Universidad de Buenos Aires Facultades de Ciencias Económicas

Carrera de Maestría en Seguridad Informática

Tesis final de Maestría

Título: "Más allá de las cámaras: Desafíos y soluciones en la video vigilancia con IA".

Autor: Esp. Lic. Nelson Lopez Baez
Director de la Tesis: Magtr. Ing. Juan Alejandro Devincenzi

Año de presentación: 2024
Cohorte: 2023

Declaración Jurada de origen de los contenidos

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

Esp. Lic. Nelson Lopez Baez

DNI 18816146

Agradecimiento:

Quiero expresar mi más profundo agradecimiento a todos aquellos que contribuyeron de manera invaluable a la culminación de mi tesis de maestría en Seguridad Informática.

En primer lugar, deseo extender mi sincero agradecimiento a mis distinguidos profesores, cuya orientación experta y dedicación fueron fundamentales en mi proceso de investigación y redacción. Sus conocimientos, consejos y críticas constructivas han sido el faro que iluminó mi camino hacia el éxito académico. Mi tutor Juan Alejandro Devincenzi, no tengo más que palabras de agradecimiento y admiración.

Asimismo, quiero reconocer y agradecer el invaluable apoyo de mis compañeros de estudio. Pasamos juntos 752 horas de clases y otras tantas de estudio, además de los preparativos de trabajos, las pruebas y errores en los laboratorios, y en especial, la visita a ARSAT, recuerdos que quedarán grabados para siempre. Nuestros debates, intercambio de ideas y colaboración en proyectos fueron fundamentales para enriquecer mi comprensión de los temas abordados en este programa de maestría. Su amistad y camaradería hicieron que este viaje académico fuera aún más gratificante y memorable.

No puedo pasar por alto el incondicional respaldo de mi familia durante este exigente, pero gratificante trayecto. A mis dos hijos, Ian y Santi, sin olvidarme de las madrugadas que el más pequeño durmió a mi lado mientras estudiaba, y a mi esposa, les debo un profundo agradecimiento por su paciencia, comprensión y sacrificio. Sus palabras de aliento, gestos de ánimo y amor incondicional fueron mi mayor motivación en los momentos de desafío y cansancio.

Este logro no solo es mío, sino también de ellos. Cada uno de ellos ha dejado una huella imborrable en este capítulo de mi vida académica, y por eso les estaré eternamente agradecido.

1. Contenido

Palabras claves:

Video Vigilancia con IA

Redes neuronales profundas.

Privacidad y Seguridad.

1. Hipótesis:

La aplicación efectiva de estrategias de protección de la privacidad, mitigación de riesgos de seguridad informática y mejora de la eficiencia y precisión de la vigilancia mediante el uso de inteligencia artificial (IA) puede fortalecer significativamente la seguridad cibernética en entornos digitales complejos. Se hipotetiza que la integración de estas tres áreas de enfoque en un marco integral de seguridad informática conducirá a una reducción notable de las vulnerabilidades, la mejora de la capacidad de respuesta ante amenazas emergentes y una protección más sólida de los datos sensibles y la infraestructura crítica. Esta hipótesis se sustenta en la premisa de que una combinación adecuada de medidas, técnicas, políticas y procesos respaldados por tecnologías avanzadas de IA puede ofrecer un enfoque holístico y proactivo para abordar los desafíos cada vez más complejos y dinámicos en el panorama de seguridad informática.

2. Resumen

La video vigilancia con inteligencia artificial (IA) [1] surgió como una poderosa herramienta de seguridad en la actualidad, ella nos brinda soluciones innovadoras para mejorar la gestión de seguridad y el monitoreo en diversos entornos. Sin embargo, su implementación plantea importantes desafíos en términos de privacidad y las leyes que la regulan, seguridad informática y el entrenamiento de redes neuronales profundas para un eficaz funcionamiento. [1]

En primer lugar, la privacidad se convierte en una preocupación central cuando se trata de la video vigilancia con IA. A medida que las cámaras se vuelven más sofisticadas, aumenta el riesgo de que la información personal y los comportamientos de las personas sean capturados y almacenados de forma indiscriminada. Es fundamental establecer marcos legales y políticas claras que protejan los derechos individuales y equilibren la necesidad de seguridad con la privacidad acordes a las leyes vigentes [2].

Desde la mirada de la seguridad informática, la video vigilancia con IA presenta vulnerabilidades que pueden ser explotadas por actores maliciosos. Estos sistemas están conectados a redes y pueden ser susceptibles a ataques cibernéticos, comprometiendo la integridad de los datos recopilados y la funcionalidad de las cámaras. La implementación de normas de seguridad adaptadas a la necesidad de cada organización se vuelve esencial para mitigar estos riesgos hacia parámetros aceptables [3].

Por otro lado, el entrenamiento de redes neuronales profundas [4] es un aspecto clave para mejorar la precisión y eficiencia de la video vigilancia con IA. En su etapa inicial, estas redes se alimentan con grandes conjuntos de datos para aprender y reconocer principalmente los patrones, lo que les permite identificar objetos, rostros y comportamientos específicos en tiempo real y alertar en consecuencia. Sin embargo, el entrenamiento de estas redes requiere una gran cantidad de datos etiquetados y algoritmos complejos, lo que plantea desafíos en términos de costos y recursos computacionales.

La video vigilancia con IA ofrece beneficios significativos en términos de seguridad y monitoreo, pero también plantea desafíos en cuanto a la privacidad, la seguridad informática y el entrenamiento de redes neuronales profundas. Es fundamental abordar estos aspectos de manera integral, mediante el establecimiento de regulaciones adecuadas, la implementación de medidas de seguridad robustas y la optimización de los procesos de entrenamiento de las redes neuronales. Solo así se podrá aprovechar plenamente el potencial de la video vigilancia con IA de manera ética y efectiva.

3. Fundamentación

Protección de la privacidad: Con el aumento de la video vigilancia y la creciente capacidad de las tecnologías de IA para el reconocimiento facial y el seguimiento de personas, la privacidad como derecho humano fundamental debe ser protegido, por ello se requiere investigar y desarrollar soluciones que equilibren la necesidad de seguridad con la protección de la privacidad individual. Esto implica explorar enfoques para minimizar la recopilación y retención innecesaria de datos personales, establecer custodias adecuadas y garantizar que el uso de la videovigilancia se ajuste a los principios éticos y legales.

Mitigación de riesgos de seguridad informática: A medida que las soluciones de video vigilancia se vuelven más interconectadas y dependientes de la infraestructura de TI, surgen desafíos de seguridad informática significativos. Investigar y comprender las vulnerabilidades potenciales, desarrollar medidas de seguridad efectivas y establecer protocolos de gestión de riesgos es esencial para proteger los sistemas de video vigilancia contra ataques cibernéticos asegurando la integridad de los datos recopilados.

Mejora de la eficiencia y precisión de la vigilancia: La investigación en entrenamiento de redes neuronales profundas para video vigilancia busca mejorar la capacidad de estas redes para identificar y analizar eventos y comportamientos relevantes en tiempo real. Al invertir en la investigación de técnicas de entrenamiento más avanzadas y eficientes, se puede lograr una mayor precisión en la detección de eventos, reducir las falsas alarmas que permitirán procesos de automatización de respuesta y optimizar el uso de los recursos de video vigilancia.

Ética y responsabilidad: La video vigilancia con IA plantea importantes desafíos éticos y de responsabilidad. Por ejemplo, ¿quién tiene acceso a los datos recopilados? ¿Cómo se garantiza la protección de los datos personales? ¿Cómo se pueden evitar los sesgos y la discriminación en el uso de la

tecnología? Investigar sobre estos temas puede ayudar a promover una cultura ética y responsable en el uso de la video vigilancia con IA.

El manejo responsable de esta tecnología llevara a las personas a entender a la vigilancia con IA, como una herramienta más, que convive en nuestra cultura y nos brinda un servicio.

4. Objetivos y Alcance

El objetivo principal de esta tesis, basada en un trabajo de especialización de mi autoría, es explorar y profundizar en el tema de video vigilancia con IA. Se abarcarán todos los aspectos relevantes de esta tecnología, desde el desarrollo de redes neuronales profundas y sus métodos de entrenamiento, hasta el análisis de los principales proveedores y equipos líderes en el campo. Además, se examinarán los costos asociados con la adquisición, instalación y mantenimiento de estos sistemas, así como el desafío de la escasez de profesionales capacitados en esta área.

Con relación a la privacidad: Abordaremos las normativas argentinas sobre la privacidad e intimidad otorgado por la Ley 25.326 de protección de datos personales, sus sanciones por incumplimiento bajo la tutela de la Dirección Nacional de Protección de Datos Personales (DNPDP). Además de las sanciones administrativas según la disposición 9/2015. Las normas constitucionales que protegen la privacidad y los datos personales en sus Art. 18;19;43.

Con relación a la seguridad informática de la video vigilancia con IA, se abordará de manera teórico-práctica, analizando tanto las leyes vigentes en Argentina como las regulaciones de la comunidad europea. Se prestará especial atención a la nueva directiva (SRI2), que sustituirá a la 2016/114, así como al reglamento de ciberseguridad de la UE, que busca garantizar un alto nivel de seguridad en las redes y sistemas de información de la Unión [5]. Además, se presentarán casos reales de ataques actuales y se llevarán a cabo laboratorios

de ataques en sistemas de video vigilancia, utilizando un enfoque ético conocido como "ethical hacking" [6] y siguiendo los seis pasos recomendados: **observación, escaneo, enumeración, análisis, explotación e informes.**

5. Machine learning & deep learning.

Machine learning (ML) y deep learning (DL) son dos subcampos de la inteligencia artificial (IA) enfocados en el desarrollo de algoritmos y modelos que pueden aprender de los datos para hacer predicciones o tomar decisiones sin ser programados explícitamente.

El machine learning es un término más amplio que abarca una variedad de técnicas y algoritmos utilizados para enseñar a las máquinas a aprender de los datos, reconocer patrones y hacer predicciones o tomar decisiones basadas en ese aprendizaje. Puede ser categorizado en tres tipos principales: **aprendizaje supervisado, aprendizaje no supervisado y aprendizaje por refuerzo**.

El deep learning, por otro lado, es un subconjunto del machine learning que utiliza **redes neuronales** con muchas capas para aprender representaciones complejas de los datos. Ha ganado una atención significativa y ha logrado resultados impresionantes en una variedad de aplicaciones como la visión por computadora, el procesamiento del lenguaje natural y el reconocimiento de voz.

En resumen, el machine learning es un campo más amplio que incluye el deep learning como una técnica específica y poderosa para aprender de los datos. Ambos campos tienen aplicaciones prácticas en muchas áreas, incluyendo finanzas, atención médica, marketing, ciencia de datos y mucho más.

5.1 Machine learning.

La idea fundamental detrás del machine learning es permitir que las computadoras aprendan automáticamente a partir de datos sin tener que ser programadas manualmente para realizar tareas específicas.

Existen tres tipos principales de aprendizaje en el machine learning:

5.1.1 Aprendizaje supervisado:

Es un tipo de aprendizaje automático (machine learning) donde un modelo es entrenado utilizando datos previamente etiquetados para predecir las respuestas correctas (clasificación o regresión). Esto significa que el modelo recibe un conjunto de datos de entrenamiento con entradas y salidas correspondientes, y se le enseña a identificar patrones en los datos para que pueda hacer predicciones precisas sobre nuevas entradas.

En el aprendizaje supervisado, el objetivo es desarrollar un modelo que pueda hacer predicciones precisas en nuevos datos, no solo en los datos utilizados para entrenar el modelo. El modelo utiliza los datos de entrenamiento para aprender cómo se relacionan las entradas y las salidas, y luego puede aplicar ese conocimiento a nuevas entradas para hacer predicciones precisas.

El aprendizaje supervisado se puede utilizar en una variedad de tareas, como clasificación, regresión y detección de objetos. En la clasificación, el modelo se entrena para predecir una salida discreta, como una etiqueta o una categoría. En la regresión, el modelo se entrena para predecir una salida continua, como un valor numérico. En la detección de objetos, el modelo se entrena para identificar objetos en una imagen o un video.

Un ejemplo de aprendizaje supervisado sería la predicción del precio de una casa en función de ciertas características, como el número de habitaciones, el tamaño del lote y la ubicación. El modelo se entrena utilizando un conjunto de datos de casas y sus precios correspondientes. El modelo aprende cómo se relacionan las características de una casa con su precio, y luego puede hacer predicciones precisas sobre el precio de una nueva casa en función de sus características.

5.1.2 Aprendizaje no supervisado:

Es un tipo de aprendizaje automático (machine learning) donde un modelo se entrena en un conjunto de datos no etiquetados para identificar patrones o estructuras en los datos sin una guía explícita. En otras palabras, el modelo debe encontrar relaciones ocultas y patrones en los datos por sí solo, sin conocer de antemano cuáles son las respuestas correctas.

A diferencia del aprendizaje supervisado, donde el modelo recibe un conjunto de datos etiquetados con entradas y salidas correspondientes, en el aprendizaje no supervisado, el modelo solo tiene acceso a un conjunto de datos de entrada sin etiquetar. El objetivo es encontrar patrones en los datos que permitan agrupar, clasificar o reducir la complejidad de los datos de entrada.

Existen diferentes enfoques de aprendizaje no supervisado, entre ellos:

Clustering, reducción de dimensionalidad, análisis de componentes principales, asociación. [7, p. 94]

Clustering: Es una técnica de aprendizaje no supervisado mas populares en el que se busca dividir un conjunto de datos en grupos o clusters que tengan características similares entre sí. El objetivo del clustering es encontrar patrones o estructuras en los datos sin necesidad de tener etiquetas o categorías previas.

Existen diferentes algoritmos de clustering, pero todos ellos buscan agrupar los datos en función de la distancia o similitud entre ellos. Un ejemplo común de algoritmo de clustering es el k-means, que divide los datos en k grupos o clusters de manera que la distancia intra-cluster (entre los puntos de un mismo grupo) sea mínima y la distancia inter-cluster (entre los puntos de distintos grupos) sea máxima.

El clustering tiene numerosas aplicaciones en diferentes campos, como el análisis de datos, la minería de datos, la bioinformática, la clasificación de imágenes, la segmentación de clientes y la detección de fraudes. Por ejemplo, en la segmentación de clientes, el clustering se puede utilizar para dividir a los clientes en grupos según sus características, como edad, género, ingresos o preferencias, lo que puede ayudar a las empresas a diseñar estrategias de marketing personalizadas.

