Galeano, Diana Elizabeth

Proyecto: procedimientos básicos para la elaboración de estudios de seguridad y protección de instalaciones físicas de instituciones públicas o privadas de la ciudad de Jesús María (Córdoba)

Tesis para la obtención del título de posgrado de Especialista en Dirección de Organizaciones Públicas

Director: Somoza, Luis Alberto Gabriel

UNIVERSIDAD CATÓLICA DE CÓRDOBA - INSTITUTO DE CIENCIAS DE LA ADMINISTRACIÓN

ESPECIALIZACIÓN EN DIRECCIÓN DE ORGANIZACIONES PÚBLICAS

TRABAJO FINAL DE GRADO PARA LA OBTENCIÓN DEL TÍTULO DE POSGRADO EN DIRECCIÓN DE ORGANIZACIONES PÚBLICAS

TEMA: “PROYECTO: PROCEDIMIENTOS BÁSICOS PARA LA ELABORACIÓN DE ESTUDIOS DE SEGURIDAD Y PROTECCIÓN DE INSTALACIONES FÍSICAS DE INSTITUCIONES PÚBLICAS O PRIVADAS DE LA CIUDAD DE JESUS MARÍA (CÓRDOBA)”

Alumno: Lic. Diana Elizabeth Galeano

Director: Dr. Luis Alberto Gabriel Somoza

Córdoba 2023

ÍNDICE

AGRADECIMIENTOS

Esta tesis alcanzó su presentación final por haber contado con la participación desinteresada de diferentes amigos, colegas y especialistas en diferentes momentos de su elaboración. A mis profesores, por compartir sus vivencias, conocimientos y experiencias académicas. A todos ellos, les estoy altamente agradecida.

Mis agradecimientos al director de tesis, el Dr. Luis Alberto Gabriel Somoza, quien, durante todo este tiempo, siempre tuvo voces de ánimo y marcada vehemencia respecto a la orientación profesional del trabajo para poder llegar al resultado que se advierte en este documento.

También estoy agradecida de manera especial a mi familia y a mi conviviente, quienes sembraron en mí el espíritu de superación y perseverancia, por su amistad, apoyo, por su compañía, ánimo y motivación en este extraordinario proceso.

ABSTRACT/RESUMEN

Esta investigación está compuesta por cinco (5) capítulos, donde se describió en profundidad los criterios a considerar en la protección de Instalaciones Físicas para cualquier tipo de empresa u organización, manifestando así, de manera breve y clara lo desarrollado: en el primer capítulo se muestra el marco conceptual, donde se detalla la elección del tema del tema con el fin de mostrar el procedimiento que se llevó a cabo para su desarrollo. En el segundo capítulo se muestra el marco referencial, el cual detalla sobre los aspectos fundamentales en la elaboración de un informe de seguridad. En el tercer capítulo se muestra el marco metodológico donde se detalla la metodología utilizada y donde aparecen los resultados que nos arrojó el análisis efectuado sobre las empresas públicas y privadas de la Localidad de Jesús María. En el cuarto capítulo, se encuentra descripta la propuesta. Finalmente, en el quinto capítulo, se detalla las conclusiones a las que se arribaron luego de haber efectuado el análisis correspondiente de los objetivos y recolección de datos.

CAPÍTULO I “PLANTEAMIENTO DEL PROBLEMA”

1.1. El Problema

En un mundo globalizado, donde la interacción con personas e instituciones se llevan a cabo con mayor rapidez y apertura que en cualquier momento de nuestra historia, la propensión a ser víctima de eventos indeseados (ataques físicos o cibernéticos, robos, atentados, entre otros) es una realidad cada vez más palpable, lo que motiva a la activación del sentido natural de supervivencia y protección como instinto vital.

Bajo este panorama, desde la familia hasta las instituciones que conforman la sociedad pueden o han sido víctimas, en muchos casos sin darse cuenta o, peor aún, sin denunciar dichos eventos, de situaciones de indefensión o zozobra, que sin dudas ha repercutido en el libre desempeño de actividades o funciones que desequilibran el libre desenvolvimiento de los integrantes de la familia, de instituciones públicas o privadas y los trabajadores que dentro de ellas hacen vida.

En función de esta realidad, resulta necesario tener un conocimiento amplio acerca de cuáles son los puntos débiles y las fortalezas que, en el caso de esta investigación, poseen las instituciones que conforman una sociedad, aprovechando aquellas oportunidades que permitan la planificación de la seguridad física de instalaciones públicas o privadas, conformando un esquema de seguridad que represente una medida sólida en la prevención de eventos indeseados mediante una metodología de evaluación constante, así como la eficiencia en la prestación de servicios eficientes y seguros.

El contexto en el cual se desarrollará esta investigación es la Cuidad de Jesús María, ubicada a una distancia de 48 Km al Norte de la capital de Córdoba, con una población estimada en el año 2010 de 31,602 habitantes (INDEC, 2010). En esta región confluye la importante Ruta Nacional Nº 9, parte del sistema de corredores de comercialización que unen las ciudades del Mercosur lo que hace que en la zona haya un constante tránsito pesado sobre una planicie al pie de las sierras, formando un aglomerado urbano con la ciudad de Colonia Caroya y Sinsacate.

Todo este contexto ha contribuido al deterioro de la convivencia social donde prolifera el individualismo y la inseguridad en detrimento de la imagen urbana de la ciudad, elementos que insisten en el mantenimiento de un clima de creciente inseguridad urbana, con los efectos negativos que esto trae al funcionamiento de la ciudad, el deterioro de la calidad de vida de sus habitantes y en la dificultad de atraer inversionistas y visitantes (Análisis de la ciudad de Jesús María, 2021).

Consecuentemente la ciudad tiende a la trivialización, a la creación o apuesta de cuerpos de Seguridad Privada, a grupos de Alerta Temprana o de Protección Vecinal, lo que conlleva a la fragmentación de servicios públicos, la aparición del racismo y la xenofobia, entre otros (Borja, 2000), todos conformantes de un clima que auspicia el acontecimiento de eventos indeseados que ponen en peligro el desenvolvimiento de funciones o actividades por parte de las instituciones públicas o privadas que dan vida a la ciudad.

En función de ello, surge la necesidad de sistematizar de forma documental y procedimental las actividades relacionadas a los Estudios de Seguridad de instalaciones físicas aplicadas a las organizaciones que, independientemente, sean públicas o privadas se verían beneficiadas con esta propuesta, a los efectos de que las mismas cumplan con las medidas mínimas de seguridad (Lezana Veliz, 2011)

El tema propuesto para este proyecto es: **"PROCEDIMIENTOS BÁSICOS PARA LA ELABORACIÓN DE ESTUDIOS DE SEGURIDAD Y PROTECCIÓN DE INSTALACIONES FÍSICAS DE INSTITUCIONES PÚBLICAS O PRIVADAS DE LA CIUDAD DE JESUS MARÍA (CÓRDOBA)",** a razón que no se posee un Manual de carácter público específico en la mencionada temática para su abordaje, dificultando el trabajo al personal que desarrolla actividades dentro de los establecimientos, en cuanto al proceso de control, análisis y evaluación del sistema de seguridad física de las respectivas instalaciones.

El proyecto de Manual, a presentar aquí, será confeccionado con la intención de desarrollar una planificación acertada para el estudio de seguridad a implementar (Vallejo Rosero, 2005) y establecer correctamente los niveles de seguridad adecuados a emplear, a los efectos de prevenir riesgos y amenazas contra las personas, efectos e instalaciones.

Conforme lo recién expuesto, como **interrogante a resolver** se plantea: ¿Cuáles serían los procedimientos básicos para la elaboración de estudios de seguridad y protección de instalaciones físicas de instituciones públicas o privadas?, conociendo estos procedimientos se espera brindar una alternativa de solución que permita minimizar los eventos indeseados que pongan en riesgo la seguridad y el orden dentro de las instituciones pública o privadas de la Ciudad de Jesús María (Córdoba).

1.2. Justificación de la elección del tema y sus antecedentes

Desde la perspectiva social, la investigación propuesta representa un avance en la corrección de las debilidades en el sistema de seguridad de las instituciones públicas o privadas de la ciudad, mediante el mejoramiento de los protocolos que garanticen la seguridad de las instalaciones físicas y de las personas que hacen uso de las mismas, propiciando un clima de bienestar urbano que contribuya al mejor desenvolvimiento del desarrollo.

Adicionalmente, el ejercicio de un sistema de seguridad por parte del personal que labora dentro de las instituciones de la ciudad sensibilizaría a sus trabajadores hacia la identificación y prevención de eventos indeseados en su lugar de trabajo.

Por último, esta investigación revelaría resultados que pudieran ser aprovechados por instituciones de diferentes zonas del país, aportando un instrumento primordial para su desarrollo mediante la generación de un clima de confianza en el funcionamiento de la sociedad argentina.

1.3. Objetivos

1.3.1. General

- Definir los procedimientos básicos para la elaboración de estudios de seguridad y protección de instalaciones físicas de instituciones públicas o privadas.

1.3.2. Específicos

- Diagnosticar la situación actual en materia de seguridad y protección de instalaciones físicas de instituciones públicas o privadas de la ciudad de Jesús María (Córdoba).
- Caracterizar los procedimientos básicos fundamentales que debe poseer un sistema de seguridad de instalaciones físicas para instituciones públicas o privadas.
- Elaborar la estructura para un Manual de procedimientos básicos de estudios de seguridad y protección en instalaciones físicas públicas o privadas.

CAPÍTULO II “MARCO REFERENCIAL”

2.1. Antecedentes

El origen de la Seguridad emerge desde el comienzo de la civilización en el planeta tierra, ya sea para protegerse de los peligros naturales, el clima, otros seres humanos, etc., por lo que de alguna manera han ideado distintas formas para mejorar la calidad de vida de las personas a través de la historia, como por ejemplo, ocultarse en cuevas, fabricar sus propias herramientas para caza, alimentación y vestimenta, la construcción de sus propias cabañas y viviendas, entre otras, que conllevó al surgimiento de las primeras poblaciones a lo largo de la extensión del territorio.

En la actualidad, el aumento de la población, el proceso de industrialización, la globalización, los avances de la Tecnología de la Información y Comunicación (TIC) y la denominada Era Digital 4.0 (Schwab, 2016), ha evolucionado, acelerado y ampliado los estándares de gestión de la seguridad tradicional por una mayor demanda de exigencia y eficiencia técnica en la protección de la integridad física, la información y los bienes materiales de las personas físicas o jurídicas de cualquier comunidad.

Etimológicamente, la palabra “seguridad” proviene del latín securitas o securus que significa, ausencia de peligro, daño o riesgo.[1]

2.2. Marco teórico

2.2.1. Seguridad Física de instalaciones

Uno de los antecedentes relacionados con el tema, lo plantea Domínguez, (2013) propone un modelo de seguridad física para plantas industriales de proceso de alimentos de consumo masivo, cuya investigación se basó en la identificación de amenazas y vulnerabilidades que generan riesgos a la integridad de personas, operaciones y bienes de este tipo de instalaciones industriales y propone acciones para una adecuada gestión de estos.

La metodología aplicada se fundamenta en una investigación de campo de las operaciones de la planta de proceso y sus zonas de influencia, en una visión cuantitativa y con perspectiva cualitativa (interpretativa) a través de una entrevista concreta al Gerente de Planta así como también en una amplia consulta bibliográfica, donde los resultados obtenidos fueron de utilidad para posibilitar el planteamiento de un modelo apropiado de un sistema de

[1] Foro de Seguridad. (Sin Fecha). *Qué es la Seguridad*. Foro de Profesionales Latinoamericanos de Seguridad. Fecha de consulta: 30 de junio de 2021. Extraído de: https://www.gestiondelriesgo.com/artic/discipl/4163.htm

seguridad física que permita una adecuada gestión de los riesgos identificados, entonces, en consideración se plantea como primera hipótesis de trabajo que "*A mayores acciones preventivas mediante lineamientos específicos como informes e investigaciones que describan las posibles amenazas y riesgos en una empresa u organización o propuestas de sistemas de seguridad física adecuados, se evitarán o anularán los peligros que amenazan con el buen desenvolvimiento de la organización"*

El aporte o relación de este antecedente es desarrollar medidas de seguridad física como un valor agregado para evitar la destrucción total o parcial de una instalación por parte de saboteadores, ladrones, espías o cualquier otra persona dirigida por elementos subversivos que pretendan con sus acciones crear desconcierto, inseguridad y consternación dentro de la ciudadanía. Es por esta razón que, como segunda hipótesis resalta que *"A mayor ausencia de lineamientos, directrices o procedimientos básicos fundamentales de seguridad sobre la infraestructura, personas y efectos, muy probablemente serán mayores las situaciones que puedan atentar contra la seguridad física de la empresa y sus efectos como así también de la seguridad integral de las personas que trabajan allí diariamente".*

La comprensión de la seguridad física, un tema que abarca multiplicidad de aspectos a considerar, según su aplicación, debe ser conceptualizado siguiendo los lineamientos más actuales para el análisis de la problemática planteada. En función de ello se considerarán los lineamientos de la American Society for Industrial Security (ASIS , 2009), que plantea la promoción de acciones inmediatas, una vez se haya detectado el acontecimiento no deseado, de medidas que busquen retardar, dificultar o promover la reacción de aquellas acciones que fueron planificadas en contra de la instalación vulnerada en el menor tiempo posible con el fin de neutralizar dichos eventos.

