, que se garantiza que el sistema se encuentre disponible siempre, impidiendo cualquier interrupción del servicio (corte eléctrico, fallos en el hardware o problemas en el software).

La norma ISO 27001 se publicó el 25 de setiembre del 2013, y forma parte de la familia de la ISO 27000, cuenta con las bases para que un sistema para gestionar el aseguramiento de la data se realice en forma adecuada, es por esto que es una norma internacional de buenas prácticas en el que la organización demuestra ante su entorno que la información que maneja se encuentra asegurada siguiendo los mecanismos y controles adecuados de acuerdo a la mencionada norma.

Al implementar la norma ISO 27001 se obtendrían entre los aspectos principales:

- Una adecuada mejora continua de los procesos en la organización.
- Un estándar en la empresa en cuanto a requisitos de documentación y registros.

- Se evaluarán y gestionarán los riesgos en la organización a través del modelo Planificar, Hacer, Verificar y Actuar – PDCA.
- Los activos se encontrarán protegidos, utilizando políticas y controles para la evaluación como medidas para prevenir y contrarrestar riesgos.

Hay varios beneficios que puede contribuir la normativa ISO 27001 implementando diferentes directrices que ésta enuncia. Los cuáles mencionaremos a continuación:

- Autorizar auditorías que verifiquen la seguridad de toda la información en procesos, servicios y productos en la organización.
- El cumplimiento de las directivas para resguardar la seguridad en redes y sistemas de información.
- Evadir obstáculos legales por infracciones en la seguridad de datos.
 - Utilizar las prácticas a la hora de recabar datos personales, asimismo a la hora de realizar copias de seguridad o de distribuir datos.
 - Cumplir las solicitudes de los interesados y las organizaciones en cuanto a los aspectos de seguridad de información.
 - Lograr la delantera comercial ante los competidores que no efectúan las normas de protección de datos.
 - Economizar tiempo, recursos y dinero en el establecimiento de componentes de seguridad de información.
- Economizar costos asociados con los incidentes de seguridad.

- La empresa debe lograr mejorar su reputación empresarial y un discernimiento positivo en el ecosistema del trabajo.

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

El tipo de investigación que se realizó fue aplicada con diseño cuasi experimental, de acuerdo a los siguientes motivos:

3.1.1 Tipo de investigación

Según Ander - Egg (2011, pág 42) la investigación aplicada depende de descubrimientos para tener una vía a la solución de problemas aplicando los conocimientos adquiridos en la una investigación básica. Además, se procura que la aplicación de la solución en un problema sea inmediata, en vez de basarse en el desarrollo de teorías sobre posibles soluciones. Mientras que, para Muñoz (2011, pág. 26) se emplean los conocimientos que nacen de la indagación pura para solucionar dificultades de representación práctica, empírica y tecnológica para un progreso y beneficio de sectores productivos de bienes y servicios de la comunidad.

En base a que en una investigación de tipo aplicada se procuran emplear los progresos y efectos de la investigación básica para utilizarlos en la incubación del bienestar de la sociedad; se seleccionó este tipo de investigación debido a que no se encontraba una gestión de seguridad de información, lo cual era un problema muy grave ante la amenaza de pérdida o sustracción de información de personas ajenas a la unidad policial o de personal que labora en dicha institución pero que no conocen sobre las amenazas que existen o que conociéndolas, utilizan las malas prácticas para vulnerar o distorsionar la información de la Secretaría Ejecutiva de la Policía Nacional del Perú.

3.1.2 Diseño de investigación

Para Bernal Torres (2010, pág. 146): “Los modelos cuasiexperimentales se distinguen de los experimentales auténticos debido a que en aquellos el indagador despliega poco o ninguna intervención sobre las inestables extrañas, los colaboradores de la averiguación se pueden determinar aleatoriamente a los conjuntos y en ocasiones se dispone de grupo de control.

Estos modelos comúnmente manejan conjuntos ya determinados.

Algunos de los modelos cuasiexperimentales son:

- Diseños de un conjunto con medida precedente y posterior.
- Diseños con un conjunto de cotejo equivalente.
- Diseños con series de turnos interrumpidos.”

Figura 4: Diseño de comparación con dos grupos estáticos

Esquema del diseño:	Grupo experimental	X	O ₁
	Grupo control	-	O ₂

Fuente: Bernal Torres, 2010

Donde:

- X** : variable independiente (programa de capacitación).
- O₁** : Valores de indicadores de medición de la variable dependiente durante el tiempo de realización del experimento (Post-test).
- O₂** : Valores de indicadores de medición del grupo de control en antes de la realización del experimento (Grupo control – Pre test).

Como se puede visualizar en la figura, se formaron dos grupos; el primer grupo (denominado grupo experimental) recibió capacitación sobre medidas de seguridad implementadas en la Secretaría Ejecutiva de la Policía Nacional del Perú, mientras que, el segundo grupo sirvió de grupo de control, por lo tanto, no recibió capacitación.

Otra de las razones por la que se escogió este diseño es que el investigador no puede alterar los valores de la variable independiente a voluntad ni establecer grupos experimentales de manera aleatoria; sin embargo, sí puede encajar una manera parecida al diseño experimental en su colección de datos. De esta forma, la investigación cuasiexperimental es aquella en la que incurra una muestra del experimento con los mismos grupos y las mismas variables del fenómeno estudiado, puesto que, no pueden alterarse ni manipularse, pero el diseño del experimento admite la formulación de una hipótesis y la especificación de la forma de adquirir los datos que ocasionen las respuestas conseguidas de la conducta del fenómeno, lo que permite confirmar o rebatir la hipótesis. Muñoz (2011, pág. 97).

3.2. Variables y operacionalización

3.2.1 Definición Conceptual

3.2.1.1 Variable Independiente (VI): ISO 27001

Precisa de forma general, independiente de los componentes ambientales de institución (entorno, contexto, activos de las TIC, información, cultura organizacional, entre otros) y de los métodos de la empresa (políticas, procedimientos, procesos, entre otros), lo que corresponde a planificación, implantación, verificación y control de

un sistema para la gestión del aseguramiento de la data, empezando con un análisis de riesgos y la planificación e implantación de la solución a los mismos para su atenuación. (UNIR, 2020)

3.2.1.2 Variable Dependiente (VD): Seguridad de Información

Es el extenso número de componentes de tipo tecnológicos, de capital humano, económico, negocios, legal, de cumplimiento, la misma que discurre no sólo aspectos informáticos y de telecomunicaciones sino también en el ámbito físico y medioambientales. (Areitio, 2008)

3.2.2 Definición Operacional

Se tuvo la definición operacional con respecto a la variable independiente (VI), la cual fue la ISO 27001, norma internacional que conjuntamente con la ISO 27002 nos da una serie de controles para la medición de integridad, confidencialidad y disponibilidad se aplicaron valores en cada una de las escalas.

Mientras que, con respecto a la definición operacional de la variable dependiente (VD), que trata sobre la Seguridad de Información, se observaron los métodos apropiados para ejecución de controles en la cual se conservó una muestra menor a los entregados por el nivel gerencial. Además, de una serie de medidas adoptadas para que el personal que labora en la Secretaría Ejecutiva de la Policía Nacional del Perú conozca (mediante capacitaciones) los diferentes aspectos del aseguramiento de los datos.

En el Anexo 05, se evidenció la operacionalización de variables mostrando las variables de investigación, su descripción (tanto conceptual como operacional), dimensión, indicador correspondiente. Mientras que, en el Anexo 06 se muestra la matriz de consistencia del proyecto.

3.2.3 Operacionalización de variables

Ver Anexo 05.

3.3. Población, Muestra y Muestreo

3.3.1 Población

La población consiste en la recolección de un grupo de elementos o individuos que tienen atributos comunes, con la finalidad ser estudiados y conseguir conclusiones concretas para establecer resultados.

De acuerdo a la magnitud de la población investigada, el resultado sería finito o infinito. En caso, el resultado de los grupos estudiados es infinito, estos se describen como conceptuales o artificiales, puesto que, toda población concluye con un resultado determinado al ser investigada. Enciclopedia Económica (2018).

En la presente averiguación, la población a estudiar estará constituida por los veinticuatro (24) trabajadores, tanto personal policial y civil que laboran en la Secretaría Ejecutiva de la Policía Nacional del Perú cuya sede se encuentra en el distrito de El Rímac.

3.3.2 Muestra

La muestra es un subconjunto o parte del universo o población en que se efectuará la indagación. Existen operaciones para conseguir la suma de los dispositivos de la muestra como fórmulas y lógica. De este modo, se puede inferir que la muestra es una porción característica de la población.

La muestra para la presente investigación será el Diseño de discontinuidad en la regresión (DDR), pues su conformación básica constituye una medida o variable antes y una medida posterior, que manifiesta el resultado del método. Este tipo de diseño, el razonamiento de asignación de las unidades a los conjuntos se conoce.

La presente investigación se ha dividido la población en dos grupos de doce (12) trabajadores, en el que el primer grupo será de control y el segundo grupo es el de tratamiento.

3.3.3 Muestreo

El muestreo no probabilístico implica la selección de elementos desde una población usando procedimientos no aleatorios. Las técnicas de muestreo no probabilísticas son típicamente menos rigurosas y menos representativas que las técnicas de muestreo probabilísticas. (Bobenrieth, 2012 pág. 938).

3.4. Técnicas e instrumentos de recolección de datos

Para la presente investigación, se usaron la Observación y la Encuesta.

3.4.1 Técnica: Observación

Según (Arias, 2012 pág. 69) menciona que “la observación es una capacidad que conta en visualizar u obtener mediante la visión, de manera sistemática, cualquier acción, actividad o contexto que se origine en el entorno o en comunidad, en relación a algunas metas de indagación preestablecidas”.

3.4.2 Validez

De acuerdo a Arias (2012 pág. 90) un cuestionario es válido cuando las preguntas o ítems tienen una correspondencia directa con los objetivos de la investigación. En otras palabras, las preguntas consultarán solamente lo que se procura conocer o medir.

Para determinar el nivel de validez de constructo a través de juicio de los expertos, el cual estuvo conformado por 3 ingenieros de sistemas, los cuales calificaron a los instrumentos con el siguiente puntaje:

Tabla 1: Validez de cuestionario: Seguridad de Información

Especialista 1
90.8

Fuente: Elaboración propia

El detalle de esta calificación, se presenta en el Anexo 07.

Tabla 2: Validez de entrevista: Seguridad de Información

Especialista 1
94.8

Fuente: Elaboración propia

El detalle de esta calificación, se presenta en el Anexo 08.

3.4.3 Confiabilidad

La confiabilidad de acuerdo a Frias-Navarro (2020) no es del test sino de las puntuaciones obtenidas en el instrumento de medida.

La fiabilidad de la consistencia interna de la herramienta se consigue evaluar con el alfa de Cronbach. Esto se puede conseguir a través de un grupo de ítems que se esperan que midan el mismo constructo o una única dimensión teórica de un constructo latente.

La confiabilidad de los resultados se determinó en base al coeficiente de Alfa de Cronbach, el cual tuvo como resultado de 0.819 para la encuesta de Seguridad de Información. Los detalles de dicho resultado se adjuntan en el Anexo 11.

3.4.4 Técnicas de recolección de datos:

En esta indagación se manejó como pericia de recolección de datos el cuestionario y como instrumento la encuesta, la cual incluye 15 preguntas relacionadas a la seguridad de información en las oficinas de la Secretaría Ejecutiva PNP, que se han realizado al grupo de control de 12 personas:

<https://docs.google.com/forms/d/1DxMd53HOGWxukWXLfTkObHaWUwkAgWhuW2DkMfKFcnM/edit?usp=sharing>

3.5. **Procedimientos**

En el trabajo de investigación se recabó información importante para el estudio a través del cuestionario antes mencionado, llenado por el personal que labora en la Secretaría Ejecutiva PNP.

Además, el instrumento de observación fue validado por tres expertos cuyo objetivo fue medir la confiabilidad en el aseguramiento de los datos en las diferentes oficinas de la SECEJE PNP.

3.6. **Método de análisis de datos**

Los datos han sido extraídos de la encuesta, y de entrevista y los resultados han sido tabulados, procesados y analizados en el software SPSS v20.

3.7. **Aspectos éticos**

Para la realización de la presente investigación se utilizaron los valores y principios éticos que se superponen en la Policía Nacional del Perú, además de los valores y principios éticos de la Universidad César Vallejo que en la carrera de Ingeniería de Sistemas han sido aplicados. Por lo que, la información se mantiene en total reserva y confidencialidad.

IV. IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

4.1. Fase 0: Estudio de factibilidad

4.1.1 Factibilidad técnica

La factibilidad técnica de esta tesis se da debido a que se han proporcionado los recursos necesarios para la puesta en marcha del proyecto.

4.1.2 Factibilidad operativa

La factibilidad operativa de esta tesis se da debido a que se cuenta con el apoyo y asesoramiento de la Dirección de Tecnologías y Comunicaciones – DIRTIC PNP, además el resultado del proyecto tendrá un impacto positivo en el aseguramiento de los datos en la Secretaría Ejecutiva de la PNP.

4.1.2 Factibilidad económica

La presente tesis es viable económicamente, debido a que la Secretaría Ejecutiva está dispuesta a mejorar el aseguramiento de los datos en la Unidad Policial.

4.2. Fase 1: Contexto de la organización

4.2.1 Descripción de la institución

La empresa

La Secretaría Ejecutiva de la PNP, es la entidad de carácter sistémica, técnica, normativa y Ejecutiva, delegado a planificar, conducir y supervisar los sistemas administrativos de la institución policial, amparado en la orientación de gestión por resultados, priorizando y

optimizando la utilización de los recursos públicos para favorecer al cumplimiento de las funciones operativas de la institución.

Misión

Ser la entidad sistémica, técnica, normativa líder de la gestión administrativa policial que favorecerá al proceso de modernización institucional, buscando colocarse como un ente rector del Sector Interior.

Visión

Entidad de más alto nivel administrativo dentro de la Policía Nacional del Perú y posee a su cargo las Direcciones Ejecutivas de Administración, Planeamiento y Presupuesto, Tecnologías de Comunicación y Estadística, Personal, Infraestructura y Equipamiento y Asesoría Jurídica.

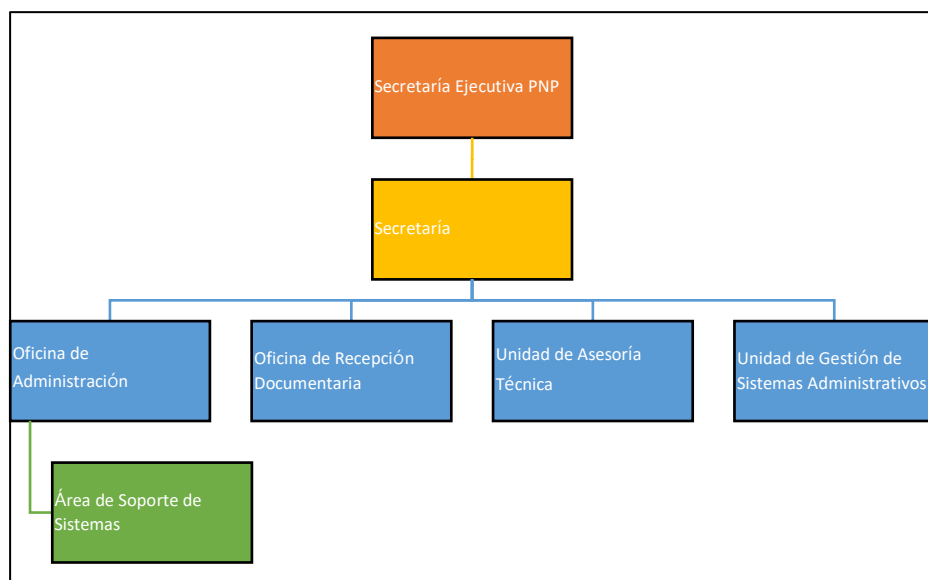


Figura 5. Organigrama de la Secretaría Ejecutiva de la PNP.

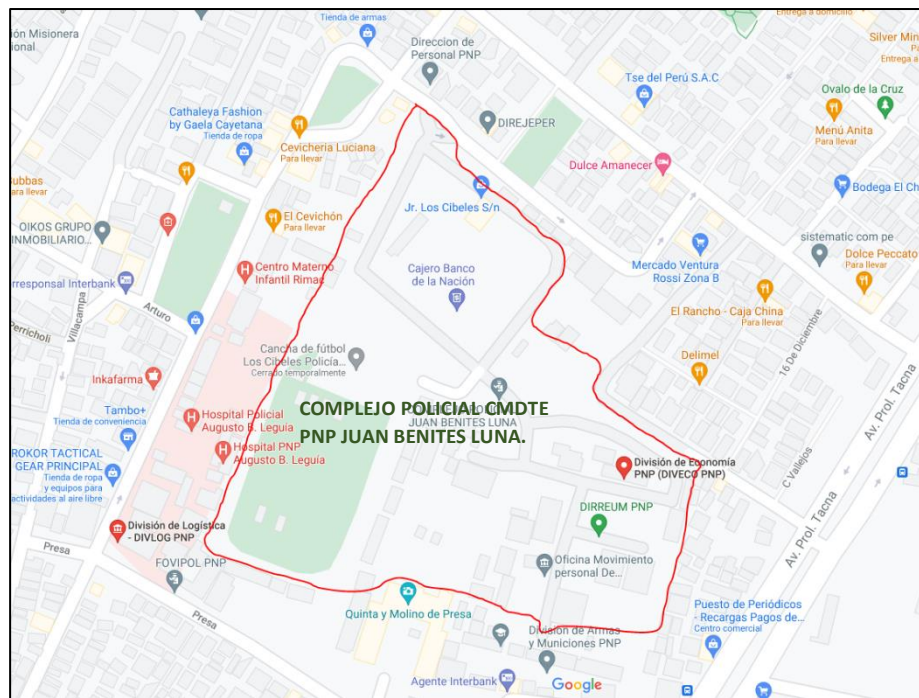


Figura 6. Ubicación de la Secretaría Ejecutiva de la PNP. Google Maps (2020).

