COMANDO DE EDUCACIÓN Y DOCTRINA DEL EJÉRCITO

ESCUELA MILITAR DE CHORRILLOS

“CORONEL FRANCISCO BOLOGNESI”


TESIS PARA OPTAR

EL TITULO PROFESIONAL DE LICENCIADO EN CIENCIAS MILITARES CON MENCION EN INGENERIA

# “FILTRACIÓN DE INFORMACIÓN EN REDES SOCIALES Y SUS RIESGOS EN LA SEGURIDAD FÍSICA E INSTALACIONES DE LOS CADETES CUARTO AÑO DE LA ESCUELA MILITAR DE CHORRILLOS “CORONEL FRANCISCO BOLOGNESI”, 2019

PRESENTADO POR:

LINARES FLORIAN BRAYAN ROBERT

RETO HERNÁNDEZ RODRIGO DE JESÚS

VILLALBA PORTUGAL JULIO CESAR HANS

Lima - Perú

2019

# Dedicatoria

A todos los hombres de la lucha silenciosa que sin mayor ambición que ver al Perú pacificado, ofrendaron su vida para subir a la gloria eterna, sin ofrendas, sin buscar reconocimientos, ni exigir pagos, porque nuestra vocación de servicio no tiene paga, nos enorgullece entregar la vida justa, el morir como debe morir un hombre, un soldado defendiendo su honor, su dignidad nuestra sagrada patria.

## Pensamientos

Se puede abandonar a una patria dichosa y triunfante. Pero amenazada, destrozada y oprimida no se le deja nunca; se le salva o se muere por ella.

Maximilien Robespierre

## Agradecimiento

En la realización y ejecución de esta tesis participaron alumnos quienes directamente apoyaron la mano de obra, a los padres de familia que en determinado momento apoyaron con los materiales que se utilizaron, a los docentes que en su momento apoyaron, dando tiempo a los alumnos. A los asesores que apoyaron y permitieron realizar el proyecto. Posiblemente el cambio no se logró en todo, pero con el seguimiento que se la dado en todo este tiempo hemos notado que realmente puede existir un cambio dentro de nuestra institución, cuando se trabaja en equipo y se da la muestra de cooperación y colaboración entre sus integrantes.

# Presentación

Señores miembros del jurado

Dando cumplimiento a las normas establecidas en el Reglamento de Grados y Títulos de la Escuela Militar de Chorrillos para optar la licenciatura en Ciencias Militares, presentamos la Tesis titulada:

## "FILTRACIÓN DE INFORMACIÓN EN REDES SOCIALES Y SUS RIESGOS EN LA SEGURIDAD FISICA E INSTALACIONES, DE LOS CADETES DE CUARTO AÑO EN LA ESCUELA MILITAR DE CHORRILLOS "CORONEL FRANCISCO BOLOGNESI", 2019

- Investigador Temático: Reto Hernández Rodrigo de Jesús
- Investigador Metodológico: Linares Florián Brayan Robert
  Villalba Portugal Julio Cesar Hans

La investigación tiene por finalidad garantizar un sistema de seguridad física e instalaciones a través del control en la información en redes sociales que posibilite una mejora en el desempeño dela gestión de seguridad de los cadetes de cuarto año de la EMCH ; este trabajo de investigación se presenta para obtener el título de Licenciado en ciencias militares en cumplimiento al Reglamento de Grados y Títulos de la Escuela Militar. Por lo expuesto señores miembros del jurado, pongo a vuestra disposición esta investigación para ser evaluada esperando su aprobación.

Atentamente

Los autores

# Índice de contenido


Dedicatoria ii

Agradecimiento iii

Presentación iv

Índice de contenido v

Índice de Figuras. vii

Índice de Tables viii

Resumen ix

Abstract x

Introducción xi

CAPITULO I: PROBLEMA DE INVESTIGACIÓN 13

1.1. Planteamiento del Problema 13
1.2. Formulación del Problema 15
1.2.1 Problema General 15
1.2.2 Problemas Específicos. 16
1.3. Objetivos 16
1.3.1 Objetivo General. 16
1.3.2 Objetivos Específicos. 16
1.4. Justificación 16
1.5. Limitaciones 17
1.6. Viabilidad 18

CAPITULO II: MARCO TEÓRICO 19
2.1. Antecedentes. 19
2.2. Bases Teóricas 23
2.3. Definición de Términos Básicos 42
2.4. Hipótesis 57
2.4.1 Hipótesis General.
2.4.2 Hipótesis Específicas.
2.5. Variables 58
2.5.1 Definición Conceptual

2.5.2 Definición Operacional.

CAPITULO III: DISEÑO METODOLÓGICO 61

3.1. Enfoque 61
3.2. Tipo 61
3.3. Diseño 61
3.4. Método 61
3.5. Población / Muestra 62
3.6. Técnicas/Instrumentos para recolección de datos 62
3.7. Validación y Confiabilidad del Instrumento 63
3.8. Procedimientos para el tratamiento de datos 64
3.9. Aspectos éticos 65

CAPITULO IV: RESULTADOS 66

4.1. Descripción 66
4.2. Interpretación 68
4.3. Discusión 72

CONCLUSIONES 74
Primera Conclusión.
Segunda Conclusión.
Tercera Conclusión.

RECOMENDACIONES 75
Primera Recomendación.
Segunda Recomendación.
Tercera Recomendación.

REFERENCIAS 76

APA (Orden Alfabético, etc.)

ANEXOS 79

1. Base de Datos. 80
2. Matriz de Consistencia. 83
3. Instrumentos de Recolección. 86
4. Documento de Validación del Instrumento. 88
5. Constancia de entidad donde se efectuó la investigación. 90
6. Compromiso de autenticidad del documento. 92

# Índice de Figuras

Pagina

Figura N° 1 Comunicado DINFE, Sobre el uso de las redes sociales para el personal Militar. 23

Figura N° 2 Diagrama muestra un árbol de decisiones para la identificación de riesgos relacionados con la información. 60

Figura N° 3 Cuadro estadístico sobre la filtración de información en las redes sociales. 66

Figura N° 4 Cuadro estadístico de muestra sobre la Seguridad Física e Instalaciones 67

# Índice de tablas


| | | Pagina |
|---|---|---|
| Tabla 1 | General de población Muestra, tamaño de la muestra = 146 | 62 |
| Tabla 2 | Interpretación del coeficiente de confiabilidad para cada variable de estudio. | 63 |
| Tabla 3 | Resultados del análisis de confiabilidad del instrumento que mide la variable 1. | 64 |
| Tabla 4 | Resultados del análisis de confiabilidad del instrumento que mide la variable 2 | 64 |
| Tabla 5 | Distribución de las frecuencias de la Variable 1 | 66 |
| Tabla 6 | Distribución de las frecuencias de la Variable 2 | 67 |

# Resumen

El presente trabajo de investigación tiene como objetivo determinar la filtración de información en redes sociales y los riesgos en la seguridad física e instalaciones, cadetes de cuarto año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2019.

El tipo de investigación utilizado fue de tipo básico, con un nivel descriptivo y correlacional, el diseño de la investigación es no experimental. La muestra estuvo conformada por 146 cadetes de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”. La técnica que se utilizó es la encuesta y los instrumentos de recolección de datos fueron dos cuestionarios aplicados a los cadetes de la mencionada Escuela. En la elaboración del cuestionario se utilizó la Escala de Likert y para su validez el estadístico Alfa de Cronbach, asimismo para la validez de las hipótesis se utilizó el estadístico Rho de Spearman.

Con referencia al objetivo general: determinar las filtraciones de información en redes sociales en la seguridad física e instalaciones, cadetes de cuarto año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2019 se concluye que existe un grado de correlación positiva alto y un nivel de significación estadística, entre las filtraciones de información en las redes sociales y la seguridad física e instalaciones, cadetes de cuarto año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”. Lo que se demuestra con el estadístico de Spearman (sig. bilateral = .000 < 0.01; Rho = .734).

Palabras Clave: Filtración de información, Redes sociales, seguridad física e instalaciones.

# Abstract

The purpose of this research work is to determine the risks of information leakage in social networks in physical security and facilities, fourth-year cadets of the Chorrillos Military School "Coronel Francisco Bolognesi", 2019.

The type of research used was basic, with a descriptive and correlational level, the research design is non-experimental. The sample consisted of 146 cadets of the Chorrillos Military School "Colonel Francisco Bolognesi". The technique used is the survey and the data collection instruments were two questionnaires applied to the cadets of the aforementioned School. In the preparation of the questionnaire, the Likert Scale was used and for its validity the Cronbach Alpha statistic, also for the validity of the hypotheses, the Spearman Rho statistic was used.

With reference to the general objective: to determine the risks of information leakage in social networks in physical security and facilities, fourth-year cadets of the Chorrillos Military School “Coronel Francisco Bolognesi”, 2019 concludes that there is a high degree of positive correlation and a level of statistical significance, between the risks of information leaking in social networks and physical security and facilities, fourth-year cadets of the Chorrillos Military School "Colonel Francisco Bolognesi". What is demonstrated with the Spearman statistic (bilateral sig. = .000 <0.01; Rho = .734).

Keywords: Information filtering, social networks, physical security and facilities.

# INTRODUCCION

En el mundo actual el internet como cambio tecnológico más importante de los últimos tiempos se ha acelerado de manera vertiginosa por lo que el presente trabajo de investigación trata sobre las actividades de actores nacionales que atentan contra la seguridad militar, en este sentido el grave peligro que representa la develación o publicación de información de carácter reservada en las redes sociales.

En el ámbito militar la divulgación de información clasificada está contemplada como delito de infidencia, por lo que es necesario que los elementos o dependencias encargadas de velar por la seguridad dicten normas y procedimientos que regulan la publicación de información en documentos, videos, audios y fotografías de instalaciones y/o actividades castrenses en las redes sociales (Página web, Blogs, Facebook, YouTube, Whatsapp, Twitter, Instagram y otros) para el personal militar y civil, que pongan en riesgo los Activos Críticos de propiedad de la Escuelas Militar de Chorrillos "Coronel Francisco Bolognesi" del Comando de Educación y Doctrina del Ejército.

Por otro lado, proteger los Activos Críticos Institucionales (Personal, Infraestructura física, informaciones, procesos, actividades, operaciones, Infraestructura cibernética), garantizando su seguridad, previniendo, minimizando y neutralizando los riesgos provenientes de actores ajenos a los intereses institucionales y del propio personal, mediante la aplicación de medidas de contrainteligencia, a fin de evitar su publicación en medios de comunicación no autorizados.

En tal sentido, el personal de cadetes de IV año de la Escuela Militar de Chorrillos, deberá adoptar una serie de medidas de seguridad militar, orientadas a prevenir los riesgos de la filtración de información a través de las redes sociales personales que ponen en riesgo la seguridad de las informaciones, quedando expuestos que dicha información quede en manos de la delincuencia o en manos del enemigo externo, y cometer actos de infidencia o en algunos casos comprometidos en actos de espionaje, que puedan mellar la imagen de la institución.

La estructura de esta tesis consta de Siete (07) capítulos, en el capítulo I se considera todo lo relacionado al Problema de Investigación donde se encuentra inmerso el personal de cadetes del IV año de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", los mismos que viene publicando y filtrando de manera sistemática información de carácter clasificado en las redes sociales como

En el capítulo II se desarrolla el marco teórico de la concepción de algunos autores referente a este caso materia de investigación, así como en las últimas décadas las nuevas TIC han impactado en la vida de los seres humanos, en el capítulo III se hace referencia al Marco Metodológico, donde básicamente responde a la necesidad académica de conocer la situación actual de la filtración de informaciones en las redes sociales y los riesgos en la seguridad física y de las instalaciones de los cadetes de IV año de la Escuela Militar de Chorrillos, en el capítulo IV se menciona los Resultados en base al trabajo de campo y encuestas que determinarán las variables en cuanto a la filtración de información, las que terminarán con las conclusiones producto de las investigaciones realizadas al tema de investigación, las que generarán las Recomendaciones correspondientes mediante el dictado de medidas para minimizar los riesgos existentes, culminando este trabajo de investigación con las referencias bibliográficas de autores mencionados en la tesis materia de investigación.

La finalidad de esta breve introducción es despertar el interés en la lectura de este tipo de información tecnológica que tiene que ver con la seguridad en las personas y las instalaciones. lo que permitirá tomar en cuenta diferentes fases de comunicación a través del Internet.

"FILTRACION DE INFORMACION EN REDES SOCIALES Y SUS RIESGOS EN LA SEGURIDAD FISICA E INSTALACIONES, DE LOS CADETES DE CUARTO AÑO DE LA ESCUELA MILITAR DE CHORRILLOS "CORONEL FRANCISCO BOLOGNESI", 2019

# CAPITULO I: PROBLEMA DE INVESTIGACION

## 1.1. Planteamiento del Problema:

Los conflictos desde que el hombre aparece en el mundo siempre se han originado por puntos de vista diferentes entre dos o más personas o sociedades o países. Sin embargo, con el transcurrir de los años estos conflictos han cambiado de forma y de fondo llegando a nuestra situación actual en la que se puede observar como la guerra informativa e ha convertido en algo nuevo; en los conflictos recientes se ha observado como Internet permite a cualquier actor realizar operaciones informativas con una facilidad y efectividad asombrosa. En efecto, tal y como hemos podido observar en Israel, Líbano, Palestina, Siria, Ucrania, Crimea o en el Estado Islámico, el empleo de sistemas tecnológicos como la plataforma multicanal y redes sociales como Facebook, Twitter, Instagram, Flickr o Youtube, permite a cualquier persona recopilar una enorme cantidad de información sobre sus potenciales adversarios e influir en la opinión pública mediante actividades de propaganda y contra propaganda.

Tomando en cuenta estas afirmaciones se puede afirmar que las Fuerzas Armadas de muchos países no pueden estar al margen de este tipo de acontecimientos, por lo que también se han subido al sistema de comunicación informática y al carro de las redes sociales, especialmente para utilizarlas como herramienta de inteligencia y comunicación estratégica. Sin embargo, el uso que su personal hace de los mismos supone una amenaza para la seguridad y defensa nacional.

La tecnología avanza, sus plataformas y entornos evolucionan al mismo tiempo que las integramos en nuestra vida. En muchas ocasiones el ritmo de evolución de la tecnología hace que la integremos en nuestra vida sin tener demasiada consciencia del tema. Por eso pensamos que conviene pararse a reflexionar. Con este objetivo hoy te traemos este post sobre las amenazas en Redes Sociales.

Pero las redes sociales son un medio, neutro en sí mismo, que puede aportar aspectos positivos, pero también negativos para la vida de los usuarios de este tipo de comunicación; es por esa razón que hoy también se considera el lado oscuro de las redes sociales, en el que veremos las principales amenazas y consecuencias que han propiciado. Como dijo Jorge Drexler, "la maquina la hace el hombre, y es lo que el hombre hace con ella" lo que define su utilidad, ya sea para bien o para mal.

Podemos afirmar que hoy en día muchas personas no podrían vivir sin hacer uso de algunas de las social networks que están activas. Aplicaciones como Facebook o Twitter reciben cada día la visita de millones de usuarios, buscando contactar con otras personas o publicar todo aquello que hacen desde que se levantan hasta que se van a la cama. Además de suponer un riesgo para su seguridad, un uso descontrolado de estas plataformas también puede derivar hacia situaciones peligrosas para el individuo.

En el Ejército del Perú, la tecnología particularmente las redes sociales ha sido aprovechada por las diferentes dependencias militares a nivel nacional, utilizándolos para interactuar y compartir información de interés común, pero existe mucha preocupación por el Comando del Ejército porque sus miembros en general están utilizándolos para subir información clasificada. sin tener el mínimo de conciencia de seguridad.

En la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", el problema básicamente se presenta con el personal de cadetes del IV año, ubicado dentro de las instalaciones del Comando de Educación y Doctrina del Ejercito (COEDE), los mismos que vienen publicando y filtrando de manera sistemática información de carácter clasificado, en las diferentes redes sociales como Página web, Blogs, Facebook, YouTube, Whatsapp, etc, en algunos casos subiendo fotografías con uniforme y portando armamento, en lugares de entrenamiento, en desfile, en instrucción, en zona de vivac, en Marcha de Campaña en la región cruz de hueso, en ceremonias estrictamente castrenses, evidenciando las diversas

actividades internas que se realizan en el interior de la instalación militar, propios de la formación de un cadete en la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, vulnerando y trasgrediendo las medidas de seguridad de las informaciones.

Estos hechos desde el punto de vista seguridad, trasgreden y ponen en riesgo la seguridad de las informaciones, toda vez que personal de cadetes de la Escuela Militar de Chorrillos de manera voluntaria o involuntaria, consciente o inconsciente y de manera sistemática vienen publicando información clasificada, exponiendo su integridad física y la de sus familiares teniendo en consideración que actualmente nuestro país la delincuencia o el crimen organizado según estadísticas se incrementa día a día, pudiendo ser objeto de chantaje y/o extorsiones por parte de estos delincuentes, por personal antisistema o por Agentes Enemigos que pudieran estar realizando actos de Espionaje en nuestro País, lo que denota la falta de conciencia de seguridad.

## 1.2 Formulación del problema

La filtración de información en las redes sociales generan riesgos en la seguridad física e instalaciones de los cadetes de cuarto año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”

### 1.2.1 Problema General

¿De que manera la filtración de información en las redes sociales se relaciona con los riesgos en la seguridad física e instalaciones, en los cadetes de cuarto año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2019?

### 1.2.2 Problemas específicos

- ¿De qué manera la filtración de información en las redes sociales se relaciona con los riesgos en la seguridad física, en los cadetes de cuarto año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2019?

- ¿De qué manera la filtración de información en las redes sociales se relaciona con los riesgos en la seguridad de las instalaciones, en los cadetes de cuarto año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2019?

## 1.3 Objetivos

### 1.3.1 Objetivo general

Determinar la filtración de información en las redes sociales se relaciona con los riesgos en la seguridad física e instalaciones, en los cadetes de cuarto año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2019

### 1.3.2 Objetivos Específicos

- Determinar como la filtración de información en las redes sociales se relaciona con los riesgos en la seguridad física, en los cadetes de cuarto año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, ¿2019?