Este tipo de actuaciones es conocido como "Seguridad en Profundidad", la que se constituye en un esquema de defensa en profundidad, es decir que, en base al entorno vulnerado, bien sea desde el perímetro exterior de la instalación hasta el recinto final, deben ser protegidos considerando dos niveles de protección, Entorno Global de Seguridad y el Entorno Local de Seguridad (Delegada, 2009).

Por su parte, Galviz (2019) indica que el objetivo principal de la seguridad física es identificar y evaluar los peligros y riesgos a los que están expuestas las instalaciones, bienes, personas, procesos y servicios de una organización, es por esto que se busca prevenir o minimizar el riesgo de aprovechar las vulnerabilidades en las instalaciones o componentes de la empresa. Estos se diseñan para reducir la posibilidad de que se materialicen los riesgos potenciales.

2.2.2. Riesgos

Los riesgos son aquellas situaciones o acciones que pueden amenazar la seguridad o la integridad física de una instalación, incluyendo las personas y los bienes materiales ubicados en ella (Pérez, 2017). Los riesgos, por tanto, son las condiciones que pueden poner bajo peligro la seguridad o integridad física de alguna instalación y que pueden ser materializados produciendo los daños en las distintas áreas de la institución para lo cual fueron planificados (Greenberg & Lowrie, 2010).

Los riesgos a los que se enfrentan las organizaciones en la actualidad son múltiples. Estos riesgos pueden ser financieros, de seguridad, de reputación, de relaciones públicas, de cumplimiento, de responsabilidad social, entre otros. Las organizaciones deben estar preparadas para identificar y gestionar estos riesgos de manera adecuada para minimizar los posibles impactos negativos.

Por ende, la mejor defensa resulta ser la prevención, para lo cual deben conocerse aquellos riesgos que pudieran representar eventos potencialmente no deseados, para que de esta manera puedan aplicarse aquellas medidas diseñadas y adoptadas para la preservación de una instalación, incluyendo todos aquellos bienes materiales, documentos y personas que en ella ejercen labores.

2.2.3. Barreras

Una vez que se ha determinado cuales son los riesgos potenciales a considerar para conformar un plan de prevención, se emplean diversas herramientas para garantizar que las medidas de seguridad minimicen o eliminen de ser posible aquellos daños ocasionados por los riesgos mencionados. Para ello se hace uso de barreras como elementos, bien sean naturales o artificiales, empleados como medida de protección física del resguardo de las instalaciones o de las áreas que se consideren vulnerables.

Su función principal es la de obstaculizar impidiendo o retardando la ocurrencia de eventos indeseados mediante la retención de aquellos sujetos encargados de perpetrarlas, pudiendo considerar que las medidas preventivas sean exitosas y hayan logrado neutralizar la amenaza (Pedraza, 2006).

2.2.4. Perímetros de seguridad

Las instalaciones se pueden proteger mediante rejas, cercas, compuertas y torniquetes para crear una seguridad adicional antes de que los visitantes tengan acceso al edificio. Estos límites definen claramente las áreas públicas y las áreas de seguridad. Los activos protegidos determinan los requisitos de seguridad para las rejas. Hay varios tipos de

rejas, como alambre eléctrico, alambre de púas, calor, detección láser, concreto y rayas pintadas en el suelo (Vera, 2018)

2.2.5. Grados de restricción

El éxito de las herramientas que buscan minimizar la ocurrencia de eventos no deseados también dependerá del grado de restricción que éstas tengan, es decir, se debe delimitar aquellas áreas de las instalaciones que son más susceptibles de ataques para así otorgar un grado de restricción a las mismas mediante el uso de las herramientas anteriormente expuestas, u otras según el tipo de medidas a tomar.

Esto incluye el monitoreo de los procesos, la implementación de mecanismos de seguridad y la realización de auditorías para evaluar el nivel de riesgo. También puede ser útil el uso de herramientas de control de calidad para ayudar a identificar y controlar los errores potenciales en el proceso (Pedraza, 2006).

2.2.6. Áreas restringidas

En estas áreas, según lo expuesto, el acceso se encuentra condicionado en distintos grados, así como el movimiento que puede realizarse dentro de las mismas. Los criterios para considerar qué áreas serán restringidos, está dado por el propósito del resguardo que dentro de ellas se pretende dar, como los bienes y materiales exclusivos o clasificados, de vital importancia para las instituciones determinará su restricción dentro de una infraestructura

Estas áreas pueden incluir oficinas de alto nivel, salas de servidores, salas de informática, almacenes, archivos, salas de reuniones, etc. El control de acceso a estas áreas se puede llevar a cabo mediante la implementación de medidas de seguridad como tarjetas de identificación, identificación biométrica, códigos de acceso, etc. Además, es importante vigilar estas áreas para garantizar que las normas de seguridad se cumplan (Pedraza, 2006).

2.2.7. Áreas de exclusión

Son aquellas áreas en las que se encuentran intereses de seguridad de vital importancia, de modo que el simple acceso a ellas por parte de una persona no autorizada implicaría el acceso a los mismos intereses de seguridad o a los materiales y bienes que estén allí. En estas áreas se suelen manejar documentos y datos que son esenciales para la seguridad y defensa de un país o para el bienestar de una organización

En otras palabras, las áreas de exclusión en la seguridad de una empresa se refieren a aquellas áreas del negocio que estén sujetas a mayores exigencias en cuanto a seguridad. Estas áreas suelen exigir una mayor vigilancia, controles de acceso más estrictos, y una mayor cantidad de medidas de seguridad. Entre las áreas de exclusión más comunes suelen encontrarse los datos sensibles, la información de la empresa, los equipos de alta tecnología,

la información de los clientes, y los servidores de la empresa. Estas áreas están sujetas a mayores controles de seguridad para evitar que sean manipuladas o accedidas sin autorización (Pérez, 2017).

2.2.8. Áreas limitadas

Son aquellas donde hay un interés en proteger lo que se encuentra allí. Sin embargo, se puede evitar que personas accedan a los materiales protegidos mediante la contratación de guardias de seguridad y la implementación de otras medidas de control. También se refieren a aquellas áreas del negocio que se encuentran bajo un nivel de seguridad más bajo, como la oficina principal, los almacenes, los activos, los sistemas informáticos y el equipo de comunicación. Estas áreas requieren una vigilancia menor, controles de acceso más relajados y una menor cantidad de medidas de seguridad. Estas áreas se consideran menos críticas y están más expuestas al riesgo de violación de la seguridad. (Pérez, 2017).

2.2.9. Áreas controladas

Son de acceso restringido y se encuentran generalmente cerca de un área limitada, donde las medidas de control son menos estrictas. Esta sección es especialmente destinada al personal autorizado, cuya entrada y salida no se controla, ya que no da acceso a los intereses de protección ni a los materiales, documentos e información existentes (Pérez, 2017).

2.2.10. Garitas de seguridad

Las garitas de seguridad no deben tener módulos integrados para pernoctar, ya que solo deben contemplar el área de servicio, vigilancia, esclusa y registro. Estos espacios se deberían integrar al entorno, con sus correspondientes medidas de seguridad, para evitar que se produzcan situaciones de riesgo, como el acceso a espacios privados o la vigilancia relajada de la zona. Es importante que estas garitas sean adecuadamente equipadas para prevenir el acceso de personas no autorizadas. Además, deberían contar con iluminación adecuada para facilitar la vigilancia nocturna, así como con equipos audiovisuales para monitorizar en todo momento la seguridad de la zona (Lezana Veliz, 2011).

2.2.11. Puertas para la seguridad integral

Las puertas aumentan la seguridad de los sistemas contra el acceso no autorizado, tanto físico como remoto. Algunas técnicas sencillas que pueden ser empleadas para aumentar la seguridad incluyen el uso de cerraduras de alta seguridad, sistemas de detección de movimiento, alarmas, cámaras de vigilancia, contraseñas seguras y otros sistemas de

seguridad informática. Estas medidas pueden ayudar a evitar que los delincuentes accedan a los sistemas de información o roben o destruyan equipos o información (Lezana Veliz, 2011).

2.2.12. Factor humano en la seguridad

El principal actor en materia de seguridad es el individuo que presta los servicios de acuerdo a un contrato previamente establecido y con funciones específicas inherentes al cargo asumido. Estas funciones incluyen la vigilancia, la prevención y la detección de amenazas, el control de acceso, la gestión de incidentes, la evaluación de riesgos, entre otros.

Las primeras empresas de seguridad se centraban en ofrecer servicios para la protección de instalaciones, residencias y empresas. Estos servicios incluían vigilancia de seguridad, monitoreo de alarmas, patrullaje de guardias, verificaciones de identidad, instalación de equipos de seguridad y muchos otros. Sin embargo, con el paso del tiempo, la seguridad se ha vuelto mucho más compleja y se han desarrollado soluciones de seguridad más innovadoras y avanzadas. Estas nuevas soluciones incluyen tecnologías como el análisis de comportamiento, el reconocimiento facial, la inteligencia artificial, el análisis de amenazas cibernéticas y el monitoreo remoto. Estas soluciones permiten a las empresas de seguridad proteger mejor a sus clientes y brindarles una mayor tranquilidad.

El individuo responsable de la seguridad debe ser consciente de la importancia de su trabajo y estar preparado para responder a cualquier amenaza o incidente que pueda ocurrir. Además, debe tener conocimiento de los procedimientos de seguridad establecidos por la organización y cumplir con los mismos.

Para vincularse a este sector y proteger los bienes de los demás, es importante que la persona tenga una preparación física y psicológica adecuada para enfrentar cualquier riesgo que se presente. Esto incluye mantener un alto nivel de atención, alerta, observación e identificación de riesgos. Estas habilidades son esenciales para prevenir y mitigar riesgos y para mantener un ambiente seguro (Rosas, 2019).

2.2.13. Cámaras de seguridad

Las cámaras de seguridad se han convertido en una herramienta clave para la prevención y reducción de la inseguridad, gracias a su gran ayuda en los temas de seguridad. Estas cámaras han facilitado enormemente la tarea de monitoreo, permitiendo a las personas observar desde un lugar de comodidad lo que estas les muestran. Estas cámaras ofrecen una variedad de beneficios, como la detección de actividades sospechosas, la identificación de personas o vehículos sospechosos, la vigilancia de zonas para evitar el vandalismo y la recopilación de pruebas para ayudar en la investigación de delitos. Además, estas cámaras también pueden ayudar a reducir el costo de la seguridad al proporcionar una vigilancia continua sin la necesidad de contratar guardias de seguridad (Rosas, 2019).

CAPÍTULO III “METODOLOGÍA”

3.1. Tipo de investigación

La presente investigación fue de tipo **descriptivo** porque buscó caracterizar y detallar de manera específica la situación actual en materia de seguridad y protección de instalaciones físicas de instituciones públicas o privadas de la ciudad de Jesús María (Córdoba), así como los procedimientos básicos para la elaboración de estudios de seguridad y protección de instalaciones físicas de instituciones públicas o privadas.

3.2. Diseño y alcance de investigación

Su alcance fue **descriptivo diagnóstico,** con un componente u objetivo propositivo, debido a que su objetivo principal radica en la definición de aquellos procedimientos que pueden considerarse fundamentales para la elaboración de estudios de seguridad y protección de instalaciones físicas mediante análisis de evidencias recogidas de la realidad, propia del **diseño de investigación de campo**, tomando en cuenta que la sistematización de las actividades a llevar a cabo estuvieron orientadas a la solución del fenómeno que acontece. En este sentido Arias (2012, pág. 31), afirma que la investigación de campo “es aquella que consiste en la recolección directamente de los sujetos investigados, o de la realidad donde ocurren los hechos”. El diseño fue **no experimental** siguiendo a Hernández et al. (2014, pág. 210) que lo señalan como “La investigación que se realiza sin manipular deliberadamente variables”, en esta investigación el propósito del investigador fue observar el fenómeno acontecido dentro de su contexto natural para su posterior análisis.

3.3. Población y muestra

La población estuvo conformada por instituciones públicas o privadas de la ciudad de Jesús María (Córdoba). En este sentido, se realizó un **muestreo** de tipo **probabilístico** a fin de conformar la muestra para la recolección de datos, misma que se llevó a cabo a través de la técnica conocida como **encuesta online**, por tratarse de un procedimiento diseñado bajo condiciones de bioseguridad. Así, la muestra quedó constituida por 26 empresas de los rubros comercial, educación, servicios públicos, vigilancia y seguridad, construcción y comunicación e informática.

3.4. Operacionalización de variables

En la tabla 1 se muestra la operacionalización de las variables de la presente investigación, para lo cual se siguió el modelo de Betancur López, (2000) aunque los datos o variables aportados son de elaboración propia, en relación al tema tratado. Así, para cada variable, se estableció el tipo, el nivel de medición, las categorías o dimensiones, indicadores

y la unidad de medida. Esto con la finalidad de tener mayor precisión en la medición y exactitud de los resultados.