4.3. Fase 2: Liderazgo

4.3.1 Organigrama propuesto del comité de gestión de seguridad de información.

Debido a que la Implementación del Sistema de Gestión de Seguridad de Información se encuentra en fase inicial se ha propuesto el organigrama del comité de seguridad de información de la siguiente manera:

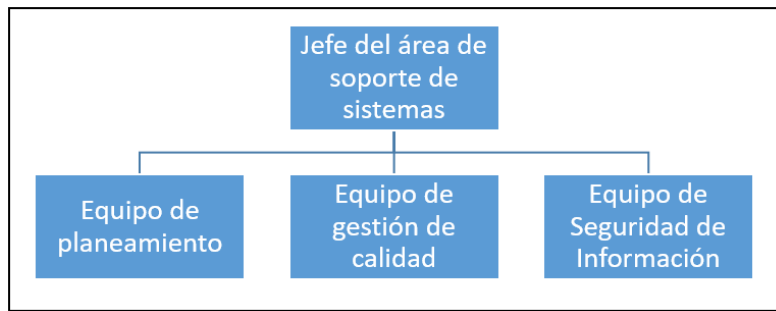


Figura 7. Organigrama propuesto del comité de seguridad de información.

4.3.2 Políticas de seguridad de información

Ver Anexo 14.

4.4. Fase 3: Planificación

4.4.1 Gestión de riesgos

Ver Anexo 15.

4.5. Fase 4: Soporte

4.5.1 Lista Maestra de Registros

Ver Anexo 16.

V. RESULTADOS

5.1. Análisis e interpretación de resultados

5.1.1 Resultados generales

Tabla 3: Estructura de la NTP/ISO 27001:2013

Estructura de la NTP/ISO 27001:2014

Fases	Nombre	Actividades principales	Entregables
0	Estudio de factibilidad	Realizar los estudios existentes de factibilidad.	Factibilidad técnica Factibilidad operativa Factibilidad económica
I	Contexto de la organización	Comprender la organización y su contexto	Misión, visión de la empresa
		Determinar el alcance del sistema de gestión de seguridad de información	Alcance
II	Liderazgo	Liderazgo y compromiso	Organigrama de comité de gestión
		Roles, responsabilidades y autoridades organizacionales.	Comité de Gestión de seguridad y hoja de funciones.
		Política	Políticas de seguridad de información.
III	Planificación	Acciones para tratar los riesgos y las oportunidades. Objetivos de seguridad de información y planificación	Gestión de riesgos
IV	Soporte	Recursos	Lista de activos Gestión de recursos
		Competencias	Gestión de competencias
		Concientización	Acuerdo de concientización y confiabilidad.
		Comunicación	Gestión de comunicaciones

5.1.2 Resultados específicos

Tabla 4: Resultados de pre-test y post-test

Resultados de pre-prueba y post-prueba para KPIs

N°	KPI1: Tiempo para reportar incidencias de seguridad de la información (minutos)		KPI2: Porcentaje de disponibilidad de la información dentro de la institución (%)		KPI3: Porcentaje de integridad de la información dentro de la institución (%)		KPI4: Tiempo para dar respuesta a una incidencia (minutos)		KPI5: Nivel de satisfacción del cliente	
	Pre-prueba	Post-prueba	Pre-prueba	Post-prueba	Pre-prueba	Post-prueba	Pre-prueba	Post-prueba	Pre-prueba	Post-prueba
1	37	12	43	96	36	99	45	15	2	4
2	43	15	50	93	45	88	32	15	2	4
3	45	5	28	95	52	82	47	15	1	4
4	45	13	31	95	34	99	38	10	1	4
5	35	11	28	93	43	88	60	15	1	3
6	33	9	41	95	52	99	35	10	1	3
7	20	5	50	99	67	99	45	15	2	4
8	45	12	52	95	45	92	45	15	1	3
9	33	11	37	94	84	95	60	10	2	3
10	35	7	45	96	52	95	40	10	2	4
11	37	5	32	96	35	99	30	10	2	4
12	30	13	36	96	30	96	30	10	1	3

Fuente: Elaboración propia

5.1.3 Análisis e interpretación de resultados

Tabla 5: Medias de los KPIs para el pre-test y post-test

Medias de los KPIs para la pre-prueba y post-prueba

Indicadores	Pre-prueba (media)	Post-prueba (media)	Comentario
KPI1: Tiempo para reportar incidencias de seguridad de la información (minutos)	36.5	9.8	-
KPI2: Porcentaje de disponibilidad de la información dentro de la institución (%)	39.4	95.2	-
KPI3: Porcentaje de integridad de la información dentro de la institución (%)	47.9	94.3	-
KPI4: Tiempo para dar respuesta a una incidencia (minutos)	42.3	12.5	-
KPI5: Nivel de satisfacción del cliente	-	-	No contrastado. Indicador cualitativo.

Nota: Fórmula para hallar el %: (procesos sin observaciones/procesos realizados)*100 = % de exactitud.

Fuente: Elaboración propia

Interpretación

Analizando la tabla anterior podemos visualizar que la media del tiempo para reportar incidencias en el aseguramiento de los datos (KPI1) ha sufrido una disminución desde que se implementaron los mecanismos de seguridad de acuerdo a la norma 27001; mientras que, el porcentaje promedio de disponibilidad de la información dentro de la institución (KPI2) y el porcentaje de integridad de la información dentro de la institución (KPI3) han aumentado después de la implementación de los mecanismos de seguridad de acuerdo a la norma 27001; a su vez, el tiempo para dar respuesta a una incidencia (KPI4) se ha reducido desde la implementación de los mecanismos antes mencionados.

A. Indicador 1: Tiempo para reportar una incidencia de seguridad de información (KPI1)

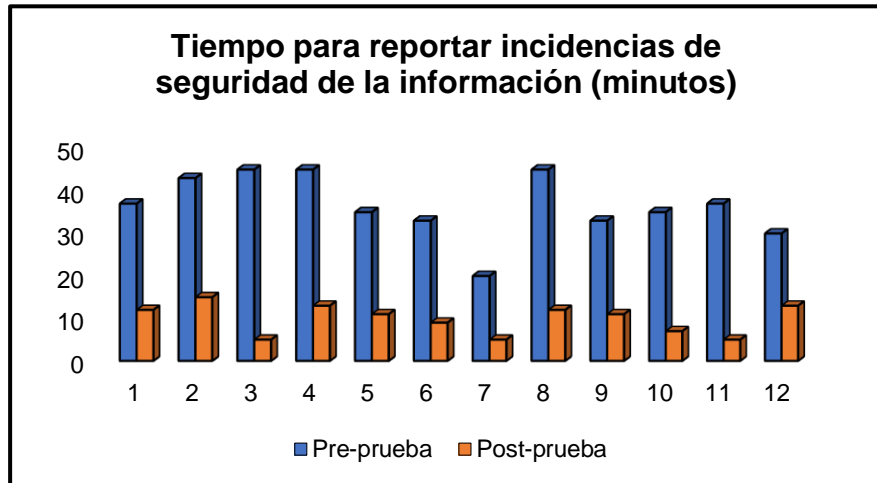


Figura 8: Resultados de Pre-Prueba y Post-Prueba para KPI1.

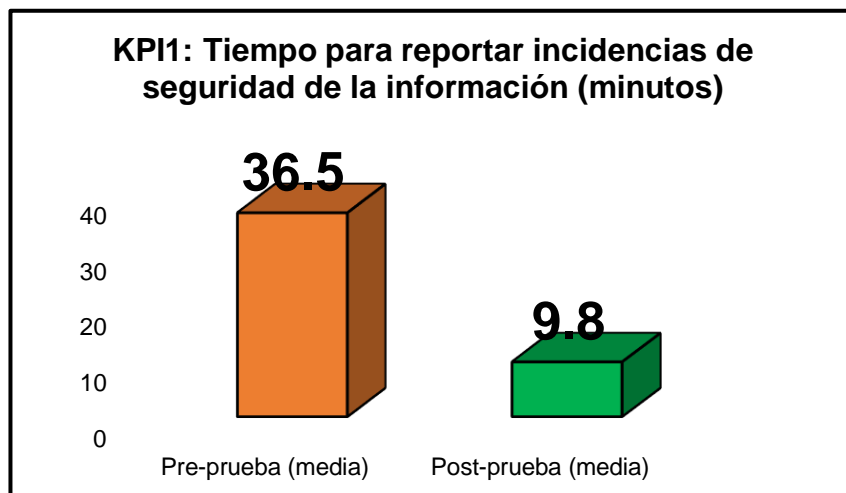


Figura 9. Media de resultados de Pre-Prueba y Post-Prueba para KPI1.

Interpretación:

Tal como se aprecia en la figura 9, la media de los resultados para reportar una incidencia en el aseguramiento de los datos es de 37 minutos antes de implementar la NTP/ISO 27001 y los controles de la NTP/ISO 27002, pero los resultados posteriores a la implementación arrojaron como media 10 minutos, es decir, el tiempo se redujo en un 27%.

B. Indicador 2: Porcentaje de disponibilidad de la información dentro de la institución (KPI2)

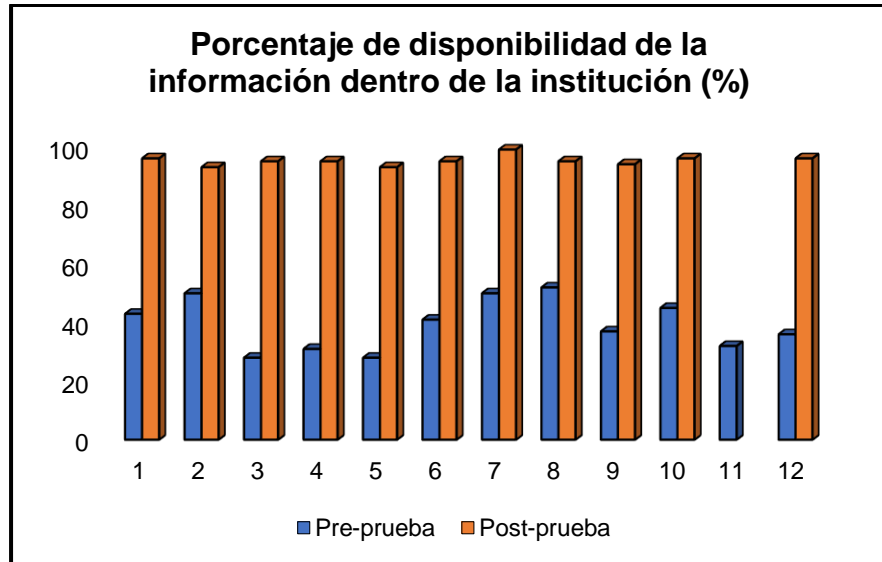


Figura 10. Resultados de Pre-Prueba y Post-Prueba para KPI2.

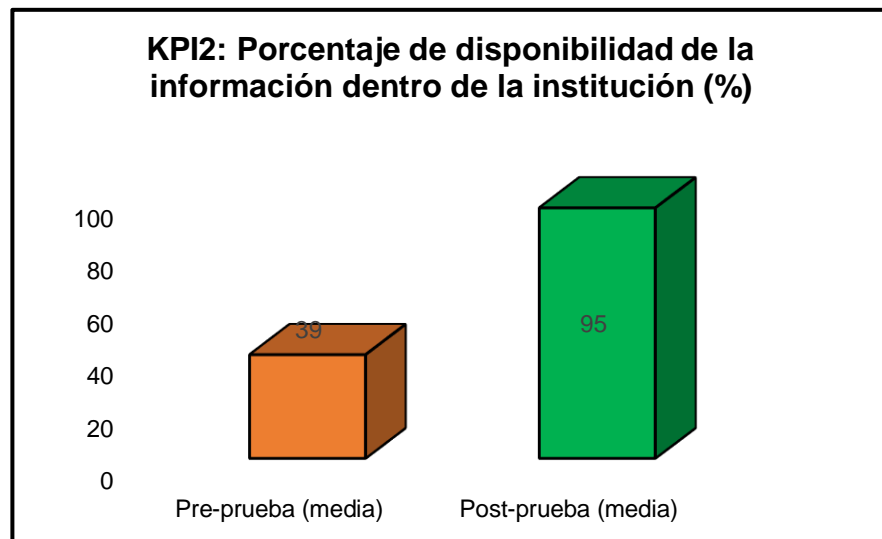


Figura 11. Media de resultados de Pre-Prueba y Post-Prueba para KPI2.

Interpretación:

Se puede apreciar en la figura 11 que antes de implementar las Normas Técnicas Peruanas de las ISO 27001 e ISO 27002, el porcentaje de disponibilidad de la información dentro de la institución era del 39%, pero luego de implementadas estas normas y controles el porcentaje pasó a ser del 95%, aumentando así la disponibilidad de la información 2.4 veces más en comparación al estado inicial.

C. Indicador 3: Porcentaje de integridad de la información dentro de la institución (%) (KPI3)

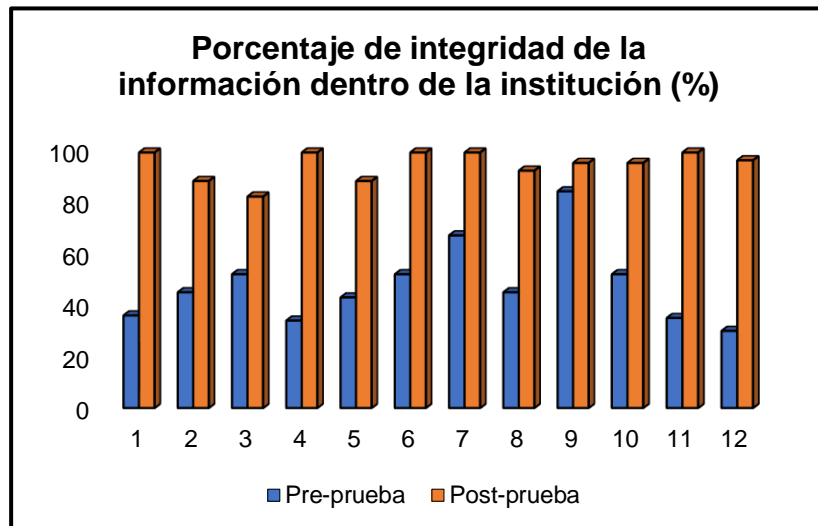


Figura 12. Resultados de Pre-Prueba y Post-Prueba para KPI3.

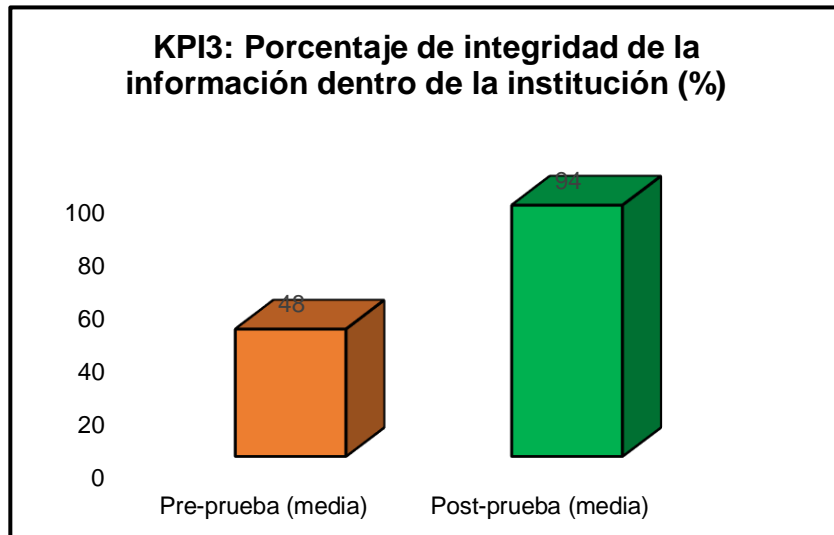


Figura 13. Media de resultados de Pre-Prueba y Post-Prueba para KPI3.

Interpretación:

Antes de la aplicación de las normas ISO 27001 e ISO 27002 y sus controles, el porcentaje de integridad de la información dentro de la institución era del 48 %, pero a consecuencia de la implementación de las normas y sus controles, el porcentaje se elevó al 94%, tal como se puede apreciar en la figura 13.

D. Indicador 4: Tiempo para dar respuesta a una incidencia (minutos) (KPI4)

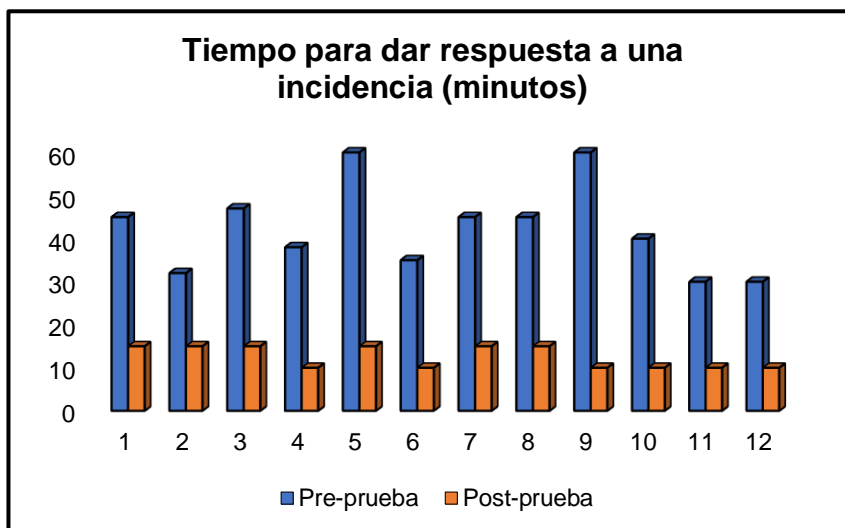


Figura 14. Resultados de Pre-Prueba y Post-Prueba para KPI4.