Sin embargo, el clustering también presenta desafíos y limitaciones. Uno de los principales desafíos es la elección del número óptimo de clusters. El número de clusters puede variar dependiendo del conjunto de datos y del objetivo del análisis, y elegir el número equivocado puede llevar a resultados inexactos o poco útiles.

Reducción de dimensionalidad: Es una técnica que se utiliza en el aprendizaje automático para reducir el número de variables o características de un conjunto de datos. La idea es eliminar características redundantes o irrelevantes y mantener solo las más importantes, lo que puede mejorar la precisión del modelo y reducir el tiempo de entrenamiento.

Existen diferentes técnicas de reducción de dimensionalidad, pero todas ellas buscan transformar el conjunto de datos de alta dimensionalidad en uno de menor dimensión, mientras se conserva la información más importante. Las

técnicas de reducción de dimensionalidad se dividen en dos categorías principales: lineales y no lineales.

Las técnicas de reducción de dimensionalidad lineales, como el análisis de componentes principales (PCA), buscan transformar los datos de alta dimensión en un conjunto de datos de menor dimensión, manteniendo la mayor cantidad posible de información. PCA, por ejemplo, busca encontrar una combinación lineal de las características originales que maximice la varianza de los datos, mientras se minimiza la pérdida de información. Una vez que se ha encontrado esta combinación, se puede reducir el número de características al conjunto de datos transformado.

Por otro lado, las técnicas de reducción de dimensionalidad no lineales, como el t-SNE (t-distributed stochastic neighbor embedding), buscan preservar la estructura no lineal de los datos de alta dimensión en un conjunto de datos de menor dimensión. Estas técnicas son útiles cuando los datos tienen una estructura no lineal, y cuando la información importante está codificada en patrones complejos de los datos.

La reducción de dimensionalidad tiene numerosas aplicaciones en diferentes campos, como el procesamiento de imágenes, la clasificación de texto y la minería de datos. Por ejemplo, en el procesamiento de imágenes, la reducción de dimensionalidad se puede utilizar para reducir el tamaño de una imagen y mejorar la velocidad de procesamiento sin perder demasiada información.

Sin embargo, la reducción de dimensionalidad también presenta desafíos y limitaciones. Uno de los principales desafíos es la selección del número óptimo de características a mantener, lo que puede requerir una evaluación exhaustiva. Además, algunas técnicas de reducción de dimensionalidad pueden perder información importante en el proceso de transformación.

Análisis de componentes principales (PCA): (PCA, por sus siglas en inglés) es una técnica de reducción de dimensionalidad que se utiliza comúnmente en el análisis de datos. PCA busca transformar un conjunto de datos de alta dimensión en un conjunto de datos de menor dimensión, al mismo tiempo que conserva la mayor cantidad posible de información.

El objetivo del PCA es encontrar una combinación lineal de las características originales que maximice la varianza de los datos, mientras que minimiza la pérdida de información. Esta combinación lineal se conoce como el primer componente principal. Luego, el PCA busca encontrar el segundo componente principal, que es una combinación lineal de las características originales que es ortogonal al primer componente y que maximiza la varianza residual.

El proceso se repite hasta que se han encontrado tantos componentes principales como características originales. Cada componente principal captura la mayor cantidad de información posible de los datos, lo que permite reducir la dimensionalidad del conjunto de datos sin perder demasiada información.

Una de las aplicaciones más comunes del PCA es la visualización de datos. En la mayoría de los casos, los datos se presentan en un espacio de alta dimensión, lo que hace que sea difícil visualizar la relación entre las diferentes variables. PCA puede reducir la dimensión del conjunto de datos a dos o tres dimensiones, lo que facilita la visualización y la interpretación de los datos.

Además, PCA se utiliza en una amplia gama de aplicaciones, como la clasificación de imágenes, la compresión de datos, la minería de datos, el procesamiento de señales y el modelado estadístico. Por ejemplo, en la clasificación de imágenes, PCA se puede utilizar para reducir la dimensión de un

conjunto de características extraídas de una imagen, lo que puede mejorar la precisión de la clasificación.

Sin embargo, también hay limitaciones en el uso del PCA. Una de las limitaciones es que PCA supone que los datos tienen una distribución gaussiana y que los componentes principales son ortogonales. Además, la selección del número óptimo de componentes principales puede ser un desafío, ya que puede haber un compromiso entre la precisión y la complejidad del modelo.

Asociación: es una técnica de aprendizaje automático que se utiliza para descubrir patrones interesantes en conjuntos de datos. El objetivo es encontrar relaciones entre diferentes variables o características en el conjunto de datos, lo que puede ayudar a los usuarios a descubrir nuevos conocimientos y a tomar decisiones informadas.

El aprendizaje de asociación se basa en la idea de que las características o variables de un conjunto de datos pueden estar relacionadas entre sí. Por ejemplo, en un conjunto de datos de ventas de una tienda, es posible que se descubra que los clientes que compran un determinado producto también compran otro producto específico. Esta información podría ser utilizada por la tienda para ofrecer promociones y ofertas especiales para estos productos relacionados y aumentar las ventas.

Una técnica común utilizada en el aprendizaje de asociación es el análisis de reglas de asociación, que busca patrones en los datos a través de la identificación de reglas que describen las relaciones entre diferentes variables. Las reglas de asociación se presentan en forma de "si-entonces", donde se describe la relación entre las variables. Por ejemplo, una regla de asociación en un conjunto de datos de ventas podría ser: "si un cliente compra un producto A, entonces también es probable que compre el producto B".

La identificación de reglas de asociación se realiza a través de algoritmos como el algoritmo de Apriori, que utiliza una combinación de frecuencia y confianza para identificar las reglas más relevantes en el conjunto de datos. La frecuencia se refiere a la cantidad de veces que se observa una regla en el conjunto de datos, mientras que la confianza mide la probabilidad de que una regla sea verdadera.

El aprendizaje de asociación tiene una amplia gama de aplicaciones, como la segmentación de clientes, la detección de fraudes, la recomendación de productos y la minería de datos. Por ejemplo, en la detección de fraudes, se puede utilizar el aprendizaje de asociación para identificar patrones de comportamiento sospechosos en los datos financieros de una empresa.

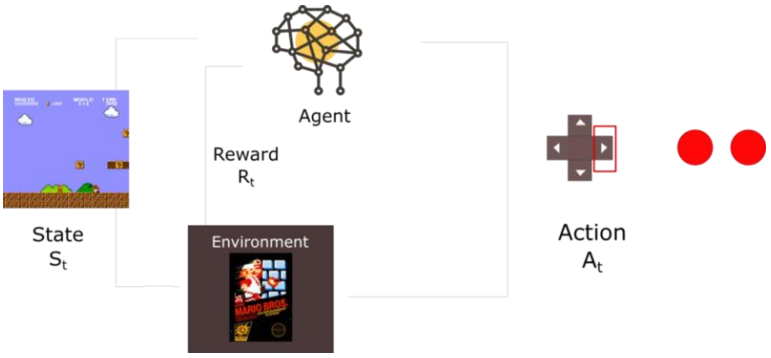
Un ejemplo de aprendizaje no supervisado sería el análisis de datos de redes sociales para identificar comunidades de usuarios que interactúan entre sí con frecuencia, incluso si estas comunidades no están etiquetadas previamente.

5.1.3 Aprendizaje por refuerzo:

Es un tipo de aprendizaje automático (machine learning) donde un agente se entrena para tomar decisiones en un entorno en función de las recompensas o castigos que recibe en respuesta a sus acciones. En otras palabras, el agente aprende a realizar acciones óptimas para maximizar la recompensa recibida del entorno. La mejor similitud a un ejemplo real es cómo los niños aprenden a través de prueba y error

En el aprendizaje por refuerzo, el agente no tiene acceso a un conjunto de datos previamente etiquetados, sino que interactúa con un entorno y recibe una recompensa o castigo en función de sus acciones. El objetivo del agente es aprender una política, que es un conjunto de acciones que debe tomar en cada estado del entorno para maximizar la recompensa total.

Un ejemplo común de aprendizaje por refuerzo es el entrenamiento de un agente de inteligencia artificial para jugar juegos complejos. El agente comienza sin conocimiento del juego, pero a través de la interacción con el entorno y la retroalimentación en forma de recompensas o castigos, aprende una estrategia óptima para ganar el juego.



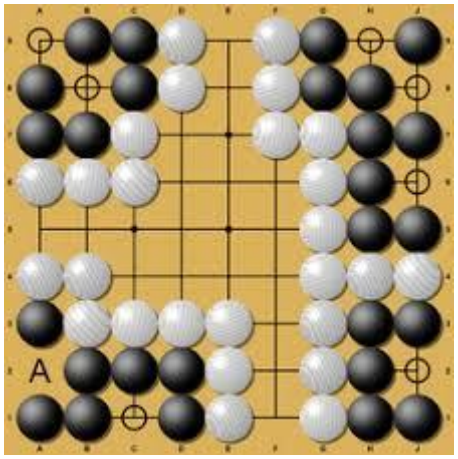
Relación de aprendizaje por refuerzo y el juego Super Mario Bros: "…Supongamos que estamos jugando al videojuego de Super Mario Bros. El entorno es el videojuego en sí, la imagen que estamos viendo en el monitor es el estado actual, las posibles acciones corresponden con los botones de movimiento en las 4 direcciones y saltar, y, por último, las recompensas serán positivas cuando derrotemos a un Woompa o completemos el nivel y negativas cuando nos eliminen o conforme pase el tiempo, ya que queremos incentivar que el agente se mueva y aprenda explorando el entorno. En la siguiente imagen se presenta un resumen de estos elementos básicos en el aprendizaje por refuerzo…" [8]

El aprendizaje por refuerzo se puede utilizar en una variedad de aplicaciones, como robótica, control de procesos y juegos. También se ha utilizado para optimizar el tráfico de red, mejorar la eficiencia energética y en el diseño de sistemas de control adaptativos.

A pesar de que el aprendizaje por refuerzo tiene muchas aplicaciones útiles, también presenta desafíos únicos. Uno de los principales desafíos es el

equilibrio entre la exploración y la explotación. El agente debe explorar diferentes acciones para aprender una política óptima, pero también debe explotar las acciones que ha aprendido para maximizar la recompensa.

Otro desafío es el diseño de la función de recompensa. La función de recompensa debe ser diseñada cuidadosamente para incentivar al agente a realizar acciones óptimas. Si la función de recompensa no se diseña correctamente, el agente puede aprender una política subóptima o incluso destructiva. [8]



Relación de aprendizaje por refuerzo y el juego de Go: Este es un juego de estrategia en el que dos jugadores intentan controlar el tablero mediante la colocación de fichas en las intersecciones de una cuadrícula. El objetivo es conseguir una mayor cantidad de territorio que el oponente. Go es un juego muy complejo y desafiante para los algoritmos de inteligencia artificial, debido a la enorme cantidad de posibles movimientos y estrategias.

El aprendizaje por refuerzo se ha utilizado para entrenar sistemas de inteligencia artificial en el juego de Go, con el objetivo de que el agente aprenda a tomar las mejores decisiones en cada situación del juego. Los algoritmos de aprendizaje por refuerzo para Go se basan en redes neuronales profundas y técnicas avanzadas de búsqueda de árboles para evaluar posibles movimientos y estrategias. Los sistemas de inteligencia artificial entrenados mediante aprendizaje por refuerzo han logrado resultados sorprendentes en Go, superando incluso a los jugadores humanos más experimentados. [9]

Relación de aprendizaje por refuerzo y el juego AlphaStar: Para entrenar a AlphaStar, se utiliza una técnica de aprendizaje por refuerzo llamada "aprendizaje por imitación". En primer lugar, se entrenan varias redes neuronales con una gran cantidad de partidas grabadas de jugadores profesionales de StarCraft II, para que puedan imitar el comportamiento humano en el juego. Luego, estas redes se utilizan para generar una gran cantidad de partidas adicionales que se utilizan para entrenar la red principal de AlphaStar mediante aprendizaje por refuerzo.

Durante el entrenamiento por refuerzo, AlphaStar juega contra sí mismo, explorando diferentes estrategias y ajustando su comportamiento en función de las recompensas y penalizaciones que recibe por sus acciones. A medida que AlphaStar juega más partidas, su red neuronal se ajusta y aprende a tomar mejores decisiones en cada situación del juego.

Además, se utilizan técnicas avanzadas de búsqueda de árboles y otros métodos de optimización para mejorar aún más el rendimiento de AlphaStar. Finalmente, el sistema es evaluado en una serie de desafíos contra jugadores humanos y otros agentes de inteligencia artificial para medir su habilidad y mejorar su rendimiento. [10]

5.2 Deep learning.

También conocido como aprendizaje profundo, es una rama del aprendizaje automático que se basa en la construcción de modelos de redes neuronales artificiales de varias capas. Estos modelos son capaces de aprender y realizar tareas complejas, como reconocimiento de imágenes, procesamiento del lenguaje natural y juegos estratégicos.

La clave del éxito del deep learning es la capacidad de las redes neuronales para aprender automáticamente a partir de grandes cantidades de datos sin necesidad de programar explícitamente las reglas que rigen el comportamiento del modelo. Esto se logra mediante la utilización de algoritmos de optimización que ajustan los parámetros del modelo para que se ajusten mejor a los datos.

Una de las principales ventajas del deep learning es su capacidad para trabajar con datos de alta dimensionalidad, como imágenes, videos y sonido. Las redes neuronales profundas pueden aprender a extraer características complejas de estos tipos de datos, lo que las hace especialmente útiles en aplicaciones de reconocimiento de imágenes y procesamiento del lenguaje natural.

El deep learning ha tenido un gran impacto en una amplia variedad de campos, incluyendo la visión artificial, la robótica, la medicina, la industria automotriz y la publicidad en línea. Por ejemplo, en la medicina, el deep learning se ha utilizado para el diagnóstico de enfermedades, el análisis de imágenes médicas y la identificación de nuevos tratamientos.