Tabla 1. Operacionalización de variables

ORD	VARIABLE	TIPO DE VARIABLE	NIVEL DE MEDICIÓN	CATEGORÍA O DIMENSIÓN	INDICADOR	UNIDAD DE MEDIDA
1	Tipo de empresa u organización	Cualitativa	Nominal	• Pública • Privada • Mixta	Porcentaje ocupacional	Porcentaje %
2	Zona o área de ubicación del Edificio de la empresa	Cualitativa	Nominal	• Urbana • Rural	Ubicación o zona de la empresa	Porcentaje %
3	Rubro de trabajo	Cualitativa	Nominal	• Educación • Comercial • Comunicaciones e informática • Vigilancia y seguridad • Construcciones • Servicios públicos • Otro	Cantidad por rubro	Porcentaje %
4	Existencia de Estudio de Seguridad	Cualitativa	Nominal	• Si • No • No sabe	Porcentaje sobre existencia de Estudios de Seguridad	Porcentaje %
5	Importancia de realizar un Estudio de seguridad	Cualitativa	Ordinal	• No es importante • Poco importante • Neutral • Importante • Muy Importante	Porcentaje sobre grado de importancia	Porcentaje %
6	Existencia de una política, programa o directriz de seguridad de su empresa	Cualitativa	Nominal	• Si • No • No sabe	Porcentaje sobre existencia de Estudios de Seguridad	Porcentaje %
7	Existencia de área, departamento o persona a cargo de la seguridad de la empresa	Cualitativa	Nominal	• Si • No • No sabe	Porcentaje sobre existencia de área, departamento o persona a cargo de la seguridad empresarial	Porcentaje %
8	Existencia de guardia de seguridad externa	Cualitativa	Nominal	• Si • No	Cantidad de guardias de seguridad perimetral	Porcentaje %
9	Existencia de cámaras de vigilancia internas y externas	Cualitativa	Nominal	• Si • No	Cantidad de cámaras de seguridad o vigilancia	Porcentaje %
10	Existencia de roles en caso de incidencias, amenazas, riesgo o ataque hacia la empresa	Cualitativa	Nominal	• Si • No • No sabe	Porcentaje sobre roles específicos de actuación ante eventos particulares	Porcentaje %

Tabla 2. Operacionalización de variables (continuación)

ORD	VARIABLE	TIPO DE VARIABLE	NIVEL DE MEDICIÓN	CATEGORÍA O DIMENSIÓN	INDICADOR	UNIDAD DE MEDIDA
11	Medidas de seguridad física de la empresa	Cualitativa	Nominal	• Medianera o muralla • Rejas	Cantidad de medidas de seguridad física de la empresa	Porcentaje %

				• Puerta o cortina metálica desplegable • Alarmas de seguridad • Puertas blindadas • Bóveda de seguridad • Vidrios blindados • Sensores de movimiento • Llave de acceso inteligente • Biométrico • Escáner de iris o retina • Detector de incendio y humo • Otro		
12	Registro de entrada y salida de personas y vehículos en la empresa	Cualitativa	Nominal	• Si • No • No sabe	Porcentaje de existencia de registros de entrada y salida de personas y vehículos	Porcentaje %
13	Libre acceso a la información de la empresa	Cualitativa	Nominal	• Si • No • No sabe	Cantidad de personas que acceden a cualquier información de la empresa	Porcentaje %
14	Existencia de clasificación de seguridad de la información	Cualitativa	Nominal	• Si • No • No estoy seguro/a	Cantidad de documentación con clasificación de seguridad	Porcentaje %
15	Clasificación de seguridad de la información más utilizada	Cualitativa	Nominal	• Pública • Confidencial • Secreta • No estoy seguro/a	Porcentaje sobre la clasificación de seguridad de información más utilizada	Porcentaje %
16	Grado de aceptación o satisfacción de la seguridad física, de personas y efectos de la empresa	Cualitativa	Ordinal	• Totalmente insatisfactoria • Insatisfactoria • Neutro • Satisfactoria • Totalmente satisfactoria	Porcentaje sobre grado de aceptación o satisfacción sobre la seguridad física	Porcentaje %
17	Existencia de carteles de señalización sobre áreas sobre áreas de acceso restringido en la empresa	Cualitativa	Nominal	• Si • No • No estoy seguro/a	Porcentaje de carteles de señalización sobre accesos restringidos	Porcentaje %

Tabla 3. Operacionalización de variables (Continuación)

ORD	VARIABLE	TIPO DE VARIABLE	NIVEL DE MEDICIÓN	CATEGORÍA O DIMENSIÓN	INDICADOR	UNIDAD DE MEDIDA
18	Grados o áreas de acceso de Seguridad en la organización	Cualitativa	Nominal	• Área de acceso publico • Área restringida • Área excluida • Área controlada • Área prohibida	Cantidad de sectores asignados con grados de seguridad en la empresa	Porcentaje %
19	Tipo de amenaza o riesgo que se detecta con mayor frecuencia en su organización	Cualitativa	Nominal	• Robo • Hurto • Sabotaje • Fraude • Delitos informáticos • Inundaciones	Cantidad de amenazas o riesgos sufridos con mayor frecuencia en la empresa	Porcentaje %

				• Incendios • De instalaciones eléctricas • Ingreso y egreso de personas extrañas a la empresa sin previo control • Otro		
20	Área con mayor cantidad de detección de problemas o incidente	Cualitativa	Nominal	• Dirección • Recursos Humanos • Finanzas y contabilidad • Producción • Auditoria y Seguridad • Seguridad e Higiene • Marketing, tecnología y ventas • Logística • Laboratorio • Comunicaciones e informática • Investigación y desarrollo • Arsenales, sala de armas o elementos radiactivos o explosivos • Aulas • Salón de usos múltiples o conferencias • Mantenimiento • Depósitos • Otro	Cantidad de problemas o incidentes detectados	Porcentaje %
21	Periodo de tiempo en que se producen mayor cantidad de incidentes	Cualitativa	Nominal	• En el primer trimestre • En el segundo trimestre • En el tercer trimestre • En el cuarto trimestre	Porcentajes de incidencias en periodos de tiempo	Porcentaje %
22	Horarios en que se detectan mayor cantidad de incidentes o amenazas	Cualitativa	Nominal	• Ente las 00 y 08 horas de la mañana • Entre las 08 y 16 horas de la tarde • Entre las 16 y 24 horas de la noche • No sabe	Porcentajes de incidencias o amenazas en un rango horario especifico	Porcentaje %

Fuente: Elaboración propia.

3.5. Técnicas e instrumentos de recolección de datos

La técnica empleada en la presente investigación fue la encuesta, correspondiendo el instrumento a un cuestionario online conformado por 22 preguntas, dirigido a los directivos y colaboradores mayores de edad integrantes de las empresas, donde se indagó aspectos como: conocimiento sobre la importancia de los estudios de seguridad, criterios básicos a considerar ante una posible eventualidad, tipos de contingencia o incidente que se produce con mayor periodicidad, tipos de medidas de seguridad que se emplean ante dichos eventos, etc.

3.6. Presentación y análisis de los resultados

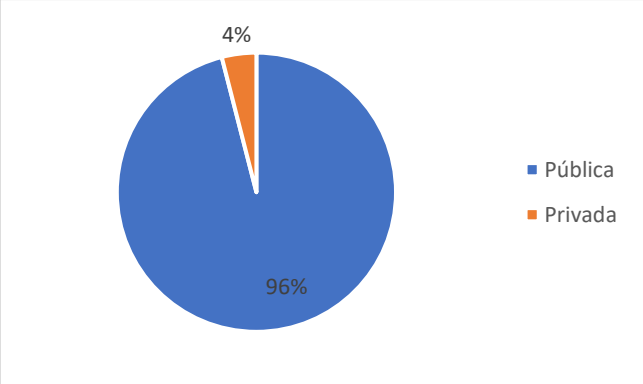
El análisis de la información recopilada tuvo como finalidad dar respuesta a los objetivos específicos planteados al comienzo de esta investigación. En este sentido permitieron conocer en qué situación se encuentran las instalaciones públicas o privadas que hacen vida en la ciudad de Jesús María (Córdoba), a fin de exponer el panorama de vulnerabilidad a la cual se encuentran sometidas estas Instituciones, así como considerar más claramente aquellos riesgos que pudieran representar la ocurrencia de un potencial evento no deseado. A continuación se muestran los resultados, en tablas para visualizar las frecuencias con sus respectivas gráficas para mostrar los porcentajes.

¿En qué tipo de empresa u organización trabaja?

Tabla 4. Distribución tipo de empresa

		Frecuencia	Frecuencia acumulada
Válido	Pública	25	25
	Privada	1	26
	Total	26	

Gráfico 1. Porcentajes tipo de empresa



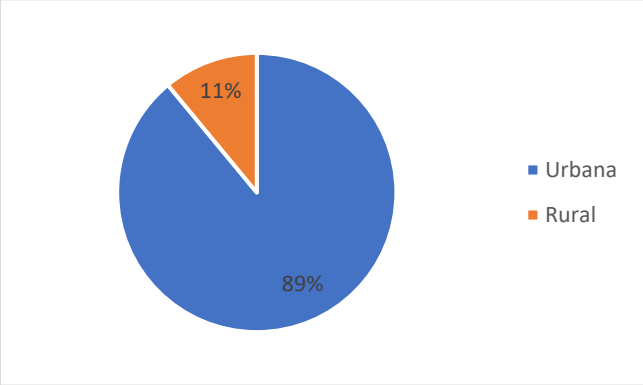
En la tabla 2 se observa que 25 participantes trabajan en la empresa pública, mientras que 1 trabaja en una empresa privada. Para una mejor comprensión de la distribución de los tipos de empresa, en el gráfico 1, se muestran los porcentajes correspondiendo el 96% a la empresa pública y un 4% a la empresa privada.

Tipo de zona o área de ubicación del Edificio de la organización donde trabaja

Tabla 5. Distribución área de ubicación de la empresa

		Frecuencia	Frecuencia acumulada
Válido	Urbana	23	23
	Rural	3	26
	Total	26	

Gráfico 2. Porcentajes área de ubicación de la empresa



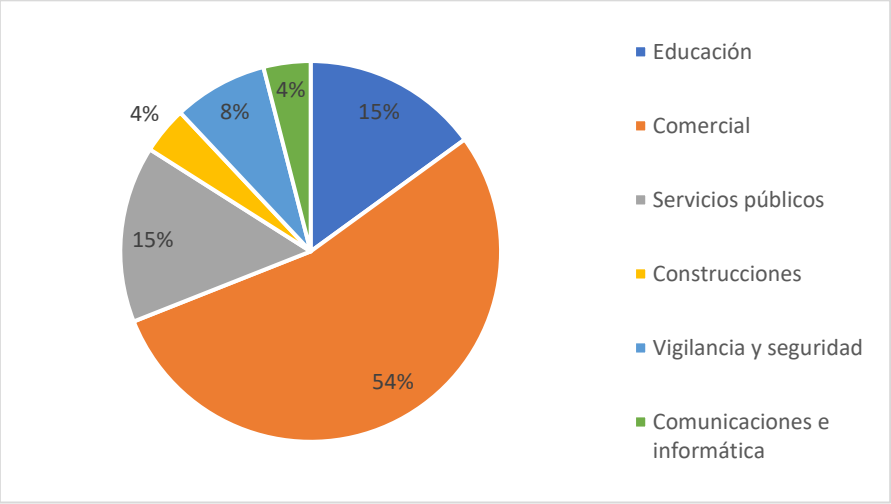
Los resultados que se aprecian en la tabla 3 señalan que entre los participantes que conforman la muestra, 23 indican que la empresa se ubica en una zona urbana y 3 afirman que la empresa se ubica en una zona rural. En el gráfico 2 se presentan los resultados en términos de porcentajes, correspondiendo el 89% a empresas en zona urbana y un 11% a las ubicadas en zona rural, es decir, la mayoría de las empresas se ubican en zonas urbanas.

Rubro de trabajo

Tabla 6. Distribución rubro de la empresa

		Frecuencia	Frecuencia acumulada
Válido	Educación	4	4
	Comercial	14	18
	Servicios públicos	4	22
	Construcciones	1	23
	Vigilancia y seguridad	2	25
	Comunicaciones e informática	1	26
	Total	26	

Gráfico 3. Porcentajes rubro de la empresa



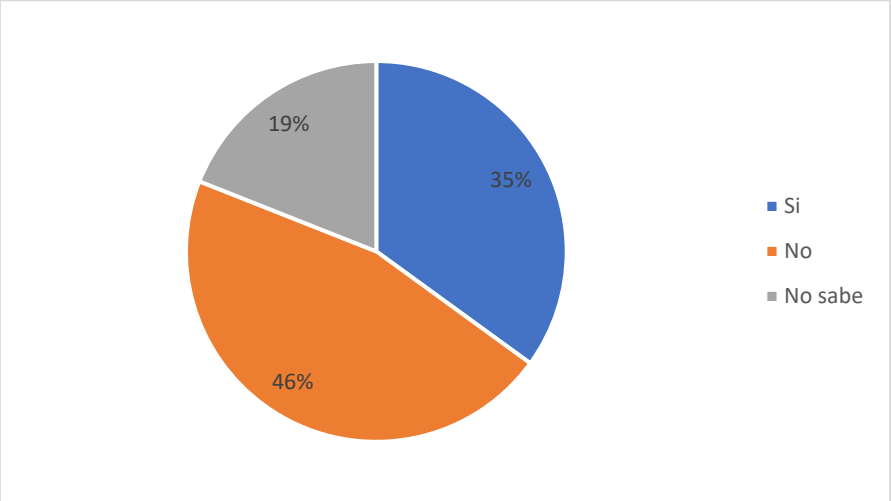
Los resultados en la tabla 4 muestran que 14 participantes del estudio dicen que la empresa donde trabajan es del rubro comercial, 4 indican que es del sector educación, 4 que la empresa es de servicios públicos, 2 mencionan que le empresa es ofrece vigilancia y seguridad, 1 dice que al sector construcción y 1 a comunicación e informática. En el gráfico 3 se presentan los porcentajes de dichos rubros, a saber, 54%, 15%, 15%, 8%, 4% y 4% respectivamente. Se interpreta que, más de la mitad de las empresas, se dedica al rubro comercial.

