ESCUELA MILITAR DE CHORRILLOS
“CORONEL FRANCISCO BOLOGNESI”

GESTIÓN DE LA SEGURIDAD INFORMÁTICA Y LA IMPLEMENTACIÓN DE LA NORMA ISO/IEC 27001 EN LA ESCUELA MILITAR DE CHORRILLOS “CORONEL FRANCISCO BOLOGNESI" - AÑO 2021

Tesis para optar el Título Profesional de Licenciado en Ciencias Militares con Mención en Ingeniería

Autores

Marco Antonio Paucar Yaguno

0000-0002-4505-5641

Cristian Rojas Lapa

0000-0002-6628-6537

Asesores

Mg. Carlos Wilfredo Villanueva del Castillo

0000-0002-8929-7175

Mg. Jannette Alva Navarro

0000-0003-3391-1065

Lima – Perú

2021

DEDICATORIAS

Al Dios todo poderoso por no abandonarme en mis peores momentos, mi madre y hermanos que siempre creyeron en mí y fueron mi aliento impulsando mi deseo de salir adelante, a mis compañeros de arma por enseñarme a encontrar la calma y mejorarme como hombre.

M. PAUCAR Y.

A mi familia y hermanos quienes me apoyaron dándome moral para continuar en la adversidad y salir victorioso, mis promociones de la Escuela Militar de Chorrillos que me enseñaron el trabajo en equipo y que la unión hace la fuerza.

C. ROJAS L.

RECONOCIMIENTO

A la gloriosa Escuela Militar de Chorrillos Coronel “Francisco Bolognesi” por su increíble labor formando a los futuros oficiales del Ejército del Perú.

ÍNDICE

DEDICATORIAS I

RECONOCIMIENTO I

Índice de Tablas V

Índice de Figuras VII

RESUMEN IX

ABSTRACT X

Introducción XI

1 CAPITULO I: PROBLEMA DE INVESTIGACIÓN 12

1.1 Descripción problemática 12

1.2 Delimitación de la investigación 13

1.2.1 Delimitación espacial 14

1.2.2 Delimitación temporal 14

1.2.3 Delimitación social 14

1.3 Formulación del problema 15

1.3.1 Problema General 15

1.3.2 Problemas Específicos 15

1.4 Objetivos de la Investigación 16

1.4.1 Objetivo General 16

1.4.2 Objetivos Específicos 16

1.5 Justificación e Importancia de la Investigación 17

1.5.1 Justificación metodológica 17

1.5.2 Justificación practica 17

2 CAPITULO II: MARCO TEÓRICO 18

2.1 Antecedentes de la Investigación 18

2.1.1 Antecedentes Internacionales 18

2.1.2 Antecedentes Nacionales 20

2.2 Bases Teóricas 21
2.2.1 Base Teórica (Variable Independiente) 21
2.2.2 Base Teórica (Variable Dependiente) 31
2.3 Marco Conceptual 34
3 CAPITULO III: HIPÓTESIS Y VARIABLES 37
3.1 Hipótesis General 37
3.2 Hipótesis Especificas 37
3.3 Definición Conceptual y Operacional de Variables 38
3.4 Cuadro de Operacionalización de Variables 39
4 CAPITULO IV: MARCO METODOLÓGICO 40
4.1 Método de estudio 40
4.2 Enfoque de la Investigación 40
4.3 Tipo de Investigación 40
4.4 Nivel y Diseño de la Investigación 41
4.5 Técnicas e Instrumentos para la recolección de datos 41
4.6 Población y Muestra 41
5 CAPITULO V: INTERPRETACIÓN, ANALISIS Y DISCUSIÓN DE LOS RESULTADOS 42
5.1 Análisis Descriptivo 42
5.1.1 Análisis de los Indicadores 42
5.1.2 Análisis de los Instrumentos 45
5.2 Análisis Inferencial 56
5.3 Discusión de los resultados 63
CONCLUSIONES 66
RECOMENDACIONES 68
PROPUESTA DE MEJORA 69
REFERENCIAS BIBLIÓGRAFICAS 70

ANEXOS.....73

Anexo 2: Elaboración de los Instrumentos 74

Anexo 3: Validez, confiabilidad y evaluación de instrumentos: juicio de expertos.77

Anexo 4: Bases de datos 79

Índice de Tablas

TABLA 1: CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN 33

TABLA 2: PREGUNTA 1 ¿CONSIDERA USTED QUE ES IMPORTANTE LA GESTIÓN DE LA SEGURIDAD INFORMÁTICA EN LA ESCUELA MILITAR DE CHORRILLOS "CORONEL FRANCISCO BOLOGNESI"? 45

TABLA 3: PREGUNTA 2 ¿CREE USTED QUE EL PERMANENTE MONITOREO DE LA RED AYUDA A MANTENER UNA RED SEGURA EN LA ESCUELA MILITAR DE CHORRILLOS "CORONEL FRANCISCO BOLOGNESI"? 46

TABLA 4: PREGUNTA 3 ¿CONSIDERA USTED QUE HERRAMIENTAS COMO EL PANEL DE CONTROL PERMITEN ADMINISTRAR LA RED DE MANERA EFICIENTE EN LA ESCUELA MILITAR DE CHORRILLOS "CORONEL FRANCISCO BOLOGNESI"? 46

TABLA 5: PREGUNTA 4 ¿CONSIDERA USTED QUE ES NECESARIO LA EVALUACIÓN DE RIESGOS INFORMÁTICOS PARA LA IDENTIFICACIÓN DE AMENAZAS EN LA ESCUELA MILITAR DE CHORRILLOS "CORONEL FRANCISCO BOLOGNESI"? 47

TABLA 6: PREGUNTA 5 ¿CONSIDERA USTED QUE LAS IDENTIFICACIONES DE RIESGOS INFORMÁTICOS AYUDAN A DISEÑAR PLANES DE SEGURIDAD Y ESTABLECER CONTROLES PARA LA MITIGACIÓN DE AMENAZAS EN LA ESCUELA MILITAR DE CHORRILLOS "CORONEL FRANCISCO BOLOGNESI"? 48

TABLA 7: PREGUNTA 6 ¿CREE USTED QUE ES IMPORTANTE LA APLICACIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁTICA PARA GARANTIZAR LA SEGURIDAD DE LAS TECNOLOGÍAS DE INFORMACIÓN EN LA ESCUELA MILITAR DE CHORRILLOS "CORONEL FRANCISCO BOLOGNESI"? 49

TABLA 8: PREGUNTA 7 ¿CONSIDERA USTED LA NECESIDAD DE ADOPTAR MEDIDAS DE SEGURIDAD INFORMÁTICA PARA ASEGURAR LA INTEGRIDAD DE LOS SISTEMAS INFORMÁTICOS EN LA ESCUELA MILITAR DE CHORRILLOS "CORONEL FRANCISCO BOLOGNESI"? 50

TABLA 9: PREGUNTA 8 ¿CONSIDERA USTED QUE LA IMPLEMENTACIÓN DE LA NORMA ISO/IEC 27001 PERMITIRÁ CONTAR CON UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE INFORMACIÓN (SGSI) PARA LA REDUCCIÓN DEL IMPACTO DE LOS INCIDENTES DE SEGURIDAD EN LA ESCUELA MILITAR DE CHORRILLO..... 51

TABLA 10: PREGUNTA 9 ¿CREE USTED QUE ESTÁ EXPUESTO A RIESGOS INFORMÁTICOS DENTRO DE LA ESCUELA MILITAR DE CHORRILLOS "CORONEL FRANCISCO BOLOGNESI"? 52

TABLA 11: PREGUNTA 10 ¿CONSIDERA USTED QUE LOS RIESGOS DE ACCESO QUE AFECTAN LA INTEGRIDAD DE LA INFORMACIÓN EN LOS SISTEMAS DE BASES DE DATOS SON LOS MÁS CONSTANTES EN LA ESCUELA MILITAR DE CHORRILLOS "CORONEL FRANCISCO BOLOGNESI"? 53

TABLA 12: PREGUNTA 11 ¿CREE USTED QUE SU COMPUTADOR E INFORMACIÓN PERSONAL ES VULNERABLE A AMENAZAS INFORMÁTICAS COMO MALWARE DENTRO DE LA ESCUELA MILITAR DE CHORRILLOS "CORONEL FRANCISCO BOLOGNESI"? 54

TABLA 13: PREGUNTA 12 ¿CREE USTED QUE LAS AMENAZAS LÓGICAS COMO VIRUS, PUERTOS ABIERTOS, GUSANOS Y TROYANOS PONEN EN RIESGO LA CONFIDENCIALIDAD DE SU INFORMACIÓN AL NAVEGAR EN LA RED DE LA ESCUELA MILITAR DE CHORRILLOS "CORONEL FRANCISCO BOLOGNESI"? 55

TABLA 14: RESUMEN DEL PROCESAMIENTO DE LOS CASOS 56

TABLA 15: PRUEBA DE NORMALIDAD 57

TABLA 16: CORRELACIÓN DE RHO DE SPEARMAN 58

TABLA 17: CONTRASTACIÓN DE HIPÓTESIS ESPECIFICA 1 59

TABLA 18: CONTRASTACIÓN DE HIPÓTESIS ESPECIFICA 2 59

TABLA 19: CONTRASTACIÓN DE HIPÓTESIS ESPECIFICA 3 60

TABLA 20:CONTRASTACIÓN DE HIPÓTESIS ESPECIFICA 4 61

TABLA 21: CONTRASTACIÓN DE HIPÓTESIS ESPECIFICA 5 62

TABLA 22: CONTRASTACIÓN DE HIPÓTESIS ESPECIFICA 6 62

Índice de Figuras

FIGURA 1: ESQUEMA DEL FUNCIONAMIENTO DE LA RED INALÁMBRICA 23

FIGURA 2: LOS ELEMENTOS DE LA SEGURIDAD 25

FIGURA 3: DISTRIBUCIÓN DE RESPUESTAS A LA PREGUNTA ¿CONSIDERA USTED QUE ES IMPORTANTE LA GESTIÓN DE LA SEGURIDAD INFORMÁTICA EN LA ESCUELA MILITAR DE CHORRILLOS "CORONEL FRANCISCO BOLOGNESI"? 45

FIGURA 4: DISTRIBUCIÓN DE RESPUESTA A LA PREGUNTA ¿CREE USTED QUE EL PARMENTE MONITOREO DE LA RED AYUDA A MANTENER UNA RED SEGURA EN LA ESCUELA MILITAR DE CHORRILLOS "CORONEL FRANCISCO BOLOGNESI"? 46

FIGURA 5: DISTRIBUCIÓN DE RESPUESTA A LA PREGUNTA ¿CONSIDERA USTED QUE HERRAMIENTAS COMO EL PANEL DE CONTROL PERMITEN ADMINISTRAR LA RED DE MANERA EFICIENTE EN LA ESCUELA MILITAR DE CHORRILLOS "CORONEL FRANCISCO BOLOGNESI"? 47

FIGURA 6: DISTRIBUCIÓN DE RESPUESTA A LA ¿CONSIDERA USTED QUE ES NECESARIO LA EVALUACIÓN DE RIESGOS INFORMÁTICOS PARA LA IDENTIFICACIÓN DE AMENAZAS EN LA ESCUELA MILITAR DE CHORRILLOS "CORONEL FRANCISCO BOLOGNESI"? 48

FIGURA 7: DISTRIBUCIÓN DE RESPUESTAS A LA PREGUNTA ¿CONSIDERA USTED QUE LA IDENTIFICACIÓN DE RIESGOS INFORMÁTICOS AYUDA A DISEÑAR PLANES DE SEGURIDAD Y ESTABLECER CONTROLES PARA LA INVESTIGACIÓN ESCUELA MILITAR DE CHORRILLOS "CORONEL FRANCISCO BOLOGNESI"? 49

FIGURA 8: DISTRIBUCIÓN DE RESPUESTAS A LA PREGUNTA ¿CREE USTED QUE ES IMPORTANTE LA APLICACIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁTICA PARA GARANTIZAR LA SEGURIDAD DE LAS TECNOLOGÍAS DE INFORMACIÓN EN LA ESCUELA MILITAR DE CHORRILLOS "CORONEL FRANCISCO BOLOGNESI"? 50

FIGURA 9: DISTRIBUCIÓN DE RESPUESTAS A LA PREGUNTA ¿CONSIDERA USTED LA NECESIDAD DE ADOPTAR MEDIDAS DE SEGURIDAD INFORMÁTICA PARA ASEGURAR LA INTEGRIDAD DE LOS SISTEMAS INFORMÁTICOS EN LA ESCUELA MILITAR DE CHORRILLOS "CORONEL FRANCISCO BOLOGNESI"? 51

FIGURA 10: DISTRIBUCIÓN DE RESPUESTAS A LA PREGUNTA ¿CONSIDERA USTED QUE LA IMPLEMENTACIÓN DE LA NORMA ISO/IEC 27001 PERMITIRÁ CONTAR CON UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN EN LA ESCUELA MILITAR DE CHORRILLOS "CORONEL FRANCISCO BOLOGNESI"? 52

FIGURA 11: DISTRIBUCIÓN DE RESPUESTAS A LA PREGUNTA ¿CREE USTED QUE ESTÁ EXPUESTO A RIESGOS INFORMÁTICOS DENTRO DE LA ESCUELA MILITAR DE CHORRILLOS "CORONEL FRANCISCO BOLOGNESI"?.....53

FIGURA 12: DISTRIBUCIÓN DE RESPUESTAS A LA PREGUNTA ¿CONSIDERA USTED QUE LOS RIESGOS DE ACCESO QUE AFECTAN LA INTEGRIDAD DE LA INFORMACIÓN EN LOS SISTEMAS DE DATOS SON LOS MÁS CONSTANTES EN LA ESCUELA MILITAR DE CHORRILLOS "CORONEL FRANCISCO BOLOGNESI"?.....54

FIGURA 13: DISTRIBUCIÓN DE RESPUESTAS A LA PREGUNTA ¿CREE USTED QUE SU COMPUTADOR E INFORMACIÓN PERSONAL ES VULNERABLE A AMENAZAS INFORMÁTICAS COMO MALWARE DENTRO DE LA ESCUELA MILITAR DE CHORRILLOS "CORONEL FRANCISCO BOLOGNESI"?.....55

FIGURA 14: DISTRIBUCIÓN DE RESPUESTAS A LA PREGUNTA ¿CREE USTED QUE LAS AMENAZAS LÓGICAS COMO VIRUS, PUERTOS ABIERTOS, GUSANOS Y TROYANOS PONEN EN RIESGOS LA CONFIDENCIALIDAD DE SU INFORMACIÓN EN LA ESCUELA MILITAR DE CHORRILLOS "CORONEL FRANCISCO BOLOGNESI"?.....56

FIGURA 15: DISPERSIÓN DE PUNTOS DE LA PRUEBA DE HIPÓTESIS.....59

RESUMEN

La norma ISO 27001:2013 contribuye a la protección de la información de los Sistemas Informáticos de una organización que la implemente, mediante la implementación de lineamientos y controles que la resguarde. En este trabajo se recalca la importancia de concientizar al personal en la importancia de salvaguardar la información que manejan en sus actividades laborales. El objetivo del presente trabajo es determinar la importancia de la gestion de la seguridad informatica y la norma ISO/IEC 27001 en la Escuela Militar de Chorrillos, organización encargada de formar a los futuros oficiales del Ejército del Perú. El presente trabajo es descriptivo y su diseño es no experimental de tipo transversal la población fue conformada por 84 personales que son la totalidad de cadetes del arma de comunicaciones, oficiales y personal responsable las secciones de Telemática e Inteligencia, debido a su tamaño la muestra es la totalidad de la población, a saber 84 personas, las técnicas que se utilizaron fueron las siguientes: Encuestas online, entrevistas, entrevistas y análisis documentario. Como conclusión la hipótesis general nos muestra que gestión de la seguridad informática es de gran importancia porque permite salvaguardar la información de diversas amenazas mediante el cumplimiento de objetivos de seguridad, lineados a los controles de la norma ISO/IEC 27001.