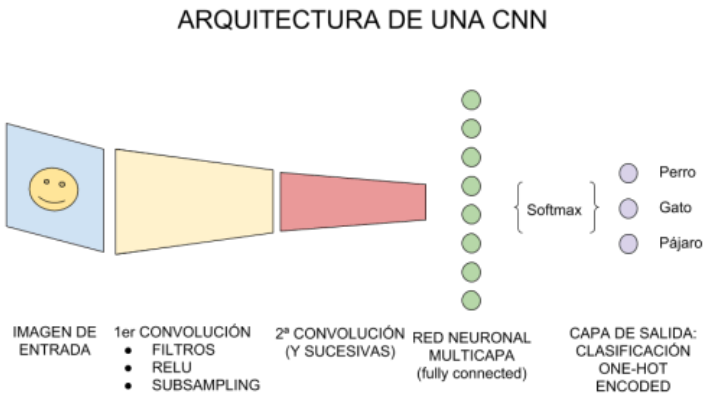
Una de las desventajas del deep learning es que puede ser computacionalmente intensivo y requerir grandes cantidades de datos para entrenar los modelos correctamente. Además, debido a la complejidad de las redes neuronales profundas, pueden ser difíciles de interpretar y explicar cómo llegaron a una determinada conclusión.

El éxito del deep learning se debe en parte al aumento en la cantidad de datos disponibles y la capacidad de procesamiento informático. Además, la comunidad científica ha trabajado arduamente en el desarrollo de nuevos algoritmos y técnicas para el entrenamiento y la optimización de redes neuronales profundas.

Entre las arquitecturas de redes neuronales profundas más utilizadas se encuentran las redes neuronales convolucionales (CNN) y las redes neuronales recurrentes (RNN).

5.2.1 Las redes neuronales convolucionales (CNN):

Son un tipo de arquitectura de redes neuronales profundas que se utilizan principalmente en aplicaciones de visión artificial, como el reconocimiento de imágenes y videos. Las CNN son capaces de detectar patrones en los datos de entrada, como bordes, formas y texturas, y utilizarlos para hacer predicciones precisas. [11]



Arquitectura básica:

Entrada: serán los píxeles de la imagen. Su altura, ancho y profundidad tendrán solo 1 color, o 3 colores para rojo, verde, azul.

Capa convolucional: procesará la salida de las neuronas conectadas en la "región local" de entrada (es decir, píxeles cercanos), calculando el producto escalar entre sus pesos (valores de píxeles) y la pequeña región a la que están conectadas en la entrada volumétrica. Por ejemplo aquí usaremos 32 filtros o lo que decidamos y este será el volumen de salida.

«CAPA RELU» aplicará la función de activación a los elementos de la matriz. **MUESTREO o SUBMUESTREO:** Reduce las dimensiones de alto y ancho pero mantiene la profundidad.

Capa "tradicional": Una red de neuronas feedforward que se conectará a la última capa de submuestreo y terminará con el número de neuronas que queremos clasificar.

La clave de la CNN es la capa de convolución, que consiste en un conjunto de filtros que se aplican a una sección del campo visual. Cada filtro se utiliza para detectar una característica específica de los datos de entrada, como bordes, esquinas, texturas, etc. Los resultados de cada filtro se pasan a través de una función de activación no lineal, como la función ReLU, que introduce no linealidad en la red y mejora su capacidad para aprender patrones complejos.

Las CNN también utilizan capas de agrupamiento, que reducen el tamaño de los datos de entrada y extraen las características más importantes. La capa de agrupamiento más común es la capa de agrupamiento máx, que toma el valor máximo en cada sección del campo visual. Esto reduce la cantidad de datos que la red tiene que procesar y ayuda a evitar el sobreajuste.

Además de las capas de convolución y de agrupamiento, las CNN también tienen capas completamente conectadas, que combinan las características extraídas en las capas anteriores para hacer predicciones finales. Las CNN se entrenan utilizando algoritmos de optimización como el descenso del gradiente estocástico y la retropropagación, que ajustan los pesos de las neuronas para que la red pueda hacer predicciones precisas.

Las CNN se han utilizado en una amplia variedad de aplicaciones de visión artificial, como el reconocimiento de objetos, el seguimiento de objetos, la detección de rostros y la clasificación de imágenes médicas. Además, las CNN

también se han utilizado en aplicaciones de procesamiento de lenguaje natural, como la generación de texto y la traducción automática.

La visión artificial: es una rama de la inteligencia artificial que se centra en desarrollar algoritmos y sistemas capaces de interpretar y analizar imágenes y videos. La visión artificial se utiliza en una amplia variedad de aplicaciones, incluyendo la robótica, el control de calidad industrial, la medicina, el transporte y la seguridad.

El objetivo principal de la visión artificial es emular la capacidad del ojo humano para capturar y procesar información visual. Esto se logra mediante el uso de técnicas de procesamiento de imágenes y de aprendizaje automático, que permiten a los sistemas de visión artificial aprender de los datos de entrada y hacer predicciones precisas.

Entre las técnicas más utilizadas en visión artificial se encuentran las redes neuronales convolucionales (CNN), que son capaces de analizar y procesar imágenes complejas, y las redes neuronales recurrentes (RNN), que son utilizadas para procesar secuencias de imágenes y videos.

La visión artificial se divide en varias áreas de aplicación, entre ellas se encuentran la detección de objetos, el reconocimiento facial, la segmentación de imágenes, la clasificación de imágenes y el seguimiento de objetos. La detección de objetos se utiliza para identificar y localizar objetos específicos en una imagen o video, mientras que el reconocimiento facial se utiliza para identificar y verificar la identidad de las personas.

La segmentación de imágenes es una técnica que permite separar los diferentes objetos presentes en una imagen, y la clasificación de imágenes se utiliza para asignar una etiqueta a una imagen determinada. El seguimiento de

objetos, por su parte, permite seguir el movimiento de un objeto a lo largo de varias imágenes o videos.

El reconocimiento de imágenes y videos: es una aplicación clave de la visión artificial. Se refiere al proceso de identificar y clasificar objetos, patrones y otros elementos presentes en imágenes y videos utilizando técnicas de aprendizaje automático y procesamiento de señales.

Existen varios enfoques para el reconocimiento de imágenes y videos. Uno de los más utilizados es el aprendizaje supervisado, que implica entrenar un modelo de aprendizaje automático con un conjunto de imágenes y etiquetas correspondientes. El modelo aprende a identificar patrones y características en las imágenes y puede clasificar nuevas imágenes en las mismas categorías.

Otro enfoque común es el aprendizaje no supervisado, que se utiliza cuando no se dispone de un conjunto de etiquetas. En este caso, el modelo intenta encontrar patrones y estructuras en los datos sin ninguna orientación explícita. Esto puede ser útil en la exploración de grandes conjuntos de datos para encontrar relaciones y estructuras ocultas.

El reconocimiento de imágenes y videos tiene numerosas aplicaciones prácticas, como la identificación de objetos en imágenes médicas, la detección de caras en sistemas de seguridad, la clasificación de productos en la industria minorista y la identificación de objetos en imágenes satelitales, entre otras.

5.2.2 Las redes neuronales recurrentes (RNN). [12] [7, p. 345]

Son un tipo de arquitectura de aprendizaje profundo que se utiliza comúnmente en el procesamiento del lenguaje natural, la generación de texto y la predicción de series de tiempo. A diferencia de las redes neuronales convolucionales (CNN), las RNN tienen conexiones recurrentes entre las

neuronas, lo que les permite capturar la información temporal en los datos de entrada.

La principal característica de las RNN es que tienen ciclos en su estructura de conexión, lo que les permite procesar secuencias de datos, como texto, audio y video, que tienen una estructura temporal. Esta capacidad de modelar secuencias las hace muy útiles en aplicaciones como el reconocimiento de voz, la traducción automática y la generación de texto.

Las RNN tienen la capacidad de recordar información de las entradas anteriores a través de su estado oculto o memoria a corto plazo (LSTM). En cada paso de tiempo, la RNN toma como entrada los datos en ese momento y la salida generada en el paso anterior, lo que permite que la red aprenda patrones en secuencias de datos a lo largo del tiempo.

A pesar de su utilidad, las RNN tienen limitaciones. Una de ellas es la dificultad para entrenarlas debido a problemas como la desaparición y explosión del gradiente. Además, a medida que se procesan secuencias más largas, la RNN puede tener dificultades para retener la información relevante de los pasos anteriores, lo que se conoce como el problema de la memoria a largo plazo.

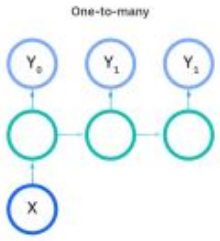
Para abordar estas limitaciones, se han propuesto diversas variantes de RNN, como las redes neuronales de memoria a corto plazo (LSTM) y las redes neuronales de memoria a largo plazo (GRU). Estas variantes utilizan diferentes mecanismos de memoria y conexiones para abordar los problemas de las RNN estándar.

Algunos tipos de redes neuronales recurrentes

One to one: son un caso especial dentro de las RNN donde la entrada y la salida son independientes y no están relacionadas secuencialmente. A diferencia de las RNN tradicionales que están diseñadas para modelar secuencias, las RNN "one to one" se utilizan cuando no hay una dependencia temporal entre los datos de entrada y salida.

la red neuronal se comporta como una red feedforward convencional, donde cada entrada se procesa de forma aislada y se genera una única salida correspondiente. No se realiza ninguna propagación de retroalimentación en el tiempo ni se capturan relaciones secuenciales.

Este tipo de arquitectura de red neuronal se utiliza comúnmente en problemas de clasificación de imágenes, donde cada imagen se considera de forma independiente y se asigna una etiqueta o categoría específica.

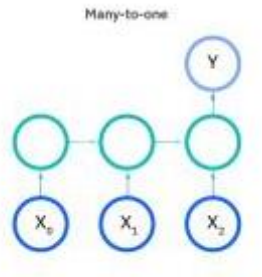


One to many: son un tipo de arquitectura en la que se proporciona una sola entrada y se generan múltiples salidas secuenciales. A diferencia de las RNN "one to one" donde la entrada y la salida son independientes, en las RNN "one to many" la salida se genera en forma de secuencia y está relacionada con la entrada inicial.

En este tipo de RNN, se procesa una sola entrada inicial y se produce una secuencia de salidas correlacionadas en función de dicha entrada. Un ejemplo común de RNN "one to many" es la generación de texto a partir de una única entrada, como la generación automática de subtítulos para imágenes.

Durante el proceso de generación, la RNN "one to many" utiliza la información de la entrada inicial para influir en la generación de cada elemento de la secuencia de salida. Cada paso de tiempo en la RNN recibe la salida anterior como retroalimentación y produce una nueva salida en función de esa retroalimentación y la entrada inicial.

Las RNN "one to many" son utilizadas cuando se desea generar una secuencia de salidas correlacionadas a partir de una sola entrada inicial, como en la generación de texto o subtítulos. Estas redes permiten capturar la dependencia temporal y generar una salida secuencialmente relacionada con la entrada.

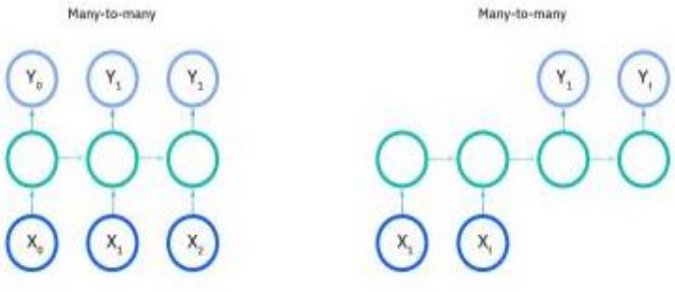


Many to one: son un tipo de arquitectura en la que se proporciona una secuencia de entradas y se produce una única salida al final de la secuencia. A diferencia de las RNN "one to many" donde se generan múltiples salidas secuenciales, en las RNN "many to one" se busca resumir o clasificar la secuencia de entrada en una única salida.

En este tipo de RNN, se procesa una secuencia de entradas y se captura la información relevante de la secuencia para producir una única salida al final. Por ejemplo, en la clasificación de sentimientos en el análisis de texto, donde se desea determinar el sentimiento general de un conjunto de palabras, se puede utilizar una RNN "many to one". La secuencia de palabras se alimenta a la red y, al final de la secuencia, se genera una salida que representa el sentimiento asociado.

Durante el procesamiento, la RNN "many to one" va capturando la información de las entradas anteriores y utiliza esta información acumulada para generar la salida final. La red puede tener capas recurrentes para capturar la

dependencia temporal y también puede utilizar técnicas de atención para enfocarse en partes relevantes de la secuencia.



Many to many: son un tipo de arquitectura en la que se proporciona una secuencia de entradas y se produce una secuencia correspondiente de salidas. En otras palabras, tanto la entrada como la salida son secuencias de datos.

En las RNN "many to many", la red neuronal procesa cada elemento de la secuencia de entrada y genera una salida correspondiente para cada elemento de la secuencia de salida. Cada paso de tiempo en la RNN está vinculado a un elemento específico tanto en la entrada como en la salida.

Umbrales, Activación y sincronizaciones de tiempo en redes recurrentes [7, p. 357]

Los umbrales son valores predefinidos que se utilizan para determinar si una neurona se activa o no. En una RNN, cada neurona tiene un umbral asociado. Después de recibir las entradas y aplicar una función de activación, la neurona compara el resultado con su umbral. Si el resultado supera el umbral, la neurona se activa y produce una salida. De lo contrario, permanece inactiva. Los umbrales son una forma de introducir un nivel de excitación requerido para que una neurona se active.

La activación se refiere al estado de una neurona en una RNN. Una neurona puede estar activada o inactiva en función de sus entradas y su umbral.

La activación de una neurona determina si transmite o no información a las neuronas posteriores en la secuencia temporal. La función de activación aplicada a una neurona en una RNN es la responsable de decidir su estado de activación en función de las entradas recibidas y los umbrales establecidos.

La **activación sincrónica** es un enfoque en redes neuronales recurrentes (RNN) donde la información se procesa de manera temporalmente discreta y sincronizada, utilizando pulsos o eventos discretos para representar y propagar la información. Este enfoque es eficiente en términos de recursos computacionales y captura relaciones temporales precisas.

Por otro lado, la **activación asincrónica** es el enfoque tradicional en RNN, donde la información se procesa de manera continua y no está sujeta a sincronización temporal precisa. Utiliza funciones de activación continuas y propaga las activaciones en forma continua a través de la red.