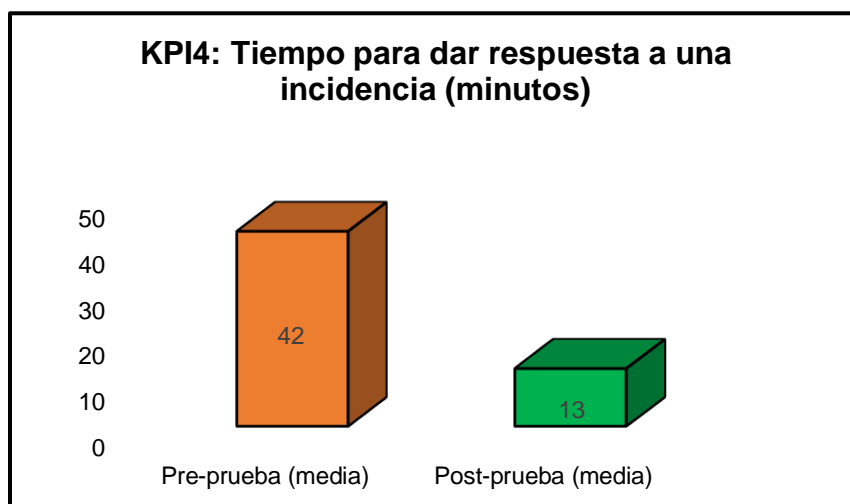


Figura 15. Media de resultados de Pre-Prueba y Post-Prueba para KPI4.

Interpretación:

El tiempo medio – en minutos - para dar respuesta a una incidencia antes de la aplicación de las medidas de acuerdo a la norma ISO 27001 y a los controles de la ISO 27002, era de 42 minutos, y debido a la aplicación de las medidas adoptadas, el tiempo para dar respuesta bajó a 13 minutos, lo cual corresponde a un decremento del 31% del tiempo de respuesta.

E. Indicador 5: Nivel de satisfacción del cliente (KPI 5)

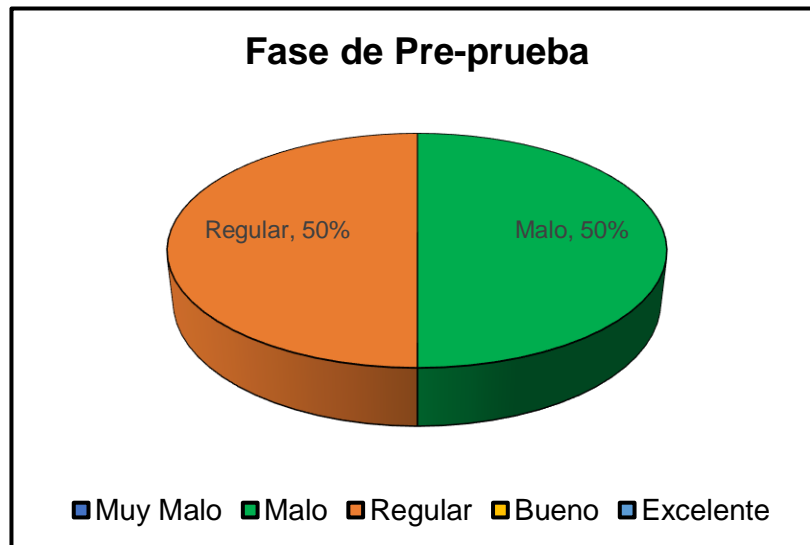


Figura 16. Gráfico de resultados de Pre-prueba para KPI5.

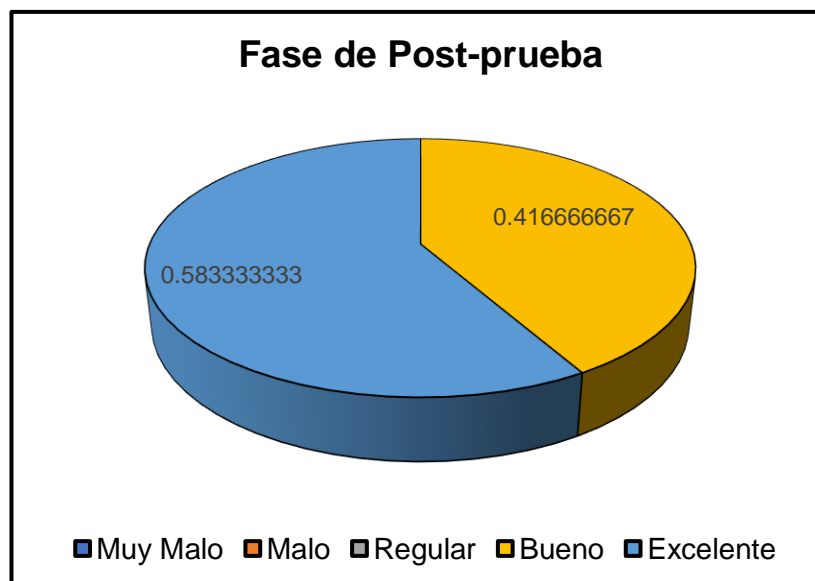


Figura 17. Gráfico de resultados de Post-prueba para KPI5.

Interpretación:

En la figura 17 vemos como el nivel de satisfacción de los clientes antes de la implementación de las normas y controles era del 50 % para malo y 50% para regular, no habiendo los tipos de satisfacción bueno y excelente. A consecuencia de la implementación de las normas y controles, el nivel de

satisfacción de los clientes cambió al 58 % para excelente y 42% para Bueno. Podemos deducir que como consecuencia de las acciones realizadas ha habido un cambio significativo en la satisfacción del cliente y por ende en el nivel cambio de perspectiva con respecto al aseguramiento de los datos.

5.1.4 Cuadro de Implementación final de la ISO 27001 y 27002.

Ver Anexo 04

5.1.5 Gráfico del estado de implementación final de la ISO 27001.

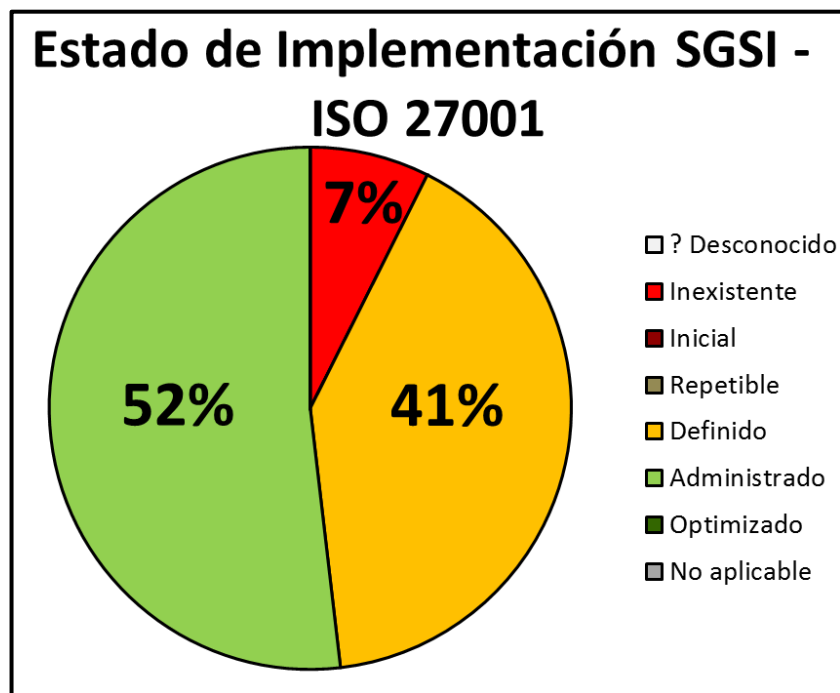


Figura 18. Estado de implementación del SGSI en la SECEJE PNP – Jul 2021.

Interpretación:

Como podemos apreciar en la figura 18, al final de la implementación de la norma ISO 27001, el estado Inexistente ha bajado a 7%, mientras que, los estados Definido y Administrado han aumentado en 41% y 52% respectivamente. Lo que demuestra que ahora existe la documentación necesaria para cumplir con el aseguramiento de los datos en la institución.

5.1.6 Gráfico del estado de implementación final de los controles de la ISO 27002.

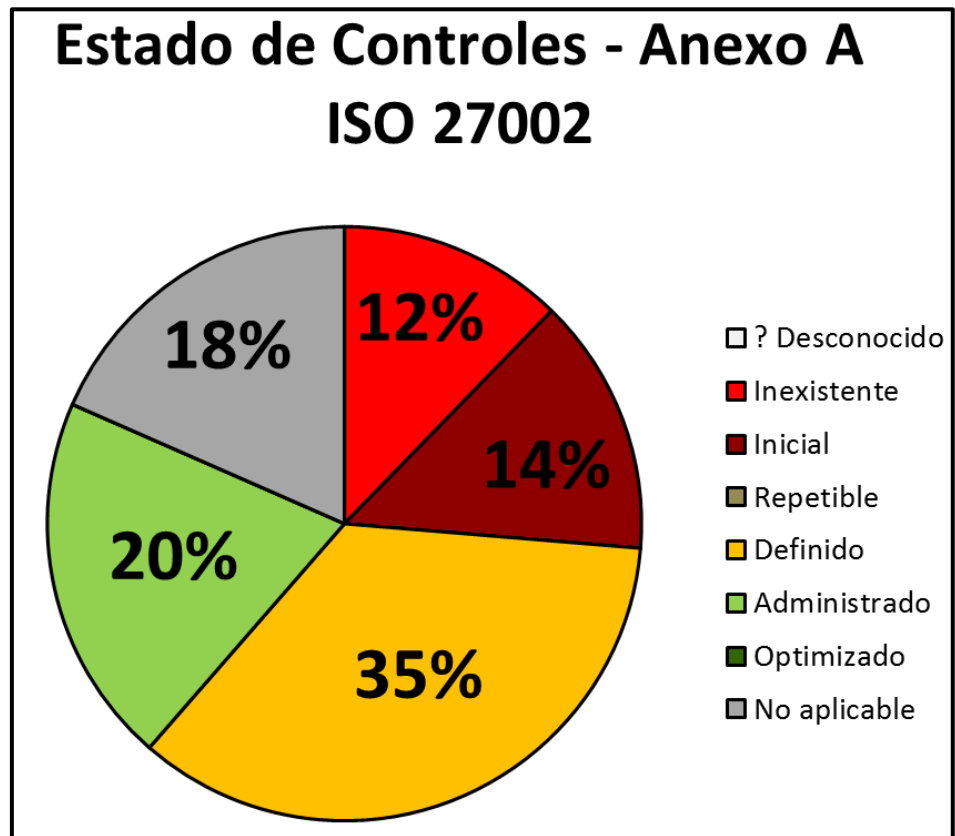


Figura 19. Estado de implementación de controles en la SECEJE PNP – Jul 2021.

Interpretación:

Como podemos apreciar en la figura 19, al final de la implementación de la norma ISO 27002 y sus controles, el estado Inexistente ha bajado a 12%, mientras que, los estados Inicial, Definido y Administrado han variado sus valores respecto a la fase inicial, siendo ahora de 14%, 35% y 20% respectivamente. Lo que demuestra que ahora existen los controles necesarios para cumplir con el aseguramiento de los datos en la institución.

5.2. **Nivel de confianza y grado de significancia**

Con el fin de verificar la hipótesis planteada, se utilizó el test de Shapiro-Wilk, cuya utilización es para las pruebas de contraste de bondad para

muestras iguales o inferiores a 50 y determinar de esta forma si la distribución es normal.

Figura 20. Fórmula del test de Shapiro-Wilk

$$W = \frac{\left(\sum_{i=1}^n a_i x_{(i)} \right)^2}{\sum_{i=1}^n (x_i - \bar{x})^2}$$

donde:

- $x_{(i)}$ (con el subíndice i entre paréntesis) es el número que ocupa la i -ésima posición en la muestra.
- es $\bar{x} = \frac{x_1 + \dots + x_n}{n}$ la media muestral;
- Las variables $a_{(i)}$ se calculan

$$(a_1, \dots, a_n) = \frac{m^\top V^{-1}}{(m^\top V^{-1} V^{-1} m)^{1/2}}$$

donde

$$m = (m_1, \dots, m_n)^\top$$

El nivel de confianza a utilizar será 95%, mientras que el grado de significancia aplicada será 5% ó 0.05.

5.3. Contrastación de hipótesis

A. Contrastación para el indicador 1: Tiempo para reportar una incidencia de seguridad de información.

Prueba de normalidad

Con el fin de verificar la hipótesis planteada, se utilizó el test de Shapiro-Wilk, que se usa para diferenciar la normalidad de un grupo de datos, en este caso si el tiempo para reportar una incidencia de seguridad de información contaban con una repartición normal, tanto para la pre-prueba como para el post-prueba, debido a la muestra de doce personas.

Ho = Los datos tienen un comportamiento normal. $\geq P = 0.05$

Ha = Los datos no tienen un comportamiento normal. $< P = 0.05$

Tabla 6. Prueba de normalidad del indicador 1

	Prueba	Shapiro-Wilk		
		Estadístico	gl	Sig.
Pre-prueba	Tiempo para reportar una incidencia de seguridad de la información	,902	12	,169
Post-prueba		,892	12	,126

Como se aprecia en la tabla, el resultado de Sig. en la Pre-prueba fue de ,169 y ,126 en la Post-prueba, resultados mayores a 0.05, por lo que, se rechaza la hipótesis nula. En este sentido, se puede decir que la información se distribuye normalmente en las dos pruebas.

Hipótesis alterna

Implementar las ISO 27001 y 27002 adaptadas para el aseguramiento de los datos en la Secretaría Ejecutiva de la Policía Nacional del Perú tiene un efecto positivo en la confidencialidad de la información en la Secretaría Ejecutiva de la Policía Nacional del Perú.

Hipótesis nula

Implementar las ISO 27001 y 27002 adaptadas para el aseguramiento de los datos en la Secretaría Ejecutiva de la Policía Nacional del Perú no tiene un efecto positivo en la confidencialidad de la información en la Secretaría Ejecutiva de la Policía Nacional del Perú.

B. Contrastación para el indicador 2: Porcentaje de disponibilidad de la información dentro de la institución.

Prueba de normalidad

Con el fin de verificar la hipótesis planteada, se utilizó el test de Shapiro-Wilk, que se usa para diferenciar la normalidad de un grupo de datos, en este caso si el porcentaje de disponibilidad de la información dentro de la institución contaban una repartición normal, tanto para la pre-prueba como para el post-prueba, debido a la muestra de doce personas.

Ho = Los datos tienen un comportamiento normal. $\geq P = 0.05$

Ha = Los datos no tienen un comportamiento normal. $< P = 0.05$

Tabla 7. Prueba de normalidad del indicador 2

	Prueba	Shapiro-Wilk		
		Estadístico	gl	Sig.
Pre-prueba	Porcentaje de disponibilidad de información	,924	12	,323
Post-prueba		,886	12	,104

Como se muestra en la tabla, el resultado de Sig. en la Pre-prueba fue de ,323 y ,104 en la Post-prueba, resultados mayores a 0.05, por lo que, se rechaza la hipótesis nula. En este sentido, se puede decir que la información se distribuye normalmente en las dos pruebas.

Hipótesis alterna

Implementar las ISO 27001 y 27002 adaptadas para el aseguramiento de los datos en la Secretaría Ejecutiva de la Policía Nacional del Perú tiene un efecto positivo en la disponibilidad de la información en la Secretaría Ejecutiva de la Policía Nacional del Perú.

Hipótesis nula

Implementar las ISO 27001 y 27002 adaptadas para el aseguramiento de los datos en la Secretaría Ejecutiva de la Policía Nacional del Perú no tiene un efecto positivo en la disponibilidad de la información en la Secretaría Ejecutiva de la Policía Nacional del Perú.

C. Contrastación para el indicador 3: Porcentaje de integridad de la información dentro de la institución.

Prueba de normalidad

Con el fin de verificar la hipótesis planteada, se utilizó el test de Shapiro-Wilk, que se usa para diferenciar la normalidad de un grupo de datos, en este caso si el porcentaje de integridad de la información dentro de la institución contaban una repartición normal, tanto para la pre-prueba como para el post-prueba, debido a la muestra de doce personas.

Ho = Los datos tienen un comportamiento normal. $\geq P = 0.05$

Ha = Los datos no tienen un comportamiento normal. $< P = 0.05$

Tabla 8. Prueba de normalidad del indicador 3

Prueba	Porcentaje de integridad de información	Shapiro-Wilk		
		Estadístico	gl	Sig.
Pre-prueba		,889	12	,114
Post-prueba		,831	12	,021

Como se muestra en la tabla, el resultado de Sig. en la Pre-prueba fue de ,114 (resultado mayor a 0.05) y ,021 en la Post-prueba (resultado menor a 0.05), por lo que, se rechaza la hipótesis nula en el pre-prueba pero en el post-prueba no se puede rechazar la hipótesis nula. En este sentido, se confirma que no ha habido una distribución normal en la post-prueba, por lo tanto, se procede a usar w-Wilcoxon.

Hipótesis alterna

Implementar las ISO 27001 y 27002 adaptadas para el aseguramiento de los datos en la Secretaría Ejecutiva de la Policía Nacional del Perú tiene un efecto positivo en la integridad de la información en la Secretaría Ejecutiva de la Policía Nacional del Perú.

Hipótesis nula

Implementar las ISO 27001 y 27002 adaptadas para el aseguramiento de los datos en la Secretaría Ejecutiva de la Policía Nacional del Perú no tiene un efecto positivo en la integridad de la información en la Secretaría Ejecutiva de la Policía Nacional del Perú.

Tabla 9. Prueba de Wilcoxon al Indicador 3

	Porcentaje_de_integridad _de_información_posttest- Porcentaje_de_integridad _de_información_pretest
Z	-3,062
Sig. Asintót.	,002

La prueba w de Wilcoxon, se aplicó debido a que los datos no se distribuyen normalmente; los resultados de esta prueba tienden a cero en relación de la probabilidad asumida de 0.05, por lo que se rechaza la hipótesis nula, ya que el porcentaje de integridad de información aumenta después de haberse implementado las normas ISO 27001 e ISO 27002 y sus controles.

D. Contrastación para el indicador 4: Tiempo de respuesta a una incidencia.

Prueba de normalidad

Con el fin de verificar la hipótesis planteada, se utilizó el test de Shapiro-Wilk, que se usa para diferenciar la normalidad de un grupo de datos, en este caso si el tiempo de respuesta a una incidencia una repartición normal, tanto para la pre-prueba como para el post-prueba, debido a la muestra de doce personas.