Palabras claves: Seguridad informática, ISO/IEC 27001, Gestión de la Seguridad Informática.

ABSTRACT

ISO 27001:2013 contributes to the protection of the information of the Computer Systems of an organization that implements it, through the implementation of guidelines and controls that protect it. This paper stresses the importance of raising awareness among staff about the importance of safeguarding the information they handle in their work activities. The objective of this paper is to determine the importance of computer security management and the ISO/IEC 27001 standard in the Military School of Chorrillos, an organization responsible for training future officers of the Peruvian Army. The present work is descriptive and its design is nonexperimental cross-sectional population was formed by 84 personnel who are all cadets of the communications weapon, officers and personnel responsible for the sections of Telematics and Intelligence, Due to its size the sample is the entire population, namely 84 people, the techniques that were used were the following: Online surveys, interviews, interviews and documentary analysis. As a conclusion the general hypothesis shows us that computer security management is of great importance because it allows to safeguard the information of various threats through the fulfillment of security objectives, lined to the controls of the standard ISO/IEC 27001.

Keywords: Computer Security, ISO/IEC 27001, Computer Security Management.

Introducción

La presente investigación pretende realizar el análisis de la importancia de la Gestión de la Seguridad Informática y la implementación de la ISO/IEC 27001 en la Escuela Militar de Chorrillos coronel “Francisco Bolognesi”. Se busca analizar las vulnerabilidades y riesgos en la gestión de seguridad Informática de la Escuela Militar, y desarrollar lineamientos y políticas para la mitigación de riesgo. El trabajo de investigación se estructuro de la siguiente manera:

En el capítulo I: Se expresa el planteamiento del problema con su respectiva descripción de la realidad problemática, las delimitaciones espaciales, social, temporal y conceptual de la investigación, así como la formulación del problema y objetivos principal y específicos del estudio. También se desarrolla la justificación e importancia, factibilidad y limitación del proyecto de investigación.

En el capítulo II: Se detalla el marco teórico conceptual, antecedentes y bases teóricas de las variables y el desarrollo de la definición de términos básicos.

En el capítulo III: Se desarrollan las hipótesis y la identificación y clasificación de las variables en cuanto a sus dimensiones e indicadores.

En el capítulo IV: Se desarrollará la metodología de la investigación en cuanto a su tipo, nivel, método y diseño, también se expresa la población y muestra, así como las técnicas, instrumentos, validez y confiabilidad, el procesamiento y análisis de datos, y finaliza con la descripción de la ética en la investigación.

En el capítulo V: Se detalla los resultados alcanzados durante la investigación, conclusiones y recomendaciones. Finalizando con la organización del estudio encontraremos en los anexos, la matriz de consistencia, el instrumento de recolección de datos, el formato de validación del instrumento y la declaratoria de autenticidad de la tesis.

CAPITULO I: PROBLEMA DE INVESTIGACIÓN

1.1 Descripción problemática

A nivel mundial, La International Organization for Standardization (ISO), es la organización encargada de crear e implementar estándares que son aplicables a cualquier organización. En su mayoría las organizaciones desconocen la magnitud de los datos que manejan, de igual manera no tienen asegurada dicha información, tampoco cuentan con un plan de seguridad para prevenir la existencia de posibles incidentes que puedan comprometer este activo importante y esto a su vez una perdida sustancial económica y administrativa (Macias, 2016).

En Latinoamérica, ESET Security Report revela que tres de cada cinco empresas sufrieron por lo menos un incidente de seguridad en la red durante 2017 y la mayoría estuvo en el top de la infección con códigos maliciosos. Los países más afectados en América Latina con ataques informáticos fueron Perú con un 25%, México con el 20%, seguido de Argentina con el 15%, Brasil con el 14% y Colombia con el 10%. Muchas compañías ignoran estos ciberataques y creen que se solucionan pagando una extorsión, cuando la perdida de datos es un problema cada vez más evidente (Muñoz, 2020).

Muchas instituciones buscan gestionar la información para la libre disposición a sus usuarios, en el momento y lugar que lo necesitan, en este proceso pude ocurrir filtraciones y flujos de información hacia personas no adecuadas. Originando un riesgo en la gestión de la información y de esta forma la institución pierde la confiabilidad de los usuarios.

En el Perú, en el 2016 se aprobó el uso obligatorio de la Norma técnica peruana “NTP ISO/IEC 27001:2014, en todas las entidades integrantes del sistema nacional de informática, teniendo como principal objetivo velar por la integridad, seguridad y disponibilidad de los datos debiendo establecerse lineamientos de seguridad de la información a fin de mitigar el riesgo de exposición de información sensible de los usuarios, siendo en gran auge la

preocupación de las empresas de contar con la certificación ISO para mejorar la seguridad de su empresa.

La Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” es una institución que gestiona activos de información de alto valor, muchos de los cuales tienen alto nivel de confidencialidad. Esta información está expuesta a diferentes peligros informáticos; desde el incremento del uso de la tecnología en las instalaciones en los últimos años, la inseguridad va en aumento, las políticas para el control de la información no están definidas en base a una norma o protocolo, los dispositivos USB y portátiles no son verificados al momento de salir e ingresar a las instalaciones, siendo vulnerable al riesgo de la perdida de información sensible y flujo de información clasificada. Frente a esta problemática se plantea realizar un análisis de la gestión de la seguridad informática y la implementación de la ISO/IEC 27001 para la gestión de riesgos, mitigación y control de incidentes para demostrar la importancia de tomar medidas para reducir la inseguridad informática en la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”.

1.2 Delimitación de la investigación

La Escuela Militar de Chorrillos “coronel Francisco Bolognesi” es una institución que gestiona información de alta confidencialidad, entre sus usuarios y de forma interinstitucional. La información está expuesta a diferentes peligros informáticos y personas ajenas a la cadena de información; haciendo de la institución un ente vulnerable frente a estos los peligros.

En relación a los antecedentes y a la problemática de la investigación, es necesario determinar la importancia de la gestion de la seguridad informática y la implementación de la norma ISO/IEC 27001, que nos orientara mediante la aplicación de las políticas de seguridad y controles para mitigar el riesgo de la información en la Escuela Militar de Chorrillos “coronel Francisco Bolognesi” y mitigar el riesgo de la información.

Las secciones de Inteligencia, telemática y cadetes de comunicaciones no son ajenas al riesgo informático que atraviesa la escuela militar, frente a esta problemática se plantea realizar el análisis de la importancia de la gestion de la seguridad informática y la implementación de la norma ISO/IEC 27001 en las oficinas administrativas y cadetes de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”.

1.2.1 Delimitación espacial:

Esta investigación se llevó a cabo en las secciones de Inteligencia, Telemática e instalaciones de la Escuela Militar de Chorrillos coronel “Francisco Bolognesi, ubicada en la Av. Escuela Militar S/N, Municipalidad de Chorrillos, provincia de Lima.

1.2.2 Delimitación temporal:

La presente investigación se llevó a cabo entre marzo y diciembre del 2021, con la recopilación de registros de entrada y salida de electrónicos, bitácoras de seguridad, registro de tránsito de documentos, bitácoras de incidencias de laptops y celulares, registros de ataque a la red, incidencias, vulnerabilidades desde el 2018 a la actualidad.

1.2.3 Delimitación social:

El grupo social objeto de estudio son los responsables de seguridad de las secciones de Inteligencia y Telemática, responsables de tecnologías de información en general y cadetes del arma de comunicaciones de la Escuela Militar de Chorrillos Coronel “Francisco Bolognesi”, sin hacer ninguna diferenciación de grados.

1.3 Formulación del problema

1.3.1 Problema General

¿Cuál es la importancia de la gestión de la seguridad informática y la implementación de la norma ISO/IEC 27001 en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi" - Año 2021?

1.3.2 Problemas Específicos

PE1: ¿Cómo el monitoreo de la red ayuda a identificar los riesgos informáticos en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"?

PE2: ¿Cómo la evaluación de riesgos informáticos permite la mitigación de amenazas informáticas en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"?

PE3: ¿Cómo la aplicación de políticas de seguridad informática permite la protección de los activos informáticos en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"?

PE4: ¿Cómo el monitoreo de la red conlleva a inventariar los activos informáticos en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"?

PE5: ¿Cómo la evaluación de riesgos informáticos favorece el control de riesgos informáticos en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"

PE6: ¿Cómo el uso de políticas de seguridad informática previene las amenazas informáticas en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"?

1.4 Objetivos de la Investigación

1.4.1 Objetivo General

Determinar la importancia de la gestión de la seguridad informática y la implementación de la norma ISO/IEC 27001 en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi" - Año 2021

1.4.2 Objetivos Específicos

OE1: Determinar cómo el monitoreo de la red ayuda a identificar los riesgos informáticos en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"

OE2: Determinar como la evaluación de riesgos informáticos permite la mitigación de amenazas informáticas en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi".

OE3: Determinar cómo la aplicación de políticas de seguridad informática permite la protección de los activos informáticos en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi".

OE4: Determinar como el monitoreo de la red conlleva a inventariar los activos informáticos en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"

OE5: Determinar como la evaluación de riesgos informáticos favorece el control de riesgos informáticos en la Escuela Militar de Chorrillos "coronel Francisco Bolognesi"

OE6: Determinar como el uso de políticas de seguridad informatica previenen las amenazas informáticas en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"

1.5 Justificación e Importancia de la Investigación

La presente investigación busca definir la importancia de la gestión de la seguridad informática y la implementación de la ISO 27001 en la mejora del proceso de gestión de la seguridad informática en un contexto de formación militar, específicamente en la Escuela Militar de Chorrillos coronel "Francisco Bolognesi", identificar los riesgos, efectos de producirse y aplicar medidas y/o políticas para reducirlos a un nivel aceptable como el DS. N° 081-2013-PCM menciona:

> "Garantizar la Integridad, Confidencialidad y Disponibilidad de la información en la Administración Pública mediante mecanismos de la Seguridad de la Información gestionada, así como articular los temas de Ciberseguridad del Estado". (p. 3)

1.5.1 Justificación metodológica

Con la finalidad de conseguir los objetivos de estudio, se utilizó un instrumento validado y confiable, el cual mide el nivel de proceso de gestión del riesgo. Para lo cual se utilizó el instrumento de cuestionario y el procesamiento de las respuestas.

1.5.2 Justificación practica

Debido a la carencia actual de una metodología que nos permita la seguridad informática en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", fue necesario que se realice el inventario de activos de información y el análisis de riesgos, la implantación de controles que sirvieron como protección ante posibles amenazas internas y externas. En tal sentido, se requiere mejorar la seguridad informática a través de la reducción de los niveles de riesgo.

CAPITULO II: MARCO TEÓRICO

2.1 Antecedentes de la Investigación

2.1.1 Antecedentes Internacionales

El uso de instrumentos facilitaría la mejora de la seguridad en la gestión de la información, como determina Santamaría (2014) en su estudio "Manual de seguridad de la información para un organismo del estado Colombiano", donde plantea un manual de seguridad de la información que permite determinar las fortalezas y debilidades de la organización ante la seguridad de información y sus controles a fin de crear estrategias que minimicen las amenazas. La revisión de los aspectos de seguridad permitió dar una valoración de los controles establecidos por la ISO 27001:2013 concluyendo en plantear políticas para que la organización se encuentre en un nivel competitivo y la mejora continua, siempre en el marco legal y normativo.

Rodríguez (2016) realizo un estudio denominado "Diseño y creación de una política de seguridad de la información (SGSI) basado en la normativa ISO 27001 para la cooperativa construcción, comercio y producción", tuvo como objetivo desarrollar un manual de políticas de seguridad de la información aplicando los controles de la ISO 27002 para la Cooperativa de ahorro y crédito Construcción, Comercio y Producción. Aplicó la norma ISO 27000 en las políticas de seguridad para la Cooperativa de ahorro y crédito construcción, comercio y producción (COOPCCP) en Quito y notó una gran diferencia del comportamiento del personal antes de aplicar las políticas de seguridad y al final de estas, los profesionales designados como líderes de procesos manejaban actividades extras como el control de accesos y permisos en plataformas web.

Otro estudio de Camargo (2017) denominado "Diseño de un sistema de gestión de la seguridad de la información (SGSI) en el área tecnológica de la comisión nacional del servicio civil - CNSC basado en la norma ISO27000 e ISO 27001" tuvo como objetivo asegurar, mantener la total confidencialidad de

la información que maneja, recibe y guarda en la entidad, evitando la posible pérdida por las amenazas del medio. La gestión de la seguridad de la información aplicando la norma ISO 27000 e ISO 27001 en las tecnologías de la Comisión Nacional del Servicio Civil (CNSC) en Bogotá D.C, utilizo la metodología de Magerit V.3, para el análisis de riesgos donde se detectó los activos críticos y el impacto que se originan en la entidad. La aplicación de la norma ISO/IEC 27001 permitió identificar que el CNSC se encuentra en alto riesgo por falta de controles, la falta de prácticas del recurso humano y la falta de una política de seguridad aprobadas por los directivos que garantice la implementación y cumplimiento.

La estructuración de un sistema de seguridad aplicando la norma NTC/ISO 27001 fue realizada por León (2018), ante un operador logístico en Bogotá D.C., se implementó políticas que contribuyen a preservar los principios de confidencialidad, integridad y el interés del personal por la seguridad de la información. Se realizó un diagnóstico de la norma ISO/IEC 27001 y se identificó que la organización cumple con 49% de controles de seguridad y los 51% restantes requiere de políticas, procedimientos, actividades y asignación de recursos para que la compañía crezca. La aplicación de una matriz de riesgos y una lluvia de ideas se identificaron los riesgos que afectan a la organización, riesgos de carácter tolerables y 5 de carácter inaceptables, para ello se estableció un tratamiento de riesgos de acuerdo a las necesidades.

La “Importancia de la norma ISO/EIC 27000 en la implementación de un sistema de gestión de la seguridad de la información” fue un estudio realizado por Regina, Mendoza, & Joel (2019) en México, donde concluye que la Implementación de un Sistema de Gestión de Seguridad de la Información debe ser estricta y metódica por cualquier empresa para garantizar la confiabilidad, disponibilidad e integridad de sus activos importantes. Para llegar a esto es necesario del apoyo de la norma ISO/EIC 27000 a fin de garantizar un marco de trabajo y administración de la seguridad de la información.

2.1.2 Antecedentes Nacionales

La investigación titulada “Factores que afectan la implementación del Sistema de Gestión de Seguridad de la Información en las Entidades Públicas Peruanas de acuerdo a la Norma Técnica Peruana NTP-ISO/IEC 27001” realizada por Seclén (2016), buscó estrategia adecuada para la recopilación de información e identificar las restricciones y facilidades que encuentran las entidades públicas y permitan la seguridad de información del sistema nacional de informática, concluyendo que, la falta de Política Estratégica de Estado, el desarrollo integral de la NTP (Normas Técnicas Peruanas), presupuesto y especialización de profesionales son los factores que afectan la implementación del Sistema de Gestión de Seguridad de la información en las entidades públicas peruanas.

La inclusión de un sistema web para la seguridad de información tuvo lugar en el estudio realizado por Aguirre (2018) para “ Implementación de un Sistema Web para la gestión de la seguridad de la información alineada a la norma ISO/IEC 27001 en una empresa de Servicios Informáticos S.A.C – La Molina” tuvo como resultado un efecto positivo para la gestión de la seguridad de la información teniendo como indicador el porcentaje de reportes entregados a tiempo y porcentaje de reportes íntegros generados.

“La aplicación de la ISO 27001 y su influencia en la seguridad de la información de una empresa privada peruana” fue un estudio realizado por Rodriguez, Cruzado, Mejía, & Alarcón (2020), donde tuvo como objetivo analizar la influencia de la norma ISO 27001 en la seguridad de la información aplicada a una empresa privada en Lima (Perú), demostrando que la norma ISO 27001 tuvo un influencia en la seguridad de la información, privacidad, integridad y disponibilidad en dicha empresa.