6. Privacidad y Ciberética.

6.1 Marco legal: Privacidad, protección de datos personales

6.1.1 Definición:

La definición y protección de la privacidad pueden variar según las entidades y jurisdicciones. A continuación, se expone una breve descripción de tres importantes entidades a nivel mundial que han abordado el concepto de privacidad:

Unión Europea (UE) - Reglamento General de Protección de Datos (RGPD): [5] La Carta de los Derechos Fundamentales de la UE establece que los ciudadanos de la Unión tienen derecho a que se protejan sus datos personales. Define la privacidad como el derecho fundamental de las personas a controlar sus datos personales. Establece que los individuos tienen el derecho de saber qué datos se recopilan sobre ellos, cómo se utilizan y tienen la capacidad de dar su consentimiento informado. Además, el RGPD establece medidas para garantizar la transparencia en el manejo de datos y promover la seguridad y la integridad de la información personal.

Estados Unidos - Ley de Privacidad del Consumidor de California (CCPA): [13] Promulgada en 2020 es la primera legislación en los Estados Unidos que emula el Reglamento General de Protección de Datos (RGPD) de la Unión Europea y se promulga como ley, se centra en la privacidad de los consumidores. Define la privacidad como el derecho de los residentes de California a conocer qué información personal se recopila sobre ellos, por qué se recopila y con quién se comparte. La CCPA otorga a los consumidores el derecho de optar por no participar en la venta de sus datos y exige a las empresas que implementen prácticas de privacidad claras.

Asia - Regulación de Protección de Datos Personales en Japón: [13] la Ley de Protección de Datos Personales (APPI por sus siglas en inglés), promulgada en 2023, establece que su gestión y aplicación recae en la Comisión de Protección de Información Personal, ente legal independiente de los gobiernos, donde se reconoce la importancia de equilibrar la innovación tecnológica con la protección de la privacidad. La ley define la privacidad como el derecho de las personas a la autodeterminación informativa y establece principios para el manejo adecuado de la información personal, promoviendo la responsabilidad de las empresas en la protección de los datos de los individuos.

6.1.2 Introducción:

La privacidad de los datos en el contexto actual es un tema de gran relevancia. Cada día, de forma automatizada, nos vemos inmersos en numerosas actividades y transacciones donde compartimos nuestros datos personales con particulares, empresas privadas y entidades públicas. Entre estas actividades destaca nuestro uso diario de Internet, donde enviamos correos electrónicos, compartimos contenido en redes sociales, descargamos archivos, participamos en chats y discusiones en línea. Además, revelamos nuestros datos al utilizar el transporte público, al pagar con tarjeta, al inscribirnos en promociones o sorteos, al realizar compras en el supermercado, al unirnos a clubes, gimnasios o cursos, y al llevar a cabo trámites en entidades públicas o empresas, entre otros ejemplos.

6.1.3 Intimidad & Privacidad:

En general ambos temas en el lenguaje cotidiano pueden tratarse de manera indistinta, pero es importante diferenciarlos en especial en sus límites y alcances definidas en las leyes de cada país.

Intimidad: [13] Según la RAE: *Zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia.*

Refiere a la información que una persona no proporcionaría en ninguna circunstancia de forma libre y consciente. Esto resalta la sensibilidad y la relevancia de los datos que están vinculados con la esfera más íntima y personal de un individuo. Son derechos fundamentales, como la inviolabilidad de las comunicaciones y el derecho a la propia imagen, que están estrechamente ligados a la protección de la privacidad y la intimidad del individuo. Se pone de manifiesto la importancia de respetar y proteger estos derechos fundamentales en el tratamiento de los datos personales.

Privacidad: [14] Según la RAE *Ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión.*

Esta definición resalta la importancia del espacio personal y confidencial de una persona, donde se espera que esté protegida de intrusiones no deseadas. La privacidad incluye el control sobre la información personal, la intimidad en las relaciones y el derecho a mantener ciertos aspectos de la vida fuera del dominio público o de terceros no autorizados. Es un derecho fundamental que garantiza la autonomía y el respeto a la individualidad de cada persona.

Los tipos de datos personales pueden variar en función de su naturaleza y la forma en que se pueden utilizar para identificar o relacionarse con un individuo específico. Algunos ejemplos comunes incluyen:

Datos de identificación: Esto incluye información como el nombre completo, la fecha de nacimiento, el número de identificación (como el DNI o pasaporte), el género y la nacionalidad.

Datos de contacto: Pueden incluir direcciones de correo electrónico, números de teléfono, direcciones postales y detalles de redes sociales.

Datos de ubicación: Pueden proporcionar información sobre la ubicación física de una persona en un momento dado, ya sea a través del GPS de un dispositivo móvil o mediante la dirección registrada en documentos como facturas o formularios.

Datos biométricos: Incluyen características físicas únicas de una persona, como huellas dactilares, reconocimiento facial, características de voz o patrones de iris, que se utilizan para la autenticación y verificación de identidad.

Datos financieros: Esto abarca información sobre cuentas bancarias, tarjetas de crédito, historial crediticio, ingresos y gastos, así como cualquier otra información relacionada con transacciones financieras.

Datos de salud: Incluyen información médica y de salud, como historias clínicas, diagnósticos, tratamientos, alergias y medicamentos recetados.

Datos laborales: Proporcionan información sobre el empleo de una persona, como historial laboral, posición actual, salario, beneficios y cualquier otra información relacionada con el trabajo.

Datos educativos: Incluyen información sobre la educación y la formación de una persona, como instituciones educativas asistidas, títulos obtenidos, calificaciones académicas y cualquier otra información relevante relacionada con la educación.

6.1.4 Intimidad & Privacidad, según las leyes en Argentina.

Ley 25.326 [15] de Protección de Datos Personales: Sancionada: octubre 4 de 2000, algunos puntos importantes que la incluyen:

Definición de datos personales: Se considera como datos personales y establece que toda información relacionada con una persona física identificada o identificable se considera como datos personales.

Principios de protección de datos: La ley establece una serie de principios que deben cumplirse al tratar datos personales, incluyendo el consentimiento informado, la finalidad específica, la calidad de los datos, la seguridad, la confidencialidad, entre otros.

Derechos de los titulares de datos: Los ciudadanos tienen derecho a acceder, rectificar, actualizar y suprimir sus datos personales, así como a oponerse al tratamiento de los mismos en ciertas circunstancias.

Obligaciones de los responsables del tratamiento: Aquellas personas o entidades que recopilan, almacenan, procesan o utilizan datos personales deben cumplir con una serie de obligaciones, como informar adecuadamente a los titulares de los datos, adoptar medidas de seguridad adecuadas y obtener el consentimiento válido cuando sea necesario.

Transferencia internacional de datos: La ley regula la transferencia de datos personales fuera del territorio argentino, exigiendo que se cumplan ciertos requisitos para garantizar un nivel adecuado de protección de datos.

En 1994, con la reforma de la Constitución Nacional de Argentina, se introdujo el artículo 43, que habilita a los ciudadanos a ejercer la "acción de habeas data". Esta acción les permite conocer, rectificar o eliminar sus datos personales almacenados en registros públicos o privados, así como conocer la finalidad de su uso. En caso de falsedad o discriminación, los ciudadanos pueden exigir la supresión, rectificación, confidencialidad o actualización de sus datos.

El 15 de noviembre de 2017, la DNPDP fue transferida a la Agencia de Acceso a la Información Pública (AAIP) mediante la Decisión Administrativa N° 1002/2017 de la Jefatura de Gabinete de Ministros. La AAIP es un ente autárquico con autonomía funcional dentro de la órbita de la Jefatura de Gabinete de Ministros.

El Decreto 1558/2001 [16] complementa la Ley 25.326 de Protección de Datos Personales en el ámbito de la administración pública nacional. Establece la creación del Registro Nacional de Bases de Datos, la designación de un responsable de la Base de Datos en cada organismo público, y define obligaciones para estos responsables, como garantizar la seguridad de la información y facilitar el acceso de los titulares a sus datos.

El decreto también establece procedimientos para que los titulares ejerzan sus derechos sobre los datos personales almacenados en las bases de datos del gobierno. Su objetivo es asegurar el adecuado tratamiento y protección de la información personal de los ciudadanos por parte de las instituciones gubernamentales.

Normas constitucionales que protegen la privacidad y los datos personales: [17]

*Constitución Nacional. Art. 18 (Protección de la propiedad privada)

*Constitución Nacional Art. 19 (Principio de Reserva).

*Constitución Nacional Art. 43, párrafo 3° (Habeas Data. Agregado en 1994).

Otras normas o marcos sobre Privacidad:

ISO/IEC 27018:2019 - Código de Práctica para la protección de IPP en nubes públicas como procesadores de IPP.

ISO/IEC 27701:2019 – Gestión de la privacidad de la Información. (extensión de las 27001 y 27002)

ISO/IEC 27030 –Lineamientos para seguridad y privacidad en Internet de las Cosas (IoT)

ISO/IEC 27045 – Seguridad y Privacidad en los procesos de Big Data

ISO/IEC TR 27550:2019 – Ingeniería de Privacidad para los procesos del ciclo de vida de los sistemas.

ISO/IEC 27556 - Marco centrado en el usuario para manejo de información de identificación personal (IPP) basado en preferencias de privacidad.

ISO/IEC TS 27570 – Lineamientos de privacidad para Smart Cities.

ISO/IEC 29101:2018 - Marco de trabajo de arquitectura de Privacidad.

ISO/IEC 29134:2017 - Lineamientos para análisis de impacto para Privacidad (PIA).

NIST SP 800-53A Rev 5 - Evaluación de controles de seguridad y privacidad en sistemas y organizaciones de información federales: construcción de planes de evaluación efectivos.

NIST SP 800-144 – Guía de seguridad y privacidad en la nube.

PCI/DSS – Estándar de Seguridad de Datos para la industria de Tarjetas de Pago.

7. Ética y Ciberética:

También conocida como ética digital o ética cibernética, se refiere al conjunto de principios éticos y valores morales que guían el comportamiento y las decisiones relacionadas con el uso de la tecnología digital, la informática y los entornos en línea. La ciberética aborda cuestiones éticas y morales específicas que surgen en el ámbito de la cibernética y la interacción humana con la tecnología digital.

Estudia cuestiones morales, legales y sociales relacionadas con la cibertecnología. UNESCO la denomina Infoética

Algunos de los temas que la ciberética aborda incluyen la privacidad en línea, la seguridad de la información, la equidad en el acceso a la tecnología, la responsabilidad en el desarrollo y uso de algoritmos y sistemas de inteligencia artificial, así como la ética en la conducta en línea, como el ciberacoso y la manipulación de la información.

El impacto de la tecnología en nuestros sistemas morales, legales y sociales es profundo y continuamente evolutivo. Aquí se examinaremos tres aspectos:

7.1 Sistemas Morales:

Desafíos Éticos Emergentes: La tecnología plantea nuevos dilemas éticos, como la privacidad digital, la toma de decisiones algorítmica, la inteligencia artificial autónoma y la manipulación de la información. Las decisiones sobre cómo desarrollar y utilizar tecnologías avanzadas a menudo involucran cuestionamientos éticos sobre lo que es correcto, justo y aceptable en términos morales.

Cambio en las Normas Sociales: La tecnología puede influir en la evolución de las normas sociales, ya sea al aceptar prácticas previamente cuestionables (por ejemplo, compartir información personal en línea, potenciada por la creciente exposición en las redes sociales) o al generar nuevas preocupaciones éticas (como la creación de deepfakes).

7.2 Sistemas Legales:

Actualización de Leyes Existentes: Los avances tecnológicos a menudo requieren la actualización de leyes existentes para abordar nuevas realidades. La legislación de privacidad, por ejemplo, puede necesitar modificaciones para hacer frente a la recopilación masiva de datos y la vigilancia digital.

Creación de Nuevas Leyes: Problemas emergentes, como la ciberseguridad y la inteligencia artificial, pueden requerir la formulación de nuevas leyes para establecer límites y salvaguardias. Estas leyes buscan equilibrar la innovación tecnológica con la protección de los derechos y valores fundamentales.

7.3 Sistemas Sociales:

Impacto en la Interacción Humana: La tecnología influye en la forma en que las personas interactúan, desde las redes sociales hasta las relaciones laborales. La comunicación digital y la colaboración en línea han alterado las dinámicas sociales y han introducido desafíos en áreas como la ciberseguridad y el ciberacoso.

Brecha Digital y Desigualdades: La disponibilidad y acceso a la tecnología pueden exacerbar las brechas sociales y económicas. Las políticas relacionadas con la conectividad y la inclusión digital se han convertido en foco para abordar estas desigualdades.

7.4 Evaluación de Leyes y Políticas:

Agilidad Legal: La velocidad del avance tecnológico a menudo supera la capacidad de los sistemas legales para mantenerse al día (según la historia primero existió el delito seguido de la ley). Esto plantea la necesidad de leyes y políticas más ágiles y flexibles que puedan adaptarse rápidamente a los cambios tecnológicos (mitigar los grises y vacíos legales en constante evolución).

Protección de Derechos Fundamentales: Las leyes y políticas deben equilibrar la promoción de la innovación con la protección de los derechos fundamentales, como la privacidad, la libertad de expresión y la no discriminación.

Cooperación Internacional: Dada la naturaleza global de la tecnología, las leyes y políticas efectivas deben considerar la cooperación internacional para abordar problemas transfronterizos y garantizar estándares éticos comunes.

Ejemplo concreto: [18]

Un ejemplo interesante fue la denominada: “*A Rape in Cyberspace*” Una violación en el ciberespacio.

La nota del periodista Julian Dibbell, titulada "Una violación en el ciberespacio", es un relato fascinante que arroja luz sobre un incidente de violación cibernética que tuvo lugar en la comunidad virtual en marzo de 1993. Dibbell narra cómo este evento impactó no solo en la estructura técnica de los programas MUD (Multi-User Dungeon), sino también en la percepción de la comunidad virtual en sí misma.