Ho = Los datos tienen un comportamiento normal. $\geq P = 0.05$

Ha = Los datos no tienen un comportamiento normal. $< P = 0.05$

Tabla 10. Prueba de normalidad del indicador 4

Prueba	Estadístico	Shapiro-Wilk	
		gl	Sig.
Pre-prueba	,903	12	,172
Post-prueba	,650	12	,000

Como se muestra en la tabla, el resultado de Sig. en la Pre-prueba fue de ,172 (resultado mayor a 0.05) y ,000 en la Post-prueba (resultado menor a 0.05), por lo que, se rechaza la hipótesis nula en el pre-prueba pero en el post-prueba no se puede rechazar la hipótesis nula. En este sentido, se confirma que no ha habido una distribución normal en la post-prueba, por lo tanto, se procede a usar w-Wilcoxon.

Hipótesis alterna

Implementar las ISO 27001 y 27002 adaptadas para el aseguramiento de los datos en la Secretaría Ejecutiva de la Policía Nacional del Perú tiene un efecto positivo en la disponibilidad de la información en la Secretaría Ejecutiva de la Policía Nacional del Perú.

Hipótesis nula

Implementar las ISO 27001 y 27002 adaptadas para el aseguramiento de los datos en la Secretaría Ejecutiva de la Policía Nacional del Perú no tiene un efecto positivo en la disponibilidad de la información en la Secretaría Ejecutiva de la Policía Nacional del Perú.

Tabla 11. Prueba de Wilcoxon al Indicador 4

	Tiempo_para_dar_respue sta_posttest - Tiempo_para_dar_respue sta_pretest
Z	-3,072
Sig. Asintót. (bilateral)	,002

La prueba w de Wilcoxon, se aplicó debido a que los datos no se distribuyen normalmente; los resultados de esta prueba tienden a cero en relación de la probabilidad asumida de 0.05, por lo que se rechaza la hipótesis nula, ya que el tiempo para dar respuesta se reduce después de haberse implementado las normas ISO 27001 e ISO 27002 y sus controles.

VI. DISCUSIÓN

6.1. Discusión.

El implementar la norma NTP/ISO-IEC 27001 en una organización conlleva a realizar grandes esfuerzos en la auditoría de todos los procesos que se manejan en la institución, para esto, se deben aplicar los controles de la ISO 27002. La realización de estos mecanismos contribuye al crecimiento de la institución y de su entorno. Sin embargo, analizando la realidad peruana, actualmente existen muy pocos profesionales que se dediquen al aseguramiento de los datos. Además, en el mercado hay muy pocas instituciones académicas que brinden carreras académicas, cursos de capacitación, cursos de especialización y diplomados en la rama de seguridad de información y/o auditoría de sistemas informáticos.

Por lo tanto, si en una institución u organización no existen profesionales en la línea de seguridad de información, los empleados de dicha organización no van a estar capacitados en delitos informáticos ni en los riesgos que se podrían generar por la falta de conocimiento en aspectos de protección de datos e información.

VII. CONCLUSIONES

7.1. Conclusiones.

- a) Antes de aplicar la norma ISO 27001 y los controles de la ISO 27002 (fase inicial) se verificaba que, para reportar un incidente de seguridad, el usuario afectado debía reportarlo a su jefe inmediato y luego éste lo reportaba al personal de sistemas; lo que aumentaba el tiempo ante una respuesta, el tiempo promedio de para reportar la incidencia era de 37 minutos, luego de la implementación el tiempo promedio fue de 10 minutos, en este caso el tiempo de respuesta se redujo en un 27%.
- b) El porcentaje de disponibilidad de la información en la Unidad de Gestión de los Sistemas Administrativos donde se hizo el estudio aumentó a un 95% en contraste con el 39% de disponibilidad inicial.
- c) El porcentaje de confidencialidad de la información en la Unidad de Gestión de los Sistemas Administrativos se ha modificado de un 48% a un 94% debido a las medidas utilizadas como: lista de registros, firma digital, acuerdo de concientización y confidencialidad de información.
- d) Antes de implementar la norma ISO 27001 y los controles de la ISO 27002, el tiempo promedio de respuesta ante un incidente de seguridad era de 42 minutos, sin embargo, con todos los mecanismos adoptados, el tiempo de respuesta pasó a ser de 13 minutos.
- e) De acuerdo a las encuestas realizadas, se puede verificar que el nivel de satisfacción del usuario aumentó luego de implementar la norma ISO 27001 y los controles de la ISO 27002 con respecto al grupo de control.

VIII. RECOMENDACIONES

8.1. Recomendaciones.

- a) Se recomienda que en las próximas investigaciones se tome en cuenta la seguridad física de las instalaciones, debido a que por problemas de coordinación con las unidades encargadas no se pudieron realizar dichas mejoras, lo que hubiera contribuido a tener ambientes más seguros.
- b) Se aconseja que la Unidad Policial organice y/o coordine cursos o talleres para capacitar al personal sobre el aseguramiento de los datos y los riesgos que puede conllevar la mala utilización de los dispositivos de almacenamiento.
- c) Se aconseja que el Comando Policial ponga más énfasis en la implementación de la norma 27001 en todas las unidades policiales a nivel nacional.
- d) Se recomienda realizar seguimientos periódicos a los mecanismos de seguridad implementados, así como, mantenerse al tanto de los cambios y actualizaciones en cuanto a las normas técnicas y estándares en el aseguramiento de los datos.
- e) Se deben realizar encuestas periódicas sobre la satisfacción de los usuarios, además de realizar pruebas a los usuarios para ver los puntos débiles que puedan originar riesgos en el aseguramiento de los datos.

REFERENCIAS

Ander - Egg, Ezequiel. 2011. *Aprender a investigar*. Córdoba : Brujas, 2011. ISBN 978-987-591-271-7.

Areitio, Javier. 2008. *Seguridad de la Información*. s.l. : Universidad de Deusto, 2008.

Arias, Fidas. 2012. *El proyecto de investigación: Introducción a la metodología científica*. Caracas : EPISTEME, 2012. ISBN: 980-07-8529-9.

Bernal Torres, César Augusto. 2010. *Metodología de la investigación*. Bogotá D.C. : Prentice Hall, 2010. ISBN E-BOOK 978-958-699-129-2.

Bobenrieth, Manuel. 2012. *Cómo investigar con éxito en ciencias de la salud*. Andalucía : s.n., 2012. ISBN 978-84-616-0995-6.

Bono, Roser. sf. *Diseños cuasi-experimentales y longitudinales*. Barcelona : Universidad de Barcelona, sf.

Carvajal, D. L., Cardona, A. y Valencia, F. J. 2019. Una propuesta de gestión de la seguridad de la información aplicado a una entidad pública colombiana. *Entre Ciencia e Ingeniería*. Manizales : s.n., 2019.

Chiavenato, Idalberto. 2007. *Introducción a la teoría general de la administración*. s.l. : McGraw-Hill Interamericana, 2007. ISBN 13: 978-970-10-5500-7.

Congreso de la República del Perú. 2002. *Ley 27658 - Ley Marco de Modernización de la Gestión del Estado*. Lima : El Peruano, 2002.

Congreso de la República del Perú. 2013. *Ley N° 30096 - Ley de Delitos Informáticos*. Lima : Editora Perú, 2013.

Enciclopedia Económica. 2018. Enciclopedia Económica. [En línea] 2018. [Citado el: 02 de 12 de 2020.] <https://enciclopediaeconomica.com/poblacion-estadistica/>.

Frias-Navarro, D. 2020. Apuntes de consistencia interna de las puntuaciones de un instrumento de medida. [En línea] 2020. [Citado el: 05 de 12 de 2020.] <https://www.uv.es/friasnav/AlfaCronbach.pdf>.

García Marco, Francisco Javier. 2011. *El concepto de información: Una aproximación transdisciplinar*. Madrid : Universidad de Zaragoza, 2011.

INSPQ. 2020. Institut national de santé publique du Québec. [En línea] 03 de 10 de 2020. [Citado el: 03 de 10 de 2020.] <https://www.inspq.qc.ca/es/centro-collaborador-oms-de-quebec-para-la-promocion-de-la-seguridad-y-prevencion-de-traumatismos/definicion-del-concepto-de-seguridad>.

ISO/IEC 27001 Information Systems Security Management Standard: Exploring the Reasons for Low Adoption. Fomin, Vladislav V., de Vries, Henk J. y Barlette, Yves. 2015. Rotterdam : s.n., 2015.

ISOTools Ecellence. 2015. SGSI Blog especializado en Sistemas de Gestión de Seguridad de la Información. [En línea] 28 de Julio de 2015. [Citado el: 03 de Octubre de 2020.] <https://www.pmg-ssi.com/2015/07/que-es-sgsi/>.

MINTIC. 2016. Seguridad y privacidad de la información. *Guía para Gestión y Clasificación de Incidentes de Seguridad de la Información*. 2016.

NQA. *ISO 27001:2013 Guía de implantación para la seguridad de la información.*

Organización Internacional de Normalización. 2013. *ISO 27001.* 2013.

Ortiz Morales, Einstein Arnold. 2018. *Controles de Seguridad según la Norma ISO/IEC 27002:2013 para el Mejoramiento de la Gestión de Seguridad de la Información.* Tingo María : s.n., 2018.

Policía Nacional del Perú. 2016. *Decreto Legislativo N° 1267 "Ley de la Policía Nacional del Perú".* Lima : El Peruano, 2016.

Real Academia Española. 2020. Real Academia Española. [En línea] 03 de Octubre de 2020. [Citado el: 03 de Octubre de 2020.] <https://dle.rae.es/gestionar>.

Salsavilca Ramos, Juan Carlos. 2017. *Implementación de la norma ISO 27001 en la Gestión de la Seguridad de la Información en la empresa Atento del Perú 2017.* Lima : s.n., 2017.

Sarmiento Astudillo, Gustavo Felipe y Gonzales Aybar, Richard Geampierre. 2019. *Implementación de la NTP/ISO 27001 para mejorar el proceso de seguridad de informaión en el departamento telemática de la oficina de economía del Ejército del Perú.* Lima : s.n., 2019.

UNIR. 2020. UNIR La Universidad en Internet. [En línea] 2020. [Citado el: 03 de 10 de 2020.] <https://www.unir.net/ingenieria/revista/iso-27001/#:~:text=La%20ISO%2027001%20es%20una,y%20aplicaciones%20que%20la%20tratan..>

Universidad César Vallejo. 2018. *Resolución de Consejo Universitario N° 0200-2018/UCV*. Trujillo : s.n., 2018.

WebFinance Inc. 2020. Business Dictionary. [En línea] 03 de 10 de 2020. [Citado el: 03 de 10 de 2020.]
<http://www.businessdictionary.com/es/definicion/gestion.html>.

ANEXOS

Anexo 03: Cuadro Fase Inicial a la Implementación de ISO 27001 y 27002.

Estado	Significado	Proporción de requerimientos SGSI	Proporción de Controles de Seguridad de la Información
? Desconocido	No ha sido verificado	0%	0%
Inexistente	No se lleva a cabo el control de seguridad en los sistemas de información.	100%	78%
Inicial	Las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de la buena suerte y de tener personal de la alta calidad.	0%	2%
Repetible	La medida de seguridad se realiza de un modo totalmente informal (con procedimientos propios, informales). La responsabilidad es individual. No hay formación.	0%	0%
Definido	El control se aplica conforme a un procedimiento documentado, pero no ha sido aprobado ni por el Responsable de Seguridad ni el Comité de Dirección.	0%	3%
Administrado	El control se lleva a cabo de acuerdo a un procedimiento documentado, aprobado y formalizado.	0%	0%
Optimizado	El control se aplica de acuerdo a un procedimiento documentado, aprobado y formalizado, y su eficacia se mide periódicamente mediante indicadores.	0%	0%
No aplicable	A fin de certificar un SGSI ,todos los requerimientos principales de ISO/IEC 27001 son obligatorios. De otro modo, pueden ser ignorados por la Administración.	0%	18%

Anexo 04: Cuadro Fase Final a la Implementación de ISO 27001 y 27002.

Estado	Significado	Proporción de requerimientos SGSI	Proporción de Controles de Seguridad de la Información
? Desconocido	No ha sido verificado	0%	0%
Inexistente	No se lleva a cabo el control de seguridad en los sistemas de información.	7%	12%
Inicial	Las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de la buena suerte y de tener personal de la alta calidad.	0%	14%
Repetible	La medida de seguridad se realiza de un modo totalmente informal (con procedimientos propios, informales). La responsabilidad es individual. No hay formación.	0%	0%
Definido	El control se aplica conforme a un procedimiento documentado, pero no ha sido aprobado ni por el Responsable de Seguridad ni el Comité de Dirección.	41%	35%
Administrado	El control se lleva a cabo de acuerdo a un procedimiento documentado, aprobado y formalizado.	52%	20%
Optimizado	El control se aplica de acuerdo a un procedimiento documentado, aprobado y formalizado, y su eficacia se mide periódicamente mediante indicadores.	0%	0%
No aplicable	A fin de certificar un SGSI ,todos los requerimientos principales de ISO/IEC 27001 son obligatorios. De otro modo, pueden ser ignorados por la Administración.	0%	18%

Anexo 05: Matriz de operacionalización de variables.

Variables	Definición Conceptual	Definición Operacional	Dimensiones	Indicadores	Escalas de Medición
Variable Independiente: ISO 27001 y 27002	Define de manera genérica, independientemente de los factores ambientales de la empresa (entorno, contexto, activos de las TIC, información, cultura organizacional, entre otros) y de los activos de los procesos de la organización (políticas, procedimientos, procesos, entre otros), cómo se planifica, implanta, verifica y registra un Sistema para gestionar el aseguramiento de la data, partiendo de un estudio de riesgos y de la proyección e implantación de la respuesta a los mismos para su mitigación. (UNIR, 2020)	La escala de medición es la integridad, confidencialidad y disponibilidad de la información, para lo cual se aplican valores a cada una de estas escalas.	Legal	Nivel de conformidad de requisitos legales	Razón
			Estratégica	Nivel de conformidad de políticas estratégicas	
			Técnica	Nivel de implementación técnica	
Variable Dependiente: Seguridad de Información	Es la extensa cantidad de elementos de tipo tecnológicos, de recursos humanos, del tipo económico, negocios, legal, de cumplimiento, la misma que discurre no sólo aspectos informáticos y de telecomunicaciones sino también aspectos físicos, medioambientales. (Azeiteiro, 2008)	Observa métodos apropiados para ejecución de controles en la cual se pretende conservar una muestra mucho menor a los entregados por el nivel gerencial.	Confidencialidad	Tiempo para reportar una incidencia de seguridad de información	Razón
Integridad			Porcentaje de integridad de la información dentro de la institución		
Disponibilidad			Tiempo para reportar una incidencia de seguridad de información		
			Porcentaje de disponibilidad de la información dentro de la institución Tiempo de respuesta a una incidencia		

Fuente: Elaboración propia

Anexo 06: Matriz de consistencia.

MATRIZ DE CONSISTENCIA

“Implementación de ISO 27001 y 27002 adaptadas para Gestión de Seguridad de Información en la Secretaría Ejecutiva de la Policía Nacional del Perú”

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES	INDICADORES	TÉCNICAS	INSTRUMENTO	METODOLOGÍA
<p>Problema principal</p> <p>¿De qué manera el implementar las ISO 27001 y 27002 adaptadas para la seguridad de la información en la Secretaría Ejecutiva de la PNP tiene efecto en la seguridad de la información en la Unidad Policial?</p> <p>Problemas específicos</p> <ul style="list-style-type: none"> PE1: ¿De qué manera el implementar las ISO 27001 y 27002 adaptadas para la seguridad de la información en la Secretaría Ejecutiva de la PNP tiene efecto en la confidencialidad de la información en la 	<p>Objetivo Principal</p> <p>Determinar el efecto de implementar las ISO 27001 y 27002 adaptadas para la seguridad de la información en la Secretaría Ejecutiva de la Policía Nacional del Perú.</p> <p>Objetivos específicos</p> <ul style="list-style-type: none"> OE1: Determinar el efecto en la confidencialidad, integridad y disponibilidad de la información al implementar las ISO 27001 y 27002 adaptadas para la seguridad de la información en la Secretaría Ejecutiva de la Policía Nacional del Perú. 	<p>Hipótesis principal</p> <p>Implementar la norma ISO 27001:2013 adaptada para la seguridad de la información en la Secretaría Ejecutiva de la Policía Nacional del Perú tiene un efecto positivo en seguridad de la información que se maneja en la Unidad Policial.</p> <p>Hipótesis específicas</p> <ul style="list-style-type: none"> HE1: Implementar las ISO 27001 y 27002 adaptadas para la seguridad de la información en la Secretaría Ejecutiva de la Policía Nacional del Perú tiene un efecto positivo en 	<p>Variable independiente</p> <p>ISO 27001</p>	<p>Nivel de conformidad de requisitos legales.</p>	<p>Entrevista</p> <p>Observación</p>	<p>Guía de entrevista</p> <p>Lista de chequeo</p>	<ol style="list-style-type: none"> Tipo de investigación Aplicada. Diseño Cuasiexperimental. Población 24 trabajadores (2 grupos de 12 trabajadores). Muestra No probabilística. Técnicas de recolección de datos <ul style="list-style-type: none"> Observación. Encuesta. Instrumentos de recolección <ul style="list-style-type: none"> Lista de chequeo. Guía de entrevista. Ficha de encuesta.
				<p>Nivel de conformidad de políticas estratégicas</p>	<p>Entrevista</p> <p>Observación</p>	<p>Guía de entrevista</p> <p>Lista de chequeo</p>	
				<p>Nivel de implementación técnica</p>	<p>Entrevista</p> <p>Observación</p>	<p>Guía de entrevista</p> <p>Lista de chequeo</p>	

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES	INDICADORES	TÉCNICAS	INSTRUMENTO	METODOLOGÍA
<p>Secretaría Ejecutiva de la Policía Nacional del Perú?</p> <p>• PE2: ¿De qué manera el implementar las ISO 27001 y 27002 adaptadas para la seguridad de la información en la Secretaría Ejecutiva de la PNP tiene efecto en la integridad de la información en la Secretaría Ejecutiva de la Policía Nacional del Perú?</p> <p>• PE3: ¿De qué manera el implementar las ISO 27001 y 27002 adaptadas para la seguridad de la información en la Secretaría Ejecutiva de la PNP tiene efecto en la disponibilidad de la información en la Secretaría Ejecutiva de la Policía Nacional del Perú?</p>	<p>• OE2: Determinar el efecto en la integridad de la información al implementar las ISO 27001 y 27002 adaptadas para la seguridad de la información en la Secretaría Ejecutiva de la Policía Nacional del Perú.</p> <p>• OE3: Determinar el efecto en la disponibilidad de la información al implementar las ISO 27001 y 27002 adaptadas para la seguridad de la información en la Secretaría Ejecutiva de la Policía Nacional del Perú.</p>	<p>la confidencialidad de la información en la Secretaría Ejecutiva de la Policía Nacional del Perú.</p> <p>• HE2: Implementar las ISO 27001 y 27002 adaptadas para la seguridad de la información en la Secretaría Ejecutiva de la Policía Nacional del Perú.</p> <p>• HE3: Implementar las ISO 27001 y 27002 adaptadas para la seguridad de la información en la Secretaría Ejecutiva de la Policía Nacional del Perú.</p>	<p>Variable Dependiente Seguridad de Información</p>	<p>Nivel de información que puede ser divulgada sin autorización.</p>	<p>Encuesta</p> <p>Observación</p>	<p>Ficha de encuesta</p> <p>Lista de chequeo</p>	
				<p>Nivel de información que puede ser modificada sin autorización.</p>	<p>Encuesta</p> <p>Observación</p>	<p>Ficha de encuesta</p> <p>Lista de chequeo</p>	
				<p>Nivel de información que es inaccesible frecuentemente.</p>	<p>Encuesta</p> <p>Observación</p>	<p>Ficha de encuesta</p> <p>Lista de chequeo</p>	

Fuente: Elaboración propia.