- Determinar como la filtración de información en las redes sociales se relaciona con los riesgos en la seguridad de las instalaciones, en los cadetes de cuarto año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, ¿2019?

## 1.4 Justificación de la investigación

### 1.4.1 Justificación teórica

La información constituye el activo más importante de una institución militar, pudiendo verse afectada por muchos factores tales como el uso indiscriminado de las redes sociales como Página web, Blogs, Facebook, YouTube, WhatsApp, etc, pudiendo ser objeto de robos, extorsiones, secuestros, chantaje. Por eso es importante que la EMCH desde el punto de vista seguridad más importante que debe resolver la Escuela Militar de Chorrillos, a través de la sección Seguridad es la protección permanente de su información crítica, dictando medidas destinadas a

prevenir o neutralizar el uso indiscriminada de las redes sociales, por parte de los Cadetes de IV año.

### 1.4.2 Justificación metodológica

Este trabajo de investigación se justifica desde el punto de vista metodológico, primero porque es una investigación del tipo Descriptiva, siendo importante subrayar que no se busca una simple descripción, debido a que la información obtenida ha sido organizada y analizada para derivar a conclusiones significativas, basadas en cuadros comparativos, de contrastación y de relaciones entre los aspectos investigados; por lo tanto, el descubrimiento de algo significativo es la meta de todo el proceso.

### 1.4.3 Justificación practica

Esta investigación se justifica desde el punto de vista práctico, pues se va a contar con actividades objetivas o prácticas que permitan su aplicación a este tipo de investigación, porque también se realizan actividades de análisis respecto a comentarios, conversaciones y testimonios de personajes resaltantes de cada una de las clases sociales que se manifestaron durante el incidente.

## 1.5 Limitaciones

En este presente trabajo se contó con algunas limitaciones particularmente de índole bibliográfico, Geográfico, económico y temporal.

En el aspecto bibliográfico no se puede visitar muchas bibliotecas excepto de la EMCH por el poco tiempo que se dispone, sin embargo se hizo todo lo posible para superar esta limitación; como aprovechar la información obtenida de medios tecnológicos, como el Internet, así como obtener información o documentos normativos, directivas, resúmenes de contrainteligencia o cualquier información relacionada al tema; más aún, se puede mencionar que la Sección Inteligencia de la Escuela Militar de Chorrillos, normalmente no proporciona información abierta por tratarse de documentos de carácter reservado, confidencial o secreto la misma que

limito nuestro trabajo para poder guiarnos y conocer el nivel de protección que cuenta el campo de las informaciones en los documentos Clasificados y sobre todo información de antecedentes protagonizadas por los cadetes de IV año; sobre riesgos en la filtración de informaciones en las redes sociales; asimismo, si existe un plan de Prevención e instrucción para que el personal conozca lo que significa "conciencia de seguridad".

En cuestión de tiempo, no se pudo contar con mucho espacio para la elaboración del proyecto ya que el Batallón de Cadetes viene desarrollando su instrucción militar y civil, paralelamente a ello, las obligaciones con algunos exámenes que se programan semanalmente.

En relación a la parte económica, existió un mínimo obstáculo debido a que se contó con el apoyo económico de nuestros padres y la propina que se recibe en la EMCH.

## 1.6 Viabilidad

El presente trabajo de investigación es viable porque se cuenta con el asesoramiento del personal de docentes, asesores de tesis de la Escuela Militar de Chorrillos que han apoyado en la corrección de las observaciones, así como el apoyo de revisores que enrumban de manera más objetiva el proyecto.

Asimismo, se ha tenido apoyo por parte de la dirección de la EMCH, por otorgar días adicionales de investigación con la salida al exterior, básicamente para realizar trabajo de campo especialmente para completar, buscar, recopilar datos o información para el presente trabajo de investigación, habiéndose programado algunos días para dicha salida, las cuales no fueron suficientes por el poco tiempo de que se dispone. Sin embrago se logró superar todos los obstáculos para lograr que este trabajo sea viable.

# CAPITULO II: Marco Teórico

## 2.1 Antecedentes

### 2.1.1 Internacional

Foltýn (2018) en su artículo Cómo la sobreexposición en redes sociales puede traer problemas, señala que a nivel internacional vivimos en una época en la que todo se comparte, donde el auge de sitios y plataformas para el networking abrieron una nueva manera de compartir todo tipo de información personal; al punto de que la divulgación de una gran cantidad de detalles personales en Internet pasó a un segundo lugar de importancia para los usuarios.

La urgencia de las personas por querer compartir no es nueva. Este comportamiento lo que hace es evidenciar el intrínseco deseo humano de querer vincularse con los otros. Por lo tanto, quizás podríamos decir que este "problema" no es responsabilidad del fenómeno digital en sí mismo, sino más bien que la incidencia de lo digital está más relacionada con el tipo de información que compartimos y a quién permitimos acceder a ella.

Sobresaturadas de información personal, las redes sociales se convirtieron en un territorio ideal para los criminales. Habiendo utilizado estos sitios como herramientas de reconocimiento, un atacante puede enviarte un mensaje dirigido (spearphishing) en el que intenta persuadirte para que visites una página falsa, que parece ser legítima, con el objetivo de robar tus credenciales y dinero. También pueden manipularte para que caigas en la trampa de abrir un adjunto infectado con un malware que actúa como un dropper de otro malware con capacidad para realizar todo tipo de cosas; incluyendo filtración de datos o grabación de todo lo que tipeamos en la computadora mediante un keylogger.

Es importante entender que el concepto de networking que se ubica en el corazón de las plataformas sociales no promueve un estado de precaución, sino todo

lo contrario. Muchas personas bajan la guardia en las redes sociales y pinchan en enlaces maliciosos que difícilmente pincharían si fuesen recibidos en un correo electrónico.

Si bien las técnicas de ingeniería social surgieron con anterioridad al arribo de las plataformas sociales online, con la llegada de las redes sociales tomaron impulso y abrieron nuevas vías para el robo de identidad, fraudes online y otro tipo de delitos.

Jiménez (2014) en su trabajo de investigación Riesgos de las redes sociales informáticas internet social network risks (España) concluye que sobre la privacidad y la seguridad puede tener un uso descuidado de las redes sociales, permite concluir que ya desde los inicios se apreciaba que hacer públicos datos personales de forma que se facilitara la identificación directa o indirecta de quien los publicaba podría suponer serios riesgos para los usuarios, pues terceros usuarios o empresas podrían utilizarlos de forma malintencionada causando todo tipo de inconvenientes, fundamentalmente los relacionados con la vulneración de derechos fundamentales, como el derecho al honor, a la intimidad personal y familiar y a la propia imagen, el derecho al secreto de las comunicaciones, el derecho a la protección de datos de carácter personal, el derecho a la protección de la propiedad intelectual e industrial y los derechos de consumidores y usuarios. [1]

### 2.1.2 Nacional

Zegarra (2018), en su estudio sobre riesgos de las redes sociales señala que los Adolescentes corren mayor riesgo de recibir contactos no deseados en redes sociales. Casi el 50% de los entrevistados en el Perú señaló que extraños intentaron obtener información personal. Además, el 43% recibió intentos repetidos para socializar a pesar de haberse negado previamente a aceptar una invitación en alguna red social.

El 63% manifestó haber estado expuesto a contenidos engañosos o fraudes en la red. Esta cifra es superior en 10 puntos al promedio global. El 62% recibió noticias falsas. El 47% sostuvo que le enviaron comentarios ofensivos y el 37% fue víctima de cyberbullying. En cuanto a riesgos de carácter sexual, el 60% recibió fotos o contenido sexual. El 41% tuvo propuestas de relaciones sexuales a través de internet.

Carmen Zegarra, directora de la Unidad de Delitos Cibernéticos de Microsoft Perú, sostuvo que el Día de Internet Seguro es una "oportunidad para impulsar un ecosistema más seguro para las personas, empresas y gobiernos, además de alentar una conducta más cívica en internet". Las mujeres de 14 a 17 años han experimentado 4.2 casos de riesgo en el último año y 3.1 en el caso de adolescentes varones. Los millenials advirtieron de 3.2 casos en el 2018, según el informe.

RPP (2013) en su artículo Los jóvenes y la violencia detrás de las redes sociales, señala que Hoy en día las redes sociales se han convertido en uno de los principales vehículos de comunicación online que con frecuencia son utilizados por los adolescentes, en su mayoría, para ampliar sus contactos, interactuar con sus amigos e intercambiar información, sea de las tareas de la escuela u otras de tipo personal como fotos, música y videos.

Uno de los principales problemas en las redes, como el Facebook y el Twitter (por citar los más difundidos), es la publicación sin reparo de fotos o videos comprometedores que de una u otra forma buscan dañar la reputación o herir los sentimientos de una persona, mediante la burla, el acoso o el chantaje sexual.

Estos cibermensajes o información mal empleada pueden poner en riesgo la integridad física y psíquica del adolescente. Algunos jóvenes pensarán que se trata de un juego, de una broma, y que lo hacen por divertirse; pero detrás de ello existen otras personas que están al acecho y buscan estas páginas para acercarse a las chicas y los chicos para chantajearles o someterlos sexualmente a sus propios intereses.

### 2.1.3 Local

En el Ejército del Perú, la tecnología particularmente las redes sociales ha sido aprovechada por las diferentes dependencias militares a nivel nacional, utilizándolos para interactuar y compartir información de interés común, pero existe mucha preocupación por el Comando del Ejército porque sus miembros en general están utilizándolos para subir información clasificada. sin tener el mínimo de conciencia de seguridad, tal es así que la Dirección de Informacion del Ejercito (DINFE) el 24 Ene 19, publico el Comunicado 001 DINFE - 2019, sobre el uso de las redes sociales para el personal militar de la institución, donde muestra su preocupación que personal de nuestra institución estaría difundiendo en las redes sociales textos, imágenes video y/o información que podría afectar la imagen institucional o la seguridad de las informaciones.

Actualmente, se ha tomado conocimiento que en el Ejercito del Perú, se viene evidenciando que personal de Cadetes de la Escuela Militar de Chorrillos del IV año, viene filtrando de manera reiterativa información de carácter reservado en las diferentes redes sociales personales como Facebook, Messenger, WhatsApp, YouTube, Twitter, etc., trasgrediendo y vulnerando las medidas de seguridad de las informaciones, denotando falta de “conciencia de seguridad”, situaciyn que pondría en riesgo su integridad física, familiar e institucional; más aún, conociendo que actualmente nuestro país es la nación con las cifras más altas de inseguridad, superado solo por Venezuela, donde hoy se vive una grave crisis social, pudiendo ser objeto de extorsión, chantaje, secuestro, robo etc.

(Ver recuadro).

EJERCITO DEL PERU
24 de enero 2019: Sobre el uso de las redes sociales para el personal militar
COMUNICADO N° 001 - DINFE

1. Se viene apreciando con mucha preocupación que personal de nuestra institución estaría difundiendo en las redes sociales textos, imágenes, videos, etc y/o información que podrían afectar la imagen institucional o la seguridad de las informaciones.
2. Al respecto existe la normativa siguiente:
   a. Anexo II - 11.2 y II - 12.1, infracciones graves del régimen disciplinario de las Fuerzas Armadas y los artículos 73° y 74° del código Penal Militar Policial.
   b. El Articulo 132° del Código Penal.
3. Los sistemas de Informacion y de Inteligencia del Ejército están realizando el seguimiento y monitoreo permanente de las redes sociales para detectar la exposición, difusión y/o comentarios que afectan la imagen institucional o la revelación de información clasificada. Los responsables serian sometidos al procedimiento disciplinario y/o denuncia penal que corresponda.
4. Se exhorta a todo el personal a continuar colaborando eficientemente en provecho de nuestra institución, rechazando todo tipo de actos que denigren la imagen institucional que los integrantes de nuestro glorioso ejercito estamos empeñados en fortalecer.

DINFE

Figura N° 1. Comunicado DINFE. Sobre el uso de las redes sociales para el personal militar

## 2.2 Bases Teóricas

Es importante considerar que la profundidad sobre la globalización y la tecnología viene incidiendo en esta idea sobre la importancia de orientar su utilización para lograr una sociedad más humana, justa e igualitaria.

La reglamentación de la Ley Nº 29131 “Ley del Régimen disciplinario de las FFAA”, en su artículo 1º establece lo siguiente:

Condición de militar

La condición de militar se opta por voluntad propia y se adquiere a través de los centros de formación, procesos de asimilación y servicio militar; se

sujeta a las condiciones de vida y restricciones propias de la carrera militar, conforme a la Constitución Política del Perú y la Ley, y en tanto permanezca en la situación militar de actividad o disponibilidad. Se sustenta en la disciplina, espíritu, honor, moral, ética y virtudes militares.

El personal militar está sujeto a un régimen especial de servicio a la patria, de acuerdo a las leyes y los reglamentos militares que regulan su organización, funciones, especialidades, preparación, empleo y disciplina.

La Ley Nº 29131 "Ley del Régimen disciplinario de las FFAA", en su artículo 9º "Regulaciones en el ejercicio de algunos derechos constitucionales", literal "a" establece lo siguiente: "A la libertad de información, opinión, expresión y difusión de pensamiento en relación con asuntos de seguridad nacional, sin previa autorización ni censura ni impedimento alguno".

En el artículo 3º del reglamento del DL Nº 1141 "Fortalecimiento y Modernización del Sistema de Inteligencia Nacional-SINA y de la Dirección Nacional de Inteligencia-DINI", define conceptos para la actividad de Inteligencia, tales como: Activos Críticos Nacionales, Amenaza, Riesgo, Impacto y Medidas de Contrainteligencia.

El Comando de Educación y Doctrina del Ejército, posee bienes tangibles e intangibles materializados en Activos Críticos, que requieren ser protegidos, administrados y custodiados para mantener la disponibilidad, integridad y confidencialidad; por lo tanto, los únicos responsables de cautelar estos Activos Críticos son los integrantes del Comando de Educación y Doctrina del Ejército. y el control estará a cargo de los diferentes niveles de Comando.

A partir del año 2000, en los teléfonos móviles aparece la

tecnología de los "Smartphone", los mismos que incorporaron funcionalidades que van mucho más allá del empleo tradicional. Hoy en día, en un solo equipo móvil se puede contar con: Acceso a internet (redes sociales), cámara de fotográfica, grabadora de audio y vídeo, GPS, bluetooth y otras funciones dependiendo de las características y tipo de equipo telefónico. Se pronostica que los dispositivos móviles generarán el 98% del tráfico de datos móviles en el año 2020. En tal sentido, los teléfonos inteligentes (Smartphone) seguirán teniendo importancia predominante en la actividad diaria de una sociedad.

La macro red de Internet y las nuevas tecnologías favorecen el desarrollo de las Instituciones, pero a la vez las exponen a ser vulnerables a actores hostiles, que pueden valerse de estos medios para extraer y publicar información de interés, que ponen en riesgo la seguridad de los Activos Críticos Institucionales.

Las Redes Sociales están cobrando gran importancia en el desarrollo de la sociedad, reflejando la necesidad del ser humano de expresión y reconocimiento que le permita vivir en sociedad.

El uso inadecuado de los servicios que ofrece el internet, así como el uso masivo de las redes sociales por parte de personal militar y civil de las Escuelas de Armas y Servicios, Unidades, Dependencias y EM del Comando de Educación y Doctrina del Ejército., pone en riesgo los Activos Críticos Institucionales (Personal, Infraestructura física, informaciones, procesos, actividades, operaciones, Infraestructura cibernética), ya que estos permiten difundir en tiempo real información común y clasificada que puede afectar a la Institución.

La seguridad se obtiene mediante la adopción de medidas destinadas a minimizar los riesgos existentes, el componente humano es determinante en el cumplimiento de los objetivos de seguridad, siendo indispensable

disponer de personal adoctrinado y de probada lealtad, lo que se consigue con una capacitación permanente.

Las informaciones, instalaciones, material d e guerra, vestimenta, actividades castrenses, procesos, operaciones militares, conferencias, video conferencias y todo lo relacionado a Activos Críticos ya sea analógicas o digitales materializadas en cualquier documento son de propiedad de las Escuelas de Armas y Servicios, Unidades, Dependencias y EM del Comando de Educación y Doctrina del Ejército.

Cada vez es mayor la necesidad de sistematizar nuestros procesos, para lo cual la tecnología es indispensable para tal fin; esta dependencia ha permitido identificar nuevas amenazas y riesgos que de materializarse generan impactos negativos a la Institución.

Las medidas de seguridad están orientadas a contrarrestar las acciones de actores ajenos a los intereses institucionales y de los que se originan por la acción de nuestro propio personal que pueden ser utilizados por terceros, aprovechando riesgos del propio personal.

Constantemente el personal militar y civil que hace uso de las redes sociales publican información sensible de Activos Críticos, en forma indiscriminada y sin control, en horas laborables o fuera de estas y en muchos casos empleando los medios disponibles para el desarrollo de su trabajo.

En las páginas web de las diferentes Escuelas de Armas y Servicios, Unidades, Dependencias y EM del Comando de Educación y Doctrina del Ejército (COEDE), se viene publicando información sensible mediante fotografías de actividades administrativas, operaciones y entrenamiento de personal militar, dicha información es de gran interés y de fácil acceso a

los actores ajenos o externos a los intereses institucionales, particularmente a las organizaciones de inteligencia, que sin tener que hacer mucho esfuerzo, obtienen información de fuente cerrada para sus fines y propósitos.

Algunas Escuelas de Armas y Servicios, Unidades, Dependencias y EM del Comando de Educación y Doctrina del Ejército (COEDE), han creado blogs, para difundir y administrar información en el ciberespacio, publicando información con fines de difundir sus actividades, sin haber evaluado las medidas de seguridad y los riesgos que estas representan y no existe un ente de control que las regule.