¿Posee la empresa u organización, un Estudio de Seguridad, vigente o no, para accionar ante distintas eventualidades?

Tabla 7. Distribución estudio de seguridad

		Frecuencia	Frecuencia acumulada
Válido	Si	9	34,6
	No	12	80,8
	No sabe	5	100,0
	Total	26	

Gráfico 4. Porcentajes estudio de seguridad



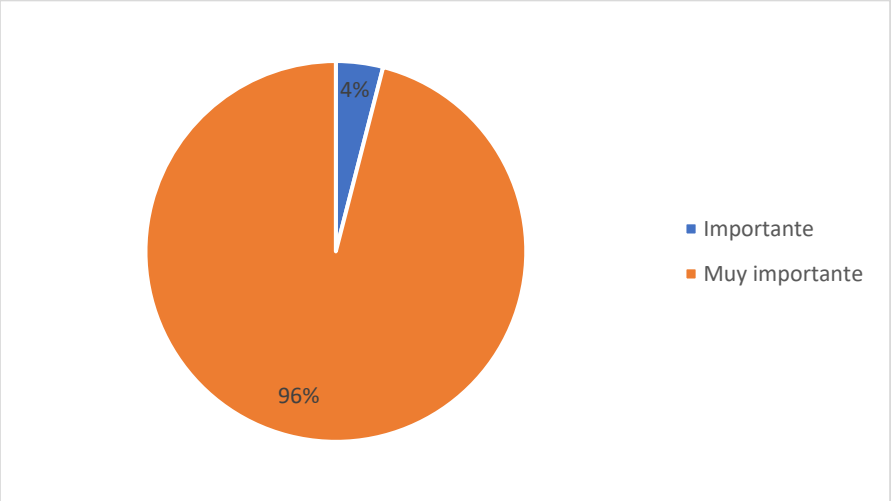
Los resultados en la tabla 5 muestran que 9 participantes del estudio afirman que la empresa donde trabajan posee un estudio de seguridad, vigente o no, para accionar ante distintas eventualidades, 12 indican que esto no es así y 5 dicen que no saben. En el gráfico 4 se presentan los porcentajes de dichas respuestas, a saber, 35%, 46% y 19% respectivamente. Es decir, casi la mitad de la muestra sostiene que no hay un estudio de seguridad.

¿Considera importante realizar un Estudio de Seguridad sobre su organización?

Tabla 8. Distribución importancia estudio de seguridad

		Frecuencia	Frecuencia acumulada
Válido	Importante	1	1
	Muy Importante	25	26
	Total	26	

Gráfico 5. Porcentajes importancia estudio de seguridad



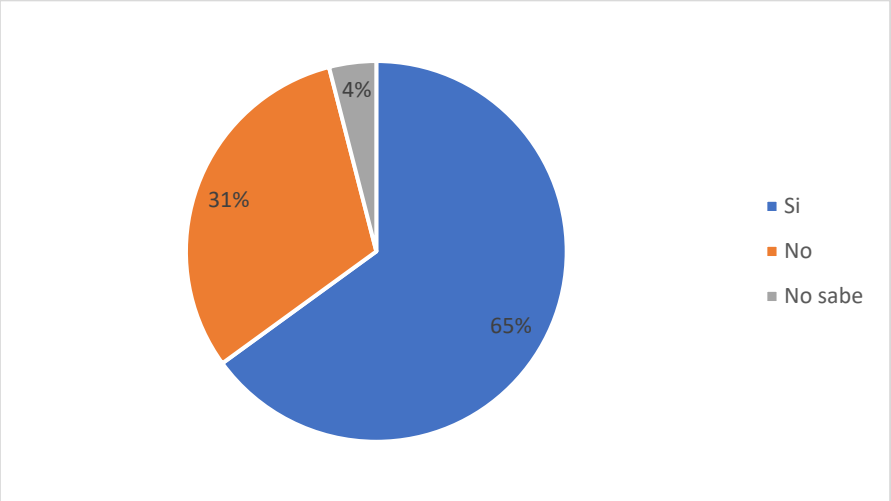
Los resultados en la tabla 6 reflejan que 25 participantes del estudio consideran que es muy importante que la empresa donde trabajan cuente con un estudio de seguridad, vigente o no, para accionar ante distintas eventualidades, mientras que 1 indicó que esto es importante. En el gráfico 5 se presentan los porcentajes de dichas respuestas, a saber, 96%, y 4% respectivamente. Se interpreta, que para toda la muestra este punto es relevante para la empresa.

¿Posee la empresa u organización una política de seguridad, un programa o directriz informativa que permita orientar a sus integrantes, sobre como accionar ante determinado incidente o eventualidad?

Tabla 9. Distribución política de seguridad

		Frecuencia	Frecuencia acumulada
Válido	Si	17	17
	No	8	25
	No sabe	1	26
	Total	26	

Gráfico 6. Porcentajes política de seguridad



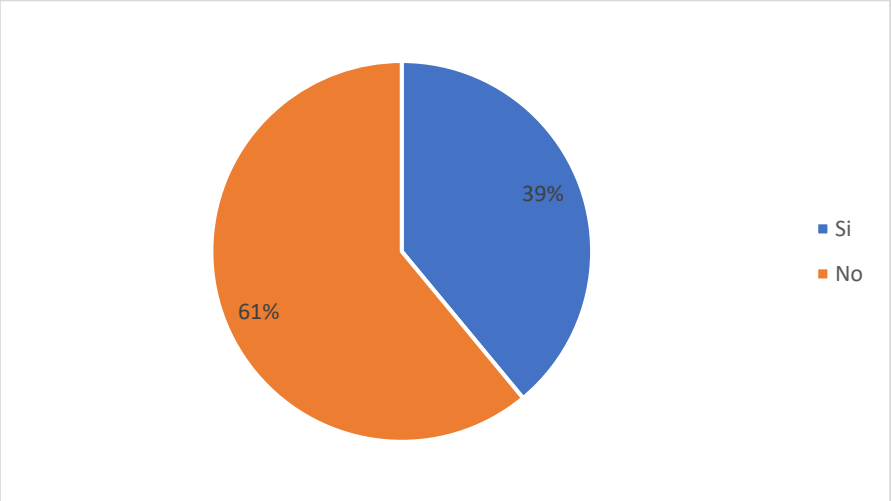
Los resultados en la tabla 7 reflejan que 17 participantes del estudio respondieron que la empresa donde trabajan cuenta con una política de seguridad, un programa o directriz informativa que permita orientar a sus integrantes, sobre como accionar ante determinado incidente o eventualidad, 8 respondieron que esto no es así, mientras que 1 indicó que no sabe. En el gráfico 6 se presentan los porcentajes de dichas respuestas, a saber, 65%, 31% y 4% respectivamente.

¿Se cuenta con vigilancia externa en la empresa (guardia de seguridad)?

Tabla 10. Distribución vigilancia externa

		Frecuencia	Frecuencia acumulada
Válido	Si	10	38,5
	No	16	100,0
	Total	26	

Gráfico 7. Porcentajes vigilancia externa



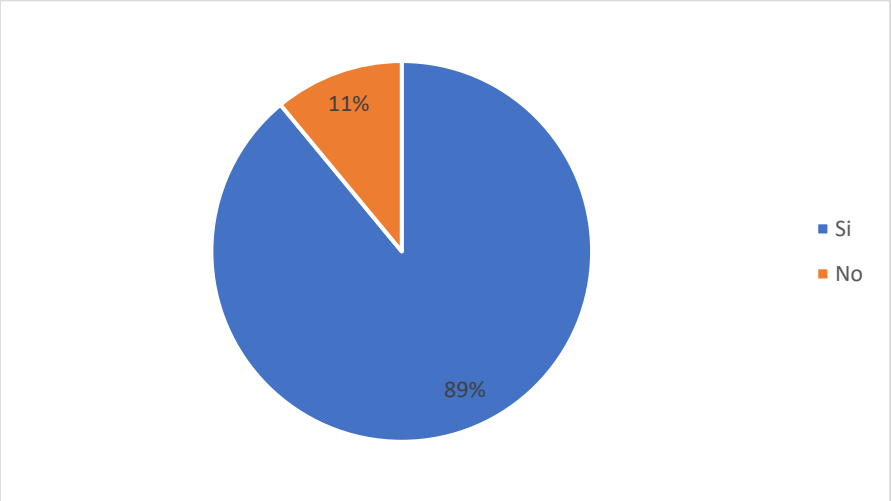
Los resultados en la tabla 8 muestran que 10 participantes del estudio afirman que la empresa donde trabajan cuenta con vigilancia externa, mientras que 10 indicaron que la empresa no cuenta con este tipo de vigilancia. En el gráfico 7 se presentan los porcentajes de dichas respuestas, a saber, 39% y 61% respectivamente. Se interpreta que la mayoría de las empresas carecen de vigilancia externa.

¿Se cuenta con cámaras de vigilancia o seguridad interna o externa en la organización?

Tabla 11. Distribución cámaras de vigilancia o seguridad interna o externa

		Frecuencia	Frecuencia acumulada
Válido	Si	23	23
	No	3	26
	Total	26	

Gráfico 8. Porcentajes cámaras de vigilancia o seguridad interna o externa



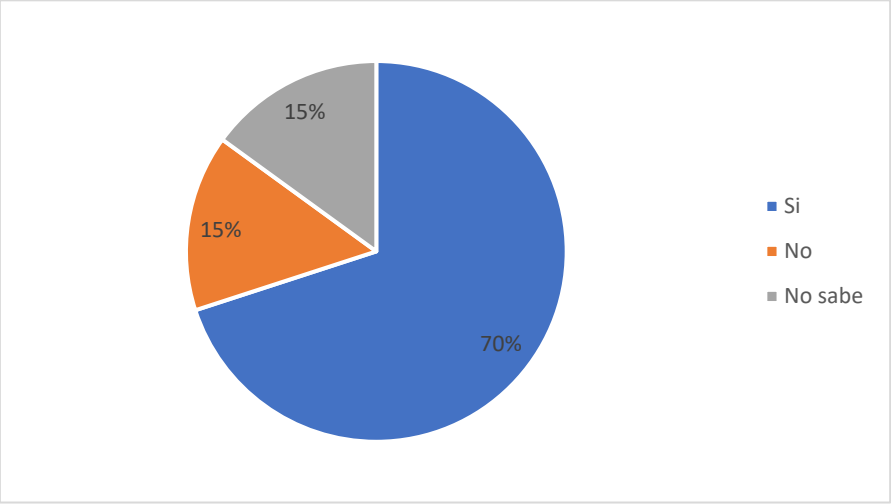
Los resultados en la tabla 9 muestran que 23 participantes del estudio afirman que la empresa donde trabajan cuenta con cámaras de vigilancia o seguridad interna o externa, mientras que 3 indicaron que la empresa no cuenta con estos equipos. En el gráfico 8 se presentan los porcentajes de dichas respuestas, a saber, 89% y 11% respectivamente. Se interpreta que la mayoría de las empresas poseen cámaras de vigilancia interna o externa.

¿Existe un rol determinado de actuación para cada integrante, ante cualquier incidente, amenaza, riesgo o ataque hacia la empresa u organización?