Anexo 07. Validación de Instrumento Seguridad de Información: Experto 01



SEGURIDAD DE INFORMACIÓN

I. DATOS GENERALES:

Apellidos y nombres: Mg. Guillermo Miguel Johnson Romero

Institución donde labora: Docente de Universidad César Vallejo

Nombre del motivo de evaluación: Ficha de Observación sobre Seguridad de Información en Secretaría Ejecutiva de la Policía Nacional del Perú.

Título de la investigación: Implementación de ISO 27001 y 27002 adaptadas para Gestión de Seguridad de Información en Secretaría Ejecutiva de Policía Nacional del Perú.

Autor: Sleem Néstor Francisco Chávarry Bonilla.

II. ASPECTOS DE LA VALIDACIÓN

INDICADORES	CRITERIOS	Deficiente 0-20%	Regular 21-50%	Buena 51-70%	Muy Buena 71-80%	Excelente 81-100%
CLARIDAD	Está formado con el lenguaje apropiado					84
OBJETIVIDAD	Está expresado en conducta observable.					89
ORGANIZACIÓN	Es adecuado el avance de la ciencia y tecnología.					88
CAPACIDAD	Comprende los aspectos de cantidad y calidad.					87
INTENCIONALIDAD	Adecuado para valorar aspectos del sistema metodológico y científico.					89
CONSISTENCIA	Está basado en aspectos técnicos, científicos, acordes a la tecnología adecuada.					90
COHERENCIA	Entre los índices, indicadores y dimensiones.					95
METODOLOGÍA	Responde el propósito del trabajo bajo los objetivos a lograr.					99
PERTINENCIA	El instrumento es adecuado al tipo de investigación.					97

PROMEDIO DE VALORACIÓN: 90.8

ORDEN DE APLICABILIDAD:

- El instrumento puede ser aplicado, tal como está elaborado.
 El instrumento debe ser mejorado, antes de ser aplicado.

Lima, junio del 2021.



Mg. Guillermo Miguel Johnson Romero
CIP 113066

Anexo 08. Validación de Instrumento: Entrevista Seguridad de Información: Experto 01



ENTREVISTA SEGURIDAD DE INFORMACIÓN

I. DATOS GENERALES:

Apellidos y nombres: Mg. Guillermo Miguel Johnson Romero

Institución donde labora: Docente de Universidad César Vallejo

Nombre del motivo de evaluación: Entrevista sobre Seguridad de Información - ISO 27001 en la Secretaría Ejecutiva de la Policía Nacional del Perú.

Título de la investigación: Implementación de ISO 27001 y 27002 adaptadas para Gestión de Seguridad de Información en Secretaría Ejecutiva de Policía Nacional del Perú.

Autor: Sleem Néstor Francisco Chávarry Bonilla.

II. ASPECTOS DE LA VALIDACIÓN

INDICADORES	CRITERIOS	Deficiente 0-20%	Regular 21-50%	Buena 51-70%	Muy Buena 71-80%	Excelente 81-100%
CLARIDAD	Está formado con el lenguaje apropiado					87
OBJETIVIDAD	Está expresado en conducta observable.					90
ORGANIZACIÓN	Es adecuado el avance de la ciencia y tecnología.					97
CAPACIDAD	Comprende los aspectos de cantidad y calidad.					94
INTENCIONALIDAD	Adecuado para valorar aspectos del sistema metodológico y científico.					98
CONSISTENCIA	Está basado en aspectos técnicos, científicos, acordes a la tecnología adecuada.					94
COHERENCIA	Entre los índices, indicadores y dimensiones.					98
METODOLOGÍA	Responde el propósito del trabajo bajo los objetivos a lograr.					99
PERTINENCIA	El instrumento es adecuado al tipo de investigación.					98

PROMEDIO DE VALORACIÓN: 94.8

ORDEN DE APLICABILIDAD:

- El instrumento puede ser aplicado, tal como está elaborado.
 El instrumento debe ser mejorado, antes de ser aplicado.

Lima, junio del 2021.



Mg. Guillermo Miguel Johnson Romero
CIP 113066

Anexo 09. Encuesta para determinar la Gestión de la Seguridad de Información en la SECEJE PNP

Encuesta para determinar la Gestión de la Seguridad de Información en la SECEJE PNP - Variable ISO 27001:2013

*Obligatorio

¿Conoce las políticas de seguridad de información en la Secretaría Ejecutiva PNP? *

Sí

No

¿Se encuentra de acuerdo con las políticas para salvaguardar la información en la SECEJE PNP? *

Sí

No

¿Se encuentra de acuerdo con las medidas disciplinarias (sanciones) adoptadas para el personal que incumpla las medidas de seguridad de información? *

Sí

No

¿Cree Ud. que se debería tomar medidas legales más drásticas para el control de la información en la SECEJE PNP? *

Sí

No

¿Está Ud. de acuerdo con las estrategias adoptadas para el aseguramiento de la información en su Unidad Policial? *

Sí

No

¿Está Ud. de acuerdo con el intervalo en el que se imparten los conocimientos por el personal de la Oficina de Tecnologías de Información y Comunicaciones de la SECEJE PNP, en cuanto a factores de riesgo en el manejo de la información? *

Sí

No

¿Está Ud. de acuerdo con las estrategias adoptadas para el control del personal en las instalaciones de la SECEJE PNP? *

Sí

No

¿Se encuentra conforme con el tiempo de respuesta, por parte de la Oficina de Tecnologías de Información, ante algún incidente que suceda a los equipos informáticos asignados? *

Sí

No

¿Se encuentra conforme con la monitorización de los incidentes que se ocasionan en las oficinas de la SECEJE PNP? *

Sí

No

Encuesta para determinar la Gestión de la Seguridad de Información en la SECEJE PNP - Variable Seguridad de Información

¿Cree Ud. que la entidad tiene que adoptar mecanismos para permitir el acceso a la información solo para el personal autorizado en el manejo de la información? *

Sí

No

¿El antivirus de los equipos informáticos a su cargo se encuentran actualizados? *

Sí

No

¿Sólo Ud. tiene acceso al equipo informático a su cargo? *

Sí

No

¿Sabe Ud. si la entidad ha implementado lineamientos contra la modificación o pérdida accidental de información? *

Sí

No

¿Sabe Ud. si la entidad ha implementado lineamientos, normas y/o estándares para recuperar la información en caso de modificación, pérdida intencional o accidental de la información? *

Sí

No

¿Sabe Ud. si la entidad ha implementado mecanismos para que la información tenga la disponibilidad adecuada? *

Sí

No

Anexo 10. Formato de Entrevista sobre Seguridad de Información – ISO 27001 en la Secretaría Ejecutiva de la Policía Nacional del Perú



Entrevista sobre Seguridad de Información - ISO 27001 en la Secretaría Ejecutiva de la Policía Nacional del Perú

Apellidos y nombres:

Institución donde labora:

Área u oficina donde labora:

Cargo que desempeña:

Entrevistador: Sleem Néstor Francisco Chávarry Bonilla.

CONTEXTO DE LA ORGANIZACIÓN

1. Diga usted, ¿Se han determinado los objetivos del Sistema de Gestión de Seguridad de Información de la organización y cualquier problema que pueda afectar su eficiencia?
2. Diga usted, ¿Se han identificado las partes interesadas incluyendo leyes aplicables, regulaciones, contratos, entre otros?
3. Diga usted, ¿Se han determinado los requerimientos y obligaciones relevantes de seguridad de la información?
4. Diga usted, ¿Existe el documento sobre alcance del Sistema de Gestión de Sistemas de Información en la Secretaría Ejecutiva de la Policía Nacional del Perú?

11. Diga usted, ¿Se han establecido y documentado los planes y objetivos de la seguridad de la información en la Secretaría Ejecutiva de la Policía Nacional del Perú?

SOPORTE

12. Diga usted, ¿Se han determinado y asignado los recursos necesarios para el Sistema de Gestión de Sistemas de Información en la Secretaría Ejecutiva de la Policía Nacional del Perú?
13. Diga usted, ¿Se han determinado, documentado y hecho disponibles las competencias necesarias en el Sistema de Gestión de Sistemas de Información en la Secretaría Ejecutiva de la Policía Nacional del Perú?
14. Diga usted, ¿Se ha implementado un programa de concientización de seguridad en la Secretaría Ejecutiva de la Policía Nacional del Perú?
15. Diga usted, ¿Se han determinado las necesidades de comunicación internas y externas relacionadas al Sistema de Gestión de Sistemas de Información en la Secretaría Ejecutiva de la Policía Nacional del Perú?
16. Diga usted, ¿Se provee la documentación requerida por el estándar requerida por la Secretaría Ejecutiva de la Policía Nacional del Perú?

17. Diga usted, ¿Se provee un título, autor, formato consistente, revisión y aprobación a los documentos que elaboran en la Secretaría Ejecutiva de la Policía Nacional del Perú?

18. Diga usted, ¿Se mantiene un control adecuado de la documentación en la Secretaría Ejecutiva de la Policía Nacional del Perú?

OPERACIÓN

19. Diga usted, ¿Se planifica, implementa, controla y documenta el proceso de gestión de riesgos del Sistema de Gestión de Seguridad de la Información en la Secretaría Ejecutiva de la Policía Nacional del Perú?

20. Diga usted, ¿Se evalúan y documentan los riesgos de seguridad regularmente y cuando hay cambios?

21. Diga usted, ¿Se ha implementado un Plan de tratamiento de riesgos y se documentan los resultados?

EVALUACIÓN DE DESEMPEÑO

22. Diga usted, ¿Se realiza un seguimiento, medición, análisis y evaluación del Sistema de Gestión de Seguridad de Información y los controles de acuerdo a las ISO 27001:2013 y 27002:2014 en la Secretaría Ejecutiva de la Policía Nacional del Perú?

23. Diga usted, ¿Se han planificado y realizado auditorías internas del Sistema de Gestión de Seguridad de Información en la Secretaría Ejecutiva de la Policía Nacional del Perú?

24. Diga usted, ¿La Administración o área responsable realiza una revisión periódica del Sistema de Gestión de Seguridad de Información en la Secretaría Ejecutiva de la Policía Nacional del Perú?

MEJORA

25. Diga usted, ¿Se han identificado, arreglado y reaccionado ante no conformidades para evitar su recurrencia documentando todas las acciones?

26. Diga usted, ¿Existe un Plan de Mejora Continua del Sistema de Gestión de Seguridad de Información en la Secretaría Ejecutiva de la Policía Nacional del Perú?

Anexo 11: Coeficiente Alfa de Cronbach

Escala: Todas las variables

Resumen del procesamiento de los casos

	N	%
Casos Válidos	12	100,0
Excluidos ^a	0	,0
Total	12	100,0

a. Eliminación por lista basada en todas las variables del procedimiento.

Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
,819	15

Anexo 12: Carta de aceptación de la empresa



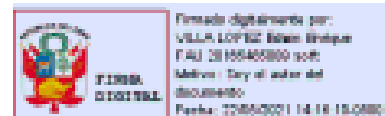
CONSTANCIA

La Secretaría Ejecutiva de la Policía Nacional del Perú, hace constar:

Que el señor, **BLEEM NÉSTOR FRANCISCO CHÁVARRY BONILLA** con DNI N° 43959898, estudiante de la **Escuela Profesional de Ingeniería de Sistemas** de la **Universidad César Vallejo**, se encuentra actualmente llevando a cabo de forma satisfactoria su Proyecto de Investigación **"Implementación de las ISO 27001 y 27002 adaptadas para Gestión de Seguridad de Información en la Secretaría Ejecutiva de la Policía Nacional del Perú"** en nuestra Institución.

Se expide el presente documento a solicitud del interesado para fines que crea conveniente

Lima, 21 de mayo del 2021.



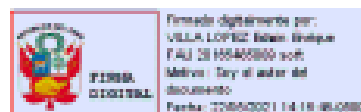
Anexo 13: Autorización para la realización y difusión de resultados de la investigación



AUTORIZACIÓN PARA LA REALIZACIÓN Y DIFUSIÓN DE RESULTADOS DE LA INVESTIGACIÓN

Por medio del presente documento, Yo Edwin Enrique VILLA LÓPEZ, identificado con DNI N° 20067448, Jefe de la Unidad de Gestión de los Sistemas Administrativos - Secretaría Ejecutiva de la Policía Nacional del Perú autorizo a Sleem Néstor Francisco Chávamy Bonilla identificado con DNI N° 43959898 a realizar la Investigación titulada: "Implementación de ISO 27001 y 27002 adaptadas para Gestión de Seguridad de Información en la Secretaría Ejecutiva de la Policía Nacional del Perú" y a difundir los resultados de la Investigación utilizando el nombre de Secretaría Ejecutiva de la Policía Nacional del Perú.

Lima, 21 de mayo del 2021.



Anexo 14: Políticas de Seguridad de Información de la Secretaría Ejecutiva de la Policía Nacional del Perú



POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA SECRETARÍA EJECUTIVA DE LA POLICÍA NACIONAL DEL PERÚ

Elaborado por: Área de Soporte de Sistemas


Versión 1.0

Noviembre 2020

	Título:	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA SECRETARÍA EJECUTIVA PNP	
	Elaborado por:	Área de Soporte de Sistemas	Versión 1.0


Historial de Versiones

VERSION	PARTES QUE CAMBIAN	DESCRIPCIÓN DEL CAMBIO	FECHA DE CAMBIO	MODIFICADO POR	APROBADO POR
1.0	-	Versión Inicial	-	S3 SPPP Sleem CHÁVARRI B.	GRAL. PNP Mario Fernando ARATA BUSTAMANTE

	Título:	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA SECRETARÍA EJECUTIVA PNP	
	Elaborado por:	Área de Soporte de Sistemas	Versión 1.0

Índice

1.- OBJETIVO	1
2.- ALCANCE	1
3.- BASE LEGAL	1
4.- PROPÓSITO	2
5.- AUTORIZACIÓN	3
6.- EDICIÓN Y DISTRIBUCIÓN	3
7.- REVISIONES Y MODIFICACIONES	3
8.- ORGANIGRAMA	3
9.- POLÍTICAS DE SEGURIDAD DE INFORMACIÓN	4
9.1 Adquisición y utilización de hardware	4
9.2 Utilización de Software	5
9.3 Seguridad del Área de Soporte de Sistemas	5
9.4 Adquisición de Software	5
9.5 Recursos informáticos	6
9.6 Clasificación, tratamiento y conservación de la información	6
9.7 Seguridad de recursos humanos	6
9.8 Respaldo y recuperación de la información	7
9.9 Asignación de usuario	7
9.10 Seguridad de información	8
9.11 Manejo de impresoras	9
9.12 Acceso a Internet	9
10.- PLAN DE CONTINGENCIA	10
11.- CONTINUIDAD DE LA SEGURIDAD DE INFORMACIÓN	10
12.- IMPREVISTO	10
13.- VIGENCIA	11
14.- APROBACIÓN	11

	Título:	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA SECRETARÍA EJECUTIVA PNP	
	Elaborado por:	Área de Soporte de Sistemas	Versión 1.0

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN EN LA SECRETARÍA EJECUTIVA DE LA POLICÍA NACIONAL DEL PERÚ

1.- OBJETIVO:

Los objetivos de las Políticas de Tecnologías de la Información de la Secretaría Ejecutiva de la Policía Nacional del Perú, son los siguientes:


- a) Crear y definir las políticas generales y específicas que faciliten la ejecución de las actividades de tecnología de la información en las diferentes oficinas de la Secretaría Ejecutiva de la Policía Nacional del Perú.
- b) Promover el uso adecuado de los recursos humanos, logísticos y activos tecnológicos adecuados.
- c) Normar los procesos de información con la finalidad de mejorar el rendimiento de las Oficinas y áreas de la Secretaría Ejecutiva de la Policía Nacional del Perú (Oficina de Administración, Unidad de Gestión de los Sistemas Administrativos, Unidad de Asesoría Técnica, Unidad de Trámite Documentario).
- d) Establecer las Políticas para resguardo y garantía de acceso apropiado de la información de la Secretaría Ejecutiva de la Policía Nacional del Perú.

2.- ALCANCE:

El presente documento es aplicable a las áreas y oficinas de la Secretaría Ejecutiva de la Policía Nacional del Perú, así como los funcionarios públicos, servidor civil de carrera y servidor de actividades complementarias, colaboradores, en adelante "Usuarios", que utilicen los activos de información administrados y/o propiedad de la Policía Nacional del Perú.