La Infraestructura Física que el Estado ha puesto a disposición de las Escuelas de Armas y Servicios, Unidades, Dependencias y EM del Comando de Educación y Doctrina del Ejército, para el cumplimiento de la misión está conformada por aquellos bienes materiales construidos por el hombre, de carácter fijo, de los que se obtiene información de interés para la Seguridad Nacional, los mismos que tienen que ser cautelados en todo momento y corrigiendo aquellas irregularidades que algunos integrantes del Ejército hacen o pretenden realizar.

En la actualidad se viene detectando publicaciones en internet (redes sociales) con información sensible, que afectan la imagen institucional y la seguridad de los Activos Críticos Institucionales. Estas publicaciones tienen como promotor a personal militar y empleados civiles en actividad que laboran en las Escuelas de Armas y Servicios, Unidades, Dependencias y EM del Comando de Educación y Doctrina del Ejército. Estas publicaciones van desde:

- Fotografías de actividades administrativas (distribución de alimentos, instrucción, mantenimiento, entre otras) mostrando en forma inadecuada imágenes que afectan a la institución.

- Actividades que comprometen la confidencialidad del material de guerra (armamento, munición, explosivos, etc) y la ubicación de las instalaciones militares que almacenan este material.
- Actividades de operaciones y entrenamiento militar (desplazamientos de tropas, ejercicios de tiro, zonas de vivac, operaciones contraterroristas, entre otras).

- Actividades de instrucción en cursos militares en las diferentes escuelas de instrucción.

- Actividades militares con información del recorrido de sus visitas hacia las diferentes instalaciones militares (Escuelas de formación, entrenamiento, marchas de campaña, etc.), de la cual se pueden obtener informaciones de interés a organizaciones de Inteligencia extranjeras, permitiéndoles en algunos casos: Identificar la ubicación de estas instalaciones, capacidad y disponibilidad del material bélico, rutinas e itinerarios de las dependencias, rutas de acceso y de evacuación, evaluar el grado de entrenamiento, nivel de liderazgo y moral del personal militar, entre otras que son consideradas información de fuente cerrada.

- Publicación de información relacionada al personal militar (Datos personales, cambios de colocación, plan de cambios, nombramiento a cursos castrenses, entre otras).

- Personal Militar que recibe información con comentarios negativos provenientes de personas desafectas, los mismos que replican dicha información a sus contactos con un like (me gusta), contribuyendo con el mal empleo de estos medios y a la vez generando una corriente de opinión negativa que afectan la imagen y la seguridad de los Activos Críticos Institucionales.

El personal militar en la situación de actividad, cualquiera sea su jerarquía y cargo se encuentra obligado a dar cumplimiento al presente documento, de su derecho fundamental de información, opinión y expresión, con el fin de no desproteger los intereses institucionales y nacionales que cautelan las Escuelas de Armas y Servicios, Unidades, Dependencias y EM del Comando de Educación y Doctrina del Ejército.

El personal civil que labora bajo los distintos regímenes laborales en el Comando de Educación y Doctrina del Ejército, mediante el presente documento se encuentra obligado a acatar la regulación para la publicación de información sensible en documentos, videos, audios y fotografías de instalaciones y/o actividades castrenses.

El uso de esta tecnología exige a que el personal militar y civil sea permanentemente adoctrinado para que adopte medidas destinadas a minimizar los riesgos existentes, así determinar el cumplimiento de los objetivos de seguridad.

La Dirección de Informaciones del Ejército será la encargada de autorizar, regular y controlar el uso de las páginas web/blogs de las Escuelas de Armas y Servicios, Unidades, Dependencias y EM del Comando de Educación y Doctrina del Ejército (COEDE), que lo soliciten. La información que se difunda en las páginas web/blogs deberán de estar orientadas a contribuir y fortalecer la imagen institucional, resalten los valores y tradiciones hacia la sociedad.

En los departamentos o secciones donde se formulen documentos con información sensible que ponga en riesgo la seguridad militar e imagen institucional, los Comandantes Generales, Directores, Jefes de Oficina y/o dependencias militares del Ejército deberán restringir el uso permanente de teléfonos celulares con capacidad de acceso a internet, cámaras fotográficas, grabadora de audio y video, bluetooth y otras funciones que faciliten la

obtención y difusión de cualquier tipo de información en tiempo real.

Está prohibido que el personal militar y civil, aprovechando su condición difunda o publique información sensible (documentos, fotografías de operaciones, instrucción, desplazamientos, vídeos, audios u otros) a través de las redes sociales, usando cualquier medio disponible.

Asimismo, está prohibido que el personal militar y civil del Escuelas de Armas y Servicios, Unidades, Dependencias y EM del Comando de Educación y Doctrina del Ejército (COEDE), realicen comentarios tendenciosos sobre otras publicaciones y retrasmitan mensajes haciendo uso de las diferentes capacidades que brinda el ciberespacio. El personal militar y civil que por cualquier circunstancia reciba este tipo de comentarios deberá dar cuenta a su comando respectivo.

Disposiciones emanadas por el Jefe de Estado Mayor del COEDE

El O/M N° 138/U-3.d.2.d del 10 Abr 19, dentro de sus disposiciones menciona lo siguiente: Se viene detectando la falta de "CONCIENCIA DE SEGURIDAD" por parte del personal militar quienes vienen realizando publicaciones empleando las redes sociales (Facebook, Youtube, WhatsApp, Twitter, Instagram y otros), muchas veces conteniendo información de carácter clasificada afectando los activos críticos Institucionales, re3iterando que dichos actos son considerados "DELITO DE INFIDENCIA" de acuerdo a lo prescrito en la Ley N° 29131 "Ley del régimen Disciplinario de las Fuerzas Armadas".

El O/M N° 139/U-3. d.2.d del 10 Abr 19, dentro de sus disposiciones menciona lo siguiente: Los Oficiales de Seguridad de cada dependencia deberá de llevar un registro de personal autorizado por las oficinas de información de su ámbito de responsabilidad, para la toma de fotografías, grabaciones de videos y un registro de las actividades donde participa este

personal.

Asimismo, Los Oficiales de Seguridad deberán controlar que durante las reuniones Oficiales en las cuales se trate temas de interés institucional, el personal del Ejército no deberá de ingresar con dispositivos electrónicos, que puedan vulnerar la seguridad militar, tales como cámaras fotográficas, grabadoras de audio y video, dispositivos electrónicos que enmascaran actividades de espionaje.

El O/M N° 119/U-3. d.2.d del 20 Mar 19, dentro de sus disposiciones menciona lo siguiente: considerando que las actividades, procesos y operaciones que realiza la institución deben de mantener la confidencialidad, en todo momento al personal militar debe evaluar el riesgo y el impacto que puede generar la difusión de una publicación o comentario tendencioso en las redes sociales, aplicativos de mensajería instantánea u otros medios no autorizados por el Comando.

El Oficio N° 114 del 11 Mar 19, dicta normas para minimizar los riesgos de los sistemas de información en las dependencias del Ejército, contenidas en los sistemas de información y medios informáticos e impedir que sean utilizados por un enemigo declarado o potencial y que llegue a su conocimiento por indiscreción, negligencia o traición del propio personal.

Los Oficiales de Seguridad de las dependencias militares del COEDE, deberán instruir de manera permanente al personal militar y civil sobre los riesgos existentes con la filtración y publicación de información clasificada en las redes sociales personales, pudiendo ser objeto de un acto delictivo provenientes del crimen organizado, personal antisistema o ser reclutado por Agentes Enemigos para actividades de espionaje. Toda esta información permite considerar los siguientes términos:

### 2.2.1 Tecnología de Información y Comunicación (TIC)

Para Cabero las TIC: "En líneas generales podríamos decir que las nuevas tecnologías de la información y comunicación son las que giran en torno a tres medios básicos: la informática, la microelectrónica y las telecomunicaciones; pero giran, no sólo de forma aislada, sino lo que es más significativo de manera interactiva e interconexionadas, lo que permite conseguir nuevas realidades comunicativas". Cabero (1998: 198)

Existen múltiples instrumentos electrónicos que se encuadran dentro del concepto de TIC, la televisión, el teléfono, el video, el ordenador. Pero sin lugar a duda, los medios más representativos de la sociedad actual son los ordenadores que nos permiten utilizar diferentes aplicaciones informáticas (presentaciones, aplicaciones multimedia, programas ofimáticos...) y más específicamente las redes de comunicación, en concreto Internet.

Es a partir de este hecho que ha comenzado a considerarse la influencia que estas tecnologías pudieran tener en el desarrollo personal de quienes la usan, especialmente en los grupos de desarrollo de mayor influencia, como son los niños, adolescentes y jóvenes Oliva, Hidalgo, Moreno, Jiménez, Antolín & Ramos, (2012). Dentro de las influencias positivas que algunas investigaciones han encontrado en el grupo antes mencionado, tenemos que los menores que han nacido y crecido con el desarrollo de las tecnologías modernas, especialmente en el uso de la computadora, manejan mejores recursos de información, se expresan mejor por escrito, facilitando la expresión de sentimientos, emociones, inquietudes, entre otros, llegando incluso, en algunos casos, a obtener un mejor rendimiento escolar. Oliva et al., (2012).

La tecnología además de tener aspectos positivos tiene aspectos negativos como llegar a depender de aparatos tecnológicos (celulares,

reproductores de música, computadoras, televisor, entre otros...), de las redes sociales (videojuegos en línea, foros de discusión, uso indiscriminado del chat, etc.) que genera dependencia psicológica, es decir, evasión de los problemas, modificación del estado de ánimo, pérdida de control y focalización, además se han dejado de utilizar como fuente de información los libros, ya que son remplazados por páginas de Internet que nos brindan la información que deseamos.

Adicción a las redes sociales: Las TIC

Simplifican los quehaceres cotidianos, facilitando la búsqueda, hallazgos e intercambio de información diversa en el menor tiempo posible, y no solo ello, sino que propician el contacto con otras personas de manera fácil, sin considerar el tema de la distancia. De esta forma, como se citó previamente, existe un uso positivo de estas tecnologías; sin embargo, también se observa actualmente el abuso de las mismas, las cuales pueden llegar a provocar cambios y alteraciones en el comportamiento y en la conducta de las personas, dentro de ellas se han identificado los siguientes: aislamiento, indicadores de ansiedad, disminución de la autoestima, poco autocontrol de acciones relacionados al uso de las tecnologías. CODAPA, (Confederación Andaluza de Asociaciones de Madres y Padres del Alumnado por la Educación Pública 2011).

### 2.2.2 Autoestima

La autoestima es uno de los constructos psicológicos más conocidos y tratados en los últimos años, su estudio, involucra conocer lo más profundo del ser humano, considerándose como una característica importante en la vida de las personas.

Como una primera definición podríamos entender a la autoestima como el valor que nos asignamos a nosotros mismos, y que se relaciona con

la aceptación de nuestros aspectos positivos y negativos, sentirnos bien con lo que somos y encontrarnos satisfechos con nuestros logros y consigo mismo.

Para Rosenberg (1965, citado en Sánchez, 1999) la autoestima, desde una aproximación sociocultural, seria definida como "una actitud, tanto positiva como negativa, que la gente tiene sobre sí misma" (p. 3). Concibiéndose a ésta como producto de las influencias de la cultura, la sociedad, la familia y las relaciones interpersonales. De lo que se desprende que la autoestima seria proporcional al grado en que el individuo es capaz de medirse de forma positiva respecto a una serie de valores.

Páez, Zubieta, Mayordomo, Jiménez y Ruiz (2004) definen a la autoestima como la actitud que las personas tienen sobre sí mismo, es decir su autoconcepto, a nivel cognitivo; a nivel afectivo, abarcaría sentimientos de valor y respeto sobre sí; y a nivel conductual, a un mejor afronte ante los hechos estresantes, es decir una mejor adaptación y bienestar personal.

### 2.2.3 Analfabetismo audiovisual.

La educación en medios de comunicación tiene como función básica la formación de la conciencia crítica y el desarrollo de actitudes activas y creativas en los estudiantes. El fenómeno del analfabetismo audiovisual es una realidad palpable en nuestra sociedad. El consumo masivo e indiscriminado de los medios no lleva parejo un conocimiento de los códigos del lenguaje audiovisual, provocando situaciones de indefensión ante sus mensajes.

La Educación para los Medios de Comunicación, representa un proceso que tiende a problematizar tanto el contenido como la relación que establece el sujeto receptor con los medios de comunicación. En definitiva,

se trata de incentivar una mirada sin prejuicio, a través de la cual los jóvenes se sitúen como consumidores de la televisión, la radio o el cine, sin culpa de serlo, y conocer los gustos o preferencias espontáneos que se poseen, los vacíos que cubren, las necesidades que satisfacen, buscando entender a qué patrones culturales, sociales, de sexo o edad corresponden.

En segundo lugar, confrontar estas experiencias espontáneas con el sentido que los mensajes pretenden comunicar. El Consejo Internacional de Cine y Televisión estableció que por Educación en materia de Comunicación cabe entender el estudio, la enseñanza y el aprendizaje de los medios modernos de comunicación y de expresión, a los que se considera parte integrante de una esfera de conocimientos específica y autónoma en la teoría y en la práctica pedagógica, a diferencia de su utilización como medios auxiliares para la enseñanza y el aprendizaje en otras esferas del conocimiento, como las Matemáticas, la Ciencia y la Geografía. UNESCO, (1984, 8).

La cultura de la interacción

El carácter de interactividad de las TIC ha favorecido una nueva forma de cultura que autores tales como Tapscott (1997), Naval, Sábada, Bringué y Pérez Alonso-Geta (2003) y Gil, Feliú, Rivero y Gil (2003), entre otros, la han denominado «cultura de la interacción».

Tapscott (1997:51) conceptualizó la cultura de la interacción refiriéndose a «la nueva cultura». En el sentido más amplio la define como:

Los patrones socialmente transmitidos compartidos de comportamiento y formas sociales (…), ya que tienen sus raíces en la experiencia de ser joven y (…) en el hecho de formar parte de la generación más numerosa que ha existido (…).

De esta afirmación se desprende que la cultura de la interacción se manifiesta a través del uso de las TIC, principalmente en la población joven, quien construye nuevas formas de interacción mediante estas tecnologías. Chicas y chicos han incorporado a la vida cotidiana el uso de las TIC, como una herramienta de interacción, de socialización, de trabajo, de diversión etc., dentro de su contexto social y educativo.

El carácter de interactividad que poseen las TIC rompe el modelo lineal de comunicación, ya que los usuarios no sólo consumen el contenido de los medios, sino que lo comparten con otros, lo reproducen, lo redistribuyen, y lo comentan. Koerner y otros (2002).

### 2.2.4 Comunicación

Según (Nieves, 2008) la palabra Comunicación proviene del latín communis que significa común. Tanto el latín como los ISSN 1390-9541 REVISTA CIENTÍFICA COMUNICACIÓN VS TECNOLOGÍA 51 idiomas romances han conservado el especial significado de un término griego, el de "Koinoonia", que significa a la vez comunicación y comunidad.

Tradicionalmente, la comunicación se ha definido como «el intercambio de sentimientos, opiniones, o cualquier otro tipo de información mediante habla, escritura u otro tipo de señales». Todas las formas de comunicación requieren un emisor, un mensaje y un receptor destinado, pero el receptor no necesita estar presente ni consciente del intento comunicativo por parte del emisor para que el acto de comunicación se realice. En el proceso comunicativo, la información es incluida por el emisor en un paquete y canalizada hacia el receptor a través del medio. Una vez recibido, el receptor decodifica el mensaje y proporciona una respuesta Berlok (1969)

### 2.2.5 Tecnología

Según el Glosario de la (UNESCO, 1999), Tecnología es el conjunto de conocimientos científicos y empíricos para alcanzar un resultado práctico: un producto, un proceso de fabricación, una técnica, un servicio, una metodología.

Según Ciapuscio (1999) la tecnología es el conjunto de conocimientos técnicos, científicamente ordenados, que permiten diseñar y crear bienes y servicios que facilitan la adaptación al medio ambiente y satisfacer tanto las necesidades esenciales como los deseos de la humanidad.

### 2.2.6 Relación entre medios de comunicación y tecnología.

La Evolución de la Comunicación Humana desde la perspectiva tecnológica. La búsqueda constante del hombre por satisfacer cada vez mejor su necesidad de comunicación ha sido el impulso que ha logrado la instauración en el mundo de instrumentos cada día más poderosos y veloces en el proceso comunicativo. Sólo basta una retrospectiva para definir cómo el ser humano ha logrado evolucionar sus formas de comunicación: Desde rudimentarios métodos como la escritura jeroglífica, pasando por la invención del alfabeto y del papel, dando un leve salto hasta la llegada de la imprenta, y apenas uno más para la aparición del teléfono, el cine, la radio y la televisión. Todos estos instrumentos han sido ciertamente un avance en las formas de comunicación del hombre y, prácticamente todos, han sido posibles gracias a la tecnología, que a su vez ha sido el instrumento cuya evolución ha determinado el avance de la humanidad.

Desde siempre, el hombre ha tenido la necesidad de comunicarse con los demás, de expresar pensamientos, ideas, emociones; de dejar huella de sí mismo. Así también se reconoce en el ser humano la necesidad de buscar, de saber, de obtener información creada, expresada y transmitida por otros. La

creación, búsqueda y obtención de información son pues acciones esenciales a la naturaleza humana. Tal vez por eso los grandes saltos evolutivos de la humanidad tienen como hito la instauración de algún nuevo instrumento de comunicación.

La tecnología es justamente el medio que ha permitido responder cada vez mejor a las necesidades humanas facilitando y simplificando procesos. Cordeiro expresa al respecto que "…la tecnología es la que precisamente ayuda al progreso de la humanidad. Gracias a la tecnología avanzamos más y tenemos más tiempo para nosotros mismos. Cada revolución tecnológica provoca transformaciones fundamentales que conllevan al mejoramiento de la vida de los seres humanos". La computación y la informática son apenas un ejemplo de las capacidades inventivas de la humanidad dirigidas en estos tiempos urbanos a simplificar las actividades del hombre.

Según Mc Anany, Citado por Canga Larequi, (1988) la Tecnología es: "El resultado de una aplicación racional de principios científicos y de ingeniería a la invención y la manufactura de una herramienta destinada a lograr ciertas tareas específicas."