García (2020) en su estudio “Propuesta de un sistema de gestión de seguridad de la información basado en la norma ISO 27001 para la oficina de tecnologías de información del Gobierno Regional Piura; 2020”, el desarrollo de su investigación a los trabajadores del Gobierno Regional de Piura muestra

insatisfacción en la situación actual de la gestión en la información del Gobierno Regional de Piura y manifiesta la necesidad de contar con un sistema de gestión de seguridad de la información basado en la norma ISO 27001 a fin de preservar la confidencialidad, integridad y disponibilidad de la información en la oficina de tecnologías de información del Gobierno Regional Piura.

Otro estudio basado en la influencia de la ISO 27001:2013 en una municipalidad del Perú realizado por Bustamante, Valles, Cuellar, & Lévano (2021) aplicó una encuesta a los trabajadores de la municipalidad antes y después de la norma ISO 27001:2013, evidenciando que las políticas de seguridad de la información influyeron positivamente en la gestión de la seguridad de la información dentro de la Subgerencia de Recaudación y Fiscalización Tributaria de la Municipalidad Distrital de Morales.

2.2 Bases Teóricas

2.2.1 Base Teórica (Variable Independiente)

2.2.1.1 Gestión de la seguridad informática

Según Solarte et al., (2015).

La seguridad de la información o informática se relaciona los procesos, metodologías y procedimientos para proteger la información o datos confidenciales de una institución.

Estos procesos se construyen con ayuda de los estándares de calidad, protocolos, normas y metodologías para minimizar el riesgo de ante las amenazas de la infraestructura tecnológica. (p. 407)

La seguridad de la información seria definida según ISACA (2012, como se citó en Aburto, 2020.) al “asegurar que, dentro de la empresa, la información está protegida contra su divulgación a usuarios no autorizados

(confidencialidad), modificación inadecuada (Integridad) y su falta de acceso cuando se la necesita (disponibilidad)" (p. 17) .

En otro sentido la seguridad informativa tiene como objetivo garantizar, que los documentos, registros y archivos informáticos mantengan especial confiabilidad (Voutssas, 2010). La empresa y/u organización debe mantener principios informáticos que ayudaran a mantener una buena gestión de la información.

Según Gónzáles (2014) menciona los principios de confidencialidad, integridad y disponibilidad, llamada también CID. El autor define los siguiente:

- **Confidencialidad:** Es la reserva de la información de una determinada infraestructura tecnología que maneja una institución; para esto se usa herramientas que protegen el sistema de posibles amenazas.
- **Integridad**: Es la eficacia y seguridad de los elementos de la información que se encuentran almacenados en un sistema informático, en otro sentido las herramientas del sistema deben prestar la seguridad en el proceso de la información, de forma que no duplique los datos.
- **Disponibilidad:** se refiere a la presencia constante de la información almacenada en un procesador informáticos; esta herramienta permite el acceso de los datos a la medida y frecuencia que lo requiera. (p. 11)

2.2.1.2 Monitoreo de la red

Para Barrera (2009) "El monitoreo de la red inalámbrica comienza seleccionando la interfaz de red que desea monitorear. La selección de la interfaz correcta de red es fundamental para lograr los resultados de monitoreo deseados" (pg., 42).

Esquema del funcionamiento de la red inalámbrica

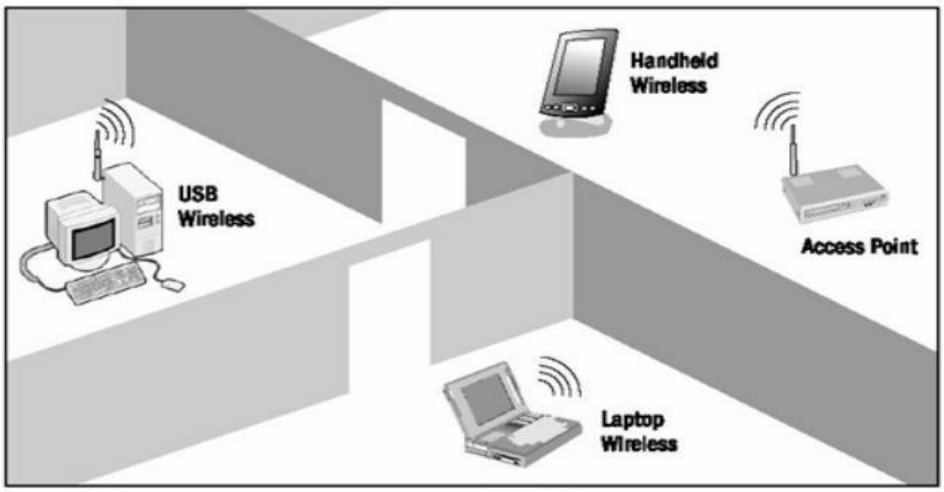

Figura 1: Esquema del funcionamiento de la red inalámbrica
Fuente: Tomado de Barrera, 2009

Una red de computadoras, también llamada red de ordenadores o red informática, es un conjunto de equipos informáticos conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información y recursos, y ofrecer servicios, (Duran, 2016) (p, 14).

Los métodos para el monitoreo y filtrado de información considerados para Barrera (2009) son las siguientes:

- **Filtrado de direcciones MAC:** Las direcciones MAC (Media Access Control) es contenida en una tarjeta de red inalámbrica y que se puede conectar a un punto de acceso.
- **Wired Equivalent Privacy (WEP):** El algoritmo WEP forma parte de la especificación 802.11, tiene la función de proteger la información que se comunican en una conexión inalámbrica mediante cifrado. WEP opera a nivel 2 del modelo OSI y es acogido para dar soluciones inalámbricas usado por muchos fabricantes.
- **Las VPN:** Una red privada virtual (Virtual Private Network, VPN) tiene como método el cifrado que consiste en crear un canal virtual privado en una red de uso público. Las VPN son muy conveniente para proteger redes inalámbricas, debido a la

función que ejerce sobre cualquier tipo de hardware inalámbrico y destacan las limitaciones de WEP.

- **802.1x:** Es un protocolo de control de acceso y autenticación basado en la relación del cliente y servidor; este sistema registra la conexión de equipos no autorizados a una red. Inicialmente el protocolo 802.1x fue creado para el uso de redes locales alambradas, pero posteriormente fue extendida a las redes inalámbricas.
- **WPA (WI-FI Protected Access):** WPA es propuesto por los miembros de la Wi-Fi para rectificar los problemas de WEP, de forma que mejora el cifrado de los datos y ofrece un dispositivo de autenticación. Para solucionar el problema de cifrado de los datos, WPA propone un nuevo protocolo para cifrado, conocido como TKIP (Temporary Key Integrity Protocol). Este protocolo se encarga de cambiar la clave compartida entre punto de acceso y cliente cada cierto tiempo, para evitar ataques que permitan revelar la clave. Igualmente se mejoraron los algoritmos de cifrado de trama y de generación de los IVs, con respecto a WEP.

2.2.1.3 Evaluación de riesgos informáticos

Según Solarte et al., (2015) en su investigación "Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001" menciona:

La evaluación de riesgos del sistema de información, la revisión de la existencia de controles de seguridad y por último el monitoreo integral de los sistemas de información nos permiten establecer el estado de una organización e identificar las causas de vulnerabilidad y proponer las soluciones de control y minimizar el riesgo.

La evaluación permite un adecuado diseño, implementación y creación de un Sistema de Gestión de Seguridad de la Información - SGSI en función al

ISO/IEC 27001, capaz de intervenir en la vulnerabilidad, amenazas y riesgos de la información que se encuentra expuesta la organización. Para que la protección de la información y una adecuada función de la gestión de la seguridad de la información es importarte la participación del todo el personal de la institución. Toda labor debe tener un proceso lógico, sistemático, documentado, que pueda ser propagado internamente para que la gestión sea eficiente y tener una correcta seguridad informática y de la información, considerando el ciclo de mejora continua (planear, hacer, verificar y actuar - PHVA). (p, 493)

2.2.1.4 Políticas de seguridad informática

"Las políticas son requisitos generalizados que deben ser escritos en papel y comunicados a ciertos grupos de personas dentro y en algunos casos fuera de la organización" (Dussan, 2006, p.88).

Los elementos de la seguridad

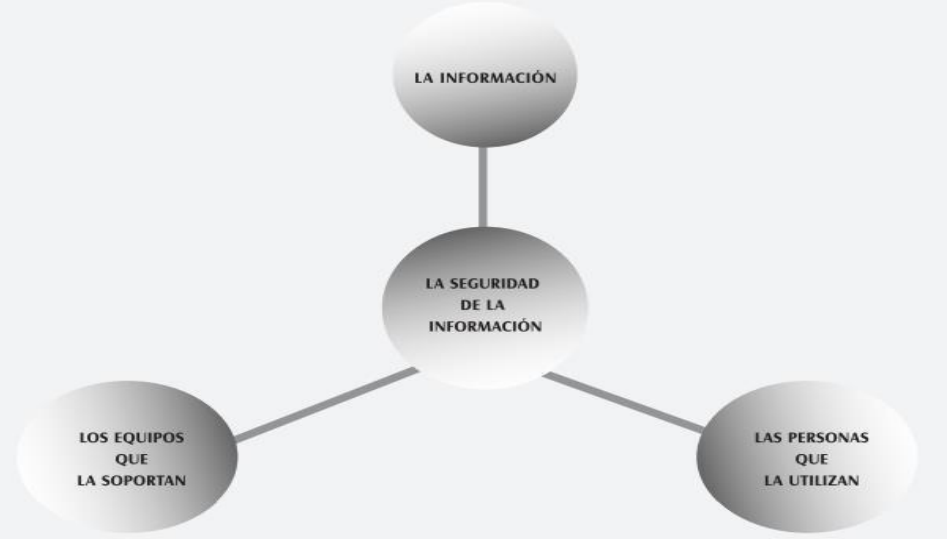

Figura 2: Los elementos de la seguridad
Fuente: Tomado de Dussan, 2006.

A. Control de acceso

Según la guía de la "Elaboración de la política general de seguridad y privacidad de la información" del MINTIC, (2016), hace referencia los mecanismos de protección, frente a la administración y responsabilidad en relación al acceso de la información, las políticas de deben ser coherentes con el control de acceso mínimo:

- **Control de acceso con usuario y contraseña:** Se busca implementar una política de control al acceso al sistema de información, para ello se debe identificar a los responsables del procedimiento de creación, modificación, suspensión o eliminación de usuarios (ID) y contraseñas. Las políticas de la empresa o entidad deben orientar a los funcionarios, contratistas o terceos las responsabilidades que tienen al obtener un usuario (ID) y una contraseña deben ser estrictamente personales e intransferibles.
- **Suministro del control de acceso:** La propuesta de implementar políticas que determinen los procedimientos para la modificación, revisión, revocación de derechos o privilegios que tiene los usuarios (ID) en una institución al ser identificados como amenazas a un proceso adecuado de gestión de la seguridad.
- **Gestión de Contraseñas:** Esta política consiste en el uso de restricciones en la calidad que debe tener las contraseñas como mecanismo de autenticación para el acceso a la red, aplicaciones o el sistema de información de la entidad. Se debe difundir de esta política a los funcionarios, contratistas o terceros de las condiciones mínimas que debe tener una contraseña para un acceso seguro al sistema de información de la entidad.
- **Perímetros de Seguridad:** Esta política condiciona los perímetros físicos de seguridad para acceder a la información en la entidad, los responsables de autorizar el acceso deben

sustentar la identificación oportuna de los funcionarios, contratistas o terceros en las instalaciones de la entidad.

- **Áreas de Carga:** Esta política plantea las restricciones a las instalaciones físicas de despacho y carga de paquetes de la institución para prevenir el acceso no autorizado a otras áreas de la entidad. Esta política determina el rastreo de los usuarios en la instalación a fin garantizar la seguridad de la información. (p. 19).

B. No repudio

La política de seguridad y privacidad comprende la capacidad de no repudio tomando las siguientes acciones:

- **Trazabilidad:** La política consiste en el seguimiento a la creación, origen, recepción, entrega de información y otros.
- **Retención:** Se debe incluir en la política de seguridad el periodo de retención o almacenamiento, que son las acciones los usuarios, esta condición debe ser informada a los funcionarios, contratistas y/o terceros de la Entidad.
- **Auditoría:** Este proceso debe ser incluido en las políticas para constatar el buen procedimiento de las partes implicadas durante el acceso a la información de la entidad.
- **Intercambio electrónico de información:** La política incluirá el intercambio de información de forma electrónica como garantía de no repudio. (p. 20)

A. Privacidad y confidencialidad

Esta política debe contener tratamiento y protección de datos personales.

- **Principios del tratamiento de datos personales:**
  - **Principio de la Legalidad:** El otorgar los datos personales a la entidad se debe manejar con la debida legalidad según las normativas vigentes.

- **Principio de finalidad:** La finalidad del porque se debe otorgar los datos personales debe ser informada al titular.
- **Principio de libertad:** La proporción de los datos personales debe ser con el consentimiento anticipado y debidamente informado del titular de los datos.
- **Principio de veracidad o calidad:** La información que otorga el titular debe ser veraz, completa, exacta, actualizada, comprobable y comprensible.
- **Principio de transparencia:** Certificar al titular de los datos que la obtención de la información sea lo solicitado.
- **Principio de acceso y circulación restringida:** el acceso de a la información solo será por el solicitante y no realizará la propagación a individuos no autorizados.
- **Principio de seguridad:** La información obtenida por el usuario deben ser manejadas con las medidas físicas, humanas y administrativas que sean necesarias para garantizar la seguridad impidiendo su adulteración, pérdida, acceso no autorizado o fraudulento.
- **Principio de confidencialidad:** todo usuario que accede o proporcione sus datos debe garantizar la reserva de dicha información.

- **Derechos de los titulares:** La política debe indicar los derechos de los titulares de los datos, tales como:
  - Saber, renovar y corroborar sus datos personales.
  - Autorización para el manejo de los datos personales del usuario.
  - Proporcionar información al usuario respecto al uso de los datos personales.
  - Acceso del titular para suspender los datos personales de la base de datos del sistema cuando lo solicite.

- Reportar insatisfacción y sugerencias del titular hacia la admiración encargada de la protección de los datos personales.

- **Autorización del titular:** Las políticas de seguridad deben contener términos que permiten autorizar el tratamiento de la información personal del titular de la misma forma cuando no se requiere la autorización.
- **Deberes de los responsables del Tratamiento:** en los lineamientos de las políticas de seguridad se debe precisar los deberes del responsable del manejo de los datos personales en la entidad.
- **Política de controles criptográficos:** Esta política consiste en especificar el tipo de seguridad, confidencialidad y autenticidad de la información en la gestión de los diferentes sistemas de información.

B. Integridad

La información debe ser conocida y aceptada por todos los funcionarios, contratistas y/o terceros de la Entidad, el manejo de la información debe ser íntegro e integral tanto interna como externa, conocida o administradas por los mismos. Toda información verbal, física o electrónica debe ser adoptada, procesada y entregada íntegramente a las personas correspondientes. (p. 21).

C. Disponibilidad del servicio e información

La política de disponibilidad debe contener los siguientes pasos:

- **Niveles de disponibilidad:** Debe hacer cumplir la disponibilidad del servicio e información acordados con los usuarios, clientes, proveedores de acuerdo a las necesidades que requieran.
- **Planes de recuperación:** Se debe incluir los planes de recuperación de la información en las políticas de seguridad, para cumplir con las necesidades que requiere la entidad.