Tabla 12. Distribución rol de cada integrante

		Frecuencia	Frecuencia acumulada
Válido	Si	18	18
	No	4	22
	No sabe	4	26
	Total	26	

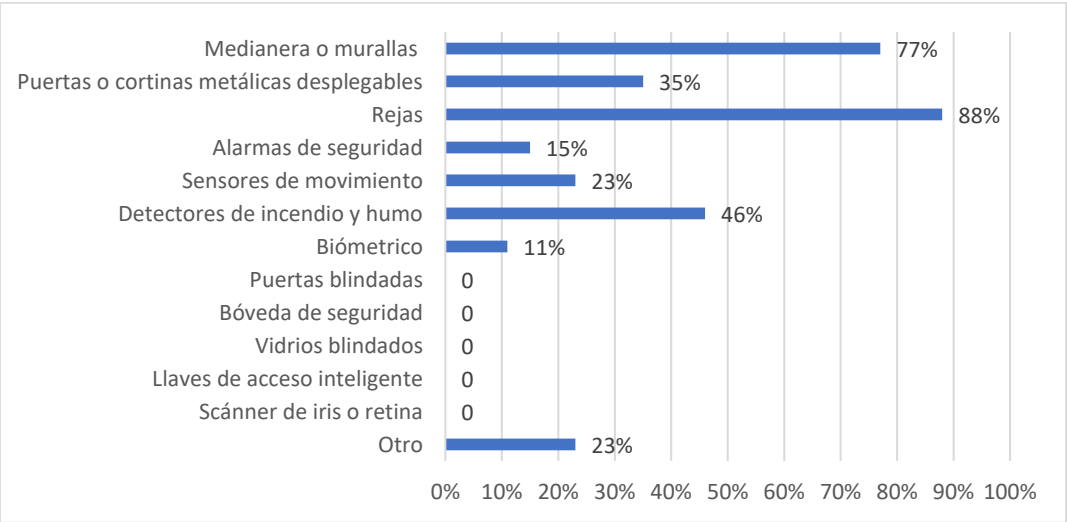
Gráfico 9. Porcentajes rol de cada integrante



Los resultados en la tabla 10 muestran que 18 participantes del estudio afirman que la empresa donde trabajan existe un rol determinado de actuación para cada integrante, ante cualquier incidente, amenaza, riesgo o ataque, 4 indicaron que esto no existe, mientras que otros 4 indicaron que no saben si en la empresa existen estos roles. En el gráfico 8 se presentan los porcentajes de dichas respuestas, a saber, 70%, 15% y 15% respectivamente. Se interpreta que en más de la mitad de las empresas existe dicho rol de actuación.

¿Cuáles son las medidas de seguridad física con la que cuenta la institución? (Aquí puede seleccionar más de una respuesta)

Gráfico 10. Porcentajes Medidas de seguridad



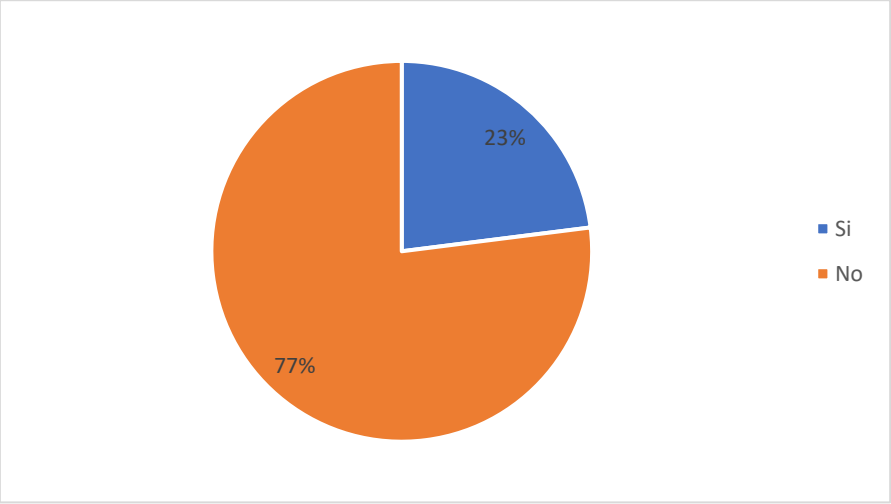
En el gráfico 10 se observa que las medidas de seguridad física más mencionadas con las que cuenta la institución, fueron las rejas con un 88%. El resto de las medidas de seguridad física correspondió a las medianeras o murallas (77%), detectores de incendio y humo (46%), puertas o cortinas metálicas desplegables (35%), sensores de movimiento (23%), otros (23%), alarmas de seguridad (15%) y biométrico (11%).

¿Existe un registro de entrada y salida de personas y vehículos en la empresa?

Tabla 13. Distribución registro de entrada y salida

		Frecuencia	Frecuencia acumulada
Válido	Si	6	6
	No	20	26
	Total	26	

Gráfico 11. Porcentajes registro de entrada y salida



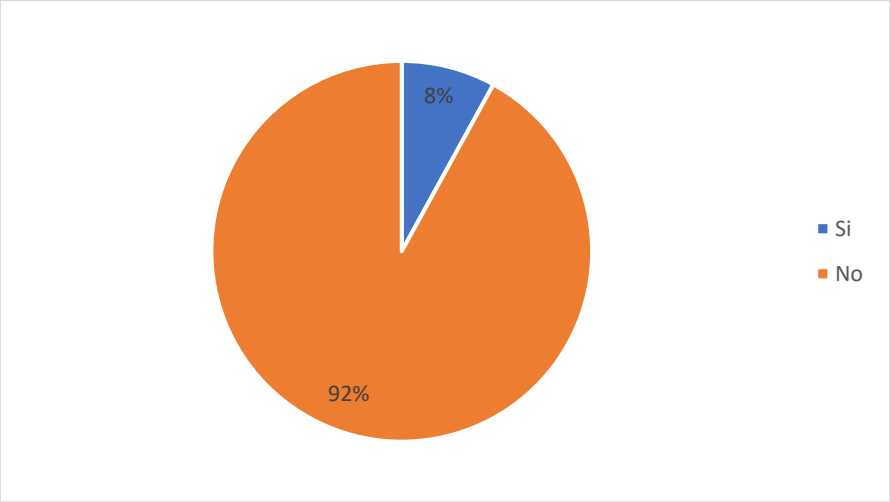
Los resultados en la tabla 11 muestran que 6 participantes del estudio afirman que en la empresa donde trabajan existe un registro de entrada y salida de personas y vehículos, mientras que 20 indicaron que este registro no existe. En el gráfico 11 se presentan los porcentajes de dichas respuestas, a saber, 23% y 77% respectivamente. Se interpreta que en más de la mitad de las empresas no existe este tipo de control.

¿Se permite el acceso de cualquier información contenida en documentos o archivos físicos o digitales a cualquier integrante de la empresa (ej.: base de datos de empleados y directivos, cuentas bancarias, transacciones, stock de mercaderías, ¿etc.)?

Tabla 14. Distribución acceso a información

		Frecuencia	Frecuencia acumulada
Válido	Si	2	2
	No	24	26
	Total	26	

Gráfico 12. Porcentajes acceso a información



Los resultados en la tabla 12 muestran que 2 participantes del estudio afirman que en la empresa donde trabajan se permite el acceso de cualquier información contenida en documentos o archivos físicos o digitales a cualquier integrante de la empresa, mientras que 24 indicaron que no se permite. En el gráfico 12 se presentan los porcentajes de dichas respuestas, a saber, 8% y 92% respectivamente.

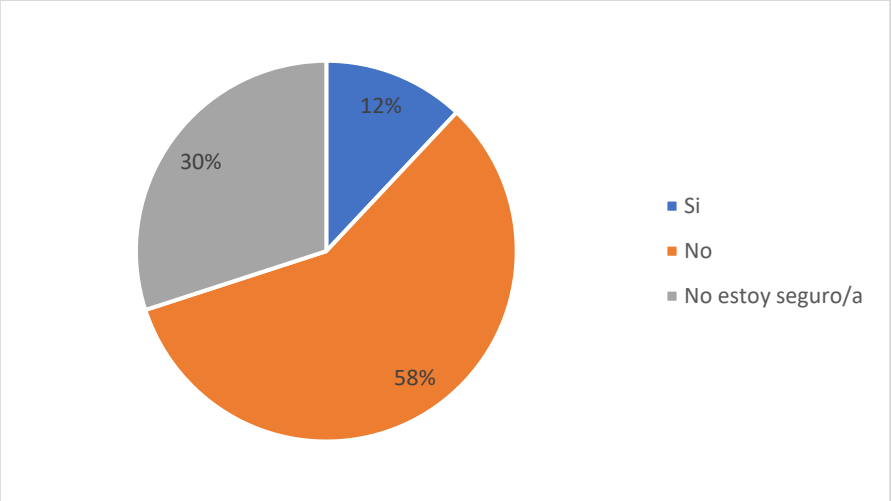
¿La documentación que maneja la organización posee una clasificación de seguridad según su importancia, sensibilidad o vulnerabilidad?

Tabla 15. Distribución clasificación de seguridad

		Frecuencia	Frecuencia acumulada
Válido	Si	3	11,5
	No	15	69,2
	No estoy seguro/a	8	100,0

Total	26	

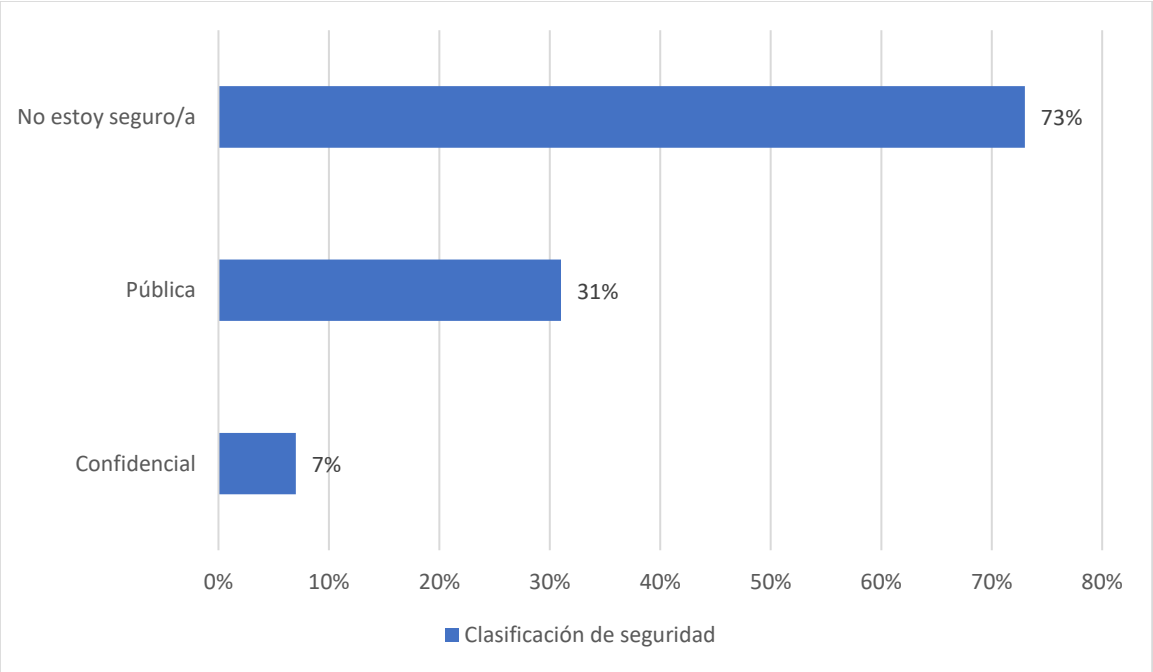
Gráfico 13. Porcentajes clasificación de seguridad



Los resultados en la tabla 13 muestran que 3 participantes del estudio afirman que la documentación que maneja la organización posee una clasificación de seguridad según su importancia, sensibilidad o vulnerabilidad, 15 participantes sostienen esto no es así, mientras que 8 indicaron que no están seguros. En el gráfico 13 se presentan los porcentajes de dichas respuestas, a saber, 12%, 58% y 30% respectivamente.

En relación a la pregunta anterior, en caso de conocer o poseer una clasificación de seguridad de manejo de la información, ¿Cuál es la clasificación de seguridad que más se utiliza? (Aquí puede seleccionar más de una respuesta)

Gráfico 14. Porcentajes clasificación de seguridad más utilizada



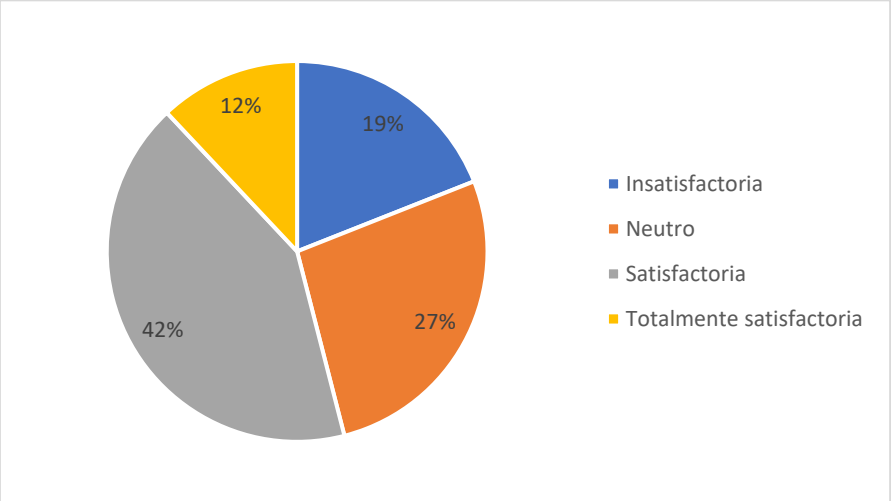
En el gráfico 14 se observa que respecto a la clasificación de seguridad de manejo de la información, más utilizada en la empresa, el 73% de los participantes respondieron que no están seguros. El 31% dice que la clasificación más utilizada es pública y un 7% dice que es confidencial.