Ahora bien, la tecnología es entonces un instrumento encaminado a obtener resultados prácticos y concretos en el campo determinado en el cual se aplica. Pablos (2001) afirma que "En todo caso, lo que encontramos es que las tecnologías modernizan el proceso, pero mantienen el producto. Éste es el gran principio de las nuevas tecnologías, entender que sólo son piezas para aligerar un procedimiento, para obtener el mismo resultado con mayores facilidades, tal vez con menor esfuerzo humano…". Por tanto, es prudente destacar que el término "Tecnología" por sí mismo es genérico, responde a todo tipo de actividad, es un vocablo que adquiere sentido real cuando se acompaña de un término complementario que se refiera con precisión, a la actividad a la cual se aplica el conocimiento científico. En este caso, la tecnología que se aplica para facilitar y mejorar el proceso de información y

comunicación humana es entonces la que se conoce como Tecnología de Información y Comunicación (TIC).

En tal sentido, Canga Larequi define la tecnología de información y comunicación como un estudio sistematizado del conjunto de procedimientos que están al servicio de la información y la comunicación. Pero la concepción de Tecnologías de Información y Comunicación no puede verse de manera aislada porque se trata de una definición que se enmarca dentro de las actividades humanas. Es así como los avances en la tecnología aplicada al proceso comunicativo dependen en cierta medida de los avances tecnológicos que la humanidad logre en otras áreas del conocimiento científico y esta evolución es la que ha permitido que el proceso comunicativo del hombre tenga hoy características casi ilimitadas en cuanto a tiempo y espacio.

Tecnologías de la información y la comunicación en la educación

Los rápidos progresos que traen consigo las nuevas tecnologías seguirán modificando las formas de elaboración, adquisición y transmisión de los conocimientos. Permitirán, además, aprovechar las posibilidades que brindan para la educación y la enseñanza al mejorar la manera de producir, organizar, difundir y controlar el saber, y de acceder al mismo. Por tanto, las tecnologías constituyen un instrumento, una herramienta importante para ser aplicada con éxito en los procesos educativos, ya sean en la educación formal regular o la educación especial. Serradas (2004).

Valdés, (2000) al tratar los retos que establecen las nuevas tecnologías de la información y la comunicación a la práctica docente actual, plantea que deben ser incorporadas a un proceso renovado y renovador de enseñanza-aprendizaje, donde se empleen en beneficio del desarrollo de competencias que permitan formar individuos para un aprendizaje a lo largo de toda la vida. Del mismo modo, agrega que deben ser utilizadas en beneficio de la atención de individualidades, sus necesidades, conocimientos previos, motivaciones

que den un carácter significativo al aprendizaje, como proceso activo de construcción de conocimientos, desarrollo de capacidades y sentimientos que generen una actitud responsable hacia sí mismo y hacia los demás.

### 2.2.7 Información y educación

El desarrollo de Internet ha significado que la información esté ahora en muchos sitios. Antes la información estaba concentrada, la transmitía la familia, los maestros, los libros. La escuela y la universidad eran los ámbitos que concentraban el conocimiento.

Rojas, (2009) explica que en la actualidad vivimos en un mundo rodeado de información, en donde los diferentes estilos de vida de las sociedades desarrolladas y los sistemas económicos están apoyadas por herramientas tales como las TIC (tecnologías de la información y comunicación), son los principales motores generadores de información. La sociedad actual se encuentra en crecimiento constante, dando origen así a ingentes cantidades de documentos, lo cual nos permite creer que estamos construyendo a escala planetaria una sociedad de la información, entendiendo por dicha sociedad a aquella en la cual la creación, distribución y manipulación de la información, forman parte trascendente de las actividades culturales y económicas, tomando en cuenta que la tecnología es una de las claves técnicas de la Sociedad de la Información.

A fines de 1980 la UNICEF adoptó el término “tercer canal” para referirse a todos los instrumentos disponibles y canales de información, comunicación y acción social (que) pueden ser usados para ayudar a transmitir los conocimientos esenciales e informar y educar a la población en asuntos sociales. Asumiendo la educación formal y no-formal como los otros dos canales educativos. UNICEF (1990).

### 2.2.8 Contrainteligencia

Es aquella parte de la función de Inteligencia que comprende el conjunto de medidas que impiden o neutralizan las actividades de espionaje, sabotaje, terrorismo y otras actividades subrepticias o clandestinas, realizadas por individuos, grupos u organizaciones extranjeras o nacionales enemigas o adversarios. DFA-CD-02-11, Ministerio de Defensa - Comando Conjunto de las Fuerzas Armadas - Doctrina de Inteligencia Conjunta - Lima - Perú - Dic 20111. Pag IX-1.

### 2.2.9 Amenaza, seguridad y censura

La amenaza viene a ser una actitud expresada o deducida, que hacen presumir riesgo, peligro o daño sobre las personas, organización o instalación. DFA-CD-02-11, Ministerio de Defensa - Comando Conjunto de las Fuerzas Armadas - Doctrina de Inteligencia Conjunta - Lima - Perú - Dic 20111. Pag IX-5.

Seguridad Permite la libertad de acción y se obtiene adoptando medidas para conservar el secreto de nuestras organizaciones, planes y actividades. Este fundamento es el más importante por ser de carácter subrepticio y de compartimentaje en las actividades de contrainteligencia. DFA-CD-02-11, Ministerio de Defensa - Comando Conjunto de las Fuerzas Armadas - Doctrina de Inteligencia Conjunta - Lima - Perú - Dic 20111. Pag IX-6.

Censura Es el control de la difusión de las informaciones de valor militar y de los mensajes antes y durante su publicación, para impedir que el enemigo obtenga información de valor militar por los medios de comunicaciones siguientes: Correspondencia, Teléfonos, Telégrafos, Pelicular, Periódicos, Estaciones de Radio y TV, etc. DFA-CD-02-11, Ministerio de Defensa - Comando Conjunto de las Fuerzas Armadas - Doctrina de Inteligencia Conjunta - Lima - Perú - Dic 20111. Pag IX-8.

## 2.3 Definición de términos básicos

2.3.1 Filtración Informativa. Según Julián Pérez Porto es una práctica que consiste en la entrega de documentación personal, secreta o información privilegiada a los medios de comunicación para que estos la difundan y poder así generar un efecto ya sea de denuncia, político, económico o de mero escándalo.

También se puede entender como filtración de información al robo de esta mediante la web usando alguna de las herramientas ya conocidas por los internautas que es Firewall y usos de virus para el robo de información.

2.3.2 Red Social.

Las redes sociales son el acto de socialización en una comunidad en línea. Una red típica sociales como Facebook, LinkedIn, MySpace o Bebo le permite crear un perfil, agregar amigos, comunicarse con otros miembros y añadir sus propios medios de comunicación.

2.3.3 Herramientas Sociales.

Las herramientas sociales (a veces llamado software social) son programas de software y plataformas que permiten a la cultura de participación - por ejemplo, blogs, podcasts, foros, wikis y vídeos compartidos y presentaciones. Es importante mencionar que los que mayormente usan este tipo de herramientas son usuarios previamente registrados en alguna red social, y cuyo éxito radica en los servicios que ofrecen y la difusión masificada de los mismos por parte de los propios usuarios que han probado y han elegido continuar usando dicha herramienta.

Fundamentalmente, el gran potencial de sitios como Twiter o Facebook radica en el servicio que brindan, ya que ofrecen la posibilidad de que sus

usuarios puedan interactuar de manera permanente con otras personas, más allá de si se conocen o no entre sí.

La clave, entonces, está en la comunicación virtual, por lo que las redes sociales se han establecido como verdaderos sistemas abiertos a toda la sociedad, sin ejercer ningún tipo de discriminación o diferenciación entre los individuos que utilizan el servicio.

### 2.3.4 Pérdida de privacidad.

Cuando los datos que se proporcionan a los administradores de las redes entran a formar parte de los archivos de estos. Al mismo tiempo, un mal uso de las redes puede llevar a facilitar datos propios, de familiares o amigos. Existe además el llamado "phising", llevado a cabo por quienes roban contraseñas de acceso de otras personas para manipular o espiar sus sesiones.

Interactividad

Las tecnologías permiten lo que hace unos años era impensable. A miles de kilómetros podemos enviar caracteres textuales de longitud limitada a través del móvil (sms), podemos obtener fotografías con nuestros propios terminales y enviarlas a la otra punta del mundo (mms), podemos emitir en directo y redirigir la señal de televisión vía satélite, e incluso somos capaces de que esas mismas imágenes, mientras se reproducen en el televisor sean grabadas en un disco duro y 'subidas' a un servidor de Internet donde pueden ofrecerse en diferido vía streaming…Esta 'macrored' creada por todos los hombres, a nivel mundial, es el resultado inequívoco del esfuerzo conjunto de todos los países por reducir el coste de las transmisiones y por conseguir, paralelamente, el aumento de capacidad de los dispositivos que almacenan la información que, paradójicamente, van reduciéndose hasta el volumen de un microchip.

Esa accesibilidad al medio permite a cientos, miles de personas interactuar en páginas web, blogs, foros, chat, redes sociales, conferencias a distancia, etc. El

grupo de usuarios alimenta el medio y el mensaje y lo hace crecer. Convenimos en que supone una buena definiciyn de ‘interactividad’ la que aporta el profesor israelí Sheizaf Rafaeli6 quien la define como "una expresión extensiva que en una serie de intercambios comunicacionales implica que el último mensaje se relaciona con mensajes anteriores a su vez relativos a otros previos". (David Caldevilla Domínguez, Las Redes Sociales…)

2.3.5 Usuario

Persona u organización que utiliza y forma parte de una red social. Por lo general, el nombre de usuario es el nombre real de la persona u organización. También es posible ver usuarios que se identifican en la red mediante un nombre diferente o similar a su nombre real. Además, en Twitter los usuarios deben añadir delante de su nombre el símbolo @. en la utilización de usuarios de la red, se pueden generar ciertos tipos de inseguridad, dentro de los que podemos citar a parientes lejanos, viejos amigos, realizar nuevos contactos profesionales y mejorar las relaciones sociales entre muchas otras cosas que pueden hacerse como con un pase de magia, están disponibles para millones de internautas de todo el mundo, a través de las más famosas redes sociales.

Esto también nos indica que, junto a estas facilidades, surgen los problemas que se generan por la falta de cuidado en el manejo de datos e información confidencial. En la actualidad estas redes sociales se convirtieron rápidamente en una «fiebre», atrayendo millones de internautas, y con ellos también se multiplicaron los problemas de seguridad. Cada día vemos distintas noticias sobre «secuestros» de perfiles y comunidades.

2.3.6 Censura

Puede definirse como la revisión, vigilancia o control de toda comunicación, realizada con el fin de evitar que la información clasificada o aquella relativa a la seguridad, lleguen a poder del enemigo. ME 38-10, Seguridad Militar, Sec II, Pfo 31. Pag 93

2.3.7 Seguridad de las Informaciones

Abarca todas las actividades tendientes a eliminar los riesgos contra la seguridad de las informaciones. DFA-CD-02-11, Ministerio de Defensa - Comando Conjunto de las Fuerzas Armadas - Doctrina de Inteligencia Conjunta - Lima - Perú - Dic 20111. Pag IX-12.

2.3.8 Escenario de riesgo

Es una situación donde la presencia de ciertos factores genera hipótesis específicas de materialización de una amenaza, con un determinado nivel de riesgo sobre uno o más activos críticos, que puede impedir o afectar el logro de nuestros objetivos.

2.3.9 Riesgo

Es la probabilidad de materialización de una amenaza con un determinado impacto, mediante la explotación de las vulnerabilidades de un activo crítico.

Riesgos internos del propio personal

Son los riesgos que se originan en nuestro mismo personal y que resultan de su propia naturaleza, de su manera de ser, de su manera de pensar y de su carácter. La mayoría de las veces estos riesgos no son ni calculados ni voluntarios, pero constituyen un peligro constante, porque no pueden ser controlados desde fuera, ya que son inherentes al individuo. Pag 7, ME 38-10, Seguridad Militar, Cap I, Sec II,1.6. c.1.

Conciencia de Seguridad

Es el conocimiento permanente de los riesgos de seguridad y de la obligación que se tiene de adoptar las medidas que sean necesarias. Pag 3, ME 38-10, Seguridad Militar, Cap I, Sec I,1.4. o.

Adoctrinamiento del Personal

Es una de las normas básicas más importantes y en la que reposa todo el armazón de la Seguridad. Permite eliminar "la ignorancia" del personal, que es el riesgo interno, más peligrosos. Esta norma consiste en desarrollar en las personas "la conciencia de Seguridad", mediante la ejecución de un buen programa de instrucción, de constante entrenamiento y de control permanente.
Pag 10, ME 38-10, Seguridad Militar, Cap I, Sec II,1.7. d Normas básica de Seguridad.

Oficial de seguridad

Es un Oficial especialista o con experiencia en Inteligencia, cuya misión específica es atender todo lo relacionado con la SEGURIDAD de la instalación a la cual pertenece. Pag 1, ME 38-10, Seguridad Militar, Cap IX, Sec I,9.1.a. Oficial de Seguridad

El papel que juega el Oficial de Seguridad en cada una de las dependencias del Ejército es importante. El no sólo debe recordar constantemente al personal de su unidad los peligros que inciden sobre ella, a través de la instrucción de seguridad, de la cual es su principal promotor, sino que debe evitar con todos los medios a su alcance que los agentes enemigos se introduzcan en la instalación.
Pag 1, ME 38-10, Seguridad Militar, Cap IX, Sec I,9.1.b. Oficial de Seguridad.

La presencia del Oficial de Seguridad en una instalación, no exime al resto del personal de velar por la seguridad de aquella, el personal tiene que comprender que la seguridad no es obra exclusiva del Oficial de seguridad, sino que a todos incumbe la misma responsabilidad de garantizarla. Pag 1, ME 38-10, Seguridad Militar, Cap IX, Sec I,9.1.c. Oficial de Seguridad.

Redes Sociales más usadas

Las redes sociales se han convertido en parte importante de la vida de las personas y el desempeño de las empresas. Hoy en día son plataformas para establecer contactos, intercambiar información, buscar trabajo y empoderar a la ciudadanía. Y a la vez son herramientas estratégicas para las organizaciones y los negocios, sobre todo para posicionar productos y servicios.

Las cifras varían dependiendo la encuesta que se tome como referencia, pero es innegable la expansión del uso de redes sociales entre los peruanos y, como consecuencia, algunas de estas plataformas se han convertido en sus favoritas, tal como se muestra a continuación:

1) Facebook: Es la red social más usada del mundo. Este espacio permite comunicarse en tiempo real con otros usuarios, intercambiando videos y fotografías personales, y si bien su uso principal siempre fue la proyección de la imagen, muchas personas la utilizan para proyectar vacíos de su personalidad. La abreviaciyn común de este servicio es "fb". Por su versatilidad, el Facebook permite realizar muchas actividades, como publicar fotos, videos, chatear (conversar con otras personas), hacer videollamadas, jugar juegos en red y hasta hacer anuncios de publicidad y marketing.

2) Twitter: Red social que permite realizar comentarios de cualquier acontecimiento en tiempo real, de manera que puedan ser visto por todas las personas que hayan abierto una cuenta en ella. Además, se puede realizar comentarios de las fotos o mensajes publicados. Se diferencia del Facebook en que la interacciyn se da a través de mensajes cortos o "Twits", sumados a otro tipo de expresiones como "hashtags" o al uso de "#" para agregar más significado a las frases. Puede convertirse en foco de elevada interactividad.

3) Skype: Programa con el que se puede realizar videollamadas hacia una o varias personas en cualquier parte del mundo al mismo tiempo, de tal forma que puede utilizarse para eventos o conferencias internacionales teniendo a los participantes en diversas ciudades del mundo. Es en principio un

programa de comunicación; sin embargo, para algunas personas puede convertirse en una fuente de socialización disfuncional al tratar de conseguir amigos o conocidos de otras partes del mundo por el sólo hecho de llenar vacíos de comunicación o reconocimiento.

4) Whatsapp: Programa que permite enviar mensajes de manera rápida e ilimitada a un costo mínimo. Para utilizar esta red social se necesita celulares (Smartphone) que hayan descargado dicha aplicación o servicio. De esta manera se crea consumo pues al no tener un teléfono capaz de ejecutar el programa, las personalidades débiles se sienten excluidas o subestimadas. Acta (Herediana Vol. 57, octubre 2015 - marzo 2016)

Leyes y normas que regula y restrieguen la publicación de información:

En la actualidad no se dispone de dispositivos legales que regulen o restrinjan la publicación de información mediante el uso de las redes sociales.

La Constitución Política del Perú, establece en su artículo 168, que "Las leyes y los reglamentos respectivos determinan la organización, las funciones, las especialidades, la preparación y el empleo; y norman la disciplina de las Fuerzas Armadas y de la Policía Nacional.

El art. 38° señala que "todos los peruanos tienen el deber de honrar al Perú y proteger los intereses nacionales, así como respetar, cumplir y defender la constitución y el ordenamiento jurídico de la nación",

El Decreto Legislativo Nº 1134 "Ley de Organización y Funciones del Ministerio de Defensa", establece en su artículo 15º, que "El Ejército del Perú (…) se rige por la Constitución Política del Perú, su propia normativa, el presente Decreto Legislativo y demás normas legales pertinentes".

La Ley Nº 27815 "Ley del Código de Ética de la Función Pública", modificado por la Ley Nº 28496, de fecha 18Abr05, reglamento dado mediante Decreto Supremo Nº 033-2005-PCM, establece algunas definiciones a tener en cuenta por parte de los funcionarios públicos cualquiera sea su condición, tales como: Bienes del estado, Ética Pública, Información Privilegiada, Intereses en Conflicto, Servidor Público.

El Reglamento del Ejército "Correspondencia Militar" (RE 31-62), establece que la directiva es un documento que contiene normas, procedimientos o disposiciones, que emite un Comando determinado, para orientar la acción de los comandos subordinados.