- **Interrupciones:** Las políticas de gestión de la seguridad debe contemplar las interrupciones en el mantenimiento de los servicios que afecten la disponibilidad del mismo.
- **Acuerdos de Nivel de servicio:** Se debe tener en cuenta las consideraciones de los niveles de servicio ante las interrupciones.
- **Segregación de ambientes:** Se debe entender que la información debe estar ordenada en ambientes para minimizar el nivel de riesgo y minimizar el impacto de la disponibilidad del servicio durante las fases de desarrollo, pruebas y producción.
- **Gestión de Cambios:** en las políticas de seguridad se debe considerar la gestión de cambios para que los procesos de producción afecten mínimamente en la disponibilidad y se manejen en condiciones controladas. (p. 22).

D. Registro y auditoria

Esta política cuida por el sustento de las evidencias de las actividades y acciones que afectan los activos de información.

- **Responsabilidad:** La Oficina de Control Interno tiene la responsabilidad de dirigir auditorias periódicas a los sistemas de información y posteriormente de informar de dichos resultados.
- **Almacenamiento de registros:** En las políticas de seguridad se debe proponer un registro de copias de la base de datos como media de seguridad para el correcto funcionamiento; en dichas copias se debe contener también un registro de auditorías internas.
- **Normatividad:** las políticas de seguridad deben ser cumplidas y las auditoria debe garantizar dicho cumplimiento según el reglamento de la entidad.
- **Garantía cumplimiento:** La política de auditoría debe garantizar el cumplimiento de los controles, la eficiencia de los sistemas, el control de las políticas o reglamentos y procedimientos de la entidad.

- **Periodicidad:** Se debe garantizar la revisión periódica de los niveles de riesgos al que se enfrenta la entidad estas medidas deben estar plateadas en las políticas de seguridad y constatadas mediante auditorias. (p. 23)

2.2.2 Base Teórica (Variable Dependiente)

2.2.2.1 Implementación de la norma ISO/ IEC 27001

Según Montaño (2011), refiere a las normas ISO/IEC 27000 como:

> Estándares en la fase de desarrollo por la ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), focalizadas a gestionar la seguridad de la información para cualquier tipo de organización (p.22).

Según Solarte, Enriquez, & Benavides (2015) menciona que:

Las normas ISO/IEC 27001 y la ISO/IEC 27002 detallan las obligaciones que debe tener una organización para implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de la Seguridad Interna (GSI), también menciona la forma de implementación de los controles de seguridad hacia las necesidades de una organización (p. 494)

2.2.2.2 Riesgo informático

Según Santana (2012, mencionado en Quiroz, 2017) "El riesgo es la posibilidad de que una amenaza se produzca, dando lugar a un ataque al equipo" (p. 685).

Otro autor menciona los riesgos informáticos como problemas potenciales, que inquietan a los sistemas de información y al equipo de cómputo, el riesgo se puede presentar por las vulnerabilidad y amenaza, (Solarte et al., 2015).

2.2.2.3 Amenaza informática

La amenaza informática se manifiesta por sucesos no deseados que pueden perturbar los insumos informáticos al punto de dañarlos (Voutssas, 2010).

De debe tomar en cuenta los recursos informáticos donde se puede originar la amenazas, según Gónzáles (2014) son:

1. HARDWARE: Es el conjunto de instrumentos tangibles de un procesador informático.
2. SOFTWARE: Es el conjunto de programas o procesadores intangibles del ordenador informático.
3. DATOS: Conjunto de información almacenada en el ordenador informático.
4. PERSONAS: Conjunto de individuos que hacen uso del sistema de información.
5. DOCUMENTACIÓN: Conjunto de hojas o páleles con información tanto físicos como informático.
6. SUMINISTROS: conjunto de materiales o herramientas que ayudan a evidenciar o almacenar la información. (p. 10)

2.2.2.4 Activos Informáticos

Según Aliaga, (2013 citado por Leiva, 2016) el estándar ISO 27005, se pueden identificar dos tipos de activos: los primarios y los de soporte. Los primarios, según este estándar, son los procesos e información más sensibles para la organización. Los activos de soporte, son los activos que dan el debido soporte a estos activos primarios.

Para Sotelo, Torres, & Rivera, (2012) activos de información son los Servicios Tecnología de Información (TI) formado por un conjunto de activos TI como se muestra en la siguiente tabla.

Tabla 1: Clasificación de activos de información

Categoría de activos de información		
Identificador	Condición	Ejemplos
STI	Servicios TI	Aplicación más infraestructura de la Tecnología de la Información de soporte
SW	Software / Aplicaciones	Conformada por aplicaciones, herramientas de desarrollo, sistemas operativos, y utilitarios
	Hardware / equipos	Servidores (S.O.), PCs, routers, hubs, firewalls, USB, medio magnético, gabinetes, cajas fuertes, salas, mobiliario, sistema de alarma, etc.
	Soportes de información	SAN, discos, cintas, USB, CD, DVD.
	Redes de comunicaciones	Medios de transporte que llevan datos de un sitio a otro
	Datos / Información	BD, archivos de datos, contratos y acuerdos, documentación del sistema, información de investigación, manuales de usuario, material de entrenamiento, de operación, procedimientos de soporte, planes de continuidad y contingencia, acuerdos
	Equipamiento auxiliar	Equipamiento de soporte a los sistemas de información (UPS, Generados, Aire acondicionado, cableado, etc.)
	Locales / Instalaciones	Lugares donde se hospedan los sistemas de Información, registros vitales y comunicaciones
	Personal / RR.HH.	Personas, calificaciones, experiencia y capacidades (usuarios, proveedores, personal de TI)
	Productos generales	Vigilancia, servicios de impresión, computación, telecomunicaciones, eléctrica, agua, etc.

2.3 Marco Conceptual

- **ISO/IEC:** (International Organization for Standardization) e IEC (International Electrotechnical Commission).
- **Gestión:** Gestión es la acción y el efecto de gestionar y administrar. De una forma más específica, una gestión es una diligencia, entendida como un trámite necesario para conseguir algo o resolver un asunto, habitualmente de carácter administrativo o que conlleva documentación
- **Seguridad:** Ausencia de peligro o riesgo
- **Informática:** Conjunto de conocimientos técnicos que se ocupan del tratamiento automático de la información por medio de computadoras.
- **Riesgo:** Posibilidad de que se produzca un contratiempo o una desgracia, de que alguien o algo sufra perjuicio o daño.
- **Política:** Arte o traza con que se conduce un asunto o se emplean los medios para alcanzar un fin determinado.
- **Aceptación de riesgo:** Informada decisión de tomar un riesgo en particular, la aceptación del riesgo puede ocurrir sin, con o durante el proceso de tratamiento del riesgo.
- **Evaluación de riesgos:** Es el procedimiento para la identificación del riesgo, el análisis de riesgos y la evaluación del riesgo.
- **Criterios de riesgo:** Se basan en los objetivos de la organización, y el medio externo e interno. Los criterios de riesgo pueden derivarse de las normas, las leyes, las políticas y otros requisitos.
- **Identificación de riesgos:** Identificación de riesgos consiste en la identificación de las fuentes de riesgo, eventos, sus causas y posibles consecuencias. La Identificación de riesgos puede implicar datos históricos, análisis teórico, informados y opiniones de expertos, y las necesidades de las partes interesadas.
- **Gestión de riesgos:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.
- **Procesos de gestión de riesgos:** Consiste en el seguimiento de las políticas de gestión, las prácticas y procedimientos de las distintas actividades de

comunicación, consultorías, auditorias, tratamientos y revisión del riesgo en la institución.

- **Tratamiento de riesgos:** Consiste en realizar diferentes políticas y actividades para minimizar el riesgo.
- **Activo de Información:** Es cualquier tipo de información con un gran valor para la institución, sea sus servidores, instalaciones, sus redes etc. de la misma forma que es susceptible a cualquier amenaza.
- **Amenaza:** Es una situación poco conveniente que puede ocasionar un riesgo, la amenaza siempre es desfavorable para la institución que incurre a pérdidas del valor o inadecuado funcionamiento del sistema. La amenaza puede tener causas naturales, accidental o intencionada, si esto ocurre a la vez que existe una vulnerabilidad en el sistema puede ocasionar un incidente de seguridad.
- **Control de acceso:** Los medios para garantizar que el acceso a los activos está autorizado y restringidas en base a los requerimientos del negocio y de seguridad.
- **Análisis de riesgos:** Es un procedimiento de identificación de medios vulnerables y de amenazas en el sistema informativo al que se expone una institución.
- **Confidencialidad:** Es la garantía de la protección de la información al cual solo debe ser manejado únicamente por el personal autorizado.
- **Incidente de seguridad:** Son sucesos que afectan la confidencialidad, integridad o disponibilidad de los activos de información de la empresa.
- **Integridad:** La garantía del transporte, almacenamiento o destrucción de información de un medio a otro sin ocasionar pérdidas o copias clandestinas.
- **Plan de contingencia:** Es una estrategia planificada con respaldo de un conjunto de recursos que se aplican ante la ocurrencia de amenazas esta debe ser plasmada en un Plan de Contingencia de las Tecnologías de la Información y las Comunicaciones (TIC).
- **Plan de continuidad:** Es un conjunto de planes de emergencia, financieros, de comunicación y contingencias para mitigar el impacto provocado por los riesgos informático y los procesos de negocio de una compañía.

- **Política de seguridad:** Son todas las decisiones o medidas de seguridad que una empresa requiere para la seguridad del sistema de información, debe ser de carácter normativo y documentado.
- **Protocolo:** Es un conjunto de reglas o procedimientos que permiten la comunicación de dos instituciones a fin de trasferir información.
- **Servidor:** Es un conjunto de herramientas digitales y físicas que permiten la trasferencia de información.
- **Sistema de Gestión de la seguridad de la Información (SGSI):** Son un conjunto de políticas de seguridad de la información que siguen la norma ISO/IEC 27001. Un SGSI proporciona un conjunto de procesos para gestionar de forma eficientemente la accesibilidad de la información, garantizando la confidencialidad, integridad y disponibilidad de los activos de información de tal forma que se minimicen los riesgos.
- **Vulnerabilidad:** Son las fallas y deficiencias de un programa que permiten el acceso de la información a un individuo no autorizado. Las fallas o también conocidas como agujeros de seguridad pueden ser aprovechadas por bandidos mediante exploits, para acceder a los sistemas con fines maliciosos.

CAPITULO III: HIPÓTESIS Y VARIABLES

3.1 Hipótesis General

La gestión de la seguridad informática y la implementación de la norma ISO/IEC 27001 es de alta importancia en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi" - Año 2021.

3.2 Hipótesis Especificas

H1: El monitoreo de la red ayuda a identificar significativamente los riesgos informáticos en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"

H2: La evaluación de riesgos permite significativamente la mitigación de amenazas informáticas en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi".

H3: La aplicación de políticas de seguridad informática permite significativamente la protección de los activos informáticos en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi".

H4: El monitoreo de la red conlleva a inventariar los activos informáticos para protegerlos significativamente en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"

H5: La evaluación de riesgos informáticos favorece significativamente el control de riesgos informáticos en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"

H6: El uso de políticas de seguridad informática previenen significativamente las amenazas informáticas en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"

3.3 Definición Conceptual y Operacional de Variables

Definición conceptual

Gestión de seguridad Informática

Según Solarte et al., (2015). La seguridad de la información o informática se relaciona los procesos, metodologías y procedimientos para proteger la información o datos confidenciales de una institución.

Definición Operacional

Está compuesta por las dimensiones monitoreo de la red, evaluación de riesgos informáticos y políticas de seguridad informática.

Definición conceptual

Implementación de la norma ISO/TEC 27001

Según Montaño (2011), refiere a las normas ISO/IEC 27000 como:

Estándares en la fase de desarrollo por la ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), focalizadas a gestionar la seguridad de la información para cualquier tipo de organización (p.22).

Definición operacional

Está compuesta por las dimensiones riesgos informáticos, amenazas informáticas y activos informáticos.

3.4 Cuadro de Operacionalización de Variables

Variables	Dimensiones	Indicadores	Ítems	Escala
Gestión de Seguridad Informática	Monitoreo de la Red	-Panel de control	1,2	1.-Estoy totalmente en desacuerdo 2.-No estoy de acuerdo 3.-Estoy de acuerdo 4.-Estoy totalmente de acuerdo
	Evaluación de riesgos informáticos	-Identificación de riesgos informáticos	3,4	
	Políticas de seguridad informática	-Medidas de seguridad informáticas	5,6	
Implementación de la Norma ISO/TEC 27001	Riesgos Informáticos	-Riesgos de acceso	7,8	
	Amenazas informáticas	-Amenazas lógicas	9,10	
	Activos informáticos	-Activos de información	11,12	

CAPITULO IV: MARCO METODOLÓGICO

4.1 Método de estudio

El método que se utilizo es hipotético – deductivo, procedimiento que va a partir de una hipótesis sustentada por el desarrollo teórico de una determinada ciencia, siguiendo las reglas lógicas de la deducción, permite a llegar a nuevas conclusiones y predicciones empíricas, las que a su vez son sometidas a verificación.

Según Guanipa (2010), el método hipotético – deductivo, es el conjunto de teorías y conceptos básicos, elaborando en forma deductiva las consecuencias empericas de las hipótesis, y tratar de farsearla para reunir la información pertinente. Por tanto, busca la solución a los problemas planteados. De igual manera según Bernal (2006), el método consiste en un procedimiento que parte de unas aseveraciones en calidad de hipótesis y busca reclutar o falsear tales hipótesis deduciendo de ellas con conclusiones las cuales deben confrontarse con los hechos. En tal sentido el método hipotético – deductivo llega a unas conclusiones a través de un procedimiento de inferencia o calculo formal.

4.2 Enfoque de la Investigación

El enfoque que se utilizó es Cuantitativo donde se “utiliza la recolección y el análisis de datos para contestar una o varias preguntas de investigación y probar las hipótesis establecidas previamente” (Vega et al., 2014, p 525).

4.3 Tipo de Investigación

El tipo de investigación es básica dado que aporta elementos teóricos al conocimiento científico, sin la intención de su corroboración directa e inmediata.

4.4 Nivel y Diseño de la Investigación

Esta investigación tiene un nivel descriptivo explicativo, porque busca enfatizar las propiedades, características y los perfiles importantes de personas, grupos, comunidades, así como el principal propósito de realizar estudios de tipo explicativo es conocer el comportamiento de la variable independiente sobre la dependiente, es decir causa efecto. Hernández (2014). La investigación tuvo un diseño no experimental, ya que el investigador se restringe a observar los sucesos sin intervenir en ellos.

4.5 Técnicas e Instrumentos para la recolección de datos

Se utilizó como técnica la encuesta mediante formularios online para conocer el nivel de conocimiento de la gestión de la seguridad informática y la implementación de la norma ISO/IEC 27001. Además, se empleó como instrumento el cuestionario que les fueron aplicados a los responsables de las secciones de Telemática e Inteligencia y cadetes del arma de comunicaciones de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi".

4.6 Población y Muestra

A. Población: Está representada por 84 miembros que laboran en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"; 8 individuos en la sección de Telemática, 9 individuos en la sección de Inteligencia y 67 cadetes del arma de comunicaciones.

B. La Muestra: En este estudio se consideró una muestra censal, fue seleccionada el total de 84 individuos.

CAPITULO V: INTERPRETACIÓN, ANALISIS Y DISCUSIÓN DE LOS RESULTADOS

5.1 Análisis Descriptivo

5.1.1 Análisis de los Indicadores

OBJETIVO 1: Determinar cómo el monitoreo de la red ayuda a identificar los riesgos informáticos en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"

Al inicio de la investigación se desconocía como el monitoreo de la red ayudaba a identificar los riesgos informáticos, posterior a la investigación se determinó que se da mediante el uso de un sistema que busca vulnerabilidades y problemas en la red, como los riesgos informáticos, para luego remitirlos a los responsables de la sección de telemática.

OBJETIVO 2: Determinar como la evaluación de riesgos informáticos permite la mitigación de amenazas informáticas en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi".

Al inicio de la investigación se desconocía como la evaluación de riesgos informáticos permitía mitigar amenazas, posterior a la investigación se determinó que se da mediante la identificación de activos informáticos, vulnerabilidades y la probabilidad de incidencia de riesgos informáticos, de esta manera los responsables de la sección de telemática evalúan y planifican medidas para la mitigación de amenazas mediante un firewall de Fortinet.