El título sugiere una metáfora intrigante al comparar la violación en el ciberespacio con un acto físico. La elección de palabras destaca la gravedad y la

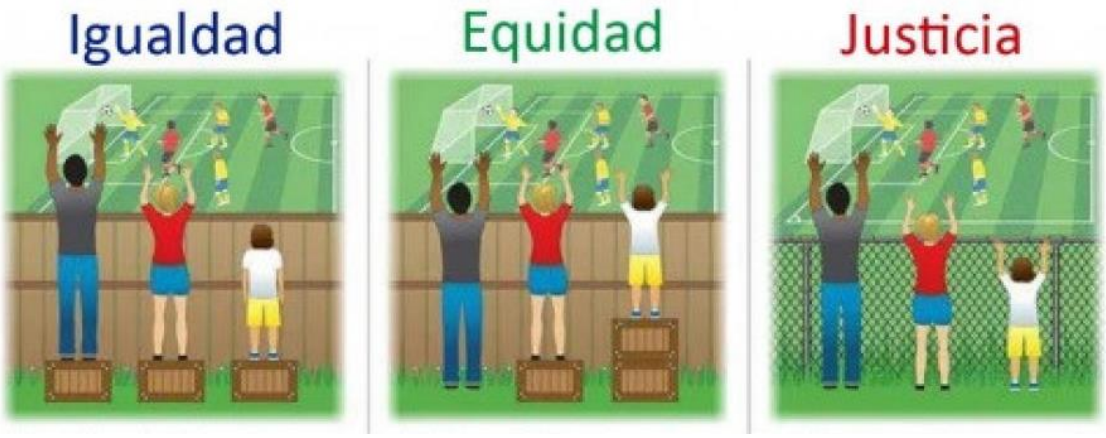
naturaleza invasiva del incidente, al tiempo que enfatiza la importancia del ciberespacio como un espacio virtual donde se pueden cometer delitos y violaciones que tienen consecuencias tangibles.

El hecho de que el evento ocurriera en 1993 subraya la novedad de los mundos virtuales en ese momento y cómo la comunidad estaba aún explorando y definiendo las reglas y normas éticas en este nuevo terreno. La descripción de las repercusiones en la comunidad virtual destaca la conexión emocional y social que las personas habían establecido en estos espacios digitales emergentes.

El cambio en el diseño del programa MUD como resultado directo de esta violación cibernética demuestra cómo los incidentes en el ciberespacio pueden tener impactos duraderos y motivar la evolución de las plataformas tecnológicas. La adaptación y mejora del diseño del programa MUD ilustra la capacidad de la comunidad virtual para aprender y ajustarse a medida que enfrenta desafíos y amenazas.

En última instancia, la nota de Julian Dibbell no solo ofrece una crónica detallada de un evento específico en la historia del ciberespacio, sino que también proporciona una ventana a la complejidad y la importancia de la vida digital y las interacciones humanas en entornos virtuales. La narrativa sirve como un recordatorio de la fragilidad y la resiliencia de las comunidades en línea, así como de la necesidad de abordar las cuestiones éticas y de seguridad en el siempre cambiante paisaje digital.

7.4.1 Justicia, equidad e igualdad:



La justicia es el principio moral y ético que busca la imparcialidad y la equidad en la distribución de derechos y recursos. Implica asegurar que cada individuo reciba lo que le corresponde de acuerdo con las normas y leyes establecidas, promoviendo la igualdad y el trato equitativo.

La equidad se refiere a la justicia distributiva que tiene en cuenta las circunstancias individuales y trata a las personas de manera justa, considerando sus necesidades, capacidades y contextos específicos. A diferencia de la igualdad, la equidad reconoce las disparidades y busca corregirlas para lograr resultados justos.

La igualdad se centra en el trato uniforme y la ausencia de discriminación. En un contexto social, implica garantizar que todos los individuos tengan los mismos derechos, oportunidades y acceso a recursos sin importar sus diferencias. La igualdad busca eliminar la discriminación y promover la justicia social.

7.4.2 STS (por sus siglas en inglés: ciencia y estudio de la tecnología o ciencia, tecnología y sociedad)

Este campo interdisciplinario examina la interacción compleja y bidireccional entre la ciencia, la tecnología y la sociedad, reconociendo que estos elementos no operan de manera aislada, sino que están intrínsecamente entrelazados y se influyen mutuamente.

Tres Errores que Deben Evitarse al Pensar sobre Tecnología (según la STS):

Determinismo Tecnológico:

Este error implica creer que la tecnología es autónoma y determina inevitablemente el curso de la sociedad. La STS destaca que la tecnología es moldeada por decisiones humanas y valores sociales, y no es un proceso inevitable e independiente.

Las tecnologías fueron desarrolladas en el seno de una sociedad con sus factores sociales e influenciadas por sus fuerzas. La sociedad y la tecnología se moldean mutuamente.

Rechace pensar en la tecnología como un objeto:

La tecnología no surge espontáneamente; es el producto de decisiones humanas deliberadas y ha sido influenciada por factores sociales. Es, en esencia, un producto de la sociedad y se desarrolla en el contexto social. Comprender que la tecnología no consiste simplemente en artefactos, sino en artefactos integrados en prácticas y valores sociales, es fundamental para percibir la estrecha relación entre ética y tecnología.

Rechace el hecho que la tecnología es neutral: [19]

La idea de que la tecnología es neutral, es decir, que no tiene ningún impacto social o ético inherente, es otro error que la STS busca rectificar. La tecnología lleva consigo valores y puede afectar de manera desigual a diferentes

grupos sociales, por lo que es esencial examinar sus implicaciones éticas y sociales.

Al no ser neutral, las decisiones que se toman al momento de crear tecnología conllevan ramificaciones sociales

7.4.3 Richard O. Mason principios PAPA. [20]

En el artículo "Four Ethical Issues of the Information Age", Richard O. Mason desarrolló y detalló los llamados principios PAPA, que son una serie de cuestiones éticas clave que deben abordarse en la era de la información. Seguridad.

Privacidad (P de PAPA): La tecnología de la información ha llevado a una mayor recopilación, almacenamiento y análisis de datos personales. El principio de Privacidad se centra en cómo se manejan y protegen estos datos, abordando cuestiones como la vigilancia masiva, la venta de datos y la privacidad en línea.

¿Qué información sobre uno mismo o las asociaciones que uno posee debe revelarse a otros, en qué condiciones y con qué salvaguardas? ¿Qué cosas pueden las personas mantener en secreto y no ser obligadas a revelar a los demás?

Acceso (A de PAPA): El acceso equitativo a la información y a la tecnología es un tema importante. La brecha digital, que se refiere a las disparidades en el acceso a la tecnología y la información entre diferentes grupos socioeconómicos, culturas y regiones, es un aspecto central del principio de Acceso.

Propiedad (P de PAPA): El principio de Propiedad se refiere a la cuestión de quién posee y controla la información y la tecnología. Esto aborda temas como los derechos de autor, la propiedad intelectual, la piratería y la distribución justa de los beneficios derivados de la innovación tecnológica.

Accuracy/Precisión (A de PAPA): La confiabilidad y la precisión de la información en la era de la información son esenciales. La propagación de

noticias falsas, la desinformación y la manipulación de datos plantean preocupaciones éticas relacionadas con la precisión de la información disponible en línea. ¿Quién es responsable de la autenticidad, fidelidad y exactitud de la información? De manera similar, ¿a quién se le debe responsabilizar por los errores en la información y cómo se va a compensar a la parte lesionada?

7.4.4 Eticistas versus Moralistas:

Los eticistas se centran en el estudio sistemático y teórico de la ética. Su enfoque tiende a ser más abstracto y académico, analizando principios éticos universales que pueden aplicarse en diversas situaciones. Los eticistas buscan desarrollar teorías éticas y marcos conceptuales que guíen la toma de decisiones éticas en general, independientemente de las circunstancias específicas o las culturas. Los Eticistas estudian la moral desde la perspectiva de la metodología filosófica; utilizan argumentos lógicos para justificar sus posturas. Están abiertos a cada lado en una disputa.

Los moralistas, por otro lado, se enfocan más en la aplicación práctica de la moral en situaciones específicas. Están interesados en las reglas y normas morales concretas que rigen el comportamiento en contextos particulares. Los moralistas tienden a ser más prácticos y pueden basar sus decisiones éticas en las normas sociales, las creencias culturales o religiosas, y las circunstancias específicas de una situación. Muchos moralistas han sido descriptos también como “sermoneadores” y “críticos”.

7.4.5 Absolutismo moral y Objetivismo moral

Son dos enfoques filosóficos en ética que comparten algunas similitudes, pero que también tienen diferencias clave en su comprensión de la moralidad. Aquí hay una explicación breve de cada uno:

El absolutismo moral sostiene que existen normas morales universales y objetivas que son aplicables en todas las situaciones, independientemente del

contexto o las circunstancias. Estas normas son consideradas como absolutas e inmutables, y no están sujetas a negociación o relativización. Los absolutistas morales argumentan que ciertas acciones son inherentemente correctas o incorrectas, sin importar el resultado o las intenciones de dichas acciones. Un ejemplo común de absolutismo moral es la creencia en que el asesinato siempre es moralmente incorrecto, sin excepciones.

Desde una perspectiva absolutista moral, la instalación y uso de cámaras de vigilancia podrían considerarse moralmente aceptables o moralmente inaceptables en todos los casos, independientemente del contexto. Por ejemplo, un absolutista moral podría argumentar que la invasión de la privacidad inherente al monitoreo constante a través de cámaras de vigilancia es siempre incorrecta, sin importar las circunstancias, ya que viola un principio ético absoluto de respeto a la privacidad individual.

El objetivismo moral es una posición filosófica que sostiene que existen verdades morales objetivas y universales que pueden ser descubiertas mediante la razón y la observación. Sin embargo, a diferencia del absolutismo moral, los objetivistas morales reconocen la posibilidad de que las normas éticas puedan tener cierta flexibilidad o adaptabilidad en función del contexto o las circunstancias particulares. Aunque las normas morales objetivas existen, pueden aplicarse de manera diferente en diferentes situaciones sin comprometer su validez objetiva. El objetivismo moral está asociado principalmente con la filosofía de Ayn Rand y su sistema ético conocido como objetivismo, que defiende la idea de que el individuo tiene derechos naturales y que el egoísmo racional es la base de una moralidad objetiva.

Desde una perspectiva objetivista moral, la instalación y uso de cámaras de vigilancia podrían ser evaluados en función de principios éticos objetivos, pero con consideración a las circunstancias particulares. Por ejemplo, un objetivista moral podría argumentar que el uso de cámaras de vigilancia en áreas públicas para garantizar la seguridad ciudadana puede ser moralmente justificado, ya que protege los derechos de las personas a la seguridad y el bienestar, siempre y

cuando se respeten ciertos límites y principios, como la proporcionalidad y la transparencia en su aplicación.

8. ISO [21]

La ISO (International Organization for Standardization) es una organización internacional independiente que establece estándares en diversos campos, desde tecnología hasta gestión de calidad, medio ambiente, seguridad, entre otros. Fundada en 1947, la ISO tiene su sede en Ginebra, Suiza, y cuenta con la participación de representantes de más de 160 países.

Los estándares de la ISO son documentos que especifican requisitos, lineamientos, procesos o características que buscan garantizar la calidad, seguridad, eficiencia y compatibilidad en una amplia gama de productos, servicios y sistemas. Estos estándares son utilizados por organizaciones, empresas, gobiernos y otras entidades para mejorar sus procesos, productos y servicios, así como para facilitar la interoperabilidad y el intercambio comercial a nivel internacional.

8.1 ISO/CEI 27001:2022

Esta norma proporciona una visión general de las normas que componen la serie 27001, es un estándar internacional que establece los requisitos para un sistema de gestión de seguridad de la información (SGSI). Publicado por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC), este estándar proporciona un marco integral para ayudar a las organizaciones a proteger la información de manera efectiva y gestionar los riesgos de seguridad de la información.

8.1.1 Contexto de la organización.

Se refiere a uno de los elementos fundamentales en la implementación exitosa de un Sistema de Gestión de Seguridad de la Información (SGSI). Específicamente, se trata de comprender y establecer el entorno en el que opera la organización, así como los factores internos y externos que pueden influir en la seguridad de la información.

8.1.2 Liderazgo

Es un elemento fundamental para el éxito en la implementación y mantenimiento de un Sistema de Gestión de Seguridad de la Información (SGSI). El liderazgo en este contexto implica el compromiso y la participación activa de la alta dirección en la promoción de la seguridad de la información en toda la organización.

8.1.3 Planificación.

Es un proceso esencial en la implementación y mantenimiento de un Sistema de Gestión de Seguridad de la Información (SGSI). La planificación en este contexto implica la identificación, evaluación y tratamiento de los riesgos de seguridad de la información, así como el establecimiento de objetivos y procesos para lograrlos.

8.1.4 Soporte

Se refiere a uno de los elementos clave necesarios para la implementación y mantenimiento efectivo de un Sistema de Gestión de Seguridad de la Información (SGSI). El soporte aborda la importancia de proporcionar los recursos, competencia, toma de conciencia y comunicación necesarios para

garantizar el funcionamiento adecuado del SGSI y el cumplimiento de los objetivos de seguridad de la información.

8.1.5 Operación.

Uno de los elementos clave necesarios para la implementación y mantenimiento efectivo de un Sistema de Gestión de Seguridad de la Información (SGSI). La operación aborda la ejecución de actividades y procesos relacionados con la seguridad de la información en el día a día de la organización.

8.1.6 Evaluación de desempeño.

Es un proceso crítico que forma parte del ciclo de mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI). Esta evaluación se realiza para medir la efectividad del SGSI y para identificar oportunidades de mejora.

8.1.7 Mejora

Es un principio fundamental que implica un compromiso continuo con la optimización y el perfeccionamiento del Sistema de Gestión de Seguridad de la Información (SGSI). La mejora continua es un ciclo que involucra la identificación de áreas de mejora, la implementación de acciones correctivas y preventivas, y la revisión regular del desempeño del SGSI para evaluar la eficacia de las mejoras realizadas.

8.1.8 Referencia de controles de seguridad de la información

Controles organizacionales: 37 controles

Cada categoría incluye varios controles específicos que una organización puede implementar para abordar los riesgos relacionados con esa área particular. En total, hay 37 controles organizacionales enumerados en ISO/IEC 27001. Estos controles proporcionan un marco sólido para establecer y mantener un SGSI efectivo y ayudan a las organizaciones a proteger sus activos de información de manera integral y sistemática.

Controles de personas: 8 controles.

Están diseñados para abordar aspectos específicos de la seguridad de la información relacionados con el factor humano. Estos controles están destinados a garantizar que el personal de la organización esté adecuadamente capacitado, consciente y comprometido con las prácticas de seguridad de la información.

Controles físicos: 14 controles

Se refieren a las medidas de seguridad diseñadas para proteger los recursos físicos de una organización, como los edificios, las instalaciones, los equipos y los soportes de almacenamiento de información, contra amenazas físicas. Estos controles tienen como objetivo garantizar la integridad, la disponibilidad y la confidencialidad de los activos físicos y la información que contienen.

Controles tecnológicos: 34 controles

Destinados a abordar aspectos específicos de la seguridad de la información relacionados con sistemas y tecnologías. Estos controles se centran en proteger los activos de información a través de medidas técnicas y tecnológicas.