El artículo 1º, literal d, numeral 6º, del Decreto Supremo Nº 002-2015-DE del 29 Ene 15, establece que por resolución de la Comandancia General se aprobarán: "Doctrinas básicas o de segundo nivel para el campo militar, manuales de procedimientos, ordenanzas, publicaciones y directivas".

## CONCEPTOS SOBRE CIBERSEGURIDAD

Es preciso considerar un concepto muy importante sobre ciberseguridad, lo cual representa un conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que se pueden utilizar para proteger los activos de las fuerzas operativas. Lo que lleva a desarrollar las siguientes interrogantes:

1) ¿Cuáles son las diferencias entre ciberseguridad y seguridad de la información en la empresa?
2) ¿Cómo se define la seguridad informática?
3) ¿Cuáles son las buenas prácticas de email y una navegación segura?

La ciberseguridad es un tema de actualidad que afecta tanto a datos personales como de la empresa, desde autónomos y Pymes hasta las multinacionales. Conocer la terminología y saber prevenir y reaccionar correctamente es imprescindible para proteger nuestra información.

También se puede considerar la seguridad de la información, definiendo como una manera sencilla de adoptar medidas preventivas para proteger la información, garantizando, confidencialidad, disponibilidad e integridad. Esta información puede estar en cualquier tipo de medio donde se almacene y es lo que intentaremos proteger.

Otra de las consideraciones es, la seguridad informática, que son todas aquellas medidas tomadas para proteger la integridad y la privacidad de la información almacenada en un sistema informático y signifique un riesgo si llega a manos de otras personas. Se puede referir a Software, base de datos y archivos entre otros.

Otro concepto sobre Ciberseguridad, Es la capacidad para minimizar el nivel de riesgo al que está expuesta la información ante amenazas o incidentes de naturaleza cibernética. La ciberseguridad tiene como foco la protección de la información digital.

## Conceptos básicos de ciberseguridad

- Amenaza: La posibilidad de que se produzca una determinada vulnerabilidad de forma satisfactoria. Se clasifican en dos tipos, internas y externas.

  Amenazas internas: Son aquellas que proceden desde dentro de la organización.

  Amenazas externas: Son aquellas que se originan fuera de la red, en la cual el atacante buscara las posibles vulnerabilidades para explotarlas.

- Vulnerabilidad: Es la debilidad a sufrir un daño, y esta debilidad será por lo tanto, la que buscará el atacante.

- Sistema operativo: Un Sistema operativo (SO), es el conjunto de programas o aplicaciones especialmente hechos para la ejecución de varias tareas, en las que sirve de intermediario entre el usuario y un equipo. Este equipo puede ser un ordenador, una tablet, el móvil u otro tipo de dispositivo. El SO maneja el hardware del equipo, administra todos los periféricos de un ordenador y es el encargado de mantener la integridad del sistema. El sistema operativo es el programa más importante de un ordenador o cualquier otro dispositivo.

Existen muchos tipos de sistemas operativos, pero entre ellos los más utilizados son Windows, Linux, Macos. En cuanto a dispositivos móviles el más usado es Android.

En relación a las manifestaciones de seguridad, se puede mencionar lo manifestado por el CCFFAA a través del siguiente dispositivo legal:

MFA-CD-03-10 MINISTERIO DE DEFENSA COMANDO CONJUNTO DE LAS FFAA DOCTRINA DE OPERACIONES EN EL CIBERESPACIO LIMA PERU - 2017

Las operaciones y acciones militares han variado en sus medios, herramientas, dispositivos e inclusive armas empleadas para lograr la supremacía y consecución de sus objetivos derivando un cambio significativo en el enfoque bélico.

Este nuevo escenario como lo es el ciberespacio, no solo se mantendrá como nuevo Teatro de Operaciones, sino que los conflictos en ese terreno se presentarán con mayor frecuencia y con mayor intensidad durante la próxima década.

Las capacidades de un adversario en el ciberespacio, pueden ser catalogadas como: accesos intrusivos a los activos de información, denegación de acceso de usuarios legítimos a los activos de su información, robo de credenciales de acceso a dichos sistemas, interceptación y manipulación de información transmitida entre activos, monitoreo de operaciones militares en ejecución, manipulación en la

configuración de sistemas de control industrial e infraestructuras críticas, entre otros.

Estos cambios tienen dos importantes implicancias a largo plazo para la planificación y realización de las operaciones:

- Tanto la obtención de datos para un análisis preciso y detallado, así como los efectos de un ataque a la confidencialidad, disponibilidad y/o integridad a la información en el ciberespacio, son tan importantes en la actualidad, como lo sería un ataque convencional.
- Las Ciberamenazas, no están esperando el Día "D" y la hora "H" para empezar a buscar y explotar vulnerabilidades en los activos de sus objetivos, este trabajo de identificación e incluso infección con software malicioso es realizado con larga anticipación al mencionado momento. Las amenazas contra la soberanía nacional pueden ir en aumento. El Estado debe prepararse para enfrentar futuras amenazas que puedan ejecutar ataques terroristas y no convencionales.

Las redes cibernéticas civiles, militares e industriales han sufrido un repunte en cuanto a ciberataques, ya sean como parte de ataques patrocinados por estados, por compañías competidoras o por acciones maliciosas, que se mantienen en el anonimato gracias a las posibilidades que ofrece el ciberespacio.

En la presente doctrina se regulan las operaciones en y a través, desde y hacia el dominio del ciberespacio, para mantener la superioridad en dicho dominio como una tarea militar fundamental.

## GLOSARIO DE TÉRMINOS

Cuando la terminología empleada sobre pasa los sistemas de comunicación, se hace necesario considerar otros términos de manera adicional, los cuales se mencionan a continuación:

- Activo de información: Conocimientos o sistemas relacionados con el tratamiento de la información que tenga valor para la organización. Pueden ser procesos, datos, aplicaciones, equipos informáticos, personal, redes, equipamiento auxiliar o instalaciones.

- Activos críticos: Conocimientos o sistemas relacionados con el tratamiento de la información que tenga valor para la organización. Pueden ser procesos, datos, aplicaciones equipos informáticos, personal, redes, equipamiento auxiliar o instalaciones.

- Análisis de riesgos: Es un proceso que comprende la identificación de activos de información, sus vulnerabilidades y las amenazas a los que se encuentran expuestos, así como la probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para tratar el riesgo.

- Análisis de vulnerabilidades: Análisis y pruebas relacionadas con la identificación de puertos abiertos, servicios disponibles y detección de vulnerabilidades en los activos de información.

- Auditoría de seguridad: Es el estudio que comprende el análisis y gestión de sistemas llevado a cabo por profesionales en Tecnologías de la Información (TI) con el objetivo de identificar, enumerar y describir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones, servidores y aplicaciones, así como verificar que cada regla de la Política de Seguridad se aplique correctamente. CENTRO DE OPERACIONES DE SEGURIDAD

- El SOC es una central de seguridad informática que previene, monitorea y controla la seguridad en las redes y en Internet. Los servicios que presta van desde el diagnóstico de vulnerabilidades hasta la recuperación de desastres, pasando por la respuesta a incidentes, neutralización de ataques, programas de prevención, administración de riesgos y alertas de antivirus informáticos.

- Cert: Equipo de Respuesta ante Emergencias Informáticas. CERT es una marca registrada en EEUU. Es el Centro de Respuesta a Incidentes de Seguridad Informática. Su función es prevenir, detectar y mitigar ataques a los sistemas informáticos. Es una organización especializada en responder inmediatamente a incidentes relacionados con la seguridad de las redes o los equipos. También publica alertas sobre amenazas y vulnerabilidades de los sistemas. En general tiene como misiones elevar la seguridad de los sistemas de los usuarios y atender a los incidentes que se produzcan.
- Certificado digital: Es un fichero informático generado por una entidad denominada Autoridad Certificadora (CA) que asocia unos datos de identidad a una persona física, organismo o empresa confirmando de esta manera su identidad digital en Internet. Es un documento electrónico que permite asociar una clave criptográfica pública a una entidad propietaria de dicha clave, y que está protegido criptográficamente para garantizar su integridad y su autenticidad.
- Ciberamenaza: Causa potencial de un incidente no deseado, el cual puede ocasionar daño a los sistemas y servicios presentes en el ciberespacio o alcanzables a través de éste. Pueden ser Internas o Externas.
- Ciberataque: Un ataque, a través del ciberespacio, dirigido al uso del espacio cibernético de un objetivo con el propósito de interrumpir, deshabilitar, destruir o controlar maliciosamente un entorno/infraestructura de computación; o destruir la integridad de los datos o robar información controlada.
- Ciberconflicto: Confrontación entre dos o más partes en que al menos una utiliza los ciberataques o ataques realizados en el ciberespacio, contra el otro.
- Cibercontrainteligencia: Negar la capacidad de Inteligencia del enemigo en el ciberespacio.
- Cibercrimen: De mayor grado que la Ciberdelincuencia, se incluyen delitos como el fraude, el robo, el chantaje, la falsificación y la malversación de caudales públicos utilizando ordenadores y redes como medio para realizarlos.

- Cibercrisis: Un evento TIC grave, no autorizado o inesperado, donde han fracasado los mecanismos automáticos previstos y los técnicos no pueden resolverlo.
- CIBERDEFENSA: Es la capacidad que tienen las Fuerzas Armadas para proteger o defender el uso del ciberespacio, así como negar, impedir o reducir el uso del ciberespacio ante posibles enemigos o actores hostiles, con acciones de defensa activas pasivas, proactivas, preventivas y reactivas.
- Ciberdefensa militar: Conjunto de recursos, actividades, tácticas, técnicas y procedimientos para preservar la Seguridad de las redes de datos y Sistemas de Comando, Control y Comunicaciones del Sector Defensa, así como permitir la explotación y respuesta sobre los sistemas necesarios, para garantizar el libre acceso al Ciberespacio de interés militar y permitir el desarrollo eficaz de las operaciones militares y el uso eficiente de los recursos.

Ciberdelincuencia: Actividades delictivas llevadas a cabo mediante el empleo del ciberespacio, ya sea para dirigirlas hacia los sistemas y servicios presentes en el mismo o alcanzables a través suyo.

- Ciberdelito: Es una actividad delictiva que emplea el ciberespacio como objetivo, herramienta o medio.

- Ciberejercicio: Acciones simuladas en escenarios ficticios del ciberespacio para el entrenamiento del personal en técnicas defensivas y ofensivas, es un ejercicio virtual, basado en un ambiente simulado y controlado de una supuesta ciberguerra o crisis ante ataques cibernéticos, con la finalidad de verificar el grado de conocimientos, entrenamiento y alistamiento del personal.
- Ciberespacio: Es un dominio global dentro del ambiente de la información, consistente de una infraestructura interdependiente y tecnológica de información en red, que incluye la internet, las redes de telecomunicaciones y sistemas informáticos junto con los procesadores y controladores que forman parte de dichos sistemas.

- Ciberespionaje: Actividades de espionaje llevadas a cabo en el ciberespacio o utilizando el ciberespacio como medio.

- Ciberguerra: Conjunto de acciones que se realizan para producir alteraciones en la información y los sistemas del enemigo, a la vez que se protege la información y los sistemas del atacante, en la que se utiliza el Ciberespacio como campo de batalla.

- Ciberincidente: Incidente relacionado con la seguridad de las TIC que se produce en el Ciberespacio.

- Ciberinteligencia: Actividades de inteligencia para la búsqueda de información, puede ser de fuente abierta o cerrada en la cual se utiliza herramientas de Tecnología de la Información y/o técnicas para lograr tal fin.

Cibersabotaje: Según la RAE, el sabotaje es el "daño o deterioro que se hace en instalaciones, productos, etc., como procedimiento de lucha contra los patronos, contra el Estado o contra las fuerzas de ocupación en conflictos sociales o políticos". En el Ciberespacio, estos daños se pueden hacer mediante el acto de piratería.

- Ciberseguridad: La Ciberseguridad se encuentra comprendida dentro de la seguridad de la información, en la cual se busca garantizar la confidencialidad, integridad y disponibilidad de los activos de la información digital y de la infraestructura que la soporta.

- Ciberterrorismo: El ciberterrorismo o terrorismo electrónico es el uso de medios de tecnologías de información, comunicación, informática, electrónica o similar con el propósito de generar terror o miedo generalizado en una población, clase dirigente o gobierno, causando con ello una violación a la libre voluntad de las personas. Los fines pueden ser económicos, políticos o religiosos principalmente.

- CSIRT: Equipo de Respuesta ante Incidencias de Seguridad. Grupo de personas habitualmente compuesto por Analistas de Seguridad organizados para desarrollar, recomendar y coordinar acciones inmediatas de mitigación para la contención, erradicación y recuperación que resultan de incidentes de seguridad informática.
- Delito informático: Conducta ilícita que afecta los sistemas y los datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de la TI o de la Comunicación.

- HACKING ÉTICO: Uso de herramientas, técnicas y metodologías para analizar, auditar, penetrar y recomendar soluciones en las redes, estaciones de trabajo, servidores y cualquier activo informático de la institución contando con la autorización y permisos de la misma.

- Seguridad de la información: Es la preservación de la confidencialidad, la integridad y la disponibilidad de la información pudiendo, además abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio.

- Seguridad informática: Es la capacidad de proteger la integridad, disponibilidad y la privacidad de la información almacenada en un sistema informático

- Vulnerabilidad informática: Defecto o debilidad en el diseño, implementación u operación de un sistema informático que habilita o facilita la materialización de una amenaza.

## 2.4 Hipótesis

### 2.4.1 Hipótesis General:

Existe una relación entre la filtración de información en las redes sociales y los riesgos en la seguridad física e instalaciones, en los cadetes de cuarto año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2019

### 2.4.2 Hipótesis especifica

Hipótesis Específica 1

Existe una relación entre la filtración de información en las redes sociales y los riesgos en la seguridad física, en los cadetes de cuarto año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, ¿2019?

Hipótesis Específica 2

Existe una relación entre la filtración de información en las redes sociales y los riesgos en la seguridad de las instalaciones, en los cadetes de cuarto año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, ¿2019?

## 2.5 Variables

Definición conceptual

El problema se presenta en el personal de cadetes del IV año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, quienes vienen publicando y filtrando de manera sistemática información de carácter clasificado, en las diferentes redes sociales como Página web, Blogs, Facebook, YouTube, Whatsapp, etc, en algunos casos subiendo información reservada como fotografías con uniforme, exhibiendo armamento, en lugares de entrenamiento, en desfile, en instrucción, en zona de vivac, en Marcha de Campaña en la región cruz de hueso, en ceremonias estrictamente castrenses, evidenciando las diversas actividades castrenses que se realizan en el interior de la instalación militar, propios de la formación de un cadete

en la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, vulnerando y trasgrediendo las medidas de seguridad de las informaciones.

Definición Operacional

En sentido estricto, quizá la diferencia radica en que una fuga implica que la información pueda ser accedida por personas o dependencias sin los privilegios para hacerlo (divulgación), mientras que la pérdida de información no necesariamente se puede relacionar con la fuga o filtración, ya que esta puede dañarse (modificación, destrucción o interrupción) sin necesidad de que un agente interno o externo pueda acceder a ella.

En este mismo sentido, también juega un papel relevante identificar al actor que materializa un riesgo sobre la información, sobre todo porque ya sea una pérdida, fuga o filtración de información puede ser debida a un agente interno o externo. A decir verdad, existen un sin número de escenarios posibles en los cuales se pueden presentar los incidentes de seguridad, debidos a amenazas o vulnerabilidades.

Por lo tanto, independientemente de la forma en la cual se denominen las soluciones de tecnología para evitar incidentes de seguridad, el enfoque de protección debe orientarse hacia identificar los vectores por los cuales la información puede ser dañada, los actores que podrían materializar un riesgo, las consecuencias que tendría un amenaza o vulnerabilidad, y por sobre todo los mecanismos empleados para reducir la probabilidad de ocurrencia o el impacto de dicho riesgo.

| ACTOR | MOTIVO | CONSECUENCIA |
|---|---|---|
| Interno/Externo | Accidental | - Divulgación<br>- Modificación<br>- Interrupción<br>- Destrucción |
| | Deliberado | - Divulgación<br>- Modificación<br>- Interrupción<br>- Destrucción |

FIGURA N° 2: El siguiente diagrama muestra un árbol de decisiones para la identificación de riesgos relacionados con la información

Por lo tanto, resulta importante contar con un enfoque de seguridad proactivo que permita conocer los posibles escenarios de riesgo. A partir de los resultados de este análisis previo, las organizaciones pueden tomar las mejores decisiones para proteger uno de sus activos más valiosos, como lo es la información. El paso posterior consiste en identificar una herramienta de seguridad capaz de brindar los controles necesarios para salvaguardarla de posibles fugas, pérdidas o filtraciones, tanto de agentes internos como externos, y de incidentes resultados tanto de actos deliberados como accidentales.

Finalmente, todo este conjunto de mecanismos de protección se implementan con objetivos de mayor alcance, como preservar la imagen y reputación del personal u organización, generar confianza entre los usuarios en cuanto a la protección de los datos, dar cumplimiento a estándares o legislaciones relacionadas con la protección de información y, en un contexto mayor, mantener la continuidad y operación de los negocios.

# CAPITULO III: MARCO METODOLOGICO

## 3.1 Enfoque

El enfoque utilizado en el siguiente trabajo es cuantitativo, en este caso se usa la recolección de datos para probar la hipótesis, en base a una medición numérica y el análisis estadístico.

## 3.2 Tipo

Descriptivo correlacional.

Según Hernández, Fernández y Baptista (2006, p.102) "miden, evalúan o recolectan datos sobre diversos conceptos (variables), aspectos, dimensiones o componentes del fenymeno a investigar" y correlacional porque según Carrasco (2008, p. 73) "busca conocer la relación que existe entre dos o más conceptos, categorías o variables en un contexto en particular".

## 3.3 Diseño

El diseño de la investigación fue de tipo no experimental: correlacional - transversal ya que no se manipuló ni se sometió a prueba las variables de estudio.