OBJETIVO 3: Determinar cómo la aplicación de políticas de seguridad informática permite la protección de los activos informáticos en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi".

Al inicio de la investigación se desconocía como la aplicación de políticas de seguridad informática permitían la protección de los activos informáticos, posterior a la investigación se determinó que las políticas de seguridad informática en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi" no estaban basadas en un estándar de seguridad ISO, sin embargo la responsables de la sección de telemática establecieron normativas, compromisos de seguridad informática, procedimientos, instrucciones y directrices con la finalidad de dar protección a los activos informáticos identificados.

OBJETIVO 4: Determinar como el monitoreo de la red conlleva a inventariar los activos informáticos en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"

Al inicio de la investigación se desconocía como el monitoreo de la red conllevaba a inventariar los activos informativos, posterior a la investigación se determinó que los responsables de la sección de telemática durante el monitoreo de la red encontraban amenazas y vulnerabilidades, por ello procedieron a identificar, clasificar y mantener los activos informáticos más importantes mediante un inventario, permitiéndoles establecer medidas de protección ante futuros incidentes.

OBJETIVO 5: Determinar como la evaluación de riesgos informáticos favorece el control de riesgos informáticos en la Escuela Militar de Chorrillos "coronel Francisco Bolognesi"

Al inicio de la investigación se desconocía como la evaluación de riesgos informáticos favorecía el control de riesgos informáticos, posterior a la investigación se determinó que la evaluación de riesgos informáticos permitía a los responsables de la sección de telemática identificar la probabilidad de incidencias informáticas favoreciendo eficientemente el control de los riesgos informáticos más posibles, permitiéndoles estar alertas ante una amenaza que afecte la seguridad de los activos informáticos.

OBJETIVO 6: Determinar como el uso de políticas de seguridad informática reducen las amenazas informáticas en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"

Al inicio de la investigación se desconocía como el uso de políticas de seguridad informática reducían las amenazas informáticas, posterior a la investigación se determinó que las políticas de seguridad informática permitían a los encargados de la sección de telemática proveer a los usuarios de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", la dirección y soporte administrativo en relación a los recursos y servicios informativos dentro de las instalaciones, de esta manera se redujeron considerablemente las amenazas informáticas durante el año con relación a los años anteriores.

5.1.2 Análisis de los Instrumentos

Se aplicó una encuesta de 12 preguntas relacionada a las variables de nuestra investigación a una muestra de 84 individuos, se muestra el siguiente resultado para cada pregunta planteada.

Tabla 2: Pregunta 1 ¿Considera usted que es importante la gestión de la seguridad informática en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Estoy en total desacuerdo	8	9.5	9.5	9.5
	No estoy de acuerdo	3	3.6	3.6	13.1
	Estoy de acuerdo	45	53.6	53.6	66.7
	Estoy totalmente de acuerdo	28	33.3	33.3	100.0
	Total	84	100.0	100.0	

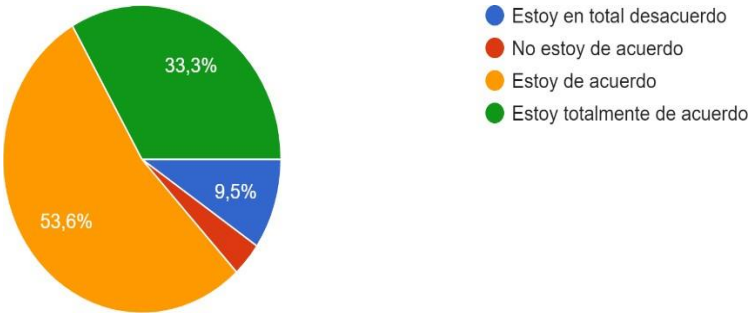

Figura 3: Distribución de respuestas a la pregunta ¿Considera usted que es importante la gestión de la seguridad informática en la escuela militar de chorrillos "Coronel Francisco Bolognesi"?

Se analizaron los resultados y se determinó que el 33.3% está totalmente de acuerdo, el 53.6% está de acuerdo, el 3.6% no está de acuerdo y el 9.5% está en total desacuerdo, con respecto a la importancia de la gestión de la seguridad informática en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi".

Tabla 3: Pregunta 2 ¿Cree usted que el permanente monitoreo de la red ayuda a mantener una red segura en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Estoy en total desacuerdo	3	3.5	3.5	3.5
	No estoy de acuerdo	12	14.3	14.3	17.8
	Estoy de acuerdo	47	56	56	73.8
	Estoy totalmente de acuerdo	22	26.2	26.2	100.0
	Total	84	100.0	100.0	

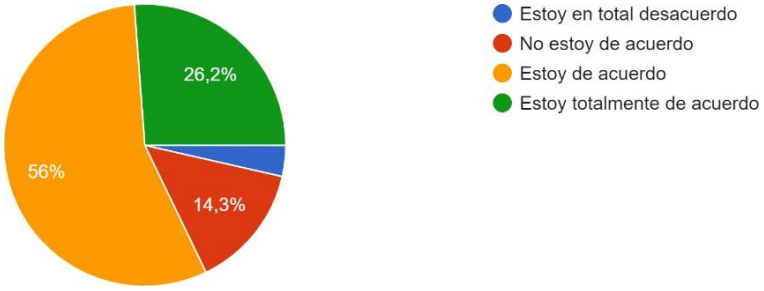

Figura 4: Distribución de respuesta a la pregunta ¿Cree usted que el parmente monitoreo de la red ayuda a mantener una red segura en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"?

Se analizaron los resultados y se determinó que el 26.2% está totalmente de acuerdo, el 56% está de acuerdo, el 14.3% no está de acuerdo y el 3.6% está en total desacuerdo, con respecto a que el permanente monitoreo de la red ayuda a mantener una red segura en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi".

Tabla 4: Pregunta 3 ¿Considera usted que herramientas como el panel de control permiten administrar la red de manera eficiente en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Estoy en total desacuerdo	4	4.8	4.8	4.8
	No estoy de acuerdo	11	13.1	13.1	17.9
	Estoy de acuerdo	51	60.7	60.7	78.6
	Estoy totalmente de acuerdo	18	21.4	21.4	100.0
	Total	84	100.0	100.0	

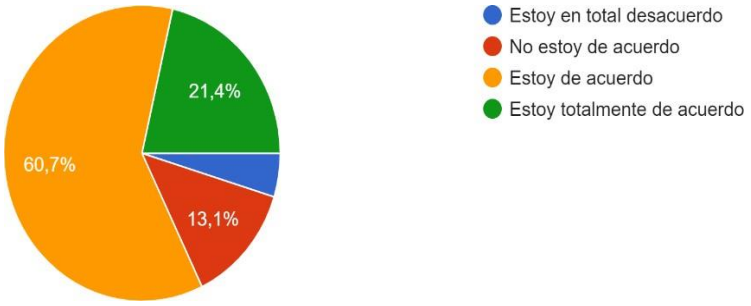

Figura 5: Distribución de respuesta a la pregunta ¿Considera usted que herramientas como el panel de control permiten administrar la red de manera eficiente en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"?

Se analizaron los resultados y se determinó que el 21.4% está totalmente de acuerdo, el 60.7% está de acuerdo, el 13.1% no está de acuerdo y el 4.8% está en total desacuerdo, con respecto a que las herramientas como el panel de control permiten administrar la red de manera eficiente en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi".

Tabla 5: Pregunta 4 ¿Considera usted que es necesario la evaluación de riesgos informáticos para la identificación de amenazas en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Estoy en total desacuerdo	3	3.6	3.6	3.6
	No estoy de acuerdo	6	7.1	7.1	10.7
	Estoy de acuerdo	50	59.5	59.5	70.2
	Estoy totalmente de acuerdo	25	29.8	29.8	100.0
	Total	84	100.0	100.0	

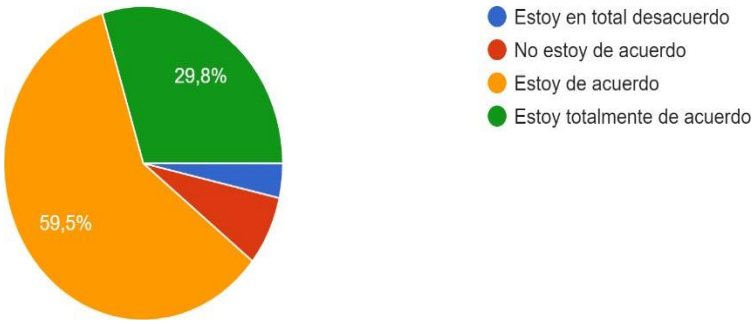

Figura 6: Distribución de respuesta a la ¿Considera usted que es necesario la evaluación de riesgos informáticos para la identificación de amenazas en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"?

Se analizaron los resultados y se determinó que el 29.9% está totalmente de acuerdo, el 59.5% está de acuerdo, el 7.1% no está de acuerdo y el 3.6% está en total desacuerdo, con respecto a que es necesario la evaluación de riesgos informático para la identificación de amenazas en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi".

Tabla 6: Pregunta 5 ¿Considera usted que las identificaciones de riesgos informáticos ayudan a diseñar planes de seguridad y establecer controles para la mitigación de amenazas en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Estoy en total desacuerdo	4	4.7	4.7	4.7
	No estoy de acuerdo	5	6	6	10.7
	Estoy de acuerdo	52	61.9	61.9	72.6
	Estoy totalmente de acuerdo	23	27.4	27.4	100.0
	Total	84	100	100.0	

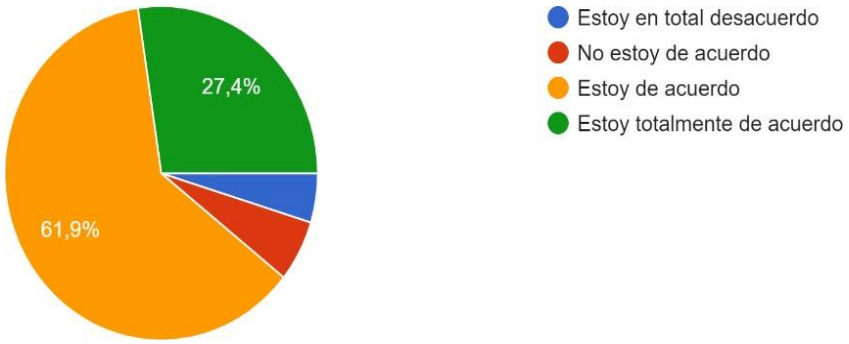

Figura 7: Distribución de respuestas a la pregunta ¿Considera usted que la identificación de riesgos informáticos ayuda a diseñar planes de seguridad y establecer controles para la investigación Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"?

Se analizaron los resultados y se determinó que el 27.4% está totalmente de acuerdo, el 61.9% está de acuerdo, el 6% no está de acuerdo y el 4.7 % está en total desacuerdo, con respecto a que la identificación de riesgos informáticos ayuda a diseñar planes de seguridad y establecer controles para la mitigación de amenazas en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi".

Tabla 7: Pregunta 6 ¿Cree usted que es importante la aplicación de políticas de seguridad informática para garantizar la seguridad de las tecnologías de información en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Estoy en total desacuerdo	4	4.8	4.8	4.8
	No estoy de acuerdo	7	8.3	8.3	13.1
	Estoy de acuerdo	53	63.1	63.1	76.2
	Estoy totalmente de acuerdo	20	23.8	23.8	100.0
	Total	84	100.0	100.0	

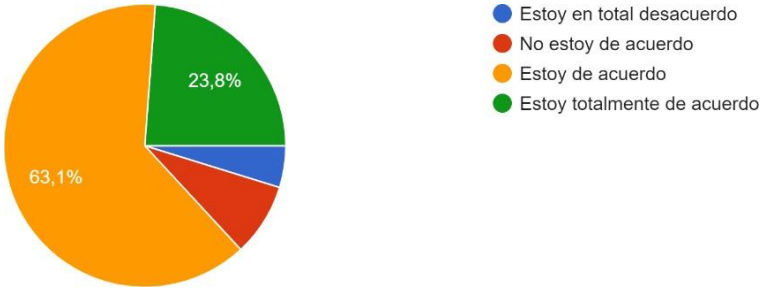

Figura 8: Distribución de respuestas a la pregunta ¿Cree usted que es importante la aplicación de políticas de seguridad informática para garantizar la seguridad de las tecnologías de información en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"?

Se analizaron los resultados y se determinó que el 23.8% está totalmente de acuerdo, el 63.1% está de acuerdo, el 8.3% no está de acuerdo y el 4.8% está en total desacuerdo, con respecto a la importancia de la aplicación de políticas de seguridad informática para garantizar la seguridad de las tecnologías de información en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi".

Tabla 8: Pregunta 7 ¿Considera usted la necesidad de adoptar medidas de seguridad informática para asegurar la integridad de los sistemas informáticos en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Estoy en total desacuerdo	4	4.8	4.8	4.8
	No estoy de acuerdo	4	4.8	4.8	9.6
	Estoy de acuerdo	53	63.1	63.1	72.7
	Estoy totalmente de acuerdo	23	27.3	27.3	100.0
	Total	84	100.0	100.0	

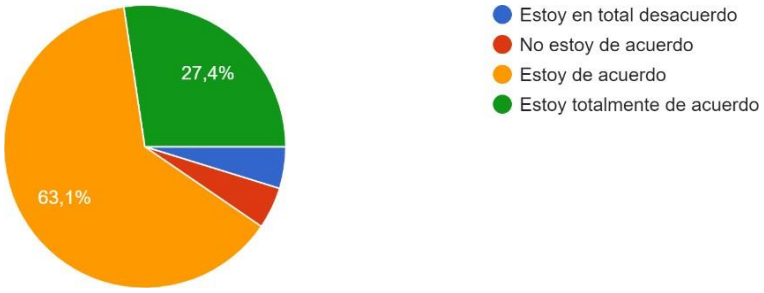

Figura 9: Distribución de respuestas a la pregunta ¿Considera usted la necesidad de adoptar medidas de seguridad informática para asegurar la integridad de los sistemas informáticos en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"?

Se analizaron los resultados y se determinó que el 27.3% está totalmente de acuerdo, el 63.1% está de acuerdo, el 4.8% no está de acuerdo y el 4.8% está en total desacuerdo, con respecto a la necesidad de adoptar medidas de seguridad informática para asegurar la integridad de los sistemas informáticos en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi".

Tabla 9: Pregunta 8 ¿Considera usted que la implementación de la norma ISO/IEC 27001 permitirá contar con un Sistema de Gestión de la Seguridad de Información (SGSI) para la reducción del impacto de los incidentes de seguridad en la Escuela Militar de Chorrillo

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Estoy en total desacuerdo	4	4.8	4.8	4.8
	No estoy de acuerdo	6	7.1	7.1	11.9
	Estoy de acuerdo	55	65.5	65.5	77.4
	Estoy totalmente de acuerdo	19	22.6	22.6	100.0
	Total	84	100.0	100.0	

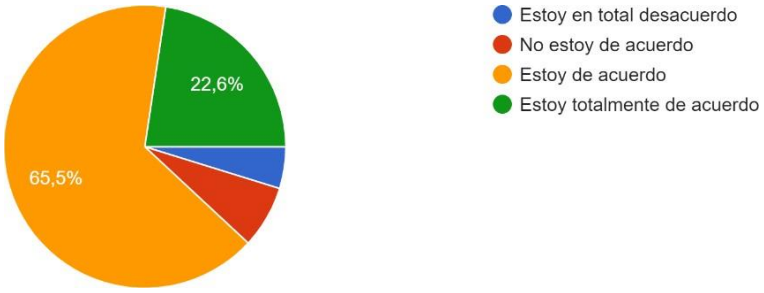

Figura 10: Distribución de respuestas a la pregunta ¿Considera usted que la implementación de la norma ISO/IEC 27001 permitirá contar con un sistema de gestión de seguridad de información en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"?