8.2 IS0/IEC 27002 Third edition 2022-02

La norma ISO 27001:2022 ha sido actualizada con cambios mínimos en sus cláusulas, manteniendo su estructura y enfocándose en los controles de seguridad. Sin embargo, el verdadero cambio se encuentra en el Anexo A, donde se presenta la norma ISO 27002:2022. Esta versión ha simplificado los dominios y controles, adoptando un enfoque preventivo/detectivo con énfasis en la seguridad de la información.

La ISO 27002:2022 ahora contiene 4 temas y 93 controles, con una reducción aparente, pero en realidad se han reorganizado y fusionado los controles existentes, además de agregar 11 controles completamente nuevos. Se destaca la importancia de los controles organizacionales y del talento humano, reconociendo que el factor humano es crucial en la seguridad de la información.

Esta nueva versión de la norma también aborda preocupaciones previas, como la falta de definición de los tipos de control y sus impactos en la seguridad de la información. Además, incluye conceptos reconocidos de ciberseguridad del framework NIST y hace hincapié en las capacidades operacionales de la organización, así como en el análisis de riesgos de seguridad. Los 11 nuevos controles se centran en la ciberseguridad y la resiliencia organizacional, abordando temas como la seguridad en la nube y el monitoreo de la seguridad física. [22] [23] [24]

ISO 27002:2022	CONTROLES
A.5 Organización	37
A.6 Personas	8
A.7 Objetos físicos	14
A.8 Tecnología	34
Total, Controles	**93**

8.3 IS0/IEC 27005 (Risk Management of Information Security)

Al aplicar ISO/IEC 27005 a la gestión de videovigilancia, las organizaciones pueden mejorar la seguridad de la información relacionada con las mismas, protegiendo así la privacidad y la integridad de los datos de video y reduciendo los riesgos asociados con el uso de sistemas de videovigilancia.

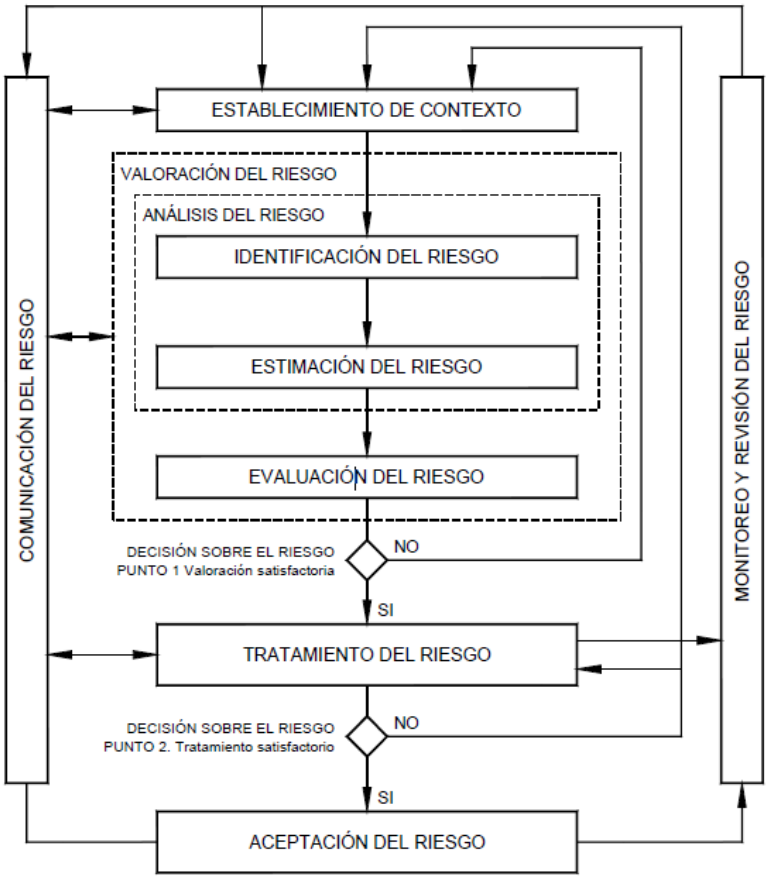
ISO/IEC 27005 es una norma internacional que proporciona directrices para la gestión de riesgos de seguridad de la información. Aplicar ISO/IEC 27005 a la gestión de videovigilancia implica seguir un proceso estructurado para identificar, analizar y tratar los riesgos relacionados con la seguridad de la información en el contexto específico de la videovigilancia.

La Gestión de Riesgos de Seguridad de la Información según la norma ISO/IEC 27005 ofrece varias ventajas significativas para las organizaciones que desean proteger sus activos informáticos y garantizar la continuidad del negocio. Proporciona un enfoque sistemático y estructurado para identificar, analizar y tratar los riesgos de seguridad de la información. Esto permite a las organizaciones gestionar sus riesgos de manera proactiva en lugar de reaccionar a incidentes una vez que ocurren.

No es la intensión desarrollar la norma en profundidad, simplemente se menciona en un resumen la actividad de la gestión de riesgo:

Proceso de SGSI	Proceso de gestión del riesgo en la seguridad de la información
Planificar	Establecer el contexto Valoración del riesgo Planificación del tratamiento del riesgo Aceptación del riesgo
Hacer	Implementación del plan de tratamiento del riesgo
Verificar	Monitoreo y revisión continuos de los riesgos
Actuar	Mantener y mejorar el proceso de gestión del riesgo en la seguridad de la información

Visión general del proceso de gestión de riesgo.



8.4ISO 9001 (Quality management systems)

La norma ISO 9001 es un estándar internacional que establece los requisitos para un sistema de gestión de calidad (SGC). Se centra en garantizar que una organización pueda proporcionar productos y servicios consistentes que cumplan con los requisitos del cliente y las regulaciones aplicables, al tiempo que busca mejorar continuamente su desempeño.

Al implementar la norma ISO 9001 en un sistema de videovigilancia, se pueden obtener varias ventajas:

- Mejora de la calidad del servicio:

Al seguir los requisitos, se establecen procesos robustos que aseguran la calidad y consistencia de los servicios de videovigilancia ofrecidos por la organización.

- Cumplimiento de los requisitos del cliente:

Enfatiza la importancia de comprender y satisfacer los requisitos del cliente. Esto significa que el sistema de videovigilancia estará alineado con las expectativas y necesidades de los clientes.

- Procesos eficientes y efectivos:

Su implementación requiere la identificación y optimización de procesos claves. Esto puede llevar a una mayor eficiencia en la operación del sistema de videovigilancia y a una mejor utilización de los recursos.

- Enfoque en la mejora continua:

Promueve la mejora continua como parte integral del sistema de gestión de calidad. Esto significa que el sistema de videovigilancia estará constantemente siendo evaluado y mejorado para satisfacer mejor las necesidades del cliente y adaptarse a los cambios en el entorno operativo.

- Mayor confianza del cliente:

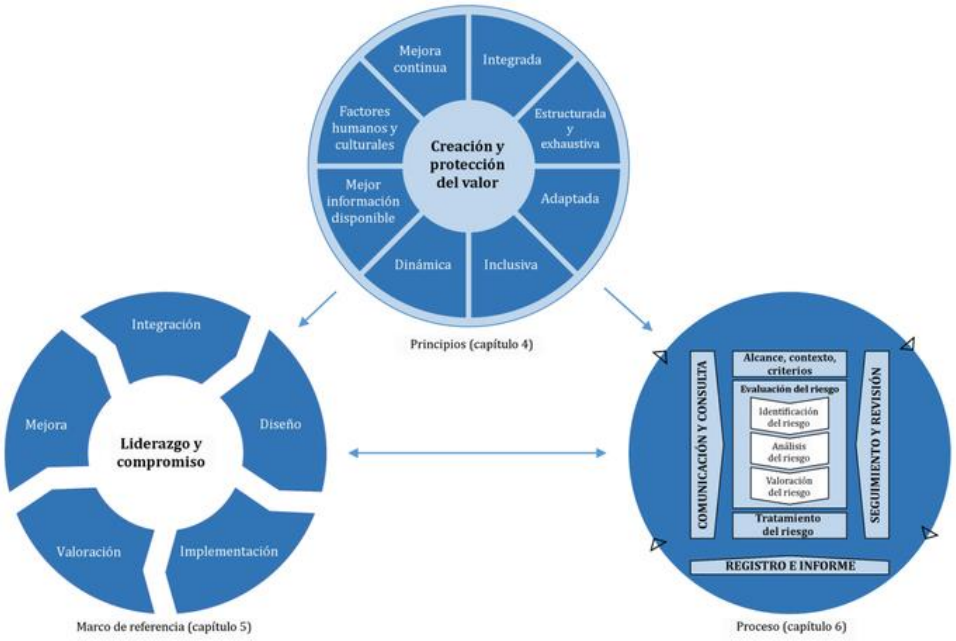
La certificación ISO 9001 puede aumentar la confianza del cliente en el sistema de videovigilancia, ya que demuestra el compromiso de la organización con la calidad y la mejora continua.

Es relevante mencionar que existen empresas de videovigilancia en la Argentina quienes obtuvieron la certificación ISO 9001.

8.5 ISO 31000: 2018 Gestión del riesgo — Directrices

Establece los principios, el marco y los procesos para la gestión de riesgos en cualquier tipo de organización. Se centra en identificar, evaluar y tratar los riesgos de manera sistemática y efectiva para mejorar la toma de decisiones y lograr los objetivos de la organización.

Principios, marco de referencia y proceso [25]



Al implementar la norma ISO 31000:2018 en un sistema de videovigilancia, se pueden obtener varias ventajas:

- Identificación de riesgos:

Permite identificar los riesgos potenciales asociados con el sistema de videovigilancia, como la pérdida de datos, el acceso no autorizado o el mal funcionamiento de equipos.

- Análisis de riesgos:

Facilita el análisis detallado de los riesgos identificados, evaluando su probabilidad de ocurrencia y su impacto potencial en el sistema de videovigilancia y en la organización en general.

- Tratamiento de riesgos:

Ayuda a desarrollar e implementar medidas de control y estrategias de mitigación para gestionar los riesgos de manera efectiva, reduciendo su probabilidad o impacto negativo.

- Mejora de la toma de decisiones:

Proporciona una base sólida para la toma de decisiones informadas sobre la gestión de riesgos en el sistema de videovigilancia, ayudando a priorizar acciones y asignar recursos de manera más eficiente.

- Mejora continua:

Promueve la mejora continua al incorporar la revisión y la retroalimentación en el proceso de gestión de riesgos, permitiendo a la organización adaptarse a los cambios en el entorno y a nuevas amenazas o vulnerabilidades.

- Cumplimiento normativo:

Ayuda a cumplir con los requisitos legales y regulatorios relacionados con la seguridad y la protección de datos en el contexto de la videovigilancia, reduciendo el riesgo de sanciones y litigios.

9. Protección y custodia de imágenes.

9.1 Vulnerabilidades en dispositivos de videovigilancia.

Las vulnerabilidades en dispositivos de videovigilancia con IA son fallas de seguridad que pueden ser explotados para acceder o manipular cámaras y sistemas de vigilancia. Estas debilidades pueden conducir a la filtración de datos sensibles o el acceso no autorizado a la red, lo que destaca la necesidad de medidas de seguridad sólidas. Algunos casos reales de accesos no autorizados.

En Abril 2024, Hackers difunden más de 200 vídeos sexuales grabados con las cámaras de seguridad de las viviendas en la Región de Murcia. [26]

En marzo de 2021 un grupo de hackers tuvo acceso a 150 mil cámaras de seguridad: espiaron a Tesla y a otras empresas, hospitales y cárceles [27]

Según detalla informe de Fortinet:

10 de mayo de 2018: Los clientes de Fortinet permanecen protegidos por la firma IPS para bloquear intentos de ataque relacionados con dispositivos TBK DVR vulnerables. (CVE-2018-9995)

1 de mayo de 2023: Con decenas de miles de DVR TBK disponibles bajo diferentes marcas, código PoC disponible públicamente y fácil de explotar, esta vulnerabilidad es un objetivo fácil para los atacantes. El reciente aumento en las detecciones de IPS muestra que los dispositivos con cámaras de red siguen siendo un objetivo popular para los atacantes. FortiGuard Labs no tiene conocimiento de ningún parche proporcionado por el proveedor y recomienda a las organizaciones que revisen los modelos instalados de sistemas de cámaras CCTV y equipos relacionados para detectar modelos vulnerables.

Según un aviso emitido por FotiGuard Labs, un atacante puede utilizar esta falla operando de manera remota activando un exploit enviado a la cookie maliciosa para omitir la autenticación y obtener privilegios elevados, accediendo así a las transmisiones de video de la cámara.

Los productos afectados, según FotiGuard Labs son: DVR4104 y DVR4216 que también se renombran como CeNova, DVR Login, HVR Login, MDVR Login, Night OWL, Novo, QSee, Pulnix, Securus y XVR 5 en 1. [28]

Otro caso notorio fue el informado el noviembre 2023 en Ekoparty por los especialistas en ciberseguridad Octavio Gianatiempo & Javier Aguinaga, han descubierto dos vulnerabilidades de LAN RCE en la implementación del protocolo de búsqueda de dispositivos activos (SADP) y el servidor SDK de Hikvision que se encuentran en varios productos Ezviz (CVE-2023-34551 y CVE-2023-34552) productos muy vendidos en nuestro país. Al explotar cualquiera de estos errores, lograron brindarle a la víctima un flujo arbitrario al canalizar su conexión con la cámara a un servidor controlado por el atacante y dejar todas las demás funciones de la cámara operativas.

Las mismas permiten tomar control total de la cámara desde la red local cableada o Wi-Fi a la cual se conecta. Una vez que un atacante toma control de la cámara, estaría en condiciones de hacer lo que desee. [29]

Al ser expuesta la vulnerabilidad, la empresa Ezviz publica los parches de seguridad, [30]

El parche publicado por Ezviz resuelve el primer parte del problema de seguridad, en la teoría, pero en la práctica podríamos preguntarnos: ¿cuántos usuarios realmente lo llevan a cabo? La toma de conciencia y las buenas prácticas de seguridad, sin dudas, es parte de la solución para resolver la segunda parte del problema.