3.- BASE LEGAL:

- Constitución Política del Perú, de 28DIC1993.
- Ley N° 27858 de 17ENE2000, Ley Marco de Modernización de Gestión del Estado.
- Ley N° 27444 – Ley de Procedimiento Administrativo General.
- Ley N° 27806 de 02AGO2002, Ley de Transparencia y Acceso a la Información Pública.
- Ley N° 29733 de 21JUL2011, Ley de Protección de Datos Personales.
- Ley N° 30057 de 03JUL2013, Ley de Servicio Civil y sus reglamentos.
- Ley N° 30096 de 21OCT2013, Ley de Daños Informáticos y su modificatoria Ley 30171.
- Ley N° 30714 de 29DIC2017, Ley de Régimen Disciplinario de la Policía Nacional del Perú.
- Decreto Legislativo 635 de 03ABR1991, promulga el Código Penal.
- Decreto Legislativo 957 de 21JUL2004, promulga el Código Procesal Penal.
- Decreto Legislativo N° 1094 de 31AGO2010, promulga el Código Penal Militar Policial.
- Decreto Legislativo N° 1287 de 16DIC2018, Ley de la Policía Nacional del Perú y sus modificatorias.
- Decreto Legislativo N° 1412 de 12SET2018, aprueba la Ley de Gobierno Digital.

	Título:	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA SECRETARÍA EJECUTIVA PNP	
	Elaborado por:	Área de Soporte de Sistemas	Versión 1.0



- Decreto Legislativo N° 1451 de SET2018, que fortalece el funcionamiento de las entidades del Gobierno Nacional, del Gobierno Regional o del Gobierno Local, a través de precisiones de sus competencias, regulaciones y funciones.
- Decreto Supremo N° 030-2002-PCM de 02MAY2002, aprueba el Reglamento de la Ley N° 27858, Ley Marco de Modernización de Gestión del Estado.
- Decreto Supremo N° 062-2017-PCM de 13SET2017, aprueba la Política Nacional de Integridad y Lucha contra la Corrupción.
- Decreto Supremo N° 028-2017-IN de 13OCT2017, aprueba el Reglamento del Decreto Legislativo N° 1287, Ley de la Policía Nacional del Perú.
- Decreto Supremo N° 118-2018-PCM de 29NOV2018, declara de interés nacional el desarrollo del Gobierno Digital, la innovación y la economía digital con enfoque territorial.
- Decreto Supremo N° 119-2018-PCM de 29NOV2018, modifica la Quinta Disposición Complementaria Final del Decreto Supremo N° 033-2018-pcm.
- Decreto Supremo N° 033-2018-PCM de 22MAR2018, creación de la Plataforma Digital Única del Estado Peruano.
- Resolución Ministerial N° 119-2018-PCM de 08MAY2018, creación del Comité de Gobierno Digital en cada entidad de administración pública.
- Decreto Supremo N° 050-2018-PCM de 14MAY2018, establece la definición de Seguridad Digital de ámbito nacional.
- Resolución Ministerial N° 305-92-IN/PNP de 17MAR1992, aprueba el reglamento del Sistema Normativo de la Policía Nacional del Perú.
- Resolución Ministerial N° 004-2016-PCM de 08ENE2016: Aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnologías de la Información, Técnicas de Seguridad, Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª. Edición", en todas las entidades integrantes del Sistema Nacional de Informática.
- Resolución Ministerial N° 168-2017-PCM de 20JUN2017, que modifica el artículo 5 de la R.M. N° 004-2016-PCM referente al Comité de Gestión de Seguridad de la Información.
- Resolución de Comandancia General N° 161-2018-COMGEN/EMG-PNP del 24NOV2018, aprueba la Directiva N° 13-25-2018-COMGEN-PNP/SECEJE-DIRTIC-DIVINF-B Normas para el uso de equipos de cómputo, acceso a los servidores de red, internet e intranet en la Policía Nacional del Perú.
- Resolución N° 129-2014/CNB-INDECOP1 de 20NOV2014, aprueba la Norma Técnica Peruana "NTP ISO/IEC 27001:2014: Tecnología de la Información, Técnicas de Seguridad, Sistemas de Gestión de Seguridad de Información. Requisitos. 2ª. Edición".
- Políticas de Seguridad de Información de la Policía Nacional del Perú – DIRTIC 2019.

4.- PROPÓSITO:

Dejar establecidas políticas de Tecnologías de Información que regirán el uso y mantenimiento de la plataforma tecnológica de la Secretaría Ejecutiva de la Policía Nacional del Perú, para asegurar su operatividad, de manera que los responsables del uso

	Título:	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA SECRETARÍA EJECUTIVA PNP	
	Elaborado por:	Área de Soporte de Sistemas	Versión 1.0

de las tecnologías disponibles, aseguren el cumplimiento de las mismas, con miras al desarrollo de un trabajo óptimo y de calidad.

5.- AUTORIZACIÓN:

El Manual de Políticas de Tecnologías de Información de la Secretaría Ejecutiva de la Policía Nacional del Perú, es aprobado, previa revisión y verificación del Secretario Ejecutivo de la Policía Nacional del Perú.

6.- EDICIÓN Y DISTRIBUCIÓN:

La edición se realizará en formato digital, colocándolo en el aplicativo WhatsApp de la Secretaría Ejecutiva. La versión en físico será comunicada por las distintas oficinas, firmando el personal el padrón de enterado correspondiente. Posteriormente, la versión en físico será archivada en la Oficina de Administración de la Secretaría Ejecutiva de la Policía Nacional del Perú, a fin que permita realizar la sustitución de las páginas cuando ocurran revisiones y modificaciones.

Recibirán un ejemplar completo del Manual:


- El Jefe de Administración de la Secretaría Ejecutiva de la PNP.
- Archivo.

7.- REVISIONES Y MODIFICACIONES:

Cualquier cambio, corrección o recomendación se comunicará al Jefe de Administración de la Secretaría Ejecutiva PNP.

B.- ORGANIGRAMA:



	Título:	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA SECRETARÍA EJECUTIVA PNP	
	Elaborado por:	Área de Soporte de Sistemas	Versión 1.0

9.- POLÍTICAS DE SEGURIDAD DE INFORMACIÓN:

El área de soporte de sistemas se encargará de verificar el uso y funcionamiento de la plataforma tecnológica y asistir permanentemente a los usuarios de la Secretaría Ejecutiva PNP.

Las políticas de tecnologías de información serán aprobadas por Secretario Ejecutivo PNP y divulgadas respectivamente por el Jefe de Administración de la Unidad Policial.

El personal que labora en la Secretaría Ejecutiva PNP, deberá conocer los documentos de políticas relativas a tecnologías de información y actuar de acuerdo a los principios consignados en ellos. Asimismo, instruir a los trabajadores de la Secretaría Ejecutiva PNP, en cuanto a su obligación de conocer y aplicar la normativa vigente sobre seguridad, para lograr un cambio positivo en la cultura organizacional.

9.1 Adquisición y utilización de Hardware

Responsabilidad del área de soporte de sistemas

El área de soporte de sistemas tiene las siguientes responsabilidades ante la adquisición, instalación, mantenimiento y funcionamiento de los equipos y dispositivos dentro de la unidad policial:


- Participará para brindar asesoramiento en los contratos de bienes y/o servicios, donde se pretenda adquirir equipos informáticos.
- Comprobará que los equipos de informáticos cumplan con las especificaciones indicadas en las solicitudes de compra.
- Realizará el mantenimiento técnico preventivo de todos los equipos informáticos de la Secretaría Ejecutiva de la PNP.
- Evaluará que el área física donde se instalará el equipo informático cumpla con óptimas condiciones para su instalación.
- Instalará el software y hardware necesarios utilizados en la Secretaría Ejecutiva de la PNP.
- Enseñará al usuario sobre el adecuado uso y manejo de los equipos y programas informáticos instalados.

Responsabilidad de los usuarios

Los equipos informáticos asignados a los usuarios, se deberán utilizar en forma adecuada, siendo responsables de acuerdo a los siguientes lineamientos:

- Utilizarán únicamente los equipos asignados para efectuar las actividades o tareas administrativas asignadas.
- No podrá traer ni efectuar solicitudes de reparación de equipos tecnológicos personales al Área de Soporte de Sistemas.
- Solicitará al Área de Soporte de Sistemas un levantamiento de los equipos informáticos necesarios que requiera el área.



	Título:	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA SECRETARÍA EJECUTIVA PNP	
	Elaborado por:	Área de Soporte de Sistemas	Versión 1.0

9.2 Utilización de Software

El área de soporte de sistemas es responsable ante la Secretaría Ejecutiva PNP de la instalación, actualización y modificación de los programas de computadores utilizados por los usuarios de la Secretaría Ejecutiva PNP.

Responsabilidad del área de soporte de sistemas

- Definirá rutas de carpetas compartidas en red para todas las áreas, para que los usuarios guarden toda su información, así poder fragmentar el acceso a la información y una mejor organización.

Responsabilidad de los usuarios

Los programas informáticos existentes en los equipos asignados a los usuarios estarán regidos por los siguientes lineamientos:

- Queda prohibida la instalación y/o descarga de juegos, videos, música y aplicaciones de páginas de Internet, que no guarden relación con la Secretaría Ejecutiva PNP.
- Está prohibido tener en las rutas de carpetas compartidas en red, archivos que no guarden relación con las labores en la Secretaría Ejecutiva PNP. Tales como:
 - Formatos de música (MP3 o similar).
 - Archivos ejecutables (EXE o similar).
 - Archivos de instalación (MSI o similar).
 - Archivos de imagen (JPG, JPEG, GIF, BMP, PNG o similar).
 - Archivos de configuración de instalación (INI, INF o similar).
 - Librerías de archivos (DLL, o similar).
 - Archivos comprimidos (ZIP, RAR, 7ZIP o similar).
 - Entre otros.
- Está prohibida desinstalación del antivirus del equipo asignado, debido a que es de alto riesgo para la seguridad de la información.
- En caso de virus informático o alguna incidencia, deberá informar al área de soporte de sistemas.



9.3 Seguridad del Área de Soporte de Sistemas


Los usuarios ajenos al área de soporte de sistemas y visitantes externos no podrán acceder al área de soporte de sistemas, sin previa autorización del Jefe de Administración de la Secretaría Ejecutiva PNP.

9.4 Adquisición de software

La adquisición y utilización del software en la Institución, deberá estar de acuerdo a las especificaciones técnicas que requiere la Unidad Policial.

Responsabilidad del área de soporte de sistemas

- Participará para brindar apoyo en la elaboración de los Términos de Referencia al adquirir o actualizar el software.

	Título:	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA SECRETARÍA EJECUTIVA PNP	
	Elaborado por:	Área de Soporte de Sistemas	Versión 1.0

- b) Comprobará que el software incluya información de instalación, mantenimiento y/o garantía del software adquirido por la Institución, para facilitar la labor del personal de soporte técnico.
- c) Deberá requerirle a los proveedores el entrenamiento en el uso de software especializado.

9.5 Recursos informáticos

El uso indebido de los recursos informáticos puede afectar negativamente el funcionamiento de los equipos de oficina; ya sean equipos de cómputo, impresoras, cables de red y equipos servidores.

Responsabilidad del área de soporte de sistemas

- a) Supervisará la asignación de equipos informáticos a los usuarios, de acuerdo con los requerimientos de las áreas.

Responsabilidades y/o prohibiciones de los usuarios

Al asignarse un dispositivo informático a un usuario, todo lo concerniente al mismo será de su responsabilidad, por lo cual:

- a) Será responsable de la custodia de los equipos informáticos asignados (computadoras de escritorio, laptops, monitores, teclados, impresoras, proyectores, dispositivos de almacenamiento, entre otros).
- b) Notificará al área de soporte de sistemas los inconvenientes o anomalías presentadas con los equipos, accesorios, impresoras, sistemas informáticos, entre otros.



9.6. Clasificación, tratamiento y conservación de la información

- a) La clasificación de la información es conforme a lo siguiente:
 - **Clasificada:** Información de carácter Secreto, Reservado o Confidencial que solo debe conocer o tener acceso personal de la Policía Nacional del Perú autorizado y los usuarios que puedan acceder a ella según su rol.
 - **Común:** De libre acceso a la información pública, con las formalidades establecidas en la Ley 27806 – Ley de Transparencia y Acceso a la Información.
- b) Para el tratamiento de la información, los usuarios deben considerar la clasificación asignada a la documentación para establecer los niveles de protección adecuados.
- c) Etiquetar la información conforme a los requisitos legales, regulatorios o contractuales.
- d) Toda información clasificada como Secreto, Reservado o Confidencial, que se requiera eliminar, debe ser destruida de modo que sea imposible su recuperación y cumpliendo la normatividad vigente.

9.7. Seguridad de recursos humanos

- a) Integrar la seguridad de la información en las etapas de selección de personal, durante el empleo y al finalizar el mismo.

	Título:	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA SECRETARÍA EJECUTIVA PNP	
	Elaborado por:	Área de Soporte de Sistemas	Versión 1.0

- b) Realizar la concientización en seguridad de la información de acuerdo a las funciones, roles y responsabilidades asignadas.
- c) En caso de transportar información clasificada se debe tomar las medidas de seguridad para evitar la pérdida, fuga de la información o algún delito en contra del bien jurídico tutelado (información).
- d) No deben realizar transmisiones y/o comunicaciones, que atenten contra la seguridad de la información de los activos de la información de la que sea administrada y/o propiedad de la Policía Nacional del Perú.

9.8. Respaldo y recuperación de la información

Responsabilidad del área de soporte de sistemas

- a) Contar con un sistema de generación de copias de respaldo (en disco, cintas y/o medio óptico), o en su defecto un procedimiento el cual permita crear, salvaguardar y recuperar copias de respaldo de los datos de los sistemas de información, equipos de cómputo, códigos fuente de aplicaciones, equipos de comunicación, equipos de seguridad y otros que se consideren críticos para la función policial; asimismo, deben ser respaldados al menos una vez por semana.
- b) Las copias de respaldo de la información, del software y de las imágenes de los sistemas de los servidores deben ser realizadas, registradas y controladas periódicamente.
- c) Definir con qué frecuencia se generan las copias de respaldo considerando su nivel de criticidad para la institución.
- d) Identificar claramente las copias de respaldo con etiquetas, que permitan identificar a qué sistema de información o servidor pertenece, fecha y hora de la realización de la copia, u otro dato que la identifique.
- e) Realizar DOS (02) copias de respaldo como mínimo, una de ellas debe ser almacenada en un lugar externo al local donde se realiza la copia de respaldo y deben contar con controles de acceso físico y condiciones ambientales adecuadas para su conservación.
- f) Realizar pruebas de restauración periódicas a las copias de respaldo, a fin de asegurar que se pueda obtener correctamente la información almacenada al momento de ser necesaria.
- g) Los medios de almacenamiento que contengan copias de respaldo y vayan a ser eliminados deben pasar por un proceso de borrado seguro y posterior eliminación o destrucción.



9.9. Asignación de usuario

El objetivo de la asignación de usuarios corresponde a establecer el acceso a los equipos informáticos de la Secretaría Ejecutiva PNP, a aquellas personas que forman parte de la misma, otorgándole el derecho y el privilegio de inicio de sesión en la red y a los sistemas administrativos de la Secretaría Ejecutiva PNP.

Responsabilidades del área de soporte de sistemas

	Título:	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA SECRETARÍA EJECUTIVA PNP	
	Elaborado por:	Área de Soporte de Sistemas	Versión 1.0

- Recepcionará la información requerida para evaluar las solicitudes de creación o modificación de usuarios en los sistemas de información por parte de la Oficina de Administración de la Secretaría Ejecutiva PNP.
- Deberá crear el usuario de los nuevos empleados, con el siguiente formato estándar: primer dígito del nombre y luego el apellido paterno del empleado, con la finalidad de otorgarle el acceso a la red de la Secretaría Ejecutiva PNP.
- Se deshabilitarán los usuarios de los empleados que hayan finalizado su contrato de trabajo, según información remitida por parte de la Oficina de Administración de la Secretaría Ejecutiva PNP.
- Suspenderá el permiso a la red a todo empleado que se encuentre bajo investigación interna por haber cometido alguna infracción en el uso de la tecnología e informará al superior inmediato dicha suspensión.

Responsabilidades de los usuarios

- Al momento de finalizar sus labores deberá percatarse que su sesión de usuario se haya cerrado de manera correcta.
- No permitirá a personas ajenas a la institución el acceso a su equipo informático asignado.

9.10. Seguridad de la información

Las medidas de seguridad deberán ser acatadas por todos los trabajadores de la Unidad Policial con el propósito de proteger la información y normar los niveles de acceso y confidencialidad, a ser observadas y cumplidas por los involucrados en el uso y mantenimiento de los activos informáticos de la institución.


Responsabilidades del área de soporte de sistemas

- Comprobará que los equipos informáticos cuenten con las medidas de seguridad correspondientes a fin de reducir los riesgos a los que puedan estar sometidos.
- Velará por la seguridad de la información que se genere diariamente.
- Deberá almacenar en un lugar seguro todas las copias de seguridad o backups ejecutadas.
- Se encargará de la instalación de programas que garanticen la seguridad de la información en los archivos compartidos.

Responsabilidades de los usuarios

- Asegurará y protegerá la información que maneja.
- No podrá transferir a terceros información considerada como confidencial sin autorización previa.
- Guardará la información de trabajo en las carpetas compartidas asignadas a cada área, garantizando así la integridad de la información.
- Deberá crear una contraseña privada, con la finalidad de acceder a los datos, servicios y programas de su equipo, asegurándose que tenga las siguientes características:
 - Ocho (08) o más caracteres.
 - Combinar letras mayúsculas, minúsculas y números.



	Título:	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA SECRETARÍA EJECUTIVA PNP	
	Elaborado por:	Área de Soporte de Sistemas	Versión 1.0

- Fácil de recordar y difícil de adivinar.
- e) No deberá compartir la contraseña creada para acceder al equipo informático asignado.
- f) No hará uso indebido de la información institucional que maneja.

9.11. Manejo de impresoras

Buscando regular la impresión de documentos innecesarios por parte de los usuarios de las impresoras asignadas y establecer un control interno se han establecido lineamientos.

Responsabilidades de soporte de sistemas

- a) Se encargará de monitorear el uso de impresoras en red.
- b) Coordinará con los encargados de área, qué personal tendrá acceso a las impresoras de red y a las impresoras disponibles en las oficinas.
- c) No se imprimirá trabajos que no guarden relación con el trabajo dentro de la Unidad Policial.
- d) Sólo se utilizarán para impresiones, tóner y tintas originales.