Se analizaron los resultados y se determinó que el 22.6% está totalmente de acuerdo, el 65.5% está de acuerdo, el 7.1% no está de acuerdo y el 4.8% está en total desacuerdo, con respecto a que la implementación de la norma ISO/IEC 27001 permitirá contar con un sistema de gestión de la seguridad de la información (SGSI) en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi".

Tabla 10: Pregunta 9 ¿Cree usted que está expuesto a riesgos informáticos dentro de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Estoy en total desacuerdo	4	4.8	4.8	4.8
	No estoy de acuerdo	7	8.3	8.3	13.1
	Estoy de acuerdo	57	67.9	67.9	81.0
	Estoy totalmente de acuerdo	16	19.0	19.0	100.0
	Total	84	100.0	100.0	

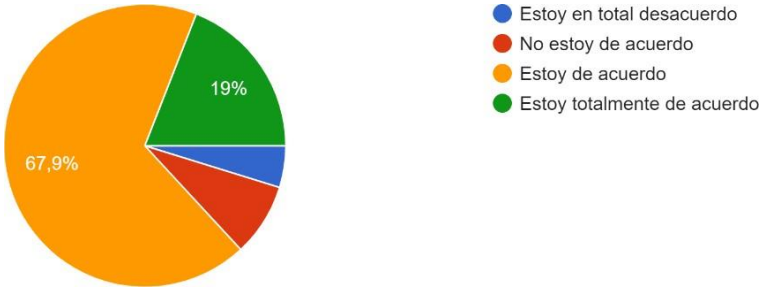

Figura 11: Distribución de respuestas a la pregunta ¿Cree usted que está expuesto a riesgos informáticos dentro de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"?

Se analizaron los resultados y se determinó que el 19% está totalmente de acuerdo, el 67.9% está de acuerdo, el 8.3% no está de acuerdo y el 4.8% está en total desacuerdo, con respecto a que están expuestos a riesgos informáticos dentro de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi".

Tabla 11: Pregunta 10 ¿Considera usted que los riesgos de acceso que afectan la integridad de la información en los sistemas de bases de datos son los más constantes en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Estoy en total desacuerdo	3	3.5	3.5	3.5
	No estoy de acuerdo	11	13.1	13.1	16.6
	Estoy de acuerdo	55	65.5	65.5	82.1
	Estoy totalmente de acuerdo	15	17.9	17.9	100.0
	Total	84	100.0	100.0	

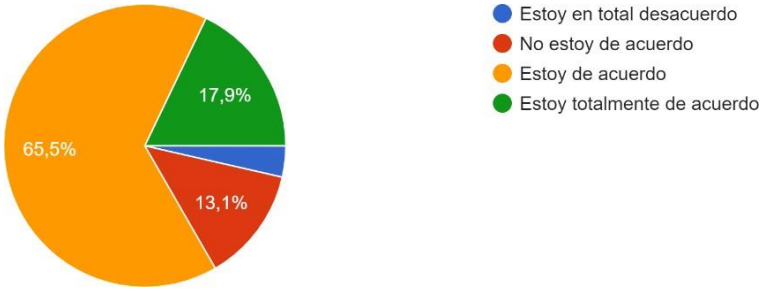

Figura 12: Distribución de respuestas a la pregunta ¿Considera usted que los riesgos de acceso que afectan la integridad de la información en los sistemas de datos son los más constantes en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"?

Se analizaron los resultados y se determinó que el 17.9% está totalmente de acuerdo, el 65.5% está de acuerdo, el 13.1% no está de acuerdo y el 3.5% está en total desacuerdo, con respecto a que los riesgos de acceso que afectan la integridad de la información en los sistemas de bases de datos son los más constantes en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi".

Tabla 12: Pregunta 11 ¿Cree usted que su computador e información personal es vulnerable a amenazas informáticas como malware dentro de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Estoy en total desacuerdo	4	4.8	4.8	4.8
	No estoy de acuerdo	7	8.3	8.3	13.1
	Estoy de acuerdo	57	67.9	67.9	81.0
	Estoy totalmente de acuerdo	16	19.0	19.0	100.0
	Total	84	100.0	100.0	

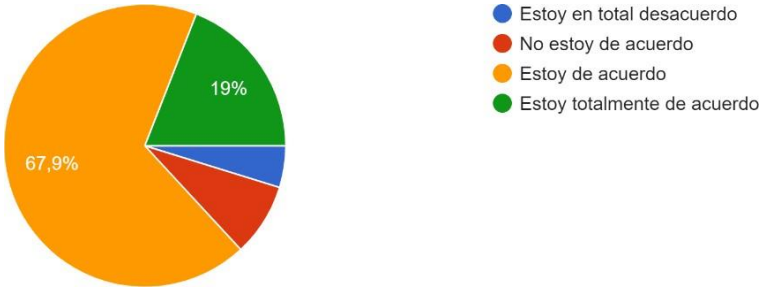

Figura 13: Distribución de respuestas a la pregunta ¿Cree usted que su computador e información personal es vulnerable a amenazas informáticas como malware dentro de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"?

Se analizaron los resultados y se determinó que el 19% está totalmente de acuerdo, el 67.9% está de acuerdo, el 8.3% no está de acuerdo y el 4.8% está en total desacuerdo, con respecto a que sus computadores e información personal es vulnerable a amenazas informáticas como malware dentro de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi".

Tabla 13: Pregunta 12 ¿Cree usted que las amenazas lógicas como virus, puertos abiertos, gusanos y troyanos ponen en riesgo la confidencialidad de su información al navegar en la red de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Estoy en total desacuerdo	4	4.8	4.8	4.8
	No estoy de acuerdo	4	4.8	4.8	9.5
	Estoy de acuerdo	55	65.5	65.5	75.0
	Estoy totalmente de acuerdo	21	25.0	25.0	100.0
	Total	84	100.0	100.0	

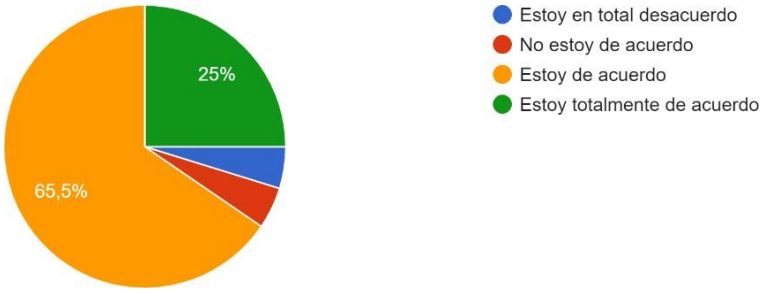

Figura 14: Distribución de respuestas a la pregunta ¿Cree usted que las amenazas lógicas como virus, puertos abiertos, gusanos y troyanos ponen en riesgos la confidencialidad de su información en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"?

Se analizaron los resultados y se determinó que el 25% está totalmente de acuerdo, el 65.5% está de acuerdo, el 4.8% no está de acuerdo y el 4.8% está en total desacuerdo, con respecto a que las amenazas lógicas como virus, puertos abiertos, gusanos y troyanos ponen en riesgo la confidencialidad de su información al navegar en la red de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi".

5.2 Análisis Inferencial

Se aplicó la encuesta a una muestra representativa de la población, para determinar si la muestra tiene una distribución normal, se realizó la prueba de normalidad también nos ayuda determinar si la muestra es de tipo paramétrica o no paramétrica. En esta prueba se platea un nivel de confianza de 95% y la significancia de 5%, se tiene el siguiente criterio de hipótesis para determinar la normalidad:

Tabla 14: Resumen del procesamiento de los casos

	Casos		
	Válidos		Total
	N	Porcentaje	
VD	84	100.0%	84
VI	84	100.0%	84

Se procesaron 84 casos válidos, para todo el análisis inferencial de resultados.

Prueba de hipótesis de normalidad

H0: La muestra obtenida tiene una distribución normal (paramétrica)

H1: La muestra obtenida no tiene una distribución normal (no paramétrica)

Criterio de decisión:

En la siguiente tabla nos muestra los estadísticos de Kolmogorov Smirnov y de Shapiro Wilk, según las condiciones de los estadísticos nos mencionan que datos menores de 50 se utiliza Shapiro Wilk y para datos mayores a 50 se utiliza Kolmogorov Smirnov. En nuestra investigación tenemos datos de 84 individuos estos son mayor a 50 por lo tanto tomaremos el criterio de Kolmogorov Smirnov.

Tabla 15: Prueba de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
VD	.359	84	.000	.794	84	.000
VI	.310	84	.000	.848	84	.000

a. Corrección de la significación de Lilliefors

Para evaluar la hipótesis planteada se considerar el criterio de decisión, según el estadístico de Kolmogorov Smirnov se tiene 0 grados de libertad siendo menor a 0.05 por esta condición, rechazamos la hipótesis nula (H0) y aceptamos la hipótesis alterna (Ha); la hipótesis alterna nos dice que la muestra obtenida no tiene una distribución normal o es de tipo no paramétrica. Con este criterio asumiremos pruebas de correlación no paramétricas, para determinar el grado de relación entre la variable X e Y, para lo cual usaremos la Rho de Spearman.

Prueba de hipótesis de correlación

H0: No existe relación significativa entre la variable (X) y la variable (Y)

H1: Existe relación significativa entre la variable (X) y la variable (Y)

Criterio de decisión:

Tabla 16: Correlación de Rho de Spearman

			VI	VD
Rho de Spearman	VI	Coeficiente de correlación	1.000	0.771**
		Sig. (bilateral)	.	0.000
		N	64	84
	VD	Coeficiente de correlación	0.771**	1.000
		Sig. (bilateral)	0.000	.
		N	64	64

**. La correlación es significativa al nivel 0,01 (bilateral).

Con esta base podemos aceptar la hipótesis general planteada La gestión de la seguridad informática y la implementación de la norma ISO/IEC 27001 es de importancia trascendental y se relaciona con la mejora de la seguridad y protección de activos de información en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi" Año 2021

Contrastación de Hipótesis Específica 1

Ha: El monitoreo de la red ayuda a identificar significativamente los riesgos informáticos en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"

Ho: El monitoreo de la red no ayuda a identificar significativamente los riesgos informáticos en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"

Tabla 17: Contrastación de Hipótesis Especifica 1

			Monitoreo de la red	Riesgo informático
Rho de Spearman	Monitoreo de la red	Coeficiente de correlación	1.000	0.748**
		Sig. (bilateral)	.	0.000
		N	84	84
	Riesgo informático	Coeficiente de correlación	0.748**	1.000
		Sig. (bilateral)	0.000	.
		N	84	84

**. La correlación es significativa al nivel 0,01 (bilateral).

Según el nivel de significancia bilateral 0,000 es menor que 0,05 lo que nos permite confirmar que:

El monitoreo de la red ayuda a identificar significativamente los riesgos informáticos en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"

Contrastación de Hipótesis Específica 2

Ha: La evaluación de riesgos permite significativamente la mitigación de amenazas informáticas en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi".

Ho: La evaluación de riesgos no permite significativamente la mitigación de amenazas informáticas en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi".

Tabla 18: Contrastación de Hipótesis Especifica 2

			Evaluación de Riesgo	Amenaza informática
Rho de Spearman	Evaluación de Riesgo	Coeficiente de correlación	1.000	0.642**
		Sig. (bilateral)	.	0.000
		N	84	84
	Amenaza informática	Coeficiente de correlación	0.642**	1.000
		Sig. (bilateral)	0.000	.
		N	84	84

**. La correlación es significativa al nivel 0,01 (bilateral).

Según el nivel de significancia bilateral 0,000 es menor que 0,05 lo que nos permite confirmar que:

La evaluación de riesgos permite significativamente la mitigación de amenazas informáticas en la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”.

Contrastación de Hipótesis Específica 3

Ha: La aplicación de políticas de seguridad informática permite significativamente la protección de los activos informáticos en la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”.

Ho: La aplicación de políticas de seguridad informática no permite significativamente la protección de los activos informáticos en la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”.

Tabla 19: Contrastación de Hipótesis Especifica 3

			Políticas de seguridad	Protección de activos informáticos
Rho de Spearman	Políticas de seguridad	Coeficiente de correlación	1.000	0.509**
		Sig. (bilateral)	.	0.000
		N	84	84
	Protección de activos informáticos	Coeficiente de correlación	0.509**	1.000
		Sig. (bilateral)	0.000	.
		N	84	84

**. La correlación es significativa al nivel 0,01 (bilateral).

Según el nivel de significancia bilateral 0,000 es menor que 0,05 lo que nos permite confirmar que:

La aplicación de políticas de seguridad informática permite significativamente la protección de los activos informáticos en la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”.

Contrastación de Hipótesis Específica 4

Ha: El monitoreo de la red conlleva a inventariar los activos informáticos para protegerlos significativamente en la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”

Ho: El monitoreo de la red no conlleva a inventariar los activos informáticos para protegerlos significativamente en la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”

Tabla 20:Contrastación de Hipótesis Especifica 4

			Monitoreo de la red	Inventariar activos informáticos
Rho de Spearman	Monitoreo de la red	Coeficiente de correlación	1.000	0.627**
		Sig. (bilateral)	.	0.000
		N	84	84
	Inventariar activos informáticos	Coeficiente de correlación	0.627**	1.000
		Sig. (bilateral)	0.000	.
		N	84	84

**. La correlación es significativa al nivel 0,01 (bilateral).

Según el nivel de significancia bilateral 0,000 es menor que 0,05 lo que nos permite confirmar que:

El monitoreo de la red conlleva a inventariar los activos informáticos para protegerlos significativamente en la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”

Contrastación de Hipótesis Específica 5

Ha: La evaluación de riesgos informáticos favorece significativamente el control de riesgos informáticos en la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”

Ho: La evaluación de riesgos informáticos no favorece significativamente el control de riesgos informáticos en la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”

Tabla 21: Contrastación de Hipótesis Especifica 5

			Evaluación de riesgo informático	Control de riesgos informáticos
Rho de Spearman	Evaluación de riesgo informático	Coeficiente de correlación	1.000	0.578**
		Sig. (bilateral)	.	0.000
		N	84	84
	Control de riesgos informáticos	Coeficiente de correlación	0.578**	1.000
		Sig. (bilateral)	0.000	.
		N	84	84

**. La correlación es significativa al nivel 0,01 (bilateral).

Según el nivel de significancia bilateral 0,000 es menor que 0,05 lo que nos permite confirmar que:

La evaluación de riesgos informáticos favorece significativamente el control de riesgos informáticos en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"

Contrastación de Hipótesis Específica 6

Ha: El uso de políticas de seguridad informática previenen significativamente las amenazas informáticas en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi

Ho: El uso de políticas de seguridad informática no previenen significativamente las amenazas informáticas en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi

Tabla 22: Contrastación de Hipótesis Especifica 6

			Políticas de seguridad	Amenazas informáticas
Rho de Spearman	Políticas de seguridad	Coeficiente de correlación	1.000	0.634**
		Sig. (bilateral)	.	0.000
		N	84	84
	Amenazas informáticas	Coeficiente de correlación	0.634**	1.000
		Sig. (bilateral)	0.000	.
		N	84	84

**. La correlación es significativa al nivel 0,01 (bilateral).

Según el nivel de significancia bilateral 0,000 es menor que 0,05 lo que nos permite confirmar que:

Los usos de políticas de seguridad informática previenen significativamente las amenazas informáticas en la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi

5.3 Discusión de los resultados

Según la prueba de correlación obtenida de Rho de Spearman el coeficiente de correlación es de 0.771 valor de correlación es positiva fuerte entre la variable X y la variable Y, de acuerdo al criterio de decisión el valor de la significancia es 0 que es menor a 0.05, por lo que el resultado indica que existe relación significativa entre la Gestión de la seguridad informática y la Implementación de la norma ISO/IEC 27001).