## 3.4 Método

El método que se emplea en el trabajo de investigación es descriptivo, consiste en describir, analizar e interpretar sistemáticamente un conjunto de hechos.

a. Descriptivo: describir interpretar y relacionar todos los métodos de inteligencia (seguridad) y riesgos de infiltración de información en la escuela militar de chorrillos

b. Inductivo: porque de los resultados obtenidos nos daremos cuenta si los métodos de la inteligencia de seguridad ayudarán en su totalidad a los cadetes de la escuela militar de chorrillos

## 3.5 Población/Muestra

La poblaciyn es el "conjunto de todos los elementos que forman parte del espacio territorial al que pertenece el problema de investigaciyn", en este caso la población lo constituye todos los Cadetes del IV año de la Escuela Militar de Chorrillos, siendo el tamaño de la población de 234 cadetes.

Tabla 1:

$$n = \frac{N * Z_{1-\alpha/2}{}^2 * p * q}{d^2 * (N-1) + Z_{1-\alpha/2}{}^2 * p * q}$$

| | | |
|---|---|---|
| Marco muestral (Población) | N | 234 |
| Alfa | α | 0.050 |
| Nivel de Confianza | 1-α | 0.975 |
| Z de (1-α) | Z (1-α) | 1.960 |
| Prevalencia de la Enf. / Prob. | p | 0.500 |
| Complemento de p | q | 0.500 |
| Precisión (error muestral) | d | 0.050 |
| Tamaño de la muestra | n | 145.65 |

Tabla 1: Tamaño de la muestra = 146

## 3.6 Técnicas/instrumentos recolección de datos

Se utilizaron las siguientes técnicas:

a. Técnicas de recolección de datos: Es una técnica que consiste en la recolección ordenada de todos los documentos referidos al tema, mediante el uso de fichas bibliográficas, Reglamentos, manuales, disposiciones del Escalón superior, referente al uso indiscriminado de las redes sociales en la institución.

b. Técnicas de observación: Se ha empleado la observación estructurada mediante el uso de cuadros, tablas y gráficos demostrativos a lo largo del proceso de investigación y la observación documental mediante fichas bibliográficas.

c. Técnica de la encuesta:

Según Sánchez (2009), "La encuesta es una técnica de recogida de informaciyn que consiste en la elección de una serie de personas que deben responderlas sobre la base de un cuestionario, en esta investigación, se aplicó un instrumento (cuestionario)" (p. 21). En este caso la investigación directa a los involucrados.

## 3.7 Validación y confiabilidad del instrumento

Se aplicará el criterio de Juicio de Expertos y el alfa de Cronbach para determinar la confiabilidad de las variables.

Para la confiabilidad de cuestionarios, se empleó la prueba Alfa de Cronbach, procesaran los datos en el Programa Estadístico SPSS versión 22.0. En la tabla 1 se presenta información referencial de interpretación de los resultados y determinar el coeficiente para cada variable en estudio.

Tabla 2

Interpretación del coeficiente de confiabilidad

| RANGOS | MAGNITUD |
|---|---|
| 0,81 a 1,00 | Muy Alta |
| 0,61 a 1,00 | Moderada |
| 0,41 a 0,60 | Baja |
| 0,01 a 0,20 | Muy baja |

Tabla 2: Fuente: Ruiz (2007)

}

Tabla 3

Resultados del análisis de confiabilidad del instrumento que mide la variable 1: Filtraciones de información en las redes sociales

Estadísticas de fiabilidad

| Alfa de Cronbach | N° de elementos |
|---|---|
| ,622 | 11 |

Como se observó en la tabla 2 y tomando como referencia la tabla 1, la variable Filtraciones de información en las redes sociales presenta un nivel de confiabilidad moderada; siendo un resultado que le da confiabilidad al instrumento.

Tabla 4

Resultados del análisis de confiabilidad del instrumento que mide la variable 2: Seguridad Física e Instalaciones

Estadísticas de fiabilidad

| Alfa de Cronbach | N de elementos |
|---|---|
| ,771 | 5 |

Como se observó en la tabla 3 y tomando como referencia la tabla 1, la variable 2 Seguridad Física e Instalaciones presento un nivel de confiabilidad moderada; siendo un resultado que le da confiabilidad al instrumento.

## 3.8 Procedimientos para el tratamiento de datos

Para efectos del tratamiento de datos se ha utilizado la escala de likert

Para contrastar las hipótesis, se empleó el Rho de Spearman y así determinar su relación.

Estadígrafo Rho de Spearman

$$\rho = 1 - \frac{6 \sum D^2}{N(N^2 - 1)}$$

Dónde:
 = Rho de Spearman N
= Muestra
D = Diferencias entre variables

## 3.9 Aspectos éticos

En este trabajo de investigación, los integrantes del grupo han demostrado la autenticidad de resultados y de no exponer y/o divulgar la información obtenida de la Escuela Militar de Chorrillos, la cual fue confidencial, además de proteger la identidad de los participantes y de los objetos que son participes en el estudio.

# CAPITULO IV: RESULTADOS

## 4.1 Descripción

Tabla 5: Distribución de las frecuencias de la Variable 1: Filtración de información en las redes sociales

V1 (filtración de información en las redes sociales)

| | | Rango | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|---|
| Válido | No existe | [ 15 - 23 ] | 7 | 4,8 | 4,8 | 4,8 |
| | Existe | [ 24 - 32 ] | 104 | 71,2 | 71,2 | 76,0 |
| | Existe mucho | [ 33 - 43 ] | 35 | 24,0 | 24,0 | 100,0 |
| | Total | | 146 | 100,0 | 100,0 | |

Figura 3:

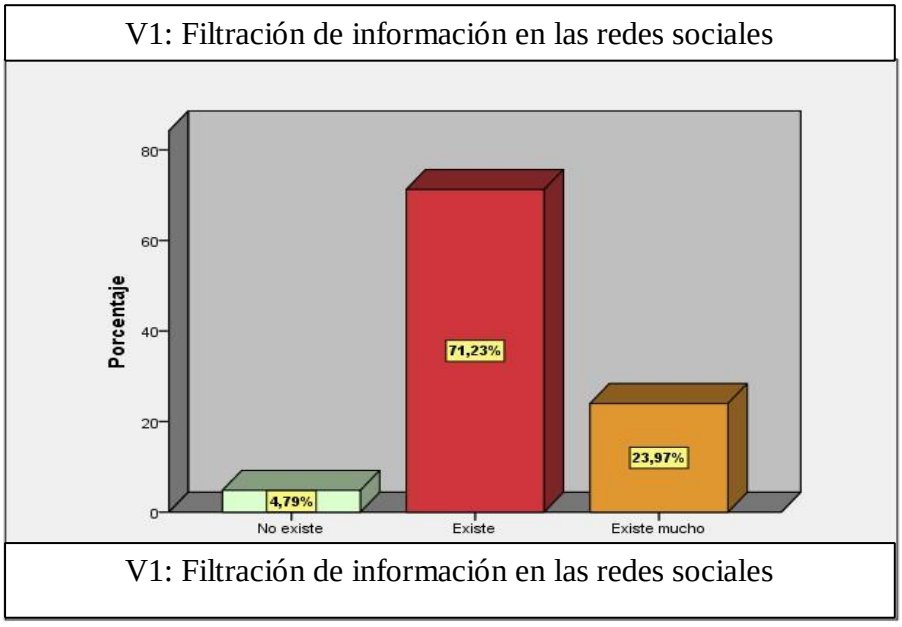


Figura 3. Filtración de información en las redes sociales

La tabla 4 y figura 1, de una muestra de 146 cadetes de IV EMCH de Educación superior el 71,23 % (104), considera que existe riesgos (35) quienes consideran que existe mucho riesgo y un 4,78% (7) consideran que no existe filtración de información. Lo que demuestra la existencia de una serie de riesgos que deben ser controlados a través de un estudio adecuado de seguridad.

Tabla 6: Distribución de las frecuencias de la Variable 2: Riesgos en la Seguridad Física e Instalaciones

V2 (Riesgos en la Seguridad Física e Instalaciones)

| | Rango | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido Regular | [ 8 - 12 ] | 7 | 4,8 | 4,8 | 4,8 |
| Buena | [ 13 - 17 ] | 11 | 7,5 | 7,5 | 12,3 |
| Muy bueno | [ 18 - 25 | 128 | 87,7 | 87,7 | 100,0 |
| Total | | 146 | 100,0 | 100,0 | |

Figura 4: Riesgos en la Seguridad Física e Instalaciones

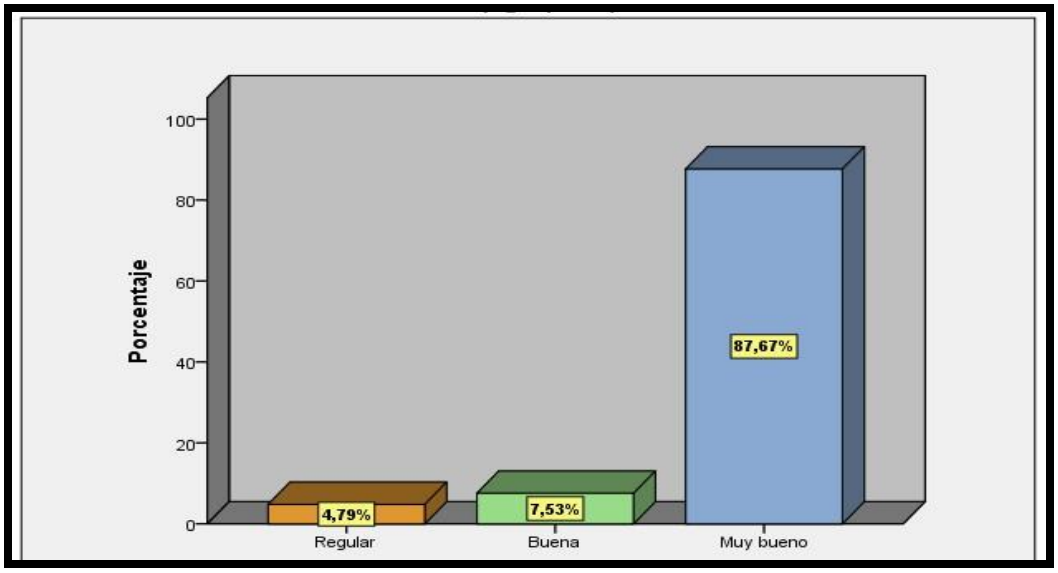


Figura 4. Riesgos en la Seguridad Física e Instalaciones

La tabla 5 y figura 2, de una muestra de 146 cadetes de IV EMCH de Educación superior el 87,67 % (128), consideran muy buena la seguridad

física e instalaciones de la Escuela Militar de Chorrillos, seguido de un 7,53% (11) que lo califican de Buena y el 4,79% (7) de regular. Lo que indica que la seguridad en las instalaciones es adecuada en su estructura.

## 4.2 Interpretación

Prueba de Hipótesis

Nivel de significancia: $\alpha = 0,05 = 5\%$ de margen máximo de error.

Regla de decisión:

$\rho \geq \alpha \rightarrow$ se acepta la hipytesis nula Ho

$\rho < \alpha \rightarrow$ se acepta la hipytesis alterna Ha

Prueba de Hipótesis General

H0 = No existe una relación entre la filtración de información en redes sociales y los riesgos en la seguridad física e instalaciones, cadetes de cuarto año de la Escuela Militar de Chorrillos “CFB”, 2019.

HG = Existe una relación entre la filtración de información en redes sociales y los riesgos en la seguridad física e instalaciones, cadetes de cuarto año de la Escuela Militar de Chorrillos “CFB”, 2019.

Rho de Spearman:

Nivel de confianza al 95%

Valor de significancia: □ □ 0.05

Correlaciones

| | | | V1 (Filtración en redes sociales agrupado) | V2 (Riesgos en la seguridad física e instalaciones agrupado) |
|---|---|---|---|---|
| Rho de Spearman | V1 (Filtración en redes sociales agrupado) | Coeficiente de correlación | 1,000 | ,734** |
| | | Sig. (bilateral) | | ,000 |
| | | N | 146 | 146 |
| | V2 (Riesgos en la Seguridad física e instalaciones agrupado) | Coeficiente de correlación | ,734** | 1,000 |
| | | Sig. (bilateral) | ,000 | |
| | | N | 146 | 146 |

**. La correlación es significativa en el nivel 0,01 (2 colas).

Los resultados arrojan una correlación de 0,734 afirmando que hay correlación positiva alta entre las 2 variables.

De otro lado, el valor de p=0,000 < 0,05, por lo que se rechaza la hipótesis nula y aceptamos la hipótesis alterna (H1): = Existe una relación entre la filtración de información en redes sociales y los riesgos en la seguridad física e instalaciones, cadetes de cuarto año de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", 2019.

Con lo cual comprobamos la validez de nuestra hipótesis general de nuestro estudio de investigación.

H0 = No Existe una relación entre la filtración de información en las redes sociales y los riesgos en la seguridad física e instalaciones, en los cadetes de cuarto año de la Escuela Militar de Chorrillos "CFB".

Hipótesis específica 1

H1 = Existe una relación entre la filtración de información y los riesgos en la seguridad física en los cadetes de cuarto año de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi".

H0 = No existe una relación entre la filtración de información y los riesgos en la seguridad física en los cadetes de cuarto año de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi".

Correlaciones

| | | | D1 (Filtración de información) | V2 (Seguridad física e instalaciones agrupado) |
|---|---|---|---|---|
| Rho de Spearman | D1 (Filtración de informacióno) | Coeficiente de correlación | 1,000 | ,702** |
| | | Sig. (bilateral) | | ,000 |
| | | N | 146 | 146 |
| | V2 (Seguridad física e instalaciones agrupado) | Coeficiente de correlación | ,702** | 1,000 |
| | | Sig. (bilateral) | ,000 | |
| | | N | 146 | 146 |

**. La correlación es significativa en el nivel 0,01 (2 colas).

Los resultados arrojan una correlación de 0,702 afirmando que hay correlación positiva alta entre las 2 variables.

De otro lado, el valor de p=0,000 < 0,05, por lo que se rechaza la hipótesis nula y aceptamos la hipótesis alterna (H1): = Existe una relación filtración de información y los riesgos en la seguridad física e instalaciones, de los cadetes de cuarto año de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi".

Con lo cual comprobamos la validez de nuestra hipótesis específica 1 de nuestro estudio de investigación.

Hipótesis específica 2

H2 = Existe una relación entre la filtración de información y los riesgos en la seguridad de las instalaciones, en los cadetes de cuarto año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”.
H0 = No existe una relación entre la filtración de información y los riesgos en la seguridad de las instalaciones, en los cadetes de cuarto año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”.

Correlaciones

| | | | D2 (Capacitación en temas de información agrupado) | V2 (Seguridad física e instalaciones agrupado) |
|---|---|---|---|---|
| Rho de Spearman | D2 (filtración de riesgos de seguridad) | Coeficiente de correlación | 1,000 | ,709 |
| | | Sig. (bilateral) | | ,024 |
| | | N | 146 | 146 |
| | V2 (Seguridad física e instalaciones agrupado) | Coeficiente de correlación | ,709 | 1,000 |
| | | Sig. (bilateral) | ,024 | |
| | | N | 146 | 146 |

Los resultados arrojan una correlación de 0,709, afirmando que hay correlación positiva alta entre las 2 variables.
De otro lado, el valor de p=0,024 < 0,05, por lo que se rechaza la hipótesis nula y aceptamos la hipótesis alterna (H1) = Existe una relación entre la filtración de información y los riesgos en la seguridad física e instalaciones, en los cadetes de cuarto año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”.

Con lo cual se comprueba la validez de la hipótesis específica 2 del estudio de investigación.

## 4.3. Discusión

De acuerdo a lo evidenciado en el presente trabajo, se puede afirmar que el inicio de las redes sociales en Internet, es mucho más vasto de lo que la mayoría de la población conoce, lo que genera un desconocimiento y uso inconsciente de las mismas. Por ende y después de mirar la importancia de las redes sociales, se puede concluir que el uso masivo de las redes sociales ha generado grandes avances culturales que, relacionados con la tecnología, ha facilitado la conexión de cualquier persona en el mundo a la Web, principalmente por el uso masivo de los dispositivos móviles, como celulares, tablas, portátiles, entre otros. Según esto, los usuarios actuales, los cuales tienen la posibilidad de navegar libremente por Internet, sin límite en el tiempo o el espacio tienen la oportunidad de usar las redes sociales para relacionarse con cualquier persona en el mundo que también esté conectada a una red social. Sin dejar al lado que la interacción entre los usuarios de las redes sociales está estrechamente atada con las relaciones que tienen y quieren conservar en el mundo físico o real.

El problema no se genera únicamente por la existencia y conectividad de las redes sociales, si no en gran medida por el desconocimiento de los usuarios, o por el uso inescrupuloso de presuntos victimarios que con un simple ánimo de burla o consientes de querer cometer un acto ilícito, efectúan actos virtuales que generan daños a terceros. Por ende, ningún estado debe permitir que los daños causados, por el uso inadecuado de las redes sociales, vulnere los derechos a la información e intimidad de los usuarios. Siendo el punto de partida para disminuir los daños o delitos derivados de hechos relacionados con las redes sociales, generar conciencia de los riesgos inherentes de las mismas, que en gran medida se infringen por la auto divulgación de la información, debido a que las redes sociales son redes públicas a las que cualquier otro usuario tiene acceso, y por ende puede usar la información que este expuesta de manera indecorosa, generando esto un posible daño relacionado con la protección del derecho de la intimidad y el buen nombre.