Responsabilidades de los usuarios

- a) No podrán imprimir documentos personales ni a terceras personas en los equipos de la Institución.
- b) Las impresoras a color solo serán utilizadas para imprimir documentos que exclusivamente requieran ser impresos a color.
- c) Deberá triturar los borradores impresos de trabajos considerados como confidenciales.
- d) Podrá utilizar borradores de trabajo, hojas recicladas que no contengan información considerada como confidencial.
- e) Hará buen uso de material de trabajo disponible en el área para sus impresiones.

9.12. Acceso a Internet

El Internet es un medio importante y eficiente de comunicación, por lo cual es importante lograr un uso equitativo y eficiente del mismo.

Responsabilidades de soporte de sistemas

- a) Coordinará con los encargados de áreas, los sitios web que el personal podrá tener acceso, bloqueando aquellas páginas que no sean relevantes para el desempeño de las funciones.
- b) Deberá monitorear el acceso a los sitios web por parte del personal e informar cualquier violación de acceso a los encargados de las áreas.
- c) Deberá informar al encargado del área, los casos continuos de violación de acceso a Internet a sitios web no relacionados con el trabajo institucional, como, por ejemplo: sitios de juegos, música, descargas, videos, entre otras; con la finalidad que se tomen las medidas disciplinarias correspondientes.

Responsabilidades de los usuarios

	Título:	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA SECRETARÍA EJECUTIVA PNP	
	Elaborado por:	Área de Soporte de Sistemas	Versión 1.0

- a) Se encuentra prohibida la transmisión y/o descargar de material obsceno o pornográfico, que contenga amenazas o cualquier tipo de información que atente contra la moral o buenas costumbres.
- b) No deberá acceder a los siguientes sitios web:
 - Redes Sociales: Facebook, Twitter, H5, entre otros.
 - Carga y Descarga de archivos: megevideo.com, megaupload.com, rapidshare.com, entre otras.
 - Streaming: Emisoras de radio por internet.
 - Otras de igual finalidad.
 Se exceptúan los sitios web: WhatsApp, Youtube, entre otras; cuando previamente hayan sido autorizadas por el jefe del área.
- c) Sólo tendrá acceso a los sitios web que guarden relación con las labores de la Institución.

10.- PLAN DE CONTINGENCIA

El propósito principal de un Plan de Contingencia en informática es buscar reanudar las actividades ante un desastre o catástrofe, a fin de que la institución pueda mitigar los efectos del mismo.

Responsabilidad del área de soporte de sistemas

- a) Deberá existir un Plan de Contingencia en caso de fallas, que permita recuperar en corto tiempo toda la información contenida en la red.

Responsabilidades de los usuarios

- a) Deberán respetar los lineamientos establecidos en el Plan de Contingencia y abocarse a colaborar con el mismo.
- b) Ante la advertencia de un desastre deberá apoyar al área de Soporte de Sistemas en la protección de los equipos.


11.- CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN

- a) Determinar los requisitos de seguridad de información al planificar la continuidad del negocio y recuperación ante desastres.
- b) Verificar los controles de continuidad de seguridad de la información establecidos e implementados en intervalos regulares y asegurar que son válidos y eficaces durante situaciones adversas.
- c) Implementar redundancias en las instalaciones de procesamiento de información para asegurar la disponibilidad de los servicios.
- d) Realizar el inventario de activos de información y la gestión de riesgo de seguridad de la información, el mismo que debe ser actualizado cada año.

12.- IMPREVISTO

Los casos que se presenten, que se encuentren vinculados al trabajo y no se encuentren contemplados en este Manual de Políticas de Seguridad de Información, serán atendidos o resueltos por el área de soporte de sistemas.



	Título:	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA SECRETARÍA EJECUTIVA PNP	
	Elaborado por:	Área de Soporte de Sistemas	Versión 1.0

13.- VIGENCIA

Este Manual entrará en vigencia a partir de la aprobación del mismo por parte del Secretario Ejecutivo de la PNP, y permanecerá por tiempo indefinido en constante revisión y/o mejora que amerite el mismo.

Este documento ha sido elaborado en el mes de noviembre del 2020.

14.- APROBACIÓN


 Steven Mator F. CHAVARRÍA BONILLA
 SS PNP
 AREA - SICUI PNP



 Mario Fernando LARREA SOTOMAYOR
 COMANDO EN JEFE
 SECRETARÍA EJECUTIVA PNP

Anexo 15: Plan de Gestión de Riesgos

 POLICIA NACIONAL DEL PERU SECRETARIA EJECUTIVA PNP	Título:	PLAN DE GESTIÓN DE RIESGOS DE LA SECRETARÍA EJECUTIVA PNP	
	Elaborado por:	Área de Soporte de Sistemas	Versión 1.0

Plan de Gestión de Riesgos (PGR)

Versión 1.0

 POLICIA NACIONAL DEL PERU SECRETARIA EJECUTIVA PNP	Título:	PLAN DE GESTIÓN DE RIESGOS DE LA SECRETARÍA EJECUTIVA PNP	
	Elaborado por:	Área de Soporte de Sistemas	Versión 1.0

Historial de revisiones

Fecha	Versión	Descripción	Autor
15-May-2021	1.0	Documento de Identificación y Análisis de Riesgos	Sleem Néstor F. Chávarry Bonilla

 POLICIA NACIONAL DEL PERU SECRETARIA EJECUTIVA PNP	Título:	PLAN DE GESTIÓN DE RIESGOS DE LA SECRETARÍA EJECUTIVA PNP	
	Elaborado por:	Área de Soporte de Sistemas	Versión 1.0

Contenido

1. INTRODUCCIÓN	4
1.1. PROPÓSITO	4
1.2. ALCANCE.....	4
1.3. DEFINICIONES, SIGLAS Y ACRÓNIMOS.....	4
1.4. REFERENCIAS.....	¡Error! Marcador no definido.
2. GESTIÓN DEL RIESGO	4
2.1. IDENTIFICACIÓN DE RIESGOS	4
2.2. ANÁLISIS DEL RIESGO	5
2.3. ACCIONES DE PREVENCIÓN Y DE CORRECCIÓN.....	10
2.4. CONTROL Y SEGUIMIENTO DE RIESGOS.....	12
3. MATRIZ DE RIESGO	14

	Título:	PLAN DE GESTIÓN DE RIESGOS DE LA SECRETARÍA EJECUTIVA PNP	
	Elaborado por:	Área de Soporte de Sistemas	Versión 1.0

1. Introducción

Con el fin de certificar el cumplimiento de las labores, un elemento clave es la Gestión de riesgos, la cual se mide en cumplimiento de plazos, costes, alcance funcional y calidad final del proyecto. Implantar una Gestión de Riesgos nos permitirá saber por adelantado de los riesgos potenciales que puedan afectar el desenvolvimiento de las labores, y la elaboración de las acciones de contingencia adecuadas para evitar su aparición o para minimizar el impacto en el trabajo, en caso de que finalmente el riesgo se verifique.

1.1. Propósito

El presente plan nos muestra el análisis de los riesgos identificados en la Secretaría Ejecutiva de la Policía Nacional del Perú. Para cada riesgo observado se valorarán sus efectos y contexto de aparición para el caso en que se convierta en un hecho. Además, se definirán estrategias para reducir la probabilidad del riesgo o para controlar sus posibles efectos.

1.2. Alcance

El ámbito del análisis de riesgos cubre las principales actividades desarrolladas en la Secretaría Ejecutiva de la Policía Nacional del Perú. Durante la realización de las actividades será necesario revisar y actualizar los contenidos del análisis de riesgos en caso de que se detecten nuevos riesgos no visibles en ese momento.

Este documento será aplicable a todas las oficinas de la Secretaría Ejecutiva de la Policía Nacional del Perú.

1.3. Definiciones, siglas y abreviaturas.

- PNP: Policía Nacional del Perú.
- SECEJE: Secretaría Ejecutiva de la Policía Nacional del Perú.
-

2. Gestión del Riesgo

2.1. Identificación de Riesgos

Listado de Riesgos, Tipo de Riesgo

ID	Descripción del Riesgo	Tipo de Riesgo
R01	Sustracción de información por personas ajenas al área.	Externo, Organizacional
R02	Abandono de cargo de un trabajador	Organizacional
R03	Falta de experiencia en tareas de planificación	Organizacional
R04	Falta de experiencia con las herramientas utilizadas	Técnico, Organizacional
R05	Mal funcionamiento de un equipo informático	Técnico
R06	Falta de seguimiento a la documentación	Organizacional
R07	Documentación elaborada fuera del tiempo permitido	Organizacional
R08	Pérdida de documentación	Externo, Organizacional
R09	Vulneración del equipo asignado a un trabajador, mediante usuario y contraseña	Externo, Organizacional
R10	Falta de comunicación entre los trabajadores de una oficina o área.	Organizacional
R11	Acceso a las oficinas de personal no autorizado	Externo

	Título:	PLAN DE GESTIÓN DE RIESGOS DE LA SECRETARÍA EJECUTIVA PNP	
	Elaborado por:	Área de Soporte de Sistemas	Versión 1.0

R12	Corte de fluido eléctrico en las oficinas	Externo
R13	Requerimientos logísticos poco claros	Organizacional
R14	Falta de realización de copias de seguridad de los equipos informáticos	Técnico
R15	Fallas en la conexión a Internet	Técnico
R16	Duplicidad de labores asignadas entre personal de diferentes oficinas	Organizacional
R17	Falta de control de asistencia del personal PNP y/o civil	Organizacional

2.2. Análisis del Riesgo

ID	Análisis del Riesgo
R01	<p>Magnitud Alta.</p> <p>Descripción Por diversas causas se puede sustraer distinto tipo de información común o reservada.</p> <p>Impacto Variable, puede suponer una catástrofe, o un simple retraso.</p> <p>Indicadores Ninguno.</p>
R02	<p>Magnitud Alta, cuando afecta a un solo miembro. Muy alta, si afecta a más de uno.</p> <p>Descripción Algun miembro del proyecto no se encuentra disponible por cualquier motivo externo (enfermedad, lesión, etc) durante un periodo corto de tiempo, y por lo tanto no puede realizar tareas relacionadas con el proyecto.</p> <p>Impacto La falta de disponibilidad de los recursos humanos puede provocar el retraso con respecto a la planificación inicial de cualquier actividad del proyecto. Teniendo en cuenta que la entrega no puede posponerse, la falta de disponibilidad de personal puede suponer una pérdida de calidad en el producto.</p> <p>Indicadores Ninguno. Al ser un riesgo por causas externas al proceso, se supone que es un riesgo difícil de predecir.</p>
R03	<p>Magnitud Media.</p>

	Título:	PLAN DE GESTIÓN DE RIESGOS DE LA SECRETARÍA EJECUTIVA PNP	
	Elaborado por:	Área de Soporte de Sistemas	Versión 1.0

	<p>Descripción</p> <p>El grupo tiene poca experiencia en la planificación de proyectos siguiendo una estructura de tareas y fechas prioritizadas.</p> <p>Impacto</p> <p>La planificación guía todo el desarrollo del proyecto. Un error en la misma puede incidir directamente en sus resultados. No obstante, la división en entregables reduce el posible impacto de los errores, permitiendo que estos puedan ser corregidos o absorbidos en entregables posteriores a la de su aparición.</p> <p>Indicadores</p> <p>Diferencias entre el desarrollo real del proyecto y la planificación estimada.</p>
R04	<p>Magnitud</p> <p>Media, cuando se trata de herramientas básicas. Alta, cuando se trata de herramientas de gestión y/o contabilidad.</p> <p>Descripción</p> <p>Las herramientas básicas de software utilizadas pueden ser básicas (como software ofimático o de documentación básica) pueden presentar una magnitud media ya que es relevante para el desarrollo del trabajo, mientras que, las herramientas de gestión y contabilidad (como SIGA, SIAP, software para elaborar proyectos, etc) son cruciales en el trabajo diario y especializado, un error en el manejo de estos aplicativos puede acarrear consecuencias altas.</p> <p>Impacto</p> <p>Puede suponer retrasos, mal manejo de los requerimientos y presupuesto asignado a la institución.</p> <p>Indicadores</p> <p>No procede.</p>
R05	<p>Magnitud</p> <p>Baja si se trata de nivel de operativo, alta si se trata de nivel estratégico.</p> <p>Descripción</p> <p>Fallas en equipo informático por falta de mantenimiento preventivo o uso inadecuado del equipo informático por parte del usuario.</p> <p>Impacto</p> <p>En el nivel operativo la magnitud es baja debido a que los labores se pueden redirigir a otro usuario, mientras que, si el equipo informático pertenece al nivel estratégico, la magnitud es alta porque en este nivel se toman decisiones en cada momento.</p> <p>Indicadores</p> <p>Cantidad de incidencias reportadas.</p>
R06	<p>Magnitud</p> <p>Medio.</p>

 POLICIA NACIONAL DEL PERU SECRETARIA EJECUTIVA PNP	Título:	PLAN DE GESTIÓN DE RIESGOS DE LA SECRETARÍA EJECUTIVA PNP	
	Elaborado por:	Área de Soporte de Sistemas	Versión 1.0

	<p>Descripción No se lleva un seguimiento de la documentación, lo que podría originar pérdida de la documentación, así como, retrasos en los tiempos permitidos para la respuesta de la información solicitada.</p> <p>Impacto Puede suponer retrasos.</p> <p>Indicaciones No procede</p>
R07	<p>Magnitud Alta.</p> <p>Descripción La documentación tiene plazos previstos en el Manual de documentación policial, si existen retrasos en la elaboración o diligenciamiento podría originar que no se informen las acciones o no se tomen decisiones oportunamente, afectando a la organización y al efectivo policial o servidor civil, ya que originaría sanciones administrativas disciplinarias.</p> <p>Impacto Puede suponer retraso o que no se tomen las decisiones oportunamente.</p> <p>Indicaciones Ninguna.</p>
R08	<p>Magnitud Alta.</p> <p>Descripción El efectivo policial o personal civil es responsable de la documentación que se le ha asignada, por lo tanto, ante la pérdida de la documentación será sujeto de investigación y de ser el caso una sanción administrativa disciplinaria.</p> <p>Impacto Puede suponer retraso o que no se tomen las decisiones oportunamente.</p> <p>Indicaciones Ninguna.</p>
R09	<p>Magnitud Alta</p> <p>Descripción El usuario es responsable de su usuario y contraseña y debe mantener la confidencialidad respecto a esta. Por ningún motivo deberá brindar el usuario y contraseña asignada a ningún otro usuario.</p> <p>Impacto Puede generar sustracción de información de carácter reservada, confidencial y/o secreta.</p> <p>Indicaciones Ninguna.</p>
R10	<p>Magnitud Media</p> <p>Descripción</p>

 POLICIA NACIONAL DEL PERU SECRETARIA EJECUTIVA PNP	Título:	PLAN DE GESTIÓN DE RIESGOS DE LA SECRETARÍA EJECUTIVA PNP	
	Elaborado por:	Área de Soporte de Sistemas.	Versión 1.0

	<p>La comunicación es importante en ambientes de trabajo, por lo tanto, los trabajadores de los equipos de trabajo y entre equipos externos dentro de la cadena de información deben estar en continua comunicación.</p> <p>Impacto Se generaría retrasos, además de que la información sería poco confiable.</p> <p>Indicaciones Ninguna.</p>
R11	<p>Magnitud Alta</p> <p>Descripción La oficina de administración de la institución debe tener reglas para controlar el acceso de personal no autorizado a las oficinas.</p> <p>Impacto Puede sufrir la sustracción de equipos de cómputo, información, ser víctima de hackers, entre otras vulnerabilidades, lo cual afectaría la confiabilidad, disponibilidad e integridad de la información.</p> <p>Indicaciones Ninguna.</p>
R12	<p>Magnitud Alta</p> <p>Descripción El corte de fluido de la energía eléctrica en ocasiones puede ser por problemas externos y en otras ocasiones es por la carga de equipos que pueden estar conectados en simultáneo.</p> <p>Impacto Puede causar pérdida de información, deterioro de los dispositivos de almacenamiento, falta de funcionamiento de los equipos tecnológicos, entre otros.</p> <p>Indicaciones Ninguna.</p>
R13	<p>Magnitud Media</p> <p>Descripción Los requerimientos logísticos deben ser claros y entendibles para que el personal a cargo pueda adquirir los productos necesarios para el buen desempeño laboral.</p> <p>Impacto Puede causar mal utilización del presupuesto asignado para materiales de oficina, entre otros.</p> <p>Indicaciones Ninguna.</p>
R14	<p>Magnitud Alta</p> <p>Descripción Las copias de seguridad sirven para respaldar la información en caso la información se pierda, sustraiga, vulnere o sea víctima de delincuencia informática.</p>

 POLICIA NACIONAL DEL PERU SECRETARIA EJECUTIVA PNP	Título:	PLAN DE GESTIÓN DE RIESGOS DE LA SECRETARÍA EJECUTIVA PNP	
	Elaborado por:	Área de Soporte de Sistemas	Versión 1.0

	Impacto Puede causar daños económicos, logísticos y de información muy altos a la organización. Indicaciones Ninguna.
R15	Magnitud Baja Descripción La conexión a Internet en ocasiones falla por problemas externos a la institución. Impacto Originaría retraso en la elaboración de la documentación. Indicaciones Ninguna.
R16	Magnitud Media Descripción La misma documentación es asignada a más de un efectivo policial y/o personal CIVIL. Impacto Originaría retraso en la derivación y respuesta de la documentación. Indicaciones Ninguna.
R17	Magnitud Media Descripción No se lleva el control de la asistencia del personal a cargo en las diferentes oficinas. Impacto Retraso en la documentación. Indicaciones Ninguna.