Similar resultado tiene la investigación realizada por García (2020) en su estudio “Propuesta de un sistema de gestión de seguridad de la información basado en la norma ISO 27001 para la oficina de tecnologías de información del Gobierno Regional Piura; 2020”, el desarrollo de su investigación a los trabajadores del Gobierno Regional de Piura muestra insatisfacción en la situación actual de la gestión en la información del Gobierno Regional de Piura y manifiesta la necesidad de contar con un sistema de gestión de seguridad de la información basado en la norma ISO 27001 a fin de preservar la confidencialidad, integridad y disponibilidad de la información en la oficina de tecnologías de información del Gobierno Regional Piura.

También tiene resultados similares la investigación realizada por Bustamante, Valles, Cuellar, & Lévano (2021) aplicó una encuesta a los trabajadores de la municipalidad antes y después de la norma ISO 27001:2013, evidenciando que las políticas de seguridad de la información influyeron positivamente en la gestión de la seguridad de la información dentro de la Subgerencia de Recaudación y Fiscalización Tributaria de la Municipalidad Distrital de Morales.

La aplicación de la norma ISO 27001 y las políticas de seguridad son necesarios en una institución así menciona (Rodríguez, 2016) cuando este aplicó las políticas de seguridad al personal de la cooperativa de ahorro y crédito evidenciando mejoras en el manejo en la plataformas web y control de acceso. Nuestra investigación concuerda con esta investigación a la aplicación de políticas de seguridad en la escuela militar donde el 63.1 % de participantes está de acuerdo a esta medida.

El riesgo que del sistema de información es frecuente en muchas instituciones, según (Camargo, 2017) la aplicación de la ISO 27000 e ISO 27001 para mantener la integridad, confidencialidad y disponibilidad de la información en el área de tecnología de la comisión nacional del servicio civil – CNSC detecto activos críticos y el impacto detectado es en la misma entidad, en este sentido concordamos con el investigador frente a los riesgos que se originan en la entidad por la falta de políticas de seguridad y una adecuada gestión informática siendo el 63.1 % de encuestados está de acuerdo en adoptar medidas de seguridad en la escuela militar de Chorrillos.

Otras medidas que aportan a la seguridad de la información es el uso de un sistema web como lo hizo (Aguirre, 2018) en una empresa de servicios informáticos SAC en la Molina este tuvo un efecto positivo en la gestión de la seguridad de la información; el reconocer los riesgos seria el comienzo de la gestión de seguridad como se refleja en la encuesta el 59.9% está de acuerdo y el 29.8% está totalmente de acuerdo con le evaluación de riesgos informáticos y la identificación de amenazas en la escuela militar de chorrillos. De esta forma se aplican las medidas de seguridad y una adecuada gestión.

Concordamos con (García, 2020) donde refleja la incomodad de los trabajadores del Gobierno Regional de Piura frente a la falta de un sistema de gestión ante la inseguridad informática; los encuestados también muestran su preocupación ante la falta de gestión de seguridad en la escuela, el 53.6% está de acuerdo a la importancia del sistema de gestión de la seguridad informática y el 53% menciona que se debe hacer un conste monitoreo a la red para mantener segura la información. Además, el 61.2% de encuestados considera que la identificación de

riesgos informáticos ayudaría a diseñar planes de seguridad y establecer controles para la mitigación.

Un estudio demuestra que la aplicación de la ISO 27001:2013 a trabajadores de la municipalidad distrital de Morales influye positivamente en la gestión de la seguridad de la información, en tal sentido según la encuesta realiza en esta investigación, la identificación de riesgos y la aplicación de políticas de seguridad mejorarían la gestión de seguridad de la información.

CONCLUSIONES

El resultado general señala que si existe relación significativa entre la Gestión de la seguridad informática y la Implementación de la norma ISO/IEC 27001). A un nivel de significancia de 0.000 menor que 0.05 y un "r" de 0,771 de nivel positivo alto. El 86.9 % de la población considera muy importante la gestión de la seguridad informática y la implementación de la norma ISO/IEC 27001 porque se encarga de garantizar la privacidad e integridad de la información guardada en los sistemas informáticos de la Escuela Militar, con el objetivo de proteger los servidores, equipos y software de los ataques o fallos, se concluye que:

- Según el nivel de significancia bilateral 0,000 es menor que 0,05 lo que nos permite confirmar que: El monitoreo de la red ayuda a identificar significativamente los riesgos informáticos en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi" y un "r" de 0,748 de nivel positivo alto. El 82.2 % de la población considera muy importante el monitoreo de la red porque ayuda a identificar los riesgos informáticos, proporcionando la información que los responsables de la sección Telemática necesitan para determinar, en tiempo real, el óptimo funcionamiento de la red en la Escuela Militar.

- Según el nivel de significancia bilateral 0,000 es menor que 0,05 lo que nos permite confirmar que: La evaluación de riesgos permite significativamente la mitigación de amenazas informáticas en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi" y un "r" de 0,642 de nivel positivo alto. El 89.3 % de la población cree muy necesario la evaluación de riesgos dado que permite la mitigación de amenazas informáticas de esta manera establecer las medidas preventivas y correctivas que nos garanticen mayores niveles de seguridad.

- Según el nivel de significancia bilateral 0,000 es menor que 0,05 lo que nos permite confirmar que: La aplicación de políticas de seguridad informática permite significativamente la protección de los activos informáticos en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi" y un "r" de 0,509 de nivel positivo

moderado. El 86.9 % de la población cree muy importante la aplicación de políticas de seguridad informática porque se encargan de brinda la protección de los activos informáticos, siendo como un plan para combatir todos los riesgos a los que puedan estar expuestas.

- Según el nivel de significancia bilateral 0,000 es menor que 0,05 lo que nos permite confirmar que: El monitoreo de la red conlleva a inventariar los activos informáticos para protegerlos significativamente en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi" y un "r" de 0,627 de nivel positivo alto. El 82.2 % de la población considera que el monitoreo de la red conlleva a inventariar los activos informáticos y protegerlos, de esta manera establecer controles para asegurar su confidencialidad.

- Según el nivel de significancia bilateral 0,000 es menor que 0,05 lo que nos permite confirmar que: La evaluación de riesgos informáticos favorece significativamente el control de riesgos informáticos en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi y un "r" de 0,578 de nivel positivo medio". El 89.3 % de la población considera que la evaluación de riesgos informáticos favorece al control de riesgos informáticos, permitiendo realizar registros de incidentes y prevenir futuros incidentes.

- Según el nivel de significancia bilateral 0,000 es menor que 0,05 lo que nos permite confirmar que: Los usos de políticas de seguridad informática previenen significativamente las amenazas informáticas en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi" y un "r" de 0,634 de nivel positivo alto. El 90.5 % de la población considera muy necesario el uso de políticas de seguridad informática dado que previenen las amenazas informáticas, orientando a los responsables de la sección de Telemática y el personal de cadetes del arma de comunicaciones la forma de actuar ante un posible riesgo.

RECOMENDACIONES

- Se recomienda revisar la metodología de mitigación de riesgos a fin de evaluar su eficacia y aplicar mejoras continuas para lograr la eficiencia.
- Se recomienda contar con una bitácora para almacenar los eventos, riesgos e incidentes de seguridad a fin de recolectar evidencias (lecciones aprendidas), donde se describan las acciones tomadas y mejoras en los mismos, con el objetivo de prevenir que dichos sucesos vuelvan a ocurrir.
- Se recomienda revisar periódicamente las políticas de seguridad informática para verificar que estén alineadas a la norma ISO/IEC 27001 y a los objetivos de la Escuela Militar.
- Se recomienda utilizar estándares y buenas prácticas que sean ampliamente aceptadas. Cabe resaltar que la norma ISO/IEC 27001:2013 te indican que es aquello que se debe controlar, pero no indica el cómo; por lo que esto depende de los responsables de la sección Telemática.
- Se recomienda implementar un Sistema de Gestion de Seguridad de la Información (SGSI) alineado periódicamente a la norma ISO/IEC 27001 y sus objetivos para cumplir la legalidad y protección de los datos, por lo que esto depende de los responsables de la sección Telemática.
- Se recomienda que cada área de la organización defina su análisis de riesgos de sus activos involucrados en cada uno de sus procesos y después monitorizar permanentemente todos los riesgos de la Escuela Militar para aplicar los controles basados en la norma ISO/IEC 27001.

PROPUESTA DE MEJORA

1. Implementar un manual sobre políticas de seguridad informática, la misma que debe ser socializada en forma periódica a fin de que se tome conocimiento por los integrantes de la institución.
2. Realizar evaluación de prevención de riesgos en forma programada a fin de evitar potenciales riesgos que dañen al personal y material de la institución.
3. Realizar una evaluación de las estrategias de enseñanzas y mejorarlas mediante aplicación de estrategias interactivas, aprendizaje basado en casos, aprendizaje basado en problemas donde se centre la enseñanza aprendizaje en el personal.
4. Implementar controles programadas en forma previa, simultánea y posterior a fin de salvaguardar la seguridad de la información.
5. Acopiar las buenas prácticas en la seguridad informática a fin de ser socializadas en la institución, lo cual permita cada vez brindar una eficiente y eficaz seguridad de la información.

REFERENCIAS BIBLIÓGRAFICAS

Aburto Zamora, K. Y. (2020). *Implantación de un sistema de gestión integrado con las normas ISO/IEC 27001: 2013 e ISO/IEC 20000-1: 2018* (Universitat Politcenica de Valencia). Retrieved from https://riunet.upv.es/bitstream/handle/10251/157546/Aburto - IMPLANTACION DE UN SISTEMA DE GESTION INTEGRADO CON LAS NORMAS ISO/IEC 27001%3A2013 E ISO/ ...pdf?sequence=1&isAllowed=y

Aguirre Ventura, J. M. (2018). *Sistema web para la gestión de la seguridad de la información alineada a la norma ISO/IEC 27001 en la empresa de Servicios Informáticos S.A.C – La Molina*. 119.

Barrera Morales, S. D. (2009). *Siatema de Análisis y monitoreo para la red inal+ambrica de la empresa "DISTRY-TEX"* (Universidad Técnica de Ambato). Retrieved from https://repositorio.uta.edu.ec/jspui/handle/123456789/293

Bustamante García, S., Valles Coral, M. Á., Cuellar Rodríguez, I. E., & Lévano Rodríguez, D. (2021). Políticas basadas en la ISO 27001: 2013 y su influencia en la gestion de seguridad de la información en municipalidades de Perú. *Enfoque UTE*, *12*(2), 69–79. Retrieved from https://doi.org/10.29019/enfoqueute.743

Camargo Ramirez, J. D. (2017). Diseño de un sistema de gestión de la seguridad de la informacion (SGSI) en el área tecnológica de la comision nacional del servicio civil - CNSC basado en la norma ISO27000 e ISO27001 (UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD). Retrieved from www.journal.uta45jakarta.ac.id

Duran Huayta, W. F. (2016). Universidad Mayor De San Andres Facultad De Tecnologia (Universidad Mayor de San Andres). Retrieved from https://repositorio.umsa.bo/handle/123456789/18742

Dussan Clavijo, C. A. (2006). Politicas de la Seguridad Informatica. *Entramado Universidad Libre Colombia.*, *2*(1.), 86-92. Retrieved from https://www.redalyc.org/pdf/2654/265420388008.pdf

García Cruz, R. A. (2020). Propuesta de un sistema de gestion de seguridad de la informacion basado en la norma ISO 27001 para la oficina de Tecnologias de

Informacion del Gobierno Regional Piura; 2020 (Univerisidad Catolica los Ángeles de Chimbote). Retrieved from http://repositorio.uladech.edu.pe/handle/123456789/20291

Gónzáles Agudelo, D. F. (2014). *El riesgo y la falta de politicas de seguridad informatica una amenaza en las empresas certificadas BASC* (Universidad Militar Nueva Granada). Retrieved from https://repository.unimilitar.edu.co/bitstream/handle/10654/12251/ENSAYO FINAL.pdf?sequence=1&isAllowed=y

Hayes, B. (1999). Diseño de encuetas, usos y métodos de análisis estadístico. México: Edit Oxford.

Leiva Peña, R. (2016). *Diseño de un Sistema de Gestión de Seguridad de la Información basado en las Normas ISO/IEC 27001 e ISO/IEC 27002 para proteger los activos de información en el proceso de suministros de medicamentos de la Red de Salud de Lambayeque 2015* (Universidad Nacional Pedro Ruiz Gallo; Vol. 66). Retrieved from https://repositorio.unprg.edu.pe/bitstream/handle/20.500.12893/1019/BC-TES-5784.pdf?sequence=1&isAllowed=y

León Cepeda, L. C. (2018). *Estructuración del sistema de seguridad de la información en el área de protección de datos para un operador logístico bajo la norma NTC/ISO 27001* (pp. 1–11). pp. 1–11. Bogotá D.C - Colombia.

MINTIC, M. de tecnologias de la informacion y comunicaciones. (2016). Elaboración de la política general de seguridad y privacidad de la información . *2016*, p. 25.

Montaño Orrego, V. (2011). La gestión en la seguridad de la información según Cobit, Itil e Iso 27000. *Revista Pensamiento Americano*, *2*(6), 21–23. Retrieved from http://www.coruniamericana.edu.co/publicaciones/ojs/index.php/pensamientoamericano/article/view/57

Quiroz Zambrano, S. M. (2017). Seguridad en Informática: Consideraciones. *Dominio de La Ciencia*, *3*(5), 676–688. Retrieved from https://dialnet.unirioja.es/servlet/articulo?codigo=6137824

Regina Baena, G., Mendoza Méndez, R. V., & Joel Coronado, E. dorantes. (2019).

Importancia de la Norma ISO/EIC 27000 en la implementacion de un sistema de gestion de la seguridad de la información. *Revista Académica de Las Contribuciones a La Economía*.

Rodriguez Baca, L. S., Cruzado Puente de la Vega, C. F., Mejía Corredor, C., & Alarcón Diaz, M. A. (2020). Aplicación de ISO 27001 y su influencia en la seguridad de la información de una empresa privada peruana. *Propósitos y Representaciones*, *8*(3), 786. https://doi.org/10.20511/pyr2020.v8n3.786

Rodríguez Guerra, J. P. (2016). *Diseño y creación de una política de seguridad de la información (SGSI) basado en la norma ISO 27000 para la Cooperativa construcción, Comercio y Producción*. UNIVERSIDAD INTERNACIONAL SEK.

Santamaría Ramirez, J. A. (2014). Manual de Seguridad de la Información para un Organismo del Estado Colombiano. *Igarss 2014*, 27.