Finalmente cabe resaltar que las normas jurídicas no son la principal forma de proteger a los usuarios de las redes sociales, por el contrario son estos mismos quienes deben cuidar su información, filtrando los datos que ingresaran a la Web; todo esto sin dejar a un lado, que en parte la no aplicación de las normas se debe al poco interés político y estatal de destinar e implementar recursos en tecnología avanzada, para desarrollar mecanismos idóneos de defensa a los usuarios de las redes sociales en Internet

# CONCLUSIONES

## Primera conclusión

Existe un alto grado de correlación positiva y un nivel de significación estadística, entre la filtración de información en las redes sociales y los riesgos en la seguridad física e instalaciones, en los cadetes de cuarto año de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi". Ello se sustenta con un valor Rho Spearman = ,734 y p= 0,000 menor a α=0,05, infiriéndose una vinculaciyn con las mencionadas variables

## Segunda conclusión

a. El 71,2% de entrevistados (104), es decir 7 de cada 10 cadetes del IV año de la Escuela Militar de Chorrillos, considera que existe filtración de información en las redes sociales. Lo cual demuestra el grado considerable de peligro de fuga de información a través de las redes sociales.

b. El 87,7% de entrevistados (128), aproximadamente 9 de cada 10 cadetes del IV año de la Escuela Militara de Chorrillos "Coronel Francisco Bolognesi", considera que los riesgos en la seguridad física e instalaciones la Escuela Militar de Chorrillos, son considerables; por lo que se puede definir que el peligro es latente y gira en torno al ciberespacio, donde la tecnología posibilita fuga de informaciones.

## Tercera conclusión

El 44,6% señala que la filtración de información en las redes sociales juega un papel importante, debido a que incrementa los riesgos en la seguridad física e instalaciones en los cadetes del IV año de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"

# RECOMENDACIONES

1. De acuerdo a la conclusión generada es necesario que la Dirección de la EMCH realice un adecuado estudio sobre la filtración de información en las redes sociales y los riesgos en la seguridad física e instalaciones, en los cadetes de cuarto año de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi". Ello se sustenta con un valor Rho Spearman = ,734 y p= 0,000 menor a $\alpha$=0,05, infiriéndose una vinculación con las mencionadas variables.
2. Se recomienda que haya una capacitación sobre las diferentes consideraciones de filtración de información en las redes sociales, que permita evitar la generación o incremento de los riesgos en la seguridad física o de las instalaciones en los cadetes de cuarto año de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi".

3. Si bien es cierto que el uso de la filtración de información en las redes sociales que pueden incrementar los riesgos en la seguridad física y de las instalaciones en los cadetes del IV año de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi"; es necesario que exista un control permanente que permita evitar el mal uso de estos sistemas tecnológicos.

4. Recomendación general: Capacitar yd dictar medidas de seguridad al personal de cadetes del IV año de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", destinadas a restringir el uso permanente de teléfonos celulares con capacidad de acceso a internet, para evitar la filtración de información en las redes sociales que atenten contra la seguridad física e instalaciones,

# REFERENCIAS

## Libros


a. Cabero, J. (1998). "Impacto de las nuevas tecnologías de la información y la comunicación en las organizaciones educativas Universidad de Sevilla España p. 198

b. Canga Larequi, Revista Latina de comunicación social "Periodismo e Internet: Nuevo medio, vieja profesión". Estudios del Mensaje Periodístico, 2001

c. Ciapuscio Guiomar Elena (1999) La terminología desde el punto de vista textual: selección, tratamiento y variación Universidad de Buenos Aires Argentina

d. Comisión Multisectorial para el Desarrollo de la Sociedad de la Información - CODESI, Resolución Ministerial N° 048-2008-PCM.

e. Foltýn Thomás autor del artículo, escrito en el marco del Día Mundial de las Redes Sociales (2018)

f. Oliva et al., (2012).

g. Oliva, Hidalgo, Moreno, Jiménez, Antolín & Ramos 2012

h. Páez, Zubieta, Mayordomo, Jiménez y Ruiz (2004)

i. Rosenberg (1965, Validación de la escala de autoestima en población general y en población clínica - Buenos Aires - Argentina

j. Plan de Desarrollo de la Sociedad de la Información en el Perú - La Agenda Digital Peruana, Decreto Supremo N° 066-2011-PCM.

k. Hernández, Fernández y Baptista (2006, p.102) Metodología de la Investigación Editorial Universidad de Zelaya México

l. Jiménez Mesa, José Riesgos de las Redes Sociales Informáticas Internet Social NETWORK RISKS, Málaga, España, 2014

m. José Luis Sampedro en Técnica y globalización1 (2002) Universidad de Madrid

n. Julián Pérez Porto Universidad de Buenos Aires - Argentina 2012


## Dispositivos Legales


a. Constitución Política del Perú, artículo 168

b. Decreto Legislativo N° 1094 "Código Penal Militar Policial".
c. La Ley Nº 27815 “Ley del Código de Ética de la Función Pública”, modificado por la Ley Nº 28496, de fecha 18Abr05, reglamento dado mediante Decreto Supremo Nº 033-2005-PCM.
d. Decreto Legislativo N° 1145 del 11Dic12.
e. Decreto L e g i s l a t i v o N° 276 Ley de bases de la carrera administrativa y su reglamento el Decreto Supremo 005-90-PCM.
f. La reglamentación de la Ley Nº 29131 “Ley del Régimen disciplinario de las FFAA”, en su artículo 1º.
g. Ley N° 29131 "Ley del Régimen Disciplinario de las FFAA"
h. Ley N°27658. Ley Marco de Modernización de la Gestión del Estado, del 30/enero/2002
i. Decreto Supremo N° 008-2013 "Reglamento de Ley del Régimen Disciplinario de las FFAA" y modificatorias (Anexo I, II y III).
j. Decreto Supremo Nº 002-2015-DE del 29 Ene 15, artículo 1º, literal D, numeral 6º.
k. El artículo 1º, literal d, num 6º, del Decreto Supremo Nº 002-2015-DE del 29 Ene 15.
l. El Decreto Legislativo Nº 1134 “Ley de Organización y Funciones del Ministerio de Defensa”.
m. El Reglamento del Ejército “Correspondencia Militar” (RE 31-62).
n. Rojas, (2009)
o. Rossemberg (1965, citado en Sánchez, 1999).
p. Sampedro José Luis (2002). Técnica y Globalización. Boletín Económico de ICE,, Nº 27.
q. Serradas (2004).
r. Tapscott (1997), Naval, Sábada, Bringué y Pérez Alonso-Geta (2003) y Gil, Feliú, Rivero y Gil (2003).

Reglamentos y Directivas

a. Comunicado N° 001 - CINFE de 24 Ene 19.
b. Ley Nº 1137 “Ley del Ejército del Perú” del 09Dic12.
c. Mc Anany, (Citado por Canga Larequi, 1988)

d. DFA-CD-02-11, Ministerio de Defensa - Comando Conjunto de las Fuerzas Armas - Doctrina de Inteligencia Conjunta - Lima - Perú - Dic 2011. Pag IX-6.
e. Directiva N° 001/CGE/DIE/B-3/03.03.11 de Mar 17
f. Directiva N° 001/COEDE/DEICI/03.03.11 de Ene 2019
g. Doctrina de Inteligencia Nacional-Fundamentos Doctrinarios
h. O/M N° 114/U-3.d.2.d/03.03.01 del 11 Mar 19
i. O/M N° 119/U-3.d.2.d/03.03.01 del 20 Mar 19
j. O/M N° 138/U-3.d.2.d/03.03.01 del 10 Abr 19
k. O/M N° 139/U-3.d.2.d/03.03.01 del 10 Abr 19
l. O/M N° 15196/DIE/B-3/03.03.11 del 22 Ene 19
m. RE 31-62 (Correspondencia Militar)
n. RE 38-10 (Seguridad Militar).
o. Reglamento Interno de la Comisión Multisectorial Permanente para el Seguimiento y Evaluaciyn del "Plan de Desarrollo de la Sociedad de la Información - La Agenda Digital Peruana" (CODESI). 2008
p. UNESCO, 1984, 8
q. UNICEF (1990).
r. Zegarra Carmen, director de la Unidad de Delitos Cibernéticos de Microsoft Perú
s. ME 38-10, Seguridad Militar, Sec II, Pfo 31. Pag 93

Internet

a. https://www.welivesecurity.com/la-es/2018/06/29/sobreexposicion-redes-sociales-puede-traer-problemas/
b. https://rpp.pe/lima/actualidad/los-jovenes-y-la-violencia-detras-de-las-redes-sociales-noticia-610799
c. http://www.clubcultura.com/clubliteratura/clubescritores/sampedro/miradas_global.htm
d. https://www.campusromero.pe/.../cuales-son-las-redes-sociales-mas-usadas-por-los-per...

# ANEXO 1

# BASE DE DATOS

# ANEXO 1: BASE DE DATOS

CUESTIONARIO SOBRE FILTRACIONES DE INFORMACIÓN EN LAS REDES SOCIALES

Estimado cadete:

El presente cuestionario es para obtener información respecto a un trabajo de investigación, para lo cual solicitamos su cooperación, respondiendo todas las preguntas. Los resultados nos permitirán proponer sugerencias para el bien de nuestra institución.

Marque con una (X) la alternativa que considera pertinente en cada caso

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| Nunca | Casi nunca | A veces | Casi siempre | Siempre |

| VARIABLE 1: FILTRACIONES DE INFORMACIÓN EN LAS REDES SOCIALES | | | | | | |
|---|---|---|---|---|---|---|
| Dimensión1: Conciencia de Seguridad | | S | CS | AV | CN | N |
| 1 | ¿En su vida personal y profesional tiene criterios de seguridad en el uso de información? | | | | | |
| 2 | ¿Consideras que las redes sociales influyen de alguna manera en tu vida diaria? | | | | | |
| 3 | ¿Crees que la publicidad en redes sociales es útil y efectiva para obtener información? | | | | | |
| 4 | ¿Consideras que las charlas sobre uso de redes sociales ayudan en la obtención de información para tus trabajos en la Escuela Militar de Chorrillos Coronel Francisco Bolognesi? | | | | | |
| 5 | ¿Tienes conocimiento sobre el sistema de ciberseguridad? | | | | | |

| | | < 1 hr | 1 a 2 horas | 2 a 3 horas | + 3 horas | |
|---|---|---|---|---|---|---|
| 6 | ¿Cuántas horas debe durar capacitación que se imparte sobre filtración de información en las redes sociales es la adecuada? | | | | | |

| | | Facebook | Whats App | Instagran | Twitter | Youtube | Google |
|---|---|---|---|---|---|---|---|
| 7 | ¿Cómo medida de seguridad, qué redes sociales usas? | | | | | | |
| 8 | En la seguridad física ¿cuál consideradas que es la Red social más importante? | | | | | | |
| 9 | En la seguridad en las instalaciones ¿cuál consideradas que es la Red social más importante? | | | | | | |

| Dimensión 2: Normas de seguridad | | SI | NO |
|---|---|---|---|
| 10 | ¿Consideras que los reglamentos ayudan a tener conocimiento de la filtración de la información en las redes sociales? | | |
| 11 | ¿Consideras que los manuales ayudan a tener conocimiento de la filtración de la información en las redes sociales? | | |

| | | | |
|---|---|---|---|
| 12 | ¿Crees que es necesario actualizar los manuales y reglamentos relacionados a la filtración de la información? | | |

# ANEXO 2

# MATRIZ DE CONSISTENCIA

# ANEXO 2: MATRIZ DE CONSISTENCIA

TÍTULO: FILTRACION DE INFORMACION EN REDES SOCIALES Y SUS RIESGOS EN LA SEGURIDAD FISICA E INSTALACIONES, CADETES CUARTO AÑO ESCUELA MILITAR DE CHORRILLOS "CORONEL FRANCISCO BOLOGNESI", 2019

<table>
<tr><th>PROBLEMA GENERAL</th><th>OBJETIVO GENERAL</th><th>HIPÓTESIS GENERAL</th><th>VARIABLES</th></tr>
<tr><td>¿Cuáles son las filtraciones de información en redes sociales en la seguridad física e instalaciones, cadetes cuarto año de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", 2019?</td><td>Determinar las filtraciones de información en redes sociales en la seguridad física e instalaciones, cadetes de cuarto año de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", 2019.</td><td>Existe una relación directa y significa entre las filtraciones de información en redes sociales y la seguridad física e instalaciones, cadetes de cuarto año de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", 2019.</td><td rowspan="3">Operacionalización de la Variable 1: Filtraciones de información en las redes sociales<br><table><tr><th>Dimensiones</th><th>Indicadores</th></tr><tr><td rowspan="3">Dimensión 1<br>Conciencia de Seguridad</td><td>Aspectos de seguridad</td></tr><tr><td>Uso de redes sociales</td></tr><tr><td>Obtención de información</td></tr><tr><td rowspan="3">Dimensión 2<br>Capacitación en temas de Ciberseguridad</td><td>Charlas</td></tr><tr><td>Ciberseguridad</td></tr><tr><td>Capacitación</td></tr></table><br>Operacionalización de la Variable 2 : Seguridad física e instalaciones<br><table><tr><th>Dimensiones</th><th>Indicadores</th></tr><tr><td rowspan="2">Dimensión 1<br>Percepción de seguridad</td><td>Seguridad en instalaciones</td></tr><tr><td>Esfuerzos de seguridad</td></tr><tr><td>Dimensión 2</td><td>Manuales</td></tr></table></td></tr>
<tr><td>PROBLEMAS ESPECÍFICOS</td><td>OBJETIVOS ESPECÍFICOS</td><td>HIPÓTESIS ESPECÍFICOS</td></tr>
<tr><td>1. ¿La falta de Conciencia en Seguridad incidirá en la seguridad física e instalaciones, cadetes cuarto año de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", 2019?<br><br>2. ¿La falta de capacitación en temas de ciberseguridad incidirá en</td><td>1. Determinar como la falta de Conciencia en Seguridad, incidirá en la seguridad física e instalaciones, cadetes cuarto año de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi", 2019<br><br>2. Determinar como la falta de capacitación en temas</td><td>1. Existe una relación directa y significa entre la falta de Conciencia en Seguridad y la seguridad física e instalaciones, cadetes de cuarto año de la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi".<br><br>2. Existe una relación directa y significativa</td></tr>
</table>

<table>
<tr><td>la seguridad física e instalaciones, cadetes cuarto año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2019?</td><td>de ciberseguridad, Incidirá en la seguridad física e instalaciones, cadetes cuarto año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”, 2019.</td><td>entre la falta de capacitación en temas de Ciberseguridad y la seguridad física e instalaciones, cadetes de cuarto año de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”.</td><td>Normas de seguridad</td><td>Medidas de seguridad<br>Vigencia de manuales<br>Malla curricular</td></tr>
<tr><td>METODOLOGÍA</td><td>POBLACIÓN Y MUESTRA</td><td>TÉCNICA E INSTRUMENTOS</td><td>VALIDEZ</td><td>CONFIABILIDAD</td></tr>
<tr><td>Enfoque: Cuantitativo y Cualitativo<br><br>Tipo de investigación: Descriptivo y correlacional<br><br>Diseño No experimental<br><br>Método inductivo</td><td>Población: 234 cadetes de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”<br>Muestra: 146</td><td>Cuestionario<br>Escala de Likert</td><td>Juicio de expertos<br>Alfa de Cronbach</td><td>Rho de Spearman</td></tr>
</table>

# ANEXO 3

# INSTRUMENTO DE RECOLECCION

# ANEXO 3: INSTRUMENTO DE RECOLECCIÓN

## CUESTIONARIO SOBRE SEGURIDAD FÍSICA E INSTALACIONES

Estimado cadete:

El presente cuestionario es para obtener información respecto a un trabajo de investigación, para lo cual solicitamos su cooperación, respondiendo todas las preguntas. Los resultados nos permitirán proponer sugerencias para el bien de nuestra institución.

Marque con una (X) la alternativa que considera pertinente en cada caso

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| Nunca | Casi nunca | A veces | Casi siempre | Siempre |

| VARIABLE 2: SEGURIDAD FISICA E INSTALACIONES | | | | | | |
|---|---|---|---|---|---|---|
| Dimensión1: Percepción de Seguridad | | S | CS | AV | CN | N |
| 1 | ¿Se siente seguro en las instalaciones de la Escuela Militar de chorrillos “Coronel Francisco Bolognesi”? | | | | | |
| 2 | ¿Cree usted que la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” realiza esfuerzos para asegurar la integridad física de los cadetes? | | | | | |
| Dimensión 2: Normas de Seguridad | | S | CS | AV | CN | N |
| 3 | ¿Existen manuales de contrainteligencia en la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”? | | | | | |
| 4 | ¿Cree usted que deben existir manuales sobre temas de ciberseguridad en la Escuela Militar de Chorrillos Coronel Francisco Bolognesi? | | | | | |
| 5 | ¿Considera usted que en la malla curricular de la Escuela Militar de Chorrillos se debe considerar una asignatura de Ciberseguridad? | | | | | |

# ANEXO 4

# DOCUMENTO DE VALIDACIÓN DE INSTRUMENTO

# ANEXO 4: DOCUMENTO DE VALIDACIÓN DE INSTRUMENTO

## FORMATO DE VALIDACION DE INSTRUMENTO POR EXPERTO

TITULO DE TESIS: “FILTRACIÓN DE INFORMACION EN REDES SOCIALES Y SUS RIESGOS EN LA SEGURIDAD FÍSICA E INSTALACIONES, CADETE DE CUARTO AÑO DE LA ESCUELA MILITAR DE CHORRILLOS “CORONEL FRANCISCO BOLOGNESI”

AUTORES:
1. BACH. LINARES FLOTRIAN BRYAN ROBERT
2. BACH. RETO HERNANDEZ RODRIGO
3. BACH. VILLALBA PORTUGAL JULIO

INSTRUCCIONES: Coloque “x” en el casillero correspondiente la valoración que su experticia determine sobre las preguntas formuladas en el instrumento.

| CRITERIOS | DESCRIPCION | VALOR ASIGNADO POR EL EXPERTO | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 10 | 20 | 30 | 40 | 50 | 60 | 70 | 80 | 90 | 100 |
| 1. CLARIDAD | Esta formado con el lenguaje adecuado. | | | | | | | | | | |
| 2. OBJETIVIDAD | Esta expresado en conductas observadas. | | | | | | | | | | |
| 3. ACTUALIDAD | Adecuado de acuerdo al avance de la ciencia. | | | | | | | | | | |
| 4. ORGANIZACIÓN | Existe una cohesión lógica entre sus elementos. | | | | | | | | | | |
| 5. SUFICIENCIA | Comprende los aspectos requeridos en cantidad y calidad. | | | | | | | | | | |
| 6. INTENCIONALIDAD | Adecuado para valorar los aspectos de la investigación. | | | | | | | | | | |
| 7. CONSISTENCIA | Basado en bases teóricas científicas. | | | | | | | | | | |
| 8. COHERENCIA | Hay correspondencia entre dimensiones, indicadores e índices. | | | | | | | | | | |
| 9. METODOLOGIA | El diseño responde al propósito de la investigación. | | | | | | | | | | |
| 10. PERTINENCIA | Es útil y adecuado para la investigación. | | | | | | | | | | |

PROMEDIO DE VALORACION DEL EXPERTO: _____
OBSERVACIONES REALIZADAS POR EL EXPERTO:
……

GRADO ACADEMICO DEL EXPERTO:_____
APELLIDOS Y NOMBRES DEL EXPERTO:_____

FIRMA:……..……..……
POST FIRMA:……..……
DNI:……

# ANEXO 5

# CONSTANCIA DE ENTIDAD DONDE SE EFECTUÓ LA INVESTIGACIÓN

ANEXO 5: CONSTANCIA DE ENTIDAD DONDE SE EFECTUÓ LA INVESTIGACIÓN

ESCUELA MILITAR DE CHORRILLOS “CORONEL FRANCISCO BOLOGNESI”

CONSTANCIA

El que suscribe Su Director Académico de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi”

HACE CONSTAR:

Que los cadetes que se mencionan han realizado la investigación en esta dependencia militar sobre el tema titulado “FILTRACION DE INFORMACION EN REDES SOCIALES Y SUS RIESGOS EN LA SEGURIDAD FISICA E INSTALACIONES, CADETES CUARTO AÑO ESCUELA MILITAR DE CHORRILLOS “CORONEL FRANCISCO BOLOGNESI”, 2019.