 POLICIA NACIONAL DEL PERÚ SECRETARÍA EJECUTIVA PNP	Título:	PLAN DE GESTIÓN DE RIESGOS DE LA SECRETARÍA EJECUTIVA PNP	
	Elaborado por:	Área de Soporte de Sistemas	Versión 1.0

Asignación de Prevención y de Corrección

ID	Plan de Prevención	Plan de Corrección
R01	Colocar políticas de acceso para personal entre las áreas y personal ajenas a estas o personal de visita.	Se revisarán las copias de seguridad para restaurar la información hasta el punto más cercano a la sustracción de información. Se iniciará una investigación para descubrir el personal involucrado en la sustracción de la información. Se adecuarán las medidas para prevenir otro intento de sustracción de información.
R02	Elaboración de adendas en el contrato del personal civil para prevenir el abandono de cargo. Elaboración de encuestas sobre clima laboral de manera periódica.	Bloqueo de las cuentas de usuario y de claves de acceso a las computadoras y a las áreas dentro de la institución. Verificación de la información - a cargo del área de sistemas - dejada en la computadora del efectivo policial y/o personal civil.
R03	Requerimientos de cursos y experiencia laboral en manejo de tareas de planificación en las convocatorias de trabajo para personal civil.	Realización de talleres de capacitación y/o actualización en las áreas de planificación.
R04	Requerimientos de cursos y experiencia laboral en manejo de herramientas utilizadas en las labores cotidianas de la institución.	Realización de talleres de capacitación y/o actualización en las herramientas utilizadas para el normal desempeño de la institución.
R05	Mantenimiento preventivo de los equipos informáticos a cargo del área de soporte de sistemas de la Secretaría Ejecutiva de la Policía Nacional del Perú. Concientización sobre el buen uso de los equipos informáticos. Elaboración de registros de equipos informáticos en la Secretaría Ejecutiva de la Policía Nacional del Perú.	Mantenimiento correctivo de los equipos de cómputo. Registro de incidencias de los equipos informáticos.
R06	Registro de documentación asignada al efectivo policial o personal civil. Registro de la documentación en el aplicativo SIGE PNP.	Tomar las medidas correctivas administrativas disciplinarias por la falta de seguimiento de la documentación asignada.
R07	Registro de documentación asignada al	Tomar las medidas correctivas

 POLICIA NACIONAL DEL PERU SECRETARIA EJECUTIVA PNP	Título:	PLAN DE GESTIÓN DE RIESGOS DE LA SECRETARÍA EJECUTIVA PNP	
	Elaborado por:	Área de Soporte de Sistemas	Versión 1.0

	efectivo policial o personal civil. Registro de la documentación en el aplicativo SIGE PNP.	administrativas disciplinarias por la elaboración de la documentación fuera del tiempo permitido.
R08	Registro de documentación asignada al efectivo policial o personal civil. Registro de la documentación en el aplicativo SIGE PNP.	Tomar las medidas correctivas administrativas disciplinarias por la pérdida de la documentación asignada.
R09	Capacitación al personal sobre el buen uso de su usuario y contraseña del equipo asignado. Concientización sobre el buen uso de los equipos informáticos.	Tomar las medidas correctivas administrativas disciplinarias por la filtración de la información. Verificar qué información ha sido vulnerada.
R10	Realizar focus group y talleres de coaching entre el personal de las distintas oficinas. Realización de encuestas de clima laboral en forma periódica.	Hablar con el personal involucrado e indagar los motivos de la falta de comunicación. Si el problema persiste entonces se procede a realizar la amonestación verbal, amonestación escrita y sanción de ser el caso.
R11	Colocar políticas de acceso para personal entre las áreas y personal ajenas a estas o personal de visita.	Se iniciará una investigación para descubrir el personal involucrado en el acceso no autorizado. Se adecuarán las medidas para prevenir otro intento de acceso no autorizado a las oficinas.
R12	Realizar un mantenimiento preventivo del cableado eléctrico en las oficinas de la institución al menos una vez al año. Adquirir UPS para los equipos informáticos.	Contratar a personal especializado para realizar el mantenimiento correctivo del cableado eléctrico. Verificar el estado de los equipos informáticos.
R13	Capacitar al personal en la correcta realización de los requerimientos.	Verificar qué requerimientos no se encuentran de acuerdo a las necesidades de la oficina. Replantear los requerimientos.
R14	Tener medidas necesarias para la aplicación de las copias de seguridad en periodos determinados. Designar al personal encargado de realizar la copia de seguridad.	Verificar la última copia de seguridad generada y realizar la copia de seguridad en la fecha. Indagar el motivo por el que no se realizó la copia de seguridad.
R15	Realizar el mantenimiento preventivo de los dispositivos y herramientas que tienen relación con el servicio de	Contactar con el proveedor de Internet para verificar si la falta es problema interno o externo a la institución.

 POLICIA NACIONAL DEL PERU SECRETARIA EJECUTIVA PNP	Título:	PLAN DE GESTIÓN DE RIESGOS DE LA SECRETARÍA EJECUTIVA PNP	
	Elaborado por:	Área de Soporte de Sistemas	Versión 1.0

	<p>Internet. Designar al personal encargado de realizar el mantenimiento preventivo. Verificar el contrato con la compañía que brinda el servicio de Internet.</p>	<p>En caso el problema sea responsabilidad de la institución, realizar el mantenimiento correctivo. Consignar la incidencia para tener un control de lo sucedido.</p>
R16	<p>Elaborar las cartas funcionales de los efectivos policiales y personal civil designando las tareas a realizar. Llevar un control de la documentación asignada a cada efectivo policial y personal civil.</p>	<p>Decidir a quién le corresponde llevar el manejo de la documentación designada.</p>
R17	<p>Establecer políticas para el control de asistencia del personal y permisos que se puedan generar.</p>	<p>Verificar las causas por el ausentismo del personal. Establecer medidas correctivas, amonestaciones y sanciones al personal involucrado.</p>

2.3. Control y Seguimiento de Riesgos

Id.	Responsable	Fecha de Terminación	Estado	Observaciones
R01	Jefe de CFAD	Indefinido	Iniciado	
R02	Jefe de CFAD Jefe de Área de Soporte de Sistemas	Indefinido	Iniciado	
R03	Jefe de CFAD Jefe de Área de Soporte de Sistemas	Indefinido	Iniciado	
R04	Jefe de Área de Soporte de Sistemas	Indefinido	Iniciado	
R05	Jefe de Área de Soporte de Sistemas	Indefinido	Iniciado	
R06	Secretaría	Indefinido	Iniciado	
R07	Secretaría	Indefinido	Iniciado	
R08	Secretaría	Indefinido	Iniciado	
R09	Jefe de Área de Soporte de Sistemas	Indefinido	Iniciado	
R10	Jefe de CFAD	Indefinido	Iniciado	
R11	Jefe de CFAD Jefe de Área de Soporte de Sistemas	Indefinido	Iniciado	
R12	Jefe de CFAD Jefe de Área de Soporte de Sistemas	Indefinido	Iniciado	
R13	Jefe de CFAD	Indefinido	Iniciado	

 POLICIA NACIONAL DEL PERU SECRETARIA EJECUTIVA PNP	Título:	PLAN DE GESTIÓN DE RIESGOS DE LA SECRETARÍA EJECUTIVA PNP	
	Elaborado por:	Área de Soporte de Sistemas	Versión 1.0

R14	Jefe de Área de Soporte de Sistemas	Indefinido	Iniciado	
R15	Encargado de redes	Indefinido	Iniciado	
R16	Secretaria	Indefinido	Iniciado	
R17	Jefe de CEAD	Indefinido	Iniciado	

Responsable: Persona o personas asignadas a la implantación de las acciones preventivas y/o correctoras

Fecha Terminación: Fecha límite en la cual todas las acciones anteriormente descritas deban haber sido ejecutadas por el responsable o responsables asignados.

Estado: Estado Actual del Riesgo y de las Acciones Preventivas y/o Correctoras.

Observaciones: Descripción de las observaciones encontradas para este riesgo (opcional).

 POLICIA NACIONAL DEL PERU SECRETARIA EJECUTIVA PNP	Título:	PLAN DE GESTIÓN DE RIESGOS DE LA SECRETARÍA EJECUTIVA PNP	
	Elaborado por:	Área de Soporte de Sistemas	Versión 1.0

3. Matriz de Riesgo

Se propone la utilización de una matriz específica que sirva de soporte para la Gestión de Riesgos. Esta matriz se utilizará en las reuniones de seguimiento y/o cuando se estime necesario (en el caso de situaciones excepcionales), y su contenido será el siguiente:

Id.	Descripción del Riesgo	Tipo Riesgo	Exposición Ocurreneta	Nivel de Impacto	Evaluación del Riesgo	Acciones de Prevención	Acción de Corrección
R01	Sustracción de información por personas ajenas al área	Producto /Proyecto	20	4	0.8	Realización de reuniones con el cliente para ver los lugares que son más vulnerables y aplicar un plan de mejora.	Se revisará la información sustraída y se procederá a restaurar mediante copia de seguridad. Se abrirá investigación para determinar personal involucrado.
R02	Abandono de cargo de un trabajador	Producto	10	4	0.4	Plan de concientización y clima laboral, así como, talleres de capacitación coaching y coaching para liberar tensiones.	Se procede a bloquear todos los accesos del trabajador y reasignar las tareas a otros miembros.
R03	Falta de experiencia en tareas de planificación	Proyecto	30	3	0.9	Realización de los requerimientos para el puesto de trabajo a contratar, solicitando cursos y experiencia para el trabajo.	Realización de cursos y capacitación y actualización de metodologías de planificación y herramientas informáticas para facilitar esta fase.
R04	Falta de experiencia con las herramientas utilizadas	Producto /Proyecto	30	3	0.9	Realización de los requerimientos para el puesto de trabajo a contratar, solicitando cursos y experiencia para el trabajo.	Realización de cursos y capacitación y actualización de metodologías de planificación y herramientas informáticas para facilitar esta fase.
R05	Mal funcionamiento de un equipo	Producto	40	2	0.8	Realización de un plan de mantenimiento	Realización de mantenimiento correctivo y registro

	Título:	PLAN DE GESTIÓN DE RIESGOS DE LA SECRETARÍA EJECUTIVA PNP	
	Elaborado por:	Área de Soporte de Sistemas	Versión 1.0

	Informáticos.					preventivo de los equipos informáticos. Control de todos los equipos informáticos por áreas.	de incidencias y soluciones de cada equipo informático, además de la situación de cada equipo.
R06	Falta de seguimiento a la documentación	Producto	50	3	1.5	Registro de documentación asignada a cada persona.	Verificación del incumplimiento y toma de acciones administrativas disciplinarias.
R07	Documentación elaborada fuera del tiempo permitido	Producto	40	4	1.6	Registro de documentación asignada a cada persona.	Verificación del incumplimiento y toma de acciones administrativas disciplinarias.
R08	Pérdida de documentación	Proyecto	30	4	1.2	Registro de documentación asignada a cada persona.	Apertura de investigación y de ser el caso toma de acciones administrativas disciplinarias.
R09	Vulneración del equipo asignado, mediante usuario y contraseña	Proyecto	50	4	2	Realización de plan de concientización, teniendo en cuenta que el usuario y contraseña asignado es de uso personal y por ningún motivo se debe compartir.	Apertura de investigación y de ser el caso toma de acciones administrativas disciplinarias.
R10	Falta de comunicación entre los trabajadores de una oficina.	Proyecto	50	3	1.5	Plan de concientización y clima laboral, así como, talleres de FOCUS GROUP , y coaching para liberar tensiones.	Conversar con el personal involucrado, en caso el problema persista realizar acciones administrativas disciplinarias.
R11	Acceso a las oficinas de personal no autorizado	Proyecto	50	4	2	Establecer las políticas de seguridad física para personal autorizado por oficinas y personas foráneas.	Se revisará la información sustraida y se procederá a restaurar mediante copia de seguridad. Se abrirá investigación para



Título:	PLAN DE GESTIÓN DE RIESGOS DE LA SECRETARÍA EJECUTIVA PNP	
Elaborado por:	Área de Soporte de Sistemas	Versión 1.0

							determinar personal involucrado.
R12	Corte de fluido eléctrico en las oficinas	Proyecto	30	4	1.2	Realizar al menos una vez al año el mantenimiento preventivo del cableado eléctrico en las oficinas.	Contratar a personal especializado para que soluciones problemas en caso el problema sea de la institución. En caso sea un problema de la empresa que presta el servicio de luz, coordinar la solución del inconveniente.
R13	Requerimientos logísticos poco claro	Proyecto	40	3	1.2	Realizar charlas al personal para la adecuada solicitud y llenado de los requerimientos logísticos.	Verificar que requerimientos no se encuentran de acuerdo a las necesidades de la oficina. Replantear los requerimientos.
R14	Falta de realización de copias de seguridad de los equipos informáticos	Proyecto	30	4	1.2	Tener medidas necesarias para la aplicación de las copias de seguridad en periodos determinados. Designar al personal encargado de realizar la copia de seguridad.	Verificar la última copia de seguridad generada y realizar la copia de seguridad en la fecha. Indagar el motivo por el que no se realizó la copia de seguridad.
R15	Fallas en la conexión a Internet	Producto	20	2	0.4	Realizar el mantenimiento preventivo de los dispositivos y herramientas que tienen relación con el servicio de Internet. Designar al personal encargado de realizar el mantenimiento preventivo. Verificar el contrato con la compañía que brinda el servicio de	Contador con el proveedor de Internet para verificar si la falla es problema interno o externo a la institución. En caso el problema sea responsabilidad de la institución, realizar el mantenimiento correctivo. Consonar la

	Título:	PLAN DE GESTIÓN DE RIESGOS DE LA SECRETARÍA EJECUTIVA PNP	
	Elaborado por:	Área de Soporte de Sistemas	Versión 1.0

						Internet.	incidencia para tener un control de lo sucedido.
R16	Duplicidad de labores asignadas entre personal de diferentes oficinas	Producto	40	3	1.2	Elaborar las cartas funcionales de los efectivos policiales y personal civil designando las tareas a realizar. Llevar un control de la documentación asignada a cada efectivo policial y personal civil.	Decidir a quién le corresponde llevar el manejo de la documentación designada.
R17	Falta de control de asistencia de personal.	Producto /Proyecto	50	3	1.5	Establecer políticas para el control de asistencia del personal y permisos que se puedan generar.	Verificar las causas por el ausentismo del personal. Establecer medidas correctivas, amonestaciones y sanciones al personal involucrado.

Id.: Identificador de Riesgo

Descripción del Riesgo: Descripción Resumida del Riesgo

Probabilidad (1 a 100): Grado de probabilidad de que el Riesgo finalmente se produzca. Se mide en una escala de 1 a 100 (porcentual).

Nivel de Impacto: Grado de Impacto en el Proyecto en el caso de que el Riesgo finalmente se produjera. Se mide en una escala de 1 a 5, siendo 1=poco influyente hasta 5=fuertemente influyente.

Probabilidad Ocurrencia: Valor numérico resultante del producto del Grado de Probabilidad por el Grado de Impacto. Este producto dará la prioridad que tendrá la gestión de este Riesgo y la implantación de sus medidas preventivas o correctoras.

Acciones Prevención: Descripción de las Acciones o Medidas a Adoptar para evitar (mitigar) la aparición final del Riesgo

Acciones Corrección: Descripción de las Acciones o Medidas a Adoptar en el caso en el que el Riesgo finalmente se haya producido.

Anexo 17: Instrucciones de llenado del Formato de Lista maestra de registros

Instrucciones de llenado del Formato: Lista Maestra de Registros

Campo del Formato	Instrucción de llenado
N°	Colocar el número correlativo del registro
Nombre del Registro	Colocar el nombre con el que se identifica el registro; por ejemplo "Ficha de inscripción".
Código	Colocar el código del formato con que se identifica al registro; por ejemplo "SE-UNIGSA-SEG-001". En caso el registro no provenga de un formato llenado, colocar tres guiones seguidos ("---").
Proceso	Colocar el nombre del proceso al cual pertenece el registro.
Propietario del registro	Colocar el nombre del puesto del dueño del proceso al cual pertenece el registro.
Custodio del registro	Señalar el nombre del puesto responsable de la custodia, conservación y disposición del registro.
Clasificación de la información	<p>Señalar la categoría de información a la cual pertenece el registro. Las categorías son las siguientes:</p> <p>a.- Común: Documentación de libre acceso a la información pública, con las formalidades establecidas por ley.</p> <p>b.- Secreta: Documentación referida a asuntos de extrema importancia o cuyo conocimiento indiscriminado podría generar problemas que afecten a la Seguridad Nacional; limitando su conocimiento a los comandos responsables.</p> <p>c.- Reservada: Documentación relacionada con la prevención y represión de la criminalidad en el país, cuya revelación puede entorpecerlas. Planes de Seguridad y Defensa de las Instalaciones Policiales, y movimiento del personal que pudiera poner en riesgo la vida e integridad de las personas involucradas o afectar la seguridad ciudadana, el armamento y material logístico comprometido en operaciones especiales y planes de seguridad y defensa del orden interno.</p> <p>d.- Confidencial: Documentación relacionada con los aspectos disciplinarios del personal o irregularidades administrativas que por su gravedad deben ser conocidos únicamente por el remitente y el destinatario, o por las personas encargadas de opinar o resolver sobre el particular.</p>

Anexo 18: Formato de Hoja de trabajo para desarrollar un planteamiento de seguridad

Hoja de trabajo para desarrollar un planteamiento de seguridad					
Recursos de la fuente			Tipo de usuario a proteger el recurso	Probabilidad de amenaza	Medidas de seguridad a implementar para proteger el recurso de la red
Número	Nombre	Importancia del recurso			

Anexo 19: Formato de Hoja de trabajo para desarrollar un plan de auditoría interna

PLAN DE AUDITORIA INTERNA						
PROCESO O ÁREA A AUDITAR:						
OBJETIVO DE LA AUDITORÍA:						
ALCANCE DE LA AUDITORÍA:						
CRITERIOS DE AUDITORÍA:						
AUDITORES						
NOMBRE DEL AUDITOR						
AUDITADO		INICIO DE LA ACTIVIDAD DE AUDITORÍA		CIERRE DE LA ACTIVIDAD DE AUDITORÍA		AUDITOR
ACTIVIDAD O CRITERIO	CARGO DEL RESPONSABLE DEL PROCESO	FECHA	HORA	FECHA	HORA	
<div style="display: flex; justify-content: space-around; align-items: center; margin-top: 20px;"> <div style="text-align: center;"> <hr style="width: 150px; margin: 0 auto;"/> <p>NOMBRE Y FIRMA AUDITOR JEFE</p> </div> <div style="text-align: center;"> <hr style="width: 150px; margin: 0 auto;"/> <p>NOMBRE Y FIRMA FIRMA DEL AUDITOR (ES)</p> </div> </div> <div style="text-align: center; margin-top: 20px;"> <hr style="width: 150px; margin: 0 auto;"/> <p>NOMBRE Y FIRMA FIRMA DEL AUDITADO</p> </div>						