9.2 Confidencialidad, Integridad y Disponibilidad.

En el contexto de la videovigilancia, la integridad, la disponibilidad y la confidencialidad son aspectos fundamentales de la seguridad de la información que deben ser protegidos para garantizar un sistema de videovigilancia eficaz y seguro. Describo estos principios y cómo se aplican en el contexto de la videovigilancia:

Integridad: Se refiere a la garantía de que los datos no han sido modificados de manera no autorizada, ya sea durante la captura, el almacenamiento o la transmisión. En el contexto de la videovigilancia, la integridad asegura que las grabaciones de vídeo no hayan sido alteradas o manipuladas de ninguna manera. Para proteger la integridad de las grabaciones de vídeo, se pueden emplear técnicas como el cifrado de datos, la firma digital y el control de acceso para prevenir modificaciones no autorizadas.

Disponibilidad: Se refiere a la garantía de que los datos están disponibles y accesibles cuando se necesitan. En el contexto de la videovigilancia, la disponibilidad implica que las cámaras de seguridad estén operativas y que las grabaciones de vídeo estén disponibles para su visualización cuando sea necesario, ya sea en tiempo real o después de un incidente. Para garantizar la disponibilidad de las grabaciones de vídeo, se deben implementar medidas de seguridad física, redundancia de sistemas y copias de seguridad regulares.

Confidencialidad: Se refiere a la protección de la información sensible contra accesos no autorizados. En el contexto de la videovigilancia, la confidencialidad implica proteger las grabaciones de vídeo de acceso no autorizado para evitar la divulgación de información sensible o privada. Para proteger la confidencialidad de las grabaciones de vídeo, se pueden emplear técnicas como el cifrado de datos, la autenticación de usuarios y el control de acceso basado en roles.

9.2.1 Contraseñas seguras

Componente vital de la seguridad de la información en cualquier organización. Esta política establece las pautas y requisitos para la creación, gestión y uso de contraseñas por parte de los empleados y usuarios autorizados. Aquí hay algunas prácticas comunes que suelen incluirse en una política de contraseñas seguras:

Longitud y complejidad: Se debe especificar una longitud mínima de contraseña y requerir que las contraseñas sean lo suficientemente complejas, con una combinación de letras mayúsculas y minúsculas, números y caracteres especiales. Se recomienda una longitud mínima de al menos 8 caracteres, pero preferiblemente más.

Cambio periódico: Se puede requerir que los usuarios cambien sus contraseñas periódicamente, por ejemplo, cada 90 días. Esto ayuda a mitigar el riesgo de que las contraseñas se vean comprometidas debido a la exposición prolongada.

Restricciones de reutilización: Se debe establecer una política que prohíba a los usuarios reutilizar contraseñas antiguas al momento de cambiarlas. Esto evita que los usuarios utilicen contraseñas comprometidas previamente o fácilmente adivinables.

Evitar información personal: Se debe instruir a los usuarios a no utilizar información personal fácilmente identificable en sus contraseñas, como nombres propios, fechas de nacimiento, números de identificación, etc.

Protección de contraseñas: Se debe enfatizar la importancia de proteger las contraseñas de forma segura, evitando compartirlas con otros, almacenarlas en lugares no seguros o escribirlas en lugares fácilmente accesibles.

Autenticación multifactorial: Se puede recomendar o requerir la autenticación multifactorial siempre que sea posible, para agregar una capa adicional de seguridad más allá de las contraseñas tradicionales.

Educación y concienciación: Es crucial proporcionar capacitación regular sobre buenas prácticas de seguridad de contraseñas y concientizar a los usuarios sobre la importancia de mantener contraseñas seguras.

Uso de herramientas de gestión de contraseñas: Se puede alentar a los usuarios a utilizar herramientas de gestión de contraseñas para generar y almacenar contraseñas de forma segura.

Auditorías y cumplimiento: Se deben realizar auditorías periódicas para garantizar el cumplimiento de la política de contraseñas y tomar medidas correctivas si se identifican violaciones o debilidades en la implementación.

Actualizaciones regulares: La política de contraseñas debe revisarse y actualizarse periódicamente para mantenerse al día con las mejores prácticas de seguridad y los cambios en el panorama de amenazas.

9.2.2 Encriptado del tráfico

El cifrado del tráfico de videovigilancia es una medida crucial para garantizar la confidencialidad e integridad de los datos transmitidos a través de la red. Describo algunas consideraciones y mejores prácticas para el cifrado del tráfico de videovigilancia:

Protocolos de cifrado seguros: Se deben utilizar protocolos de cifrado seguros como TLS (Transport Layer Security) o su predecesor SSL (Secure Sockets Layer) para proteger la comunicación entre las cámaras de videovigilancia y los dispositivos receptores o servidores de almacenamiento.

Certificados SSL/TLS válidos: Todos los dispositivos involucrados en la comunicación estén utilizando certificados SSL/TLS válidos emitidos por una

autoridad de certificación confiable. Esto ayuda a prevenir ataques de tipo "man-in-the-middle" y garantiza la autenticidad de las conexiones.

Firmware actualizado: Mantener actualizado el firmware de las cámaras de videovigilancia y otros dispositivos relacionados para asegurarte de que se beneficien de las últimas mejoras de seguridad y correcciones de vulnerabilidades.

Implementación de VPN: Considerar el uso de una red privada virtual (VPN) para establecer una conexión segura y cifrada entre las cámaras de videovigilancia y el servidor de almacenamiento centralizado. Esto proporciona un túnel seguro a través del cual se puede transmitir el tráfico de videovigilancia.

Segmentación de la red: Separar la red de videovigilancia de otras redes corporativas o de uso general mediante la segmentación de la red. Esto reduce la superficie de ataque y limita la exposición de las cámaras de videovigilancia a posibles amenazas internas.

Autenticación de dispositivos: Implementar medidas de autenticación robustas para garantizar que solo los dispositivos autorizados puedan acceder y transmitir datos a través de la red de videovigilancia.

Monitorización de tráfico: Implementar herramientas de monitorización de tráfico para detectar actividades anómalas o sospechosas en la red de videovigilancia y tomar medidas correctivas rápidas en caso de intrusión o compromiso de seguridad.

Cifrado de almacenamiento: Además de cifrar el tráfico en tiempo real, también es importante cifrar los datos almacenados en el servidor de almacenamiento para protegerlos en reposo contra accesos no autorizados.

9.2.3 Cifrado de los archivos de video vigilancia final

Los archivos finales de imágenes de videovigilancia es una práctica importante para garantizar la seguridad de los datos almacenados y proteger la privacidad de las personas grabadas. Aquí hay algunas consideraciones y mejores prácticas para implementar el cifrado de archivos finales de imágenes de videovigilancia:

Algoritmos de cifrado robustos: Utilizar algoritmos de cifrado robustos y ampliamente reconocidos, como AES (Advanced Encryption Standard), para cifrar los archivos de imágenes. Asegúrate de utilizar longitudes de clave suficientemente largas para proporcionar una seguridad adecuada.

Claves de cifrado seguras: Gestionar de forma segura las claves de cifrado utilizadas para proteger los archivos de imágenes. Emplea prácticas sólidas de gestión de claves, como el almacenamiento seguro de claves y el uso de protocolos seguros para la distribución de claves.

Cifrado de extremo a extremo: Implementar el cifrado de extremo a extremo para garantizar que los archivos de imágenes estén cifrados desde el momento en que se capturan hasta que se almacenan y se accede a ellos. Esto protege los datos en todo su ciclo de vida.

Integridad de los datos: Considerar el uso de funciones de resumen (hashing) para verificar la integridad de los archivos de imágenes cifrados. Esto ayuda a detectar cualquier modificación no autorizada en los datos cifrados.

Seguridad en el almacenamiento: Asegurarse de que los archivos de imágenes cifrados se almacenen en ubicaciones seguras, utilizando medidas adicionales como el cifrado de almacenamiento en reposo y el acceso basado en roles para proteger los datos contra accesos no autorizados.

Autenticación y autorización: Implementar controles de autenticación y autorización para garantizar que solo usuarios autorizados puedan acceder a los archivos de imágenes cifrados. Utilizar políticas de acceso basadas en roles para limitar el acceso a la información sensible.

Auditoría y seguimiento: Establecer mecanismos de auditoría y seguimiento para registrar y supervisar el acceso a los archivos de imágenes cifrados, así como cualquier actividad relacionada con la gestión de claves y la administración de usuarios.

Formación y concienciación: Proporcionar formación y concienciación regular a los empleados sobre las mejores prácticas de seguridad en la gestión y protección de datos cifrados, incluidos los archivos de imágenes de videovigilancia.

9.2.4 Seguridad en el tráfico LAN (Red de Área Local)

Es esencial para proteger los datos, garantizar la disponibilidad de los recursos de red y mitigar una variedad de amenazas, tanto internas como externas. Es un componente fundamental de la estrategia general de seguridad de la red de cualquier organización.

Utilizar SSL (Secure Sockets Layer) es una excelente medida para asegurar la comunicación entre dispositivos en una red local (LAN), como en el caso de un DVR (Digital Video Recorder). SSL proporciona cifrado de extremo a extremo, lo que significa que los datos enviados entre el DVR y los dispositivos que lo acceden están protegidos contra la interceptación de terceros.

Pasos para implementar SSL en el acceso al DVR desde la LAN

Se debe obtener un certificado SSL válido para el DVR. Si el DVR tiene un servidor web incorporado para acceder a la interfaz de usuario, hay que configurarlo para que utilice el certificado SSL. Esto implica configurar el servidor web para que acepte conexiones SSL y proporcione el certificado SSL al cliente.

Acceso seguro desde dispositivos de la LAN: Una vez que el servidor web del DVR fue configurado para SSL, los dispositivos en la LAN pueden acceder al DVR utilizando una URL segura que comience con "https://" en lugar de "http://".

Asegurarse de mantener el certificado SSL actualizado y gestionar adecuadamente las claves privadas asociadas. Esto incluye renovar el certificado antes de que caduque y proteger las claves privadas para evitar accesos no autorizados.

Al implementar SSL en el acceso al DVR desde la LAN, se protege la información transmitida entre los dispositivos y el DVR de posibles ataques de intermediarios, como el ataque de Man-in-the-Middle (MITM). Esto ayuda a garantizar la privacidad y seguridad de los datos mientras se accede al DVR dentro de la red local.

9.2.5 Uso de doble factor

La implementación de autenticación de doble factor (2FA) para acceder al DVR dentro de la red local añade una capa adicional de seguridad. Esto implica requerir dos formas de verificación para el acceso, como una contraseña junto con un código único enviado al teléfono móvil. Es esencial configurar y educar a los usuarios sobre su uso adecuado, y monitorear su efectividad regularmente para mantener la seguridad de la red local y proteger los datos del DVR contra accesos no autorizados.

9.2.6 Copia de seguridad y prueba de restauración

Son procesos críticos para garantizar la integridad y disponibilidad de los datos de video. Los procesos para su implementación podrían ser:

- Programación de copias de seguridad:

Establecer un horario regular para realizar copias de seguridad de los videos del sistema de videovigilancia. Esto puede ser diario, semanal o según la cantidad de datos que se generen y la importancia de los videos.

- Selección del método de copia de seguridad:

Decidir el método de copia de seguridad que mejor se adapte a la organización y sus recursos. Se podría utilizar almacenamiento en la nube, dispositivos de almacenamiento externo (como discos duros externos o unidades USB), servidores de archivos en red u otros dispositivos de almacenamiento local.

- Prueba de restauración regular:

Realizar pruebas periódicas de restauración para asegurarse de que las copias de seguridad sean exitosas y los videos se puedan recuperar correctamente en caso de necesidad. Esto implica restaurar una muestra representativa de videos de diferentes fechas y horas para verificar su integridad y accesibilidad.

- Verificación de la integridad de los archivos:

Antes de realizar una copia de seguridad, verifica la integridad de los archivos de video para asegurarse de que no estén corruptos. También se puede utilizar herramientas de verificación de integridad de archivos después de realizar la copia de seguridad para garantizar que los videos se hayan guardado correctamente.

- Seguridad de las copias de seguridad:

Hay que asegurarse de que las copias de seguridad estén protegidas adecuadamente contra accesos no autorizados. Utilizar cifrado para proteger los

datos sensibles y limitar el acceso a las copias de seguridad solo a personal autorizado.

- Documentación y seguimiento:

Llevar un registro de las copias de seguridad realizadas y las pruebas de restauración realizadas, incluyendo fechas, resultados y cualquier problema encontrado durante el proceso. Esto ayudará a mantener un registro claro y facilitará la resolución de problemas en caso de alguna falla.

10. Equipamientos de sistemas de videovigilancia con IA

10.1 Consideraciones al elegir un sistema de video vigilancia.

Al elegir una cámara de vigilancia con inteligencia artificial (IA), es importante considerar varios aspectos para asegurarse de que se adapte a las necesidades buscadas.

- Funcionalidades de IA:

Elegir las cámaras que ofrezcan funciones de IA específicas que se alineen a las necesidades de seguridad. Por ejemplo, algunas cámaras pueden ofrecer detección de movimiento avanzada, reconocimiento facial, seguimiento de objetos, análisis de comportamiento, o detección de intrusiones.

- Calidad de imagen:

Asegurarse que la cámara de vigilancia ofrezca una alta resolución de imagen y una buena calidad de video, ya que esto es crucial para capturar detalles importantes. La capacidad de grabación en alta definición (HD) o incluso en resolución 4K es una ventaja.

- Rango de visión nocturna:

La capacidad de la cámara para capturar imágenes claras en condiciones de poca luz o completa oscuridad es esencial. Hay que considerar aquellas cámaras con tecnología de visión nocturna de alta calidad que utilicen infrarrojos u otras tecnologías para mejorar la visibilidad en la oscuridad.

- Facilidad de instalación y configuración:

Optar siempre por cámaras que sean fáciles de instalar y configurar, preferiblemente con opciones de conexión inalámbrica que simplifiquen la instalación y reduzcan los costos de cableado.

Escalabilidad y compatibilidad con otros dispositivos y sistemas:
Asegurarse de que la cámara de vigilancia sea compatible con otros dispositivos y sistemas de seguridad que puedas tener en tu hogar o negocio. Esto puede incluir sistemas de alarma, cerraduras inteligentes, o software de gestión de video.

- Almacenamiento de datos:

Considerar cómo se almacenarán y gestionarán las grabaciones de video. Algunas cámaras ofrecen almacenamiento local a través de tarjetas de memoria o discos duros integrados, mientras que otras pueden ofrecer opciones de almacenamiento en la nube.