¿Cuál es el grado de aceptación o satisfacción que posee en relación a la seguridad del edificio en el que desempeña sus funciones diariamente, la seguridad hacia la integridad física de las personas y de los efectos de la organización?

Tabla 16. Distribución satisfacción de la seguridad

		Frecuencia	Frecuencia acumulada
Válido	Insatisfactoria	5	5
	Neutro	7	12
	Satisfactoria	11	23
	Totalmente satisfactoria	3	26
	Total	26	

Gráfico 15. Porcentajes satisfacción de la seguridad



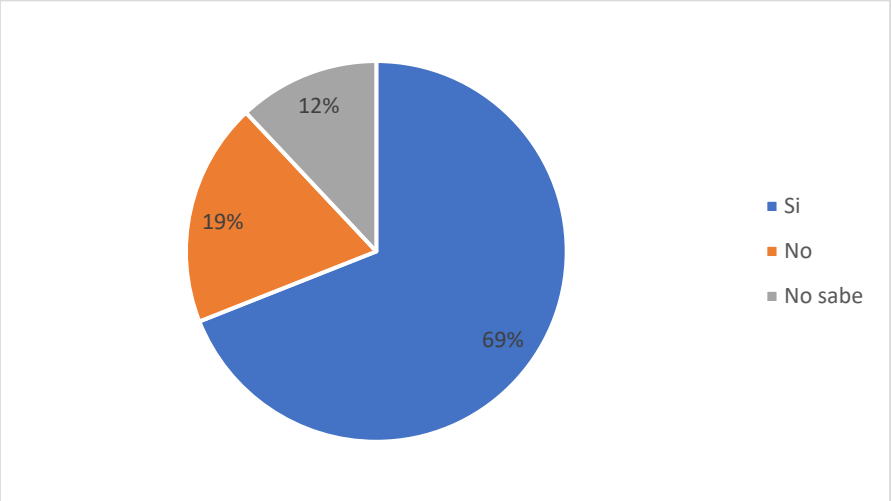
Los resultados en la tabla 14 muestran que 5 participantes del estudio se sienten insatisfechos en relación a la seguridad del edificio en el que desempeña sus funciones diariamente, la seguridad hacia la integridad física de las personas y de los efectos de la organización, 7 participantes sostienen una posición neutral, mientras que 11 indicaron sentirse satisfechos y 3 totalmente satisfechos. En el gráfico 15 se presentan los porcentajes de dichas respuestas, a saber, 19%, 27%, 42% y 12% respectivamente.

¿Existen carteles de señalización que indiquen cierto grado de restricción de acceso a un área o sector determinado en la empresa?

Tabla 17. Distribución carteles de señalización

		Frecuencia	Frecuencia acumulada
Válido	Si	18	69,2
	No	5	88,5
	No sabe	3	100,0
	Total	26	

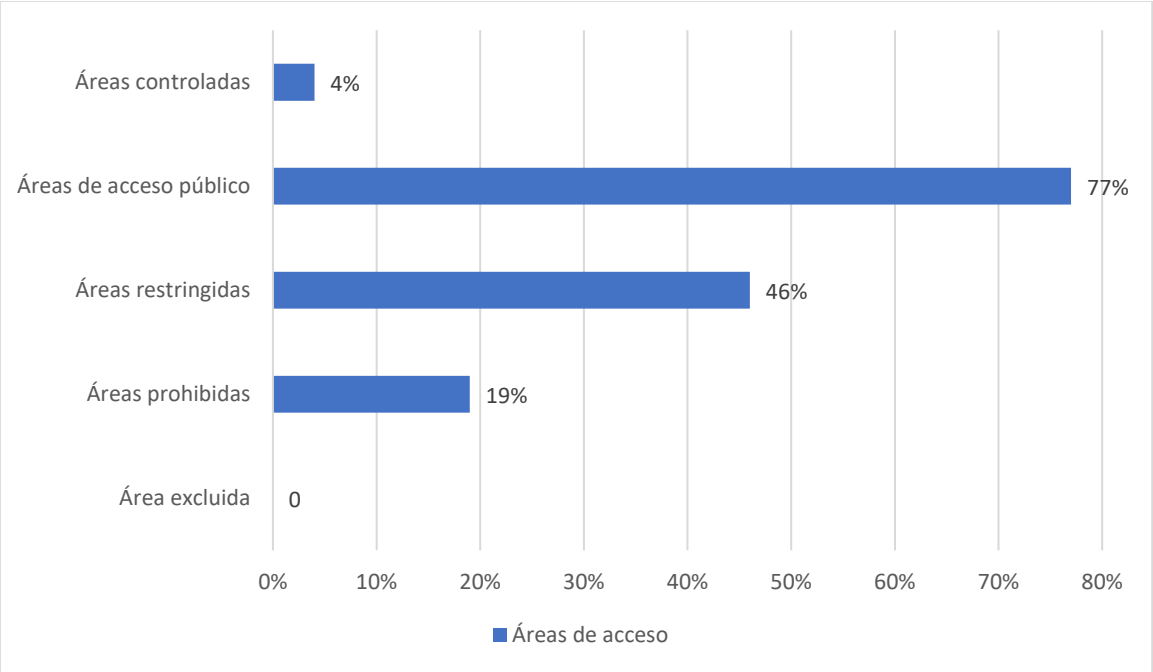
Gráfico 16. Porcentajes carteles de señalización



Los resultados en la tabla 15 muestran que 18 participantes del estudio afirman que existen carteles de señalización que indiquen cierto grado de restricción de acceso a un área o sector determinado en la empresa, 5 participantes sostienen no existen este tipo de carteles, mientras que 3 indicaron que no saben. En el gráfico 16 se presentan los porcentajes de dichas respuestas, a saber, 69%, 19% y 12% respectivamente.

En relación a la pregunta anterior, en caso de conocer o poseer las limitaciones de acceso a distintas áreas de la empresa u organización, ¿Cuáles son los grados o áreas de acceso de seguridad que se maneja en la Institución? (Aquí puede seleccionar más de una respuesta)

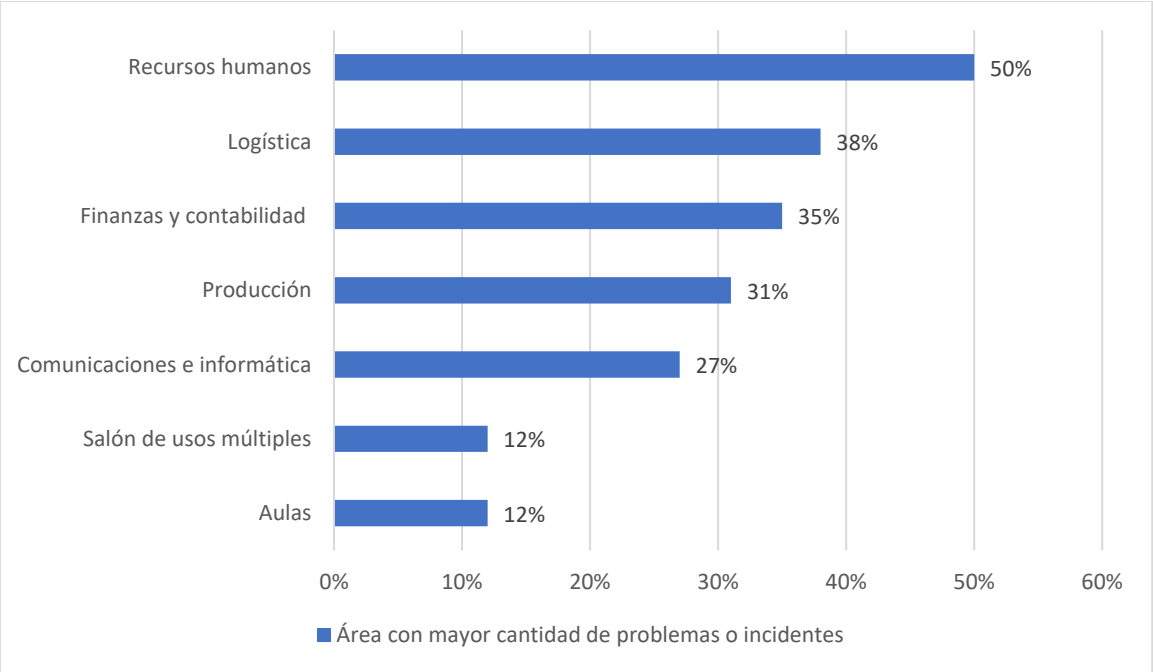
Gráfico 17. Porcentajes limitaciones de acceso



En el gráfico 17 se observa que las limitaciones de acceso a distintas áreas de la empresa u organización, más mencionadas por los participantes fueron las áreas de acceso público (77%), áreas restringidas (46%), áreas prohibidas (19%) y áreas controladas con un 4%.

¿Cuál es el área de su empresa con mayor cantidad de detecciones de problemas o incidentes? (Aquí puede seleccionar más de una respuesta)

Gráfico 18. Porcentajes área con mayores problemas o incidentes



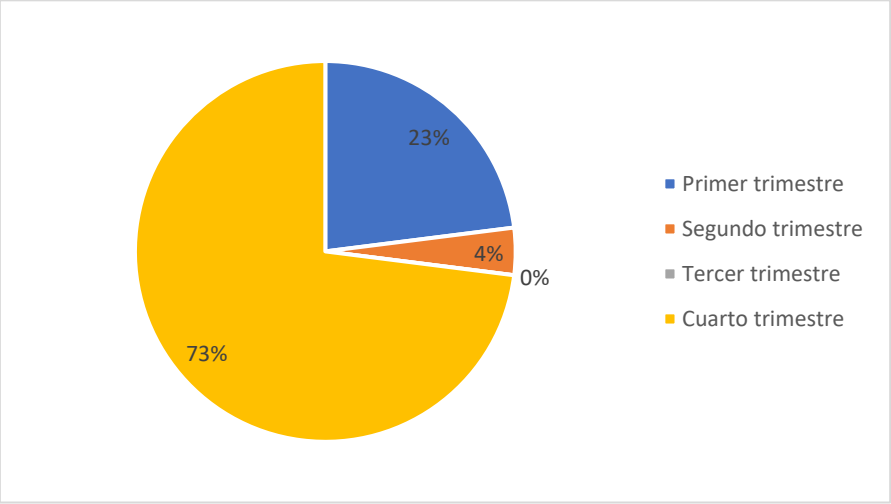
En el gráfico 18 se observa que el área de su empresa con mayor cantidad de detecciones de problemas o incidentes, más mencionadas por los participantes fueron: recursos humanos (50%), logística (38%), finanzas y contabilidad (35%), producción (31%), comunicaciones e informática (27%), salón de usos múltiples (12%) y aulas (12%).

¿En qué periodo de tiempo en que se producen mayor cantidad de incidentes en las Instalaciones?

Tabla 18. Distribución periodo de tiempo

		Frecuencia	Frecuencia acumulada
Válido	En el primer trimestre (enero, febrero, marzo)	6	6
	En el segundo trimestre (abril, mayo, junio)	1	7
	En el cuarto trimestre (octubre, noviembre, diciembre)	19	26
	Total	26	

Gráfico 19. Porcentajes periodo de tiempo



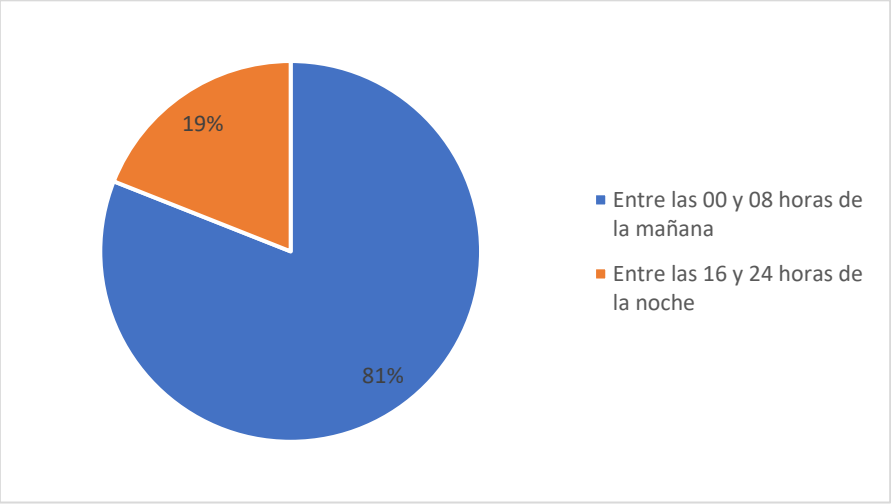
Los resultados en la tabla 16 muestran que 6 participantes del estudio afirman que el periodo de tiempo en que se producen mayor cantidad de incidentes en las Instalaciones es en el primer trimestre, 1 participantes que es en el segundo trimestre, mientras que 19 indicaron que es en el cuarto trimestre. En el gráfico 19 se presentan los porcentajes de dichas respuestas, a saber, 23%, 4% y 73% respectivamente.

¿En qué horario se detectan mayor cantidad incidentes o amenazas?