Investigadores

Bach. Linares Florián, Brayan Robert

Bach. Reto Hernández, Rodrigo De Jesús

Bach. Villalba Portugal, Julio Cesar Hans

Se le expide la presente Constancia a efectos de emplearla como anexo en su investigación.

Chorrillos,… de……..del 2019

_____

0-224396679-0+
CH. SOLDEVILLA P.
TTE CRL
JEFE DEL DIDOC - EMCH “CFB”

# ANEXO 6

# COMPROMISO DE AUTENTICIDAD DEL DOCUMENTO

# ANEXO 6: COMPROMISO DE AUTENTICIDAD DEL DOCUMENTO

Los bachilleres en Ciencias Militares LINARES FLORIAN BRAYAN ROBERT, RETO HERNÁNDEZ RODRIGO DE JESÚS y VILLALBA PORTUGAL JULIO CESAR HANS; autores del trabajo de investigación titulado "FILTRACION DE INFORMACION EN REDES SOCIALES Y SUS RIESGOS EN LA SEGURIDAD FISICA E INSTALACIONES, CADETES CUARTO AÑO ESCUELA MILITAR DE CHORRILLOS "CORONEL FRANCISCO BOLOGNESI", 2019.

Declaran:

Que, el presente trabajo íntegramente elaborado por los suscritos y que no existe plagio alguno, presentado por otra persona, grupo o institución, comprometiéndonos a poner a disposición del COEDE (EMCH "FB") y RENATI (SUNEDU) los documentos que acrediten la autenticidad de la información proporcionada; si esto lo fuera solicitado por la entidad.

En tal sentido, asumimos la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión, tanto en los documentos como en la información aportada.

Nos afirmamos y ratificamos en lo expresado, en señal de lo cual firmamos el presente documento.

Chorrillo, 03 de Diciembre del 2019

B. LINARES F.
DNI:

R. RETO H.
DNI:

J. VILLALBA P.
DNI:

# ANEXO 7

# CIBERSEGURIDAD MARCO LEGAL Y DOCTRINARIO

Sociedad de la Información

a. Ley N°27658. Ley Marco de Modernización de la Gestión del Estado, del 30/enero/2002
b. Comisión Multisectorial para el Desarrollo de la Sociedad de la Información-CODESI, Resolución Ministerial N° 048-2008-PCM.
c. Reglamento Interno de la Comisión Multisectorial Permanente para el Seguimiento y Evaluaciyn del "Plan de Desarrollo de la Sociedad de la Informaciyn - La Agenda Digital Peruana" (CODESI). 2008
d. Plan de Desarrollo de la Sociedad de la Información en el Perú - La Agenda Digital Peruana, Decreto Supremo N° 066-2011-PCM.

Gobierno Electrónico

a. Estrategia Nacional de Gobierno, Resolución Ministerial N° 274-2006-PCM.
b. Formulación y evaluación del Plan Operativo Informático de las entidades de la Administración Publica y su Guía de Elaboración, Resolución Ministerial N° 19-2011PCM.
c. Lineamientos que establecen el contenido mínimo de los Planes Estratégicos de Gobierno Electrónico, Resolución Ministerial N°61-2011-PCM.

d. Ley de Protección de datos personales N° 29733.(03/jul/2011) e. Ley de Delitos Informáticos N° 30096.(22/oct/2013)

f. Uso obligatorio de la Norma Técnica Peruana NTP-ISO/IEC 12207:2016 Tecnología de la Informaciyn. "Procesos del Ciclo de Vida del Software, 1° Ediciyn" en entidades del Sistema Nacional de Informática, Resolución Ministerial N° 041-2017-PCM.

Seguridad de la Información

a. La Constitución Política del Perú.

b. Ley N° 27806 de fecha 2 de agosto 2002 - "Ley de Transparencia y Acceso a la Información Pública" y modificatorias.

c. Resolución Jefatural N° 386-2002-INEI que aprueba la Directiva N° 016-2002/INEI/DTNP "Normas Técnicas para el almacenamiento y respaldo de la información procesada por las entidades de la Administración Pública".

d. Ley N° 28612 que norma el uso, adquisición y adecuación del software de la Administración Pública.

e. Norma Técnica Peruana NTP-ISO/IEC 27001:2014. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información (2ª Edición) en todas las entidades integrantes del Sistema Nacional de Informática, Resolución Comisión de Formalización y de Fiscalización de Barreras Comerciales no Arancelarias N° 129-2014 CNB/INDECOPI de fecha 20 de noviembre del 2014.

También se puede mencionar lo manifestado en el Capítulo II, Sección II: Marco Doctrinario en la Doctrina Básica Conjunta, en referencia al Entorno Jurídico Internacional, que indica lo siguiente: Se deberá considerar las reglas normadas en el Manual de TALLINN de Derecho Internacional aplicable a la Ciberguerra.

Ciberespacio

a. Es un dominio global formado por los sistemas de información y telecomunicaciones, y otros sistemas electrónicos, su interacción y la información que es almacenada, procesada o transmitida por estos sistemas. NATO, Ciberdefensa (2014) .

b. Las operaciones en el ciberespacio no son un sinónimo de las Operaciones de Información (IO). Las IO son un conjunto de operaciones que se pueden realizar en el ciberespacio o en otros dominios. Las operaciones en el ciberespacio pueden apoyar directamente a las IO, pero las IO no cibernéticas pueden afectar las operaciones en el ciberespacio.

c. El ciberespacio es un dominio establecido por el hombre y es por lo tanto, un dominio distinto de aquellos naturales como son el aire, tierra, mar y espacio. Requiere una atención continua de parte de los seres humanos para adaptarse a las características, alcance global y particularidades del mismo. Los Nodos del ciberespacio residen físicamente en todos los ámbitos. Las actividades en el ciberespacio pueden permitir la libertad de acción para realizar actividades en los otros dominios y las actividades en los otros dominios pueden crear efectos en y a través del ciberespacio.

d. A pesar de que las redes en el ciberespacio son interdependientes, parte de estas redes pueden quedar aisladas. El aislamiento del ciberespacio se puede lograr a través de protocolos, firewalls, encriptación y la separación física del resto de las redes. Por ejemplo, las redes clasificadas de las Fuerzas Armadas no están conectadas en todo momento a Internet, pero cada vez que lo hacen, lo deben hacer a través de protocolos, servicios y puertos seguros. La construcción de algunas redes cableadas de manera específica minimiza la mayoría de las formas de interferencia por radiofrecuencia.

e. Estos factores permiten que estas redes no queden aisladas del ciberespacio y con eso garantizan su conectividad con las redes globales.

f. Segmentos del ciberespacio están conectados y apoyados por infraestructuras físicas, sistemas electrónicos y porciones del espectro electromagnético (EMS). Los sistemas e infraestructuras evolucionan rápidamente debido a que los usuarios necesitan una mayor capacidad y velocidad de procesamiento de datos, por lo tanto, se exige el uso de porciones cada vez mayores del EMS y el uso de un mayor ancho de banda. Los sistemas suelen ser diseñados para cambiar las frecuencias en las que operan dentro del EMS, para evitar la manipulación de datos.

g. La maniobrabilidad lógica en el ciberespacio es a menudo una función de los protocolos de seguridad utilizados por los sistemas “Host”. Los sistemas intrusos que intentan conectarse a un Host seguro tendrán muchas más dificultades para acceder a la información de éstos. Además, la defensa contra sistemas no deseados que intentan entrar se encuentra fundamentalmente en los códigos o la lógica de los sistemas Host. Una vez que la conexión es establecida, cualquier intruso puede explotar una falla en la lógica para ingresar permanentemente en el sistema y maniobrar en ella mientras no sea detectado.

h. La escritura de los códigos de seguridad puede ser una forma de maniobra lógica en el ciberespacio, y por otro lado, un intruso puede crear un código para explotar una vulnerabilidad y obtener maniobrabilidad frente a los sistemas de destino.

i. Esto puede resultar muy peligroso ya que mientras el defensor se da cuenta de la presencia no deseada de un intruso dentro de su sistema, éste ya puede haber alterado el código de entrada del mismo, incluso para impedir el ingreso de los usuarios legítimos. El intruso que desee permanecer en el sistema puede tener las capacidades de instalar un software malicioso y acceder cuando lo desea.

j. Este proceso es el equivalente a las fuerzas que maniobran para ganar posiciones de ventaja en los dominios tradicionales de aire, tierra, mar y espacio. Puede presentarse casos en los que uno de ellos requiere la intervención del otro.

Desafíos de las Operaciones en el Ciberespacio

a. Las operaciones del ciberespacio ofrecen desafíos militares únicos; siendo algunos de los desafíos conocidos: el cumplimiento de la misión, un ciclo de decisión eficaz, el anonimato y sus desafíos inherentes y las diversas amenazas al ciberespacio.

b. Existe un requisito para equilibrar las acciones defensivas del ciberespacio con su impacto en las operaciones aéreas, espaciales y del ciberespacio en curso. Este requisito es el pleno conocimiento de la situación entre los dominios; su carencia

puede causar en algunos casos graves desconexiones y en otras impedir de modo significativo las operaciones.

(1) Cumplimiento de la Misión

(a) Cumplir la misión implica adoptar medidas necesarias para lograr los objetivos esenciales que contemplan dichas misiones y dar prioridad a los factores determinantes de la misión, verificar la dependencia de la misión para con el ciberespacio, la identificación de vulnerabilidades y la mitigación de riesgos asociados.

(b) El cumplimiento de la misión implica tener disponible una red segura para apoyar las operaciones militares, de tal forma que el asegurar y defender la parte de la red que apoya directamente a tales operaciones, también es prioritaria.

(c) Algunas medidas de seguridad y protección pueden incluir copias de seguridad (Backups) o replicaciones en los puntos de posible falla de la red para asegurar que la red cumpla con los requisitos de la misión. Las acciones proactivas adoptadas deben servir para asegurar que la red sea confiable, íntegra y esté disponible. Estas medidas, pueden incluir el centrar la atención en los medios de defensa en aquel segmento de la red que apoya las operaciones, para asegurar que no existan amenazas residentes en la misma.

(d) Un ambiente cibernético seguro, es aquel en el que las contramedidas adoptadas son eficaces frente a los adversarios que intentan cambiar el resultado de una misión, al negar, degradar, interrumpir o destruir nuestra capacidad cibernética o mediante la alteración del uso, el producto o la confianza en las capacidades existentes.

(e) El personal debe saber que los riesgos y vulnerabilidades a menudo son creados por las interdependencias inherentes a las redes y la integración

de sistemas a través del ciberespacio. Es imprescindible la sensibilización del usuario de los sistemas considerando que no existe la seguridad total en el ciberespacio y el factor más débil es el ser humano.

(f) Dado que la naturaleza del ciberespacio es la interconectividad, todas las operaciones del ciberespacio tienen un riesgo inherente que requiere constante atención y su mitigación. En este contexto, un riesgo asumido por uno es potencialmente asumido por todos. El tratamiento de los riesgos puede resultar en una disminución del nivel de gravedad hasta ser considerado aceptable para continuar realizando las operaciones. La implementación de servidores de seguridad, capacitación, educación y sistemas de detección y prevención de intrusiones representan algunos de los tipos de mitigación de riesgos.

(g) Al igual que en el dominio aéreo, no se trata de defender todo el dominio del ciberespacio, se trata de defender lo que es relevante para nuestras operaciones. En el ciberespacio, eso significa la protección de las rutas y los componentes útiles, ya que la acción contra los sistemas críticos degrada seriamente nuestra capacidad para luchar y ganar. Tanto si se utiliza ofensiva o defensivamente, la realización de determinadas operaciones en el ciberespacio puede requerir el acceso a sólo una muy pequeña parte de todo el ambiente cibernético. Operar con éxito en el ciberespacio puede implicar abandonar las hipótesis clásicas sobre limitaciones de distancia, tiempo y las barreras físicas presentes en otros dominios.

(h) La libertad de acción en el ciberespacio puede ser un requisito básico para el cumplimiento de la misión. Sin embargo, tener la capacidad para actuar en el ciberespacio con el fin de lograr esta libertad de acción no debe darse por sentado de manera implícita. Así como operar en el dominio del aire exige tener la capacidad y los medios para hacerlo (plataformas aéreas, pistas, etc.), las Fuerzas Armadas deben asegurarse

de contar con la suficiente capacidad (ancho de banda, componentes, etc.) para operar en el ciberespacio. Dado que hoy en día el acceso al ciberespacio permite realizar las actividades diarias, es fácil pasar por alto este requisito y nos lleva a suponer que el solo hecho de contar con esta capacidad suficiente nos garantiza la libertad de acción lo cual significa un grave error.

(i) Las operaciones en el ciberespacio tratan de garantizar la libertad de acción en todos los dominios existentes y negar la misma libertad a los adversarios. La explotación de las tecnologías disponibles, permiten mejorar las capacidades de las Fuerzas Armadas convirtiéndose en protagonistas de operaciones militares, mediante la entrega de información y las acciones que se puedan ejecutar al contar con la misma. Los enlaces del ciberespacio facilitan la defensiva, la explotación de información y las operaciones ofensivas para lograr una ventaja de la situación.

(j) El Comando Operacional de Ciberdefensa, en coordinación con sus componentes deben estar seguros que pueden establecer y mantener la superioridad en el ciberespacio y luchar contra los ataques en este dominio en cualquier momento sea que se empleen fuerzas militares o no.

(k) Las amenazas también han demostrado que pueden crear inestabilidad civil a través de ataques cibernéticos. El COCID debe mantener la capacidad para proporcionar apoyo de defensa a las autoridades civiles en el ciberespacio cuando sea necesario.

(l) El ataque cibernético masivo y sus consiguientes efectos ilustran lo rápido que los hackers maliciosos pueden afectar incluso a todo un gobierno tecnológicamente sofisticado. El COCID debe establecer políticas y directrices para garantizar la ejecución de sus funciones en la

protección de los activos críticos, en el caso que se realicen Ciberataques a dichos activos.

Amenazas a las Operaciones en el Ciberespacio

(a) En otros ámbitos, las principales amenazas a la Seguridad Nacional provienen de Estados-Nación o actores transnacionales tales como organizaciones terroristas.

(b) Grandes recursos de capital y de personal son necesarios para construir, posicionar, mantener y operar naves, aviones de combate y satélites, pero tan sólo una pequeña organización y con herramientas sencillas pueden hacer volar en pedazos estructuras y organizaciones enteras.

(c) Los adversarios buscan ventajas asimétricas y el ciberespacio ofrece oportunidades significativas para su obtención. Hay una gran variedad de amenazas a las operaciones del ciberespacio. En los párrafos siguientes se ofrece una breve descripción de cada categoría de amenaza. Estas amenazas y otras deben ser consideradas cuando se realizan las operaciones del ciberespacio.

Las Fuerzas Armadas dependen de la infraestructura del Estado y de sus recursos claves para muchas de sus actividades, incluyendo el despliegue de la fuerza, la capacitación, el transporte y sus operaciones habituales. La protección física de éstos ya no es el único problema que tienen los comandantes; hoy en día todas las organizaciones e infraestructuras críticas están bajo el control y supervisión de sistemas de adquisición de datos y redes, o sistemas de control.

Dado que la industria privada es el principal catalizador de los avances tecnológicos, los militares pueden llegar a ser cada vez más dependientes de dicha tecnología comercial. Esta dependencia puede presentar tres vulnerabilidades principales:

Propiedad extranjera: control e influencia de los proveedores. Muchas de las tecnologías comerciales (hardware y software) que el sector Defensa adquiere son desarrolladas y fabricadas con componentes fabricados por otros países. Estos

fabricantes, proveedores, proveedores de servicios y los inventores pueden ser influenciados por los adversarios, para ofrecer productos alterados que tienen incorporados puntos vulnerables tales como chips modificados o brindar las claves de acceso a dicha tecnología.

Cadena de suministro: La cadena de suministro global tiene vulnerabilidades que potencialmente pueden permitir la interceptación y alteración de los productos. Estas vulnerabilidades están presentes durante todo el ciclo de vida del producto, desde la creación del concepto de diseño, la entrega del producto y las actualizaciones de productos y soporte.

Tecnología comercial: La mayor parte de los componentes que permiten las capacidades de las operaciones del ciberespacio y del sector Defensa son comerciales y carecen de niveles de seguridad óptimos.