Seclén Arana, J. A. (2016). Factores que afectan la implementación del sistema de gestión de seguridad de la información en las entidades públicas peruanas de acuerdo a la NTP-ISO/IEC 27001. Retrieved from http://cybertesis.unmsm.edu.pe/handle/cybertesis/4884

Solarte Solarte, F. N. J., Enriquez Rosero, E. R., & Benavides Ruano, M. del C. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica - ESPOL*, *28*(5), 497–498. Retrieved from http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456/321

Sotelo Bedón, M., Torres Utrilla, J., & Rivera Ortega, J. (2012). Un Proceso Práctico de Análisis de Riesgos de Activos de Información. *IV Congreso Internacional de Computación y Telecomunicaciones Un*, 121–127. Retrieved from http://www.comtel.pe/comtel2012/callforpaper2012/P26C.pdf

Vega Malagón, G., Ávila Morales, J., Vega Malagón, A. J., Camacho Calderón, N., Becerril Santos, A., & Leo Amador, G. (2014). *Paradigmas en la investigación enfoque cuantitativo y cualitativo*. *10*(15), 523–528. Retrieved from https://core.ac.uk/reader/236413540

ANEXOS

Anexo 1: Matriz De Consistencia Lógica

Título: Gestión de la Seguridad Informática y la implementación de la norma ISO/IEC 27001 en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi" – Año 2021

PROBLEMA GENERAL	OBJETIVO GENERAL	HIPÓTESIS GENERAL	VARIABLES	METODOLOGÍA
¿Cuál es la importancia de la **gestion de la seguridad informatica** y la **implementación de la norma ISO/IEC 27001** en la Escuela Militar de Chorrillos "coronel Francisco Bolognesi" - Año 2021?	Determinar la importancia de la **gestión de la seguridad informática** y la **implementación de la norma ISO/IEC 27001** en la Escuela Militar de Chorrillos "coronel Francisco Bolognesi" - Año 2021?	**La gestión de la seguridad informatica** y la **implementación de la norma ISO/IEC 27001** es de alta importancia en la Escuela Militar de Chorrillos "coronel Francisco Bolognesi" - Año 2021.	**(Operacionalización de las variables)** **VARIABLE X** **Gestion de la Seguridad Informática** **X_1:** Monitoreo de la red - Panel de control **X_2:** Evaluación de riesgos informáticos - Identificación de riesgos informáticos **X_3:** Políticas de seguridad informática - Medidas de seguridad informáticas **VARIABLE Y** **Implementación de la norma ISO/IEC 27001** **Y_1:** Riesgos informáticos - Riesgos de acceso **Y_2:** Amenazas informáticas - Amenazas lógicas **Y_3:** Activos Informáticos - Activos de información	**Enfoque de la Investigación** Cuantitativa **Tipo de Investigación** Básica o teórica **Nivel de la Investigación** Descriptiva **Diseño de la Investigación** No experimental-Transversal **Población:** Miembros de la Sección de Inteligencia (9) Sección de Telemática (8) Cadetes de Comunicaciones (67) **Muestra:** El total de la población 67 personas **Técnicas de Procesamiento de Datos** Encuestas online, entrevistas, análisis documentario.
PROBLEMAS ESPECÍFICOS	**OBJETIVOS ESPECÍFICOS**	**HIPÓTESIS ESPECÍFICAS**		
PE1: ¿Cómo el **monitoreo de la red** ayuda a identificar los **riesgos informáticos** en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"? PE2: ¿Cómo la **evaluación de riesgos informáticos** permite la mitigación de **amenazas informáticas** en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"? PE3: ¿Cómo la aplicación de **políticas de seguridad informática** permite la protección de los **activos informáticos** en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"? PE4: ¿Cómo el **monitoreo de la red** conlleva a inventariar los **activos informáticos** en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"? PE5: ¿Cómo la **evaluación de riesgos informáticos** favorece el control de **riesgos informáticos** en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi" PE6: ¿Cómo el uso de **políticas de seguridad informatica** previenen las **amenazas informáticas** en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"?	OE1: Determinar cómo el **monitoreo de la red** ayuda a identificar los **riesgos informáticos** en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi" OE2: Determinar como la **evaluación de riesgos informáticos** permite la mitigación de **amenazas informáticas** en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi". OE3: Determinar cómo la aplicación de **políticas de seguridad informática** permite la protección de los **activos informáticos** en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi". OE4: Determinar como el **monitoreo de la red** conlleva a inventariar los **activos informáticos** en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi" OE5: Determinar como la **evaluación de riesgos informáticos** favorece el control de **riesgos informáticos** en la Escuela Militar de Chorrillos "coronel Francisco Bolognesi" OE6: Determinar como el uso de **políticas de seguridad informatica** previenen las **amenazas informáticas** en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"	H1: El **monitoreo de la red** ayuda a identificar significativamente los **riesgos informáticos** en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi" H2: La **evaluación de riesgos** permite significativamente la mitigación de **amenazas informáticas** en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi". H3: La aplicación de **políticas de seguridad informática** permite significativamente la protección de los **activos informáticos** en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi". H4: El **monitoreo de la red** conlleva a inventariar los **activos informáticos** para protegerlos significativamente en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi" H5: La **evaluación de riesgos informáticos** favorece significativamente el control de **riesgos informáticos** en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi" H6: El uso de **políticas de seguridad informática** previenen significativamente las **amenazas informáticas** en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"		

Anexo 2: Elaboración de los Instrumentos

TESIS

Gestión de la Seguridad Informática y la implementación de la norma ISO/IEC 27001 en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"

Cuestionario dirigido a cadetes del arma de Comunicaciones, Oficiales y el personal responsable de las secciones de Telemática e Inteligencia de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"

Objetivo: La presente encuesta es exclusivamente con fines de investigación científica y la información que se recoja será tratada con absoluta confidencialidad, por eso le rogamos contestar con la mayor sinceridad, para poder determinar la importancia de la Gestión de la Seguridad Informática y la norma ISO/IEC 27001 en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi" – Año 2021.

Indicaciones: Lea cuidadosamente cada pregunta y marque con un aspa (X) la respuesta que considera correcta.

	Preguntas	Estoy totalmente de acuerdo	Estoy de acuerdo	No estoy de acuerdo	Estoy totalmente desacuerdo
1	¿Considera usted que es importante la gestión de la seguridad informática en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"?				
2	¿Cree usted que el permanente monitoreo de la red ayuda a mantener una red segura en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi?				
3	¿Considera usted que herramientas como el panel de control permiten administrar la red de manera eficiente en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi?				

4	¿Considera usted que es necesario la evaluación de riesgos informáticos para la identificación de amenazas en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi?				
5	¿Considera usted que la identificación de riesgos informáticos ayuda a diseñar planes de seguridad y establecer controles para la mitigación de amenazas en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi?				
6	¿Cree usted que es importante la aplicación de políticas de seguridad informática para garantizar la seguridad de las tecnologías de información en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"?				
7	¿Considera usted la necesidad de adoptar medidas de seguridad informática para asegurar la integridad de los sistemas informáticos en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"?				
8	¿Considera usted que la implementación de la norma ISO/IEC 27001 permitirá contar con un Sistema de Gestión de la Seguridad de Información (SGSI) para la reducción del impacto de los incidentes de seguridad en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"?				
9	¿Cree usted que está expuesto a riesgos informáticos dentro de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"?				
10	¿Considera usted que los riesgos de acceso que afectan la integridad de la información en los sistemas de bases de datos son los más constantes en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi" ?				
11	¿Cree usted que su computador e información				

	personal es vulnerable a amenazas informáticas como malware dentro de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"?				
12	¿Cree usted que las amenazas lógicas como virus, puertos abiertos, gusanos y troyanos ponen en riesgo la confidencialidad de su información al navegar en la red de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"?				

Anexo 3: Validez, confiabilidad y evaluación de instrumentos: juicio de expertos

FICHA DE VALIDACION DE INSTRUMENTOS

I. DATOS GENERALES

1.1 Apellidos y nombres del experto: Julio Daniel Peña Corahua

1.2 Grado académico: Doctor

1.3 Cargo e institución donde labora: DTP EMCH

1.4 Título de la Investigación: Gestión de la seguridad informática y la implementación de la norma ISO/IEC 27001 en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi" – Año 2021

1.5 Autor del instrumento: Bach. Paucar Yaguno Marco Antonio
Bach. Rojas Lapa Cristian

1.6 Licenciatura/ Mención: Licenciado en ciencias militares con mención en Ingeniería

1.7 Nombre del instrumento: Cuestionario

INDICADORES	CRITERIOS CUALITATIVOS/CUANTITATIVOS	Deficiente 0-20%	Regular 21-40%	Bueno 41-60%	Muy Bueno 61-80%	Excelente 81-100%
1. CLARIDAD	Esta formulado con un lenguaje apropiado					95
2. OBJETIVIDAD	Esta expresado en conductas observables					90
3. ACTUALIDAD	Adecuado al alcance de ciencia y tecnología.					90
4. ORGANIZACIÓN	Existe una organización lógica.					90
5. SUFICIENCIA	Comprende los aspectos de cantidad y calidad.					85
6. INTENCIONALIDAD	Adecuado para valorar aspectos del estudio.					90
7. CONSISTENCIA	Basados en aspectos Teóricos-Científicos y del tema de estudio.					85
8. COHERENCIA	Entre los índices, indicadores, dimensiones y variables.					90
9. METODOLOGIA	La estrategia responde al propósito del estudio.					90
10. CONVENIENCIA	Genera nuevas pautas en la investigación y construcción de teorías.					95
SUB TOTAL						90
TOTAL						90

VALORACIÓN CUANTITATIVA (Total x 0.20): 18

VALORACIÓN CUALITATIVA: Excelente

OPINIÓN DE APLICABILIDAD: Aplicable

Lugar y fecha: Lima, 16 de noviembre del 2021

Firma: **Dr. Julio Peña C.**

DNI: 07657554

Anexo 4: Bases de datos

P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12
Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo
Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo
Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo
Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo
Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo
Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo
Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo
Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo
Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo
Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo
Estoy de	Estoy de	Estoy de	Estoy de	Estoy de	Estoy de	Estoy de	Estoy de	Estoy de	Estoy de	Estoy de	Estoy de

P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12
acuerdo	acuerdo	acuerdo	acuerdo	acuerdo	acuerdo	acuerdo	acuerdo	acuerdo	acuerdo	acuerdo	acuerdo
Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo
Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo
Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo
Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo
Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo
Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo
Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo
Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo
Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo
Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo
Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo

P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12
Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo
Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo
Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo
Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo
Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo
Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo
Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo
Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo
Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo
Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo
Estoy de	Estoy de	Estoy de	Estoy de	Estoy de	Estoy de	Estoy de	Estoy de	Estoy de	Estoy de	Estoy de	Estoy de

P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12
acuerdo	acuerdo	acuerdo	acuerdo	acuerdo	acuerdo	acuerdo	acuerdo	acuerdo	acuerdo	acuerdo	acuerdo
Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo
Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo
Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo
Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo
Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo
Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo
Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo
Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo
Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo
Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo
Estoy en total	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo

P1	**P2**	**P3**	**P4**	**P5**	**P6**	**P7**	**P8**	**P9**	**P10**	**P11**	**P12**
desacuerdo											
Estoy en total desacuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo
Estoy en total desacuerdo	Estoy en total desacuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo
Estoy en total desacuerdo	Estoy en total desacuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo
Estoy en total desacuerdo	Estoy en total desacuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo
Estoy en total desacuerdo	Estoy totalmente de acuerdo	Estoy de acuerdo	Estoy en total desacuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo
Estoy en total desacuerdo	Estoy totalmente de acuerdo	Estoy en total desacuerdo	Estoy en total desacuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo
Estoy en total desacuerdo	Estoy totalmente de acuerdo	Estoy en total desacuerdo	Estoy en total desacuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo
Estoy	Estoy	Estoy en	Estoy	Estoy en	Estoy de	Estoy de	Estoy de	Estoy de	Estoy de	Estoy de	Estoy de

P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12
totalmente de acuerdo	totalmente de acuerdo	total desacuerdo	totalmente de acuerdo	total desacuerdo	acuerdo	acuerdo	acuerdo	acuerdo	acuerdo	acuerdo	acuerdo
Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy en total desacuerdo	Estoy totalmente de acuerdo	Estoy en total desacuerdo	Estoy en total desacuerdo	Estoy en total desacuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo
Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy en total desacuerdo	Estoy totalmente de acuerdo	Estoy en total desacuerdo	Estoy en total desacuerdo	Estoy en total desacuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo	Estoy de acuerdo
Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy en total desacuerdo	Estoy en total desacuerdo	Estoy en total desacuerdo	Estoy en total desacuerdo	Estoy de acuerdo	Estoy en total desacuerdo	Estoy de acuerdo	Estoy en total desacuerdo
Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy en total desacuerdo	Estoy en total desacuerdo	Estoy en total desacuerdo	Estoy de acuerdo	Estoy en total desacuerdo	Estoy de acuerdo	Estoy en total desacuerdo
Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy en total desacuerdo	Estoy en total desacuerdo	Estoy en total desacuerdo	Estoy en total desacuerdo	Estoy en total desacuerdo
Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy en total desacuerdo	Estoy en total desacuerdo	Estoy totalmente de acuerdo	Estoy en total desacuerdo	Estoy en total desacuerdo
Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy en total desacuerdo	Estoy totalmente de acuerdo	Estoy en total desacuerdo	Estoy totalmente de acuerdo

P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12
Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy en total desacuerdo	Estoy totalmente de acuerdo	Estoy en total desacuerdo	Estoy totalmente de acuerdo
Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo
Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo
Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo
Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo
Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo
Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo
Estoy totalmente	Estoy totalmente	Estoy totalmente	Estoy totalmente	Estoy totalmente	Estoy totalmente	Estoy totalmente	Estoy totalmente	Estoy totalmente	Estoy totalmente	Estoy totalmente	Estoy totalmente

P1	**P2**	**P3**	**P4**	**P5**	**P6**	**P7**	**P8**	**P9**	**P10**	**P11**	**P12**
de acuerdo	de acuerdo	de acuerdo	de acuerdo	de acuerdo	de acuerdo	de acuerdo	de acuerdo	de acuerdo	de acuerdo	de acuerdo	de acuerdo
Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo
Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo
Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo
Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo
Estoy totalmente de acuerdo	No estoy de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo
Estoy totalmente de acuerdo	No estoy de acuerdo	No estoy de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	No estoy de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo
Estoy totalmente de acuerdo	No estoy de acuerdo	No estoy de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	No estoy de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo
Estoy	No estoy de	No estoy de	Estoy	Estoy	Estoy	Estoy	Estoy	Estoy	No estoy de	Estoy	Estoy

P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12
totalmente de acuerdo	acuerdo	acuerdo	totalmente de acuerdo	totalmente de acuerdo	totalmente de acuerdo	totalmente de acuerdo	totalmente de acuerdo	totalmente de acuerdo	acuerdo	totalmente de acuerdo	totalmente de acuerdo
Estoy totalmente de acuerdo	No estoy de acuerdo	No estoy de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	No estoy de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo
Estoy totalmente de acuerdo	No estoy de acuerdo	No estoy de acuerdo	No estoy de acuerdo	Estoy totalmente de acuerdo	No estoy de acuerdo	Estoy totalmente de acuerdo	Estoy totalmente de acuerdo	No estoy de acuerdo	No estoy de acuerdo	No estoy de acuerdo	Estoy totalmente de acuerdo
Estoy totalmente de acuerdo	No estoy de acuerdo	No estoy de acuerdo	No estoy de acuerdo	Estoy totalmente de acuerdo	No estoy de acuerdo	Estoy totalmente de acuerdo	No estoy de acuerdo	No estoy de acuerdo	No estoy de acuerdo	No estoy de acuerdo	Estoy totalmente de acuerdo
Estoy totalmente de acuerdo	No estoy de acuerdo	No estoy de acuerdo	No estoy de acuerdo	No estoy de acuerdo	No estoy de acuerdo	Estoy totalmente de acuerdo	No estoy de acuerdo	No estoy de acuerdo	No estoy de acuerdo	No estoy de acuerdo	Estoy totalmente de acuerdo
No estoy de acuerdo	No estoy de acuerdo	No estoy de acuerdo	No estoy de acuerdo	No estoy de acuerdo	No estoy de acuerdo	No estoy de acuerdo	No estoy de acuerdo	No estoy de acuerdo	No estoy de acuerdo	No estoy de acuerdo	No estoy de acuerdo
No estoy de acuerdo	No estoy de acuerdo	No estoy de acuerdo	No estoy de acuerdo	No estoy de acuerdo	No estoy de acuerdo	No estoy de acuerdo	No estoy de acuerdo	No estoy de acuerdo	No estoy de acuerdo	No estoy de acuerdo	No estoy de acuerdo
No estoy de acuerdo	No estoy de acuerdo	No estoy de acuerdo	No estoy de acuerdo	No estoy de acuerdo	No estoy de acuerdo	No estoy de acuerdo	No estoy de acuerdo	No estoy de acuerdo	No estoy de acuerdo	No estoy de acuerdo	No estoy de acuerdo
No estoy de acuerdo	No estoy de acuerdo	No estoy de acuerdo	No estoy de acuerdo	No estoy de acuerdo	No estoy de acuerdo	No estoy de acuerdo	No estoy de acuerdo	No estoy de acuerdo	No estoy de acuerdo	No estoy de acuerdo	No estoy de acuerdo