Tabla 19. Distribución horario detección de accidentes

		Frecuencia	Porcentaje	Porcentaje válido	Frecuencia acumulada
Válido	Entre las 00 y 08 horas de la mañana	21	80,8	84,0	84,0
	Entre las 16 y 24 horas de la noche	5	19.2	16,0	100,0
	Total	26	100,0		

Gráfico 20. Porcentajes horario detección de accidentes



Los resultados en la tabla 17 muestran que 21 participantes del estudio afirman que el horario en que se detectan mayor cantidad incidentes o amenazas es entre las 00 y 08 horas de la mañana, mientras que 5 indicaron que el horario es entre las 16 y 24 horas de la noche. En el gráfico 20 se presentan los porcentajes de dichas respuestas, a saber, 81% y 19% respectivamente.

Luego de evaluar y recolectar la información acerca de la situación actual en materia de seguridad y protección de instalaciones físicas de instituciones públicas o privadas de la ciudad de Jesús María (Córdoba), entre los hallazgos más importantes, se pudo comprobar más del 50% de las empresas encuestadas no cuenta con vigilancia externa, un 77% no existe un registro de entrada y salida de personas y vehículos, las medidas de seguridad física más mencionadas con las que cuenta la institución, fueron las rejas con un 88%. El resto de las medidas de seguridad física correspondió en menor medida a las medianeras o murallas, detectores de incendio y humo, puertas o cortinas metálicas desplegables, sensores de movimiento, otros, alarmas de seguridad y biométrico. También se develó que un 46% de las empresas, es decir, casi la mitad no poseen estudios de seguridad, aunque un 65% cuentan con políticas de seguridad 65%

Por tanto, a partir del análisis realizado a los resultados obtenidos y tomando en cuenta las debilidades en el sistema de seguridad de las instituciones públicas o privadas de la ciudad, se determinó la necesidad de elaborar la estructura para un Manual de procedimientos básicos de estudios de seguridad y protección en instalaciones físicas públicas o privadas.

CAPÍTULO IV “PROPUESTA”

En este capítulo se presenta la propuesta que consiste en la elaboración de una estructura para un manual de procedimientos básicos de estudios de seguridad y protección en instalaciones físicas públicas o privadas de la ciudad de Jesús María (Córdoba), la cual se sustenta con base a la realidad estudiada, además se justifica porque busca el mejoramiento de los protocolos que garanticen la seguridad de las instalaciones físicas y de las personas que hacen uso de las mismas, propiciando un clima de bienestar urbano.

Algunos de los procedimientos básicos para diseñar un esquema de seguridad efectivo sobre instalaciones físicas, se detallan a continuación definiéndose la estructura general del manual:

1. **Caratula**, deberá contener sello de clasificación de seguridad de la información que corresponda, conforme lo describe en el Art. 11 de la Ley 27.126 de la Agencia Federal de Inteligencia, los cuales pueden ser Secreto, Confidencial o Público[2], membrete del organismo si lo tuviera y la leyenda oficial nacional como la del año en curso “Las Malvinas son Argentinas” establecida mediante Dec. 877/2022[3], fecha de informe o estudio, Institución/Empresa/Organismo a ser estudiado, profesional a cargo, título, y año. Dependiendo de que tipo de estudio se desarrolle variará algunos datos agregándoles algunos o modificándoles otros.
2. **Índice General**, aquí se desplegará la estructura del trabajo con sus divisiones y subdivisiones generales, especificando el número de página en el que se encuentran.
3. **Introducción**, aquí se detallará sintéticamente los motivos del estudio, el porqué de su ejecución y los objetivos que se desean alcanzar.
4. **Finalidad**, en esta parte se describe con precisión la razón de ser del estudio de seguridad, su propósito, de qué forma se llevará a cabo, con qué medios, y cómo se pretende alcanzar los objetivos trazados.
5. **Marco legal de intervención**, en este apartado se desplegará la lista de la normativa legal vigente al cual responden y avalan para desarrollar el estudio de seguridad, además de adecuarse a lo establecido en la Constitución Nacional, las leyes y decretos nacionales, también el estudio de seguridad debe respetar acabadamente y adecuarse a lo estipulado a las Leyes Provinciales y a los actos que los Municipios dicten, por

[2] Art. 11, Ley 27.126. (2015). Ley de la Agencia federal de Inteligencia. Honorable Congreso de la Nación Argentina. Extraído de: https://www.argentina.gob.ar/normativa/nacional/ley-27126-243821/texto

[3] Art. 2. Decreto 877. (2022). 1983/2023 – 40 AÑOS DE DEMOCRACIA. Leyenda Oficial. Ciudad de Buenos Aires. Extraído de: https://www.boletinoficial.gob.ar/detalleAviso/primera/278685/20221230

ejemplo La Ley 25.326 de Protección de Datos Personales a nivel Nacional y La ley 9.380 y su modificatoria Ley 10.698 sobre el empleo de cámaras de seguridad, o a nivel Provincial, la Ley 10.326 que determina el Código de Convivencia de la Provincia de Córdoba.

6. **Alcance**, aquí se demarcará con exactitud los límites de investigación en cuanto al organismo a ser estudiado y las bondades que proporcionará el estudio de seguridad. Es importante establecer los límites del estudio de seguridad que se llevará a cabo.
7. **Carácter:** que se describirá el nivel o grado de confidencialidad que se le adjudicará al documento de acuerdo a la información que contiene, el que deberá plasmarse en el informe de seguridad (Secreto, Confidencial o Público).
8. **Capítulo I –** Generalidades
   - **Sección I "Diagnóstico**"

   a) Descripción de la situación actual de la Institución u Organización objeto de estudio (autoridad que ordena, profesional que ejecuta, antecedentes de estudios anteriores, ubicación, topografía, zonas críticas, sistemas de vigilancia, vulnerabilidades observadas y riesgos que pueden generar si no aplica una acción urgente al respecto)

      (1) **Vulnerabilidad y criticidad**, ya que permiten determinar el nivel de riesgo asociado a una amenaza específica y evaluar el impacto potencial de dicha amenaza. La instalación puede estar expuesta a una amenaza y la vulnerabilidad mide el riesgo de que esta amenaza se materialice. La criticidad, por otro lado, se refiere al grado en que una amenaza afecta a una instalación. Esto significa que la criticidad mide el impacto potencial de una amenaza sobre la instalación y los activos que alberga.

      (2) **Riesgos**. Esto implica identificar amenazas como el vandalismo, el robo, los incendios, los ataques de malware y otros peligros. Una vez identificadas las amenazas, se debe evaluar el riesgo asociado con cada amenaza para determinar el nivel de vulnerabilidad y criticidad de la instalación. Esto se puede lograr mediante el uso de herramientas de evaluación de riesgos, como el análisis de amenazas y vulnerabilidades (TVA), el análisis de amenazas y vulnerabilidades críticas (CATV) o el análisis de factores de riesgo (FFR). Estas herramientas ayudan a identificar y evaluar los riesgos de la instalación para que las medidas de seguridad sean lo más adecuadas y eficaces posibles.

      (3) **Análisis FODA** se utilizará para identificar y evaluar los factores que pueden afectar la seguridad de la instalación. Esto incluye identificar amenazas y evaluar la vulnerabilidad y criticidad de la instalación frente a estas amenazas. Para realizar un análisis FODA, primero se debe identificar las fortalezas,

debilidades, amenazas y oportunidades de la instalación. Luego se evalúan estos factores para determinar el nivel de riesgo asociado a cada amenaza y el impacto potencial de dicha amenaza. Esta información puede ser utilizada para tomar medidas para proteger la instalación.

(4) **Elaboración de Árbol de problemas y árbol de objetivos**. Se empleará para identificar los riesgos y evaluar los requerimientos de seguridad. El árbol de problemas servirá para identificar las amenazas y vulnerabilidades existentes en una instalación, mientras que el árbol de objetivos será útil para identificar los requerimientos de seguridad, los cuales deben cumplirse para minimizar el riesgo. La realización de un árbol de problemas y objetivos comenzará con la identificación de los riesgos, los cuales deben ser clasificados de acuerdo a su grado de prioridad. Una vez clasificados, se deben establecer los requerimientos de seguridad para minimizar cada riesgo y evaluar si existen soluciones adecuadas para los problemas. Por último, se debe monitorear el cumplimiento de los requerimientos de seguridad para garantizar la seguridad de la instalación.

(5) Elaboración de **MATRIZ DE ESTRATEGIAS**, aquí se evaluarán cuatro dimensiones: impacto, probabilidad, coste y valor. Cada estrategia de seguridad se evalúa en cada dimensión y se asigna una puntuación. Estas puntuaciones se combinan para crear una matriz de estrategias que mostrará todas las estrategias de seguridad y su prioridad. Esta matriz se puede utilizar para evaluar y comparar diferentes estrategias de seguridad y seleccionar aquellas que ofrezcan el mejor balance entre costo y beneficio.

(6) Elaboración de **PLAN DE ACTIVIDADES**, aquí se identificarán y priorizarán las acciones necesarias para mantener un nivel adecuado de seguridad. El plan de actividades debe incluir todas las acciones que se deben realizar, como la implementación de medidas preventivas, la adquisición de equipos de seguridad, el entrenamiento del personal y la supervisión de los sistemas de seguridad. El plan de actividades también debe incluir la asignación de responsabilidades para asegurar que todas las acciones sean realizadas de manera oportuna y eficaz. La realización de un plan de actividades iniciará con una evaluación de los requerimientos de seguridad. Una vez identificados los requerimientos, se deben establecer las acciones necesarias para cumplir con los mismos. Por último, se debe monitorear el cumplimiento del plan de actividades para garantizar que se mantenga un nivel adecuado de seguridad.

(7) Elaboración de **MATRIZ DE MARCO LOGICO**, aquí se identificarán los riesgos y amenazas a la seguridad, los recursos necesarios para abordar estos

riesgos, y las actividades a realizar para garantizar la seguridad de la instalación. La matriz de marco lógico también puede ser utilizada para evaluar el progreso hacia el logro de los objetivos de seguridad, y para monitorear el uso de los recursos. Para realizar una matriz de marco lógico para un estudio de seguridad física de instalaciones, se puede comenzar por identificar los objetivos, resultados esperados, recursos necesarios y actividades a realizar. Luego, estos elementos se pueden relacionar entre sí para formar la matriz de marco lógico.

- **Sección II - Áreas de seguridad/restricción**

Estas áreas específicas dentro de un establecimiento requieren un nivel de protección adicional para prevenir y controlar el acceso no autorizado a los equipos y bienes del establecimiento. Estas áreas pueden estar ubicadas en el interior, como en el caso de áreas de almacenamiento, laboratorios, oficinas, etc., o en el exterior, como en el caso de estacionamientos, patios, etc. Para realizar un estudio de seguridad, se deben identificar todas las áreas de seguridad/restricción y luego evaluar los riesgos existentes en cada una de ellas. Esto implica realizar una evaluación de los sistemas de seguridad existentes, como cámaras de seguridad, sistemas de alarma, control de acceso, etc., y luego determinar si estos sistemas son suficientes para proteger el área de forma adecuada. Si se determina que los sistemas existentes no son suficientes, se deben tomar medidas adicionales para aumentar la seguridad, como la instalación de nuevos sistemas de seguridad, la realización de auditorías periódicas, etc.

a) **Área de acceso público**, aquí el estudio de seguridad debe abordar el diseño, la infraestructura y las operaciones de esta área. Primero, se deben evaluar los requisitos generales de seguridad para el área, como la seguridad física, la seguridad del personal y la seguridad de la información. Luego, se debe evaluar el diseño de la instalación, incluyendo el diseño de la ubicación, la configuración de los edificios, la seguridad del perímetro y los sistemas de seguridad electrónica. Por último, se debe evaluar la infraestructura y las operaciones del área, incluyendo el control de acceso, los protocolos de seguridad, el mantenimiento de los equipos de seguridad y la capacitación de los empleados.
b) **Área restringida**, aquí también se debe abordar el diseño, la infraestructura y las operaciones del área restringida. Además, los protocolos de seguridad del área restringida deben ser estrictos, ya que pueden contener materiales y equipos sensibles o confidenciales. Se deben incluir medidas como: requisitos de identificación para el acceso a la zona, controles de acceso, sistemas de vigilancia, iluminación adecuada, señalización y etiquetado adecuados, instalaciones adecuadas para el almacenamiento de productos peligrosos, equipos de

protección personal para el personal, controles de seguridad de los equipos, controles de seguridad de los vehículos, protocolos para la limpieza y el mantenimiento, y un plan de contingencia. Además, los responsables de la seguridad deben estar bien entrenados para manejar cualquier situación de emergencia.

c) **Área de exclusión**, aquí se deben incluir medidas tales como la restricción del acceso a la zona a personas autorizadas, controles de acceso para registrar la entrada y salida de personas autorizadas, el uso de equipos de protección personal, señalización y etiquetado adecuados, iluminación adecuada, sistemas de vigilancia y controles de seguridad de los equipos. Además, el área de exclusión debe estar separada del resto de la instalación mediante una barrera física, como una puerta o una cerca, y deben existir protocolos para el control y la limpieza. El personal encargado de la seguridad debe estar bien entrenado para manejar cualquier situación de emergencia.

d) **Área controlada**, debe incluir medidas como la restricción del acceso a la zona a personas autorizadas, controles de acceso para registrar la entrada y salida de personas autorizadas, el uso de equipos de protección personal, señalización y etiquetado adecuados, iluminación adecuada, sistemas de vigilancia, y controles de seguridad de los equipos. Los responsables de la seguridad deben estar bien entrenados para manejar cualquier situación de emergencia, y se deben crear protocolos para el control y la limpieza. Las personas autorizadas deben tener una identificación visible y deben pasar por un sistema de chequeo de seguridad para determinar si se permite el acceso a la zona controlada.

e) **Área prohibida**, aquí se deben incluir las medidas necesarias para proteger a los trabajadores y al entorno. Estas medidas pueden incluir el uso de equipo de protección personal (EPP), el uso de instalaciones de seguridad o el cumplimiento de procedimientos de trabajo seguros. El protocolo debe especificar los requisitos para el uso de EPP, el uso de instalaciones de seguridad, la limitación de acceso al área controlada, el mantenimiento de registros de entradas y salidas del área, el control de la contaminación y el cumplimiento de los requisitos de seguridad establecidos por la legislación aplicable. También se deben incluir procedimientos para la supervisión y evaluación de la seguridad del área controlada.

9. **Capitulo II – Componentes o Sistemas de Seguridad Física**

(1) **Barreras naturales**, aquí se identificarán los elementos naturales que actúan como barreras, como los ríos, las lagunas, los pantanos, los bosques, etc. Además, se debe tener en cuenta la ubicación, la robustez y los requisitos de mantenimiento de cada barrera para garantizar que se cumplan los estándares

de seguridad requeridos. Por último, se deberá realizar una evaluación periódica para asegurarse de que las barreras se mantengan adecuadamente y que la seguridad no se vea comprometida.

(2) **Barreras artificiales**, este procedimiento implica el análisis de los riesgos asociados a la ubicación geográfica de la instalación. Incluye evaluar la topografía de la zona, los impactos de las condiciones climáticas y los efectos de las inundaciones, deslizamientos y otros fenómenos naturales. Además, se debe tener en cuenta los potenciales impactos humanos, como la contaminación, la construcción y la infraestructura, así como los riesgos asociados a la explotación de recursos naturales.

Después de evaluar todos estos riesgos, se pueden determinar cuáles barreras artificiales son necesarias para proporcionar un nivel adecuado de seguridad y protección para la instalación. Las mismas pueden incluir muros, alambradas, cercas, vigas de contención, sistemas de iluminación, sistemas de seguridad electrónica, sistemas de alarma, entre otros. Además, se deben tomar en cuenta los procedimientos de seguridad, como el registro de personas que entren o salgan de la instalación, los protocolos de seguridad para acceder a áreas restringidas, la vigilancia de la propiedad y el control de los equipos electrónicos.

(3) **Barreras múltiples**, el procedimiento a seguir deberá involucrar una evaluación de los riesgos potenciales y amenazas a la seguridad. Esta evaluación debe incluir un análisis detallado de los posibles puntos de acceso no autorizados, la identificación de los riesgos asociados con cada punto de acceso y la identificación de las barreras físicas adecuadas para prevenir el acceso no autorizado. Estas barreras pueden incluir puertas con cerraduras, vallas, cercados, cámaras de vigilancia, controles de acceso, sistemas de señalización, iluminación, alarmas, etc. Se debe tener en cuenta la ubicación, la robustez y los requisitos de mantenimiento de cada barrera para garantizar que se cumplan los estándares de seguridad requeridos. Además, se debe realizar una evaluación periódica para asegurarse de que las barreras se mantengan adecuadamente y que la seguridad no se vea comprometida.

(4) **Cercas**, aquí se debe evaluar el área y la ubicación de la misma para determinar la cantidad y tipo de protección necesaria. Esto incluye evaluar el alcance de la cerca, la altura, el material utilizado para su construcción, el método de instalación y el mantenimiento. En cuanto a la ubicación es preciso asegurarse de que no se interpone en el camino de la gente, los vectores de entrada de animales y otros elementos. También hay que evaluar si la cerca

se puede escalar fácilmente y si hay riesgos de seguridad relacionados. Por último, se deben evaluar los factores relacionados con la seguridad en la zona circundante, como la iluminación, la ubicación de equipos de vigilancia, etc.

(5) **Torres de observación, garitas o panópticos**, aquí se involucran varios pasos. Primero, se debe evaluar los riesgos que presentan las instalaciones, luego se debe seleccionar el equipo adecuado para proporcionar un nivel adecuado de seguridad y protección. También se debe realizar un estudio de impacto de la ubicación y los alrededores de la instalación para evaluar los posibles efectos de la seguridad y protección en estas áreas. Seguidamente, se deben implementar medidas de seguridad y protección tales como cámaras de vigilancia, sistemas de seguridad electrónicos, sistemas de acceso controlado, barreras físicas, entre otras. Finalmente, se debe implementar un programa de entrenamiento para los empleados para garantizar un uso apropiado del equipo.

10. **Capitulo III - Sistemas de Seguridad en relación al personal, la información y documentación**

    Aquí se deben implementar medidas de seguridad y protección adecuadas, tales como autenticación de usuarios, protección de contraseñas, gestión de acceso a la información y seguridad de la red. Se recomienda también implementar políticas de seguridad, como el uso de contraseñas seguras, la restricción de la divulgación de información confidencial y la formación de personal para la sensibilización de la seguridad. Finalmente, se recomienda la implementación de medidas de seguridad física, como la instalación de sistemas de cámaras de vigilancia, sensores de movimiento, cerraduras de seguridad, entre otros.

11. **Capitulo IV** – **Educación Institucional sobre la Seguridad Física**

    Se debe incluir la identificación de amenazas potenciales, la formulación de planes para prevenir y responder a estas amenazas, y la implementación de herramientas prácticas para fortalecer la seguridad física. Esto incluye el diseño de políticas y procedimientos para la seguridad de las instalaciones, el control de acceso, la supervisión de las áreas sensibles, la implementación de sistemas de seguridad como cámaras de vigilancia, alarmas, cerraduras, etc., y la adopción de medidas de seguridad como la vigilancia de los visitantes, la verificación de identidad y el uso de equipos de protección individual. También es importante educar a los empleados sobre sus responsabilidades en cuanto a la seguridad física y las mejores prácticas para esto, incluyendo la identificación de amenazas y la información apropiada sobre cómo responder a ellas.

12. **Capítulo V – Control, seguimiento, evaluación, inspección e informes de seguridad**

    El diseño debe ser realizado en función de la prevención, detección y respuesta a las amenazas potenciales a la seguridad. Esto incluye el desarrollo de los procedimientos para controlar el acceso a áreas sensibles, el monitoreo de cámaras de vigilancia, el uso de detectores de movimiento, sistemas de alarma, códigos de seguridad, etc. Los procedimientos también deben incluir la verificación de identidad para visitantes, la supervisión de los trabajadores y el uso de equipos de protección personal. Es importante que se realicen informes periódicos sobre la seguridad de la instalación para garantizar que se cumplan los requisitos de seguridad establecidos. Además, se debe llevar a cabo una evaluación continua de los procedimientos de seguridad para asegurar que se estén cumpliendo los estándares adecuados.

13. **Conclusión**

    Elaborar un manual de procedimientos básicos de seguridad y protección en instalaciones físicas es una tarea importante que ayudará a garantizar que los trabajadores estén protegidos y que los riesgos potenciales sean minimizados. El manual debe incluir la descripción de los procedimientos específicos que se deben seguir para garantizar la seguridad y la protección de los trabajadores. Estos procedimientos deben incluir la identificación de los peligros, el diseño de planes de seguridad, el desarrollo de planes de contingencia, el seguimiento de los resultados de la implementación de los planes y la educación sobre seguridad y protección. El manual de procedimientos debe ser revisado y actualizado regularmente para garantizar que cumpla con los requisitos actuales.

14. **Bibliografía**

    Aquí se deben mencionar los reglamentos específicos, licencias, manuales de operación, políticas y manuales de la instalación, entre otros, que se necesiten para explicar o ampliar la información contenida en el plan. Estos documentos deberán estar disponibles para su consulta si así se requiera. Además, el Plan de Seguridad debería detallar claramente cómo se usarán los documentos de referencia para cumplir con los requisitos de seguridad.

15. **Anexos**, aquí se incluiría imágenes, gráficos, esquemas, planos, croquis etc. Necesarios o que se complementen con el análisis de seguridad física de la institución objeto de estudio, los cuales deberán estar debidamente georeferenciados, además se incluirán modelos de confección de documentación a modo de ejemplo)

CAPITULO V “CONCLUSIÓN”

De acuerdo al primer objetivo de investigación el cual se refiere a diagnosticar la situación actual en materia de seguridad y protección de instalaciones físicas de instituciones públicas o privadas de la ciudad de Jesús María (Córdoba), se afirma para el presente estudio que en más de un 50% se evidenció ausencia de vigilancia externa y la inexistencia de un registro de entrada y salida de personas y vehículos. Las medidas de seguridad física mencionadas fueron las rejas, medianeras o murallas, detectores de incendio y humo, puertas o cortinas metálicas desplegables, sensores de movimiento, otros, alarmas de seguridad y biométrico. A pesar de que un porcentaje de empresas no poseen estudios de seguridad, si cuentan con políticas de seguridad.

Conforme al segundo objetivo de investigación el cual alude a caracterizar los procedimientos básicos fundamentales que debe poseer un sistema de seguridad de instalaciones físicas para instituciones públicas o privadas, se concluye que estos incluyen el establecimiento de un marco legal y un alcance de seguridad, un diagnóstico de la situación actual de la empresa, un análisis FODA, un árbol de problemas y de objetivos, una matriz de estrategias, un plan de actividades, una evaluación de la seguridad, una implementación del plan de seguridad y una revisión continua del sistema. Estos procedimientos ayudarán a garantizar que la empresa cumpla con los estándares necesarios para la seguridad física.

En concordancia al tercer objetivo de investigación el cual apunta a elaborar la estructura para un Manual de procedimientos básicos de estudios de seguridad y protección en instalaciones físicas públicas o privadas de la ciudad de Jesús María (Córdoba), se presentó la estructura de modo que garantice la seguridad y la protección de los recursos físicos, humanos y materiales.

Bibliografía

Análisis de la ciudad de Jesús María. (2021). Obtenido de https://rdu.unc.edu.ar/bitstream/handle/11086/4580/ANEXOS.pdf?sequence=2&isAllowed=y

Arias, F. (2012). *El proyecto de investigación. Introducción a la metodología científica.* Caracas: Episteme.

ASIS . (2009). *Facilities Physical Security Measures.* Alejandría, Virginia.

Betancur López, S. (2000). Operacionalización de variables. *Hacia la Promoción de la Salud, 5*, 19-28. https://doi.org/https://revistasojs.ucaldas.edu.co/index.php/hacialapromocion delasalud/article/view/1847

Borja, J. (2000). *Gestión y control de la urbanización. .* Red número siete Programa URBAL. Material inédito. Rosario. Santa Fe.

Delegada, A. (2009). *Manual para la Autoridad Delegada para la Seguridad de la información Clasificada.* Madrid. España.

Galviz, I. (2019). *Lineamientos, componentes y requisitos generales para la implementación de un plan de seguridad física, en las instalaciones de la empresa cooperativa de trabajadores de Avianca Coopava en Bogotá*. Obtenido de (Trabajo de grado). Universidad Militar Nueva Granada: https://repository.unimilitar.edu.co/bitstream/handle/10654/35886/GalvizRojasIscisAndrea2019.pdf?sequence=1&isAllowed=y

Greenberg, M., & Lowrie, K. (2010). Gestión de riesgos - Principios y directrices. *Riesgo Análisis*, 873 - 874.

Hernández, R., Fernández, C., & Baptista, P. (2014). *Metodología de la Investigación.* McGraw-Hill.

Lezana Veliz, L. (2011). *Sistema Integral de Seguridad Física aplicado a Edificio T2 Campus Central Universidad San Carlos de Guatemala*. Obtenido de (Tesis de Grado). Universidad San Carlos de Guatemala. Facultad de Arquitectura.: http://biblioteca.usac.edu.gt/tesis/02/02_2860.pdf

Pedraza, G. (2006). *Gerencia de Protección de Ejecutivos.* Andros Cero Incidentes. Bogotá. Colombia .

Pérez, D. (2017). *Análisis de vulnerabilidad de la seguridad física de instalaciones ante eventos no deseados. Caso: Centro de diagnóstico no integral*. Obtenido de (Trabajo de grado). Universidad de Carabobo. venezuela: http://mriuc.bc.uc.edu.ve/bitstream/handle/123456789/5818/dperez.pdf?sequence=1

Schwab, K. (2016). *La cuarta revolución industrial.* Editorial Debate.

Vallejo Rosero, S. (2005). *Manual de Estudio de Seguridad.* Editorial Seguridad y Defensa. Buenos Aires. Argentina.

Vera, M. (2018). *La seguridad física y su importancia en una compañía para una adecuada gestión de riesgos*. Obtenido de (Trabajo de grado). Universidad Piloto de Colombia. Colombia: http://repository.unipiloto.edu.co/handle/20.500.12277/8643