- Facilidad de uso y acceso remoto:

Buscar cámaras que ofrezcan una interfaz de usuario intuitiva y acceso remoto a través de aplicaciones móviles o software de gestión de video en línea. Esto permitirá monitorear el objetivo desde cualquier lugar en cualquier momento.

Costo: Considera tu presupuesto y busca cámaras que ofrezcan un buen equilibrio entre características y precio. Asegúrate de tener en cuenta no solo el

costo inicial de la cámara, sino también los costos continuos, como el almacenamiento en la nube si es necesario.

10.1 Ejemplo de kit completo sistema de video vigilancia hogareño con IA.

C182 4K 16CH 4 Cámara Spotlight Sistema de Seguridad PoE + Disco Duro de 4TB [31]

• **4K Ultra HD:** el sensor de imagen CMOS Ultra HD captura más luz para mejorar el color, el contraste y el rendimiento en condiciones de poca luz.

• **Starlight Night Vision:** obtenga más detalles cuando los ojos humanos no puedan ver nada. El alcance de visión nocturna es de hasta 100 pies.

• **Conexión PoE simple:** solo necesita un cable para la transmisión de energía y Ethernet. Los recorridos directos desde el puerto POE de un NVR a una cámara pueden alcanzar hasta 300 pies.

• **Campo de visión de 90°:** un campo de visión ultra amplio le permite ver y proteger más de lo que le importa.

• **Alertas de movimiento:** le avisa instantáneamente cuando la cámara detecta algo inusual.

Package Contents

x1

16CH PoE NVR with 4TB HDD

x4

8MP PoE Camera

x4

60ft Ethernet Cable

x1

48V 2.5A NVR Power Supply

x1

3.3ft Ethernet Cable

x1

6.6ft HDMI Cable

x1

USB Mouse

x4

Mounting Screw Bag

x1

Quick Start Guide

x4

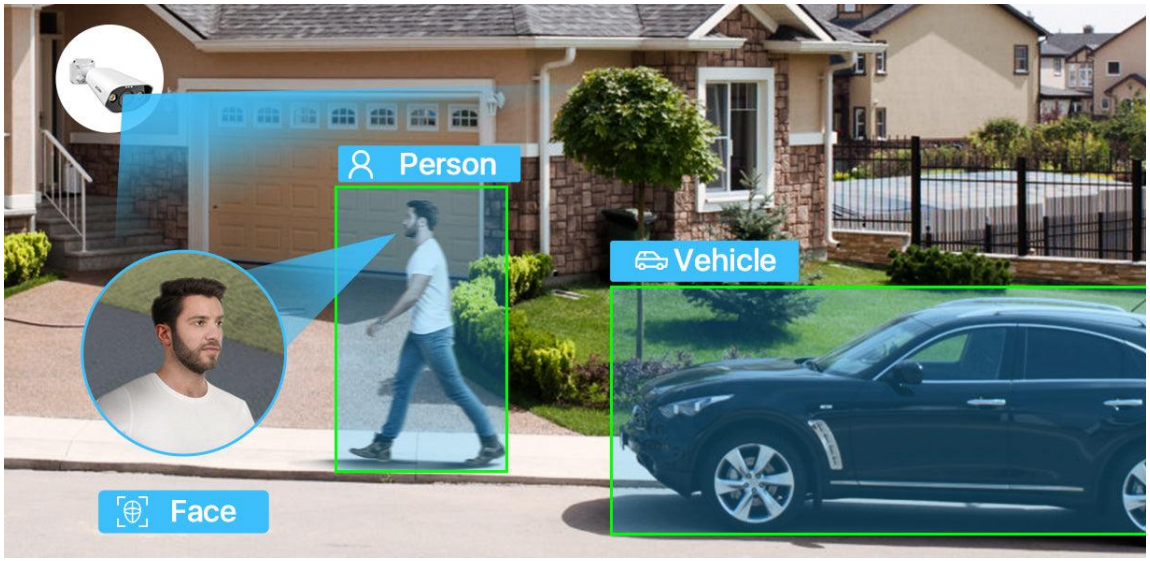
Mounting Template

x4

Warning Sticker

Product Specifications	
Max Video Resolution	4K(3840x2160)
Frame Rate	20fps
Minimum Illumination	0.012Lux (color mode); 0Lux (infrared light on)
Infrared Wavelength	850nm
Infrared Night Vision Dist	30m
White LED	Yes
Field of View	110° Horizontal
Microphone	Yes
Speaker / Siren	Yes
Storage Capacity	Up to 8TB
Remote Viewing	Yes
Environmental Rating	IP66 (Indoor/Outdoor)
Intelligent Detection	Motion/human/face/vehicle
Video Type	Full-time/alarm recording
Alarm Type	Light/sound/sound and light alarm
Software Support	ZOSI Smart (Android/IOS) AVSS (PC/MacBook)

Impulsada por tecnología de detección inteligente de IA, esta cámara identifica personas y vehículos de otros objetos.



Grabación 24 horas al día, 7 días a la semana, protección ininterrumpida

Disco duro integrado de 2 TB, los usuarios reciben grabación continua/activada por movimiento.

10.2 Sistema de video vigilancia en una organización con IA. [32]

El proyecto presenta una opción de videovigilancia para un hotel mediante videovigilancia con control de acceso, detección de rostros y personas. Ofrece detección precisa, análisis en tiempo real, automatización de tareas, mejora de la seguridad, optimización de recursos y escalabilidad para la organización. Capaz de anticiparse a las necesidades de los clientes para ofrecerles servicios que mejoren su estancia y su satisfacción.

10.2.1 Protección de perímetro.

La protección de perímetro en videovigilancia con inteligencia artificial (IA) se refiere a un sistema de seguridad diseñado para detectar y responder a intrusiones o actividades sospechosas en los límites físicos de una propiedad o instalación.

Detección de intrusos: Las cámaras de videovigilancia colocadas estratégicamente en los límites del perímetro monitorean continuamente el área en busca de cualquier actividad no autorizada. Los algoritmos de IA analizan las imágenes en tiempo real para detectar la presencia de personas u objetos que ingresen al perímetro.

Identificación de amenazas: La IA procesa las imágenes capturadas por las cámaras para identificar posibles amenazas, como personas escalando una valla, vehículos que se acercan demasiado al perímetro o la presencia de objetos abandonados cerca de la propiedad. Esto se logra mediante técnicas de detección de movimiento, reconocimiento de formas y análisis de comportamiento.

Generación de alertas: Cuando se detecta una actividad sospechosa, el sistema de videovigilancia con IA genera automáticamente una alerta para notificar al personal de seguridad o a las autoridades pertinentes. Estas alertas pueden ser enviadas a través de diferentes medios, como mensajes de texto, correos electrónicos o notificaciones en una aplicación móvil, para asegurar una respuesta rápida y efectiva.

Verificación de alarmas: Para reducir las falsas alarmas y garantizar una respuesta adecuada, el sistema de protección de perímetro con IA puede incluir mecanismos de verificación de alarmas. Esto puede implicar el uso de múltiples cámaras para confirmar la presencia de una amenaza desde diferentes ángulos o la integración con otros sistemas de seguridad, como sensores de movimiento o cercas eléctricas.

Respuesta automatizada o manual: Dependiendo de la gravedad de la amenaza detectada, el sistema puede activar respuestas automáticas, como encender luces de advertencia, activar alarmas audibles o notificar a las autoridades locales. Alternativamente, el personal de seguridad puede intervenir manualmente para evaluar la situación y tomar las medidas apropiadas según el protocolo establecido.

10.2.2 Acceso de vehículos con lectora de placas

El acceso de vehículos con lectura de placas mediante videovigilancia con inteligencia artificial (IA) es un sistema diseñado para controlar y monitorear el ingreso y salida de vehículos en una determinada área, como un estacionamiento, una comunidad cerrada o una instalación industrial.

Captura y reconocimiento de placas: Cuando un vehículo ingresa al estacionamiento, la cámara de videovigilancia captura la placa del vehículo y utiliza algoritmos de reconocimiento de placas basados en IA para identificar los caracteres alfanuméricos de la misma. Esta etapa implica el uso de técnicas de visión por computadora y aprendizaje profundo para identificar y reconocer las placas en diferentes condiciones de iluminación, ángulos de visión y tipos de vehículos.

Verificación y comparación: Una vez que se ha reconocido la placa del vehículo, el sistema la compara con una base de datos de placas autorizadas o de vehículos en lista negra. Si la placa coincide con alguna entrada en la base

de datos negativa, se activa una alerta para notificar al personal de seguridad o a las autoridades pertinentes.

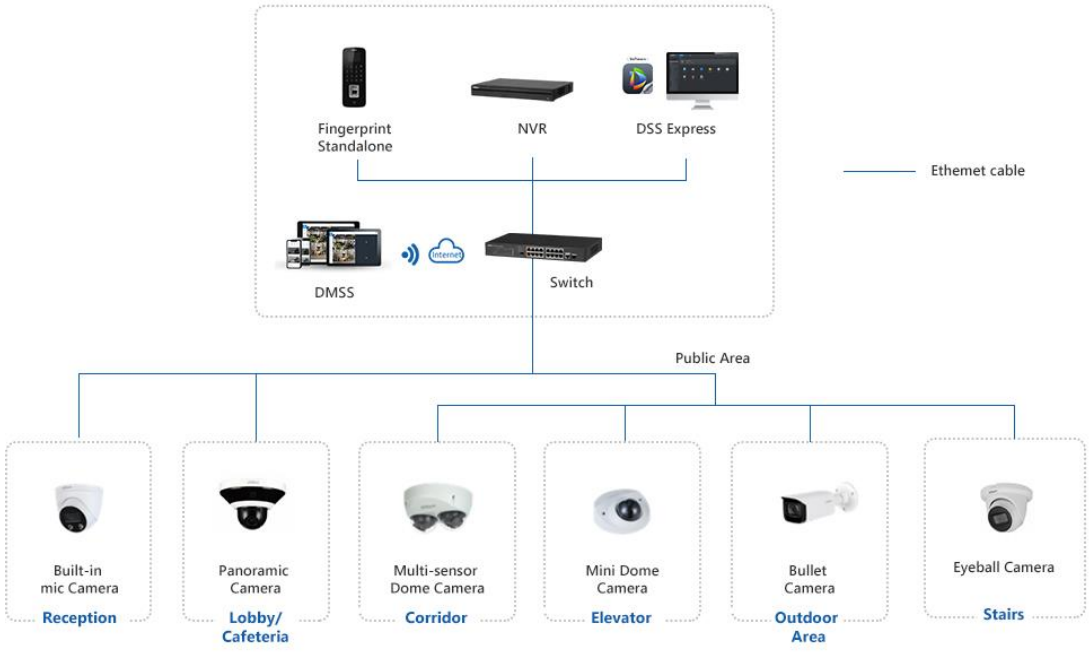
Registro de tiempo y lugar: Una vez que se ha reconocido la placa del vehículo, el sistema registra automáticamente la fecha, la hora y el lugar exacto donde se produjo la captura de la placa. Esta información se almacena en una base de datos junto con la placa del vehículo para su posterior análisis y seguimiento.

Seguimiento del movimiento del vehículo: A medida que el vehículo se mueve dentro del estacionamiento, las cámaras de videovigilancia pueden seguir capturando su placa en diferentes ubicaciones. Esto permite registrar el tiempo y el lugar de estacionamiento del vehículo en cada momento.

Análisis de datos: La información recopilada sobre el tiempo y el lugar de estacionamiento de cada vehículo se puede analizar para obtener estadísticas útiles, como la duración promedio de estacionamiento, los horarios de mayor demanda, las áreas más concurridas del estacionamiento, entre otros.

Mejora de la gestión del estacionamiento: Con la información recopilada, los administradores del estacionamiento pueden tomar decisiones informadas para mejorar la gestión y la operación del mismo. Por ejemplo, pueden ajustar las tarifas de estacionamiento según la demanda en diferentes horarios, identificar áreas con problemas de congestión o mejorar la distribución de espacios de estacionamiento disponibles.

10.2.3 Detección e identificación de clientes y trabajadores.



La gestión de acceso de personal, proveedores y clientes con cámaras de videovigilancia equipadas con inteligencia artificial (IA) es un sistema diseñado para controlar y monitorear quién tiene acceso a determinadas áreas de una instalación o negocio.

Identificación y registro de personas: Cuando una persona se acerca a un punto de acceso, como una puerta, una barrera de entrada, las cámaras de videovigilancia con IA capturan imágenes en tiempo real de la persona. Los algoritmos de IA procesan estas imágenes para identificar y reconocer a la persona.

Verificación de identidad: Una vez que la persona es reconocida, el sistema verifica su identidad comparando su rostro u otras características biométricas con una base de datos previamente registrada. Esto puede implicar el uso de sistemas de reconocimiento facial, reconocimiento de iris, huellas dactilares u otros métodos biométricos.

Autorización de acceso: Si la identidad de la persona es verificada con éxito y está autorizada para acceder al área, el sistema activa automáticamente la apertura de la puerta o barrera de acceso. Esto puede ser gestionado de manera automatizada mediante la integración con sistemas de control de acceso físico, como cerraduras electrónicas.

Registro de acceso: Cada vez que una persona accede a una determinada área, el sistema registra automáticamente la fecha, hora y otra información relevante sobre el acceso. Esto permite llevar un registro detallado de quién ha accedido a cada área en un momento dado.

Alertas y notificaciones: En caso de que se detecte un intento de acceso no autorizado o se produzca una violación de seguridad, el sistema puede generar alertas y notificaciones para informar al personal de seguridad o a las autoridades pertinentes. Esto permite una respuesta rápida y efectiva para abordar cualquier situación de riesgo.

Las cámaras, una vez instaladas y configuradas, permanecerán fijas y dirigidas hacia áreas específicas de interés. La selección de la óptica de las

cámaras se realizará cuidadosamente para permitir la observación de incidentes y la detección precisa de personas que transiten por las áreas designadas.

Es fundamental que las cámaras sean capaces de adaptarse a las condiciones ambientales del lugar, incluyendo cambios climáticos, variaciones de temperatura y condiciones de iluminación. Por esta razón, se incorporará iluminación por infrarrojos que garantice la captación de imágenes tanto durante el día como durante la noche, asegurando así una vigilancia continua y efectiva.

El sistema de detección de personas se basa en la integración de dos cámaras IP y computadoras equipadas con el software de detección de personas mediante TensorFlow, una plataforma de aprendizaje automático desarrollada por Google. Este software utiliza algoritmos avanzados para analizar imágenes y detectar patrones similares asociados con la presencia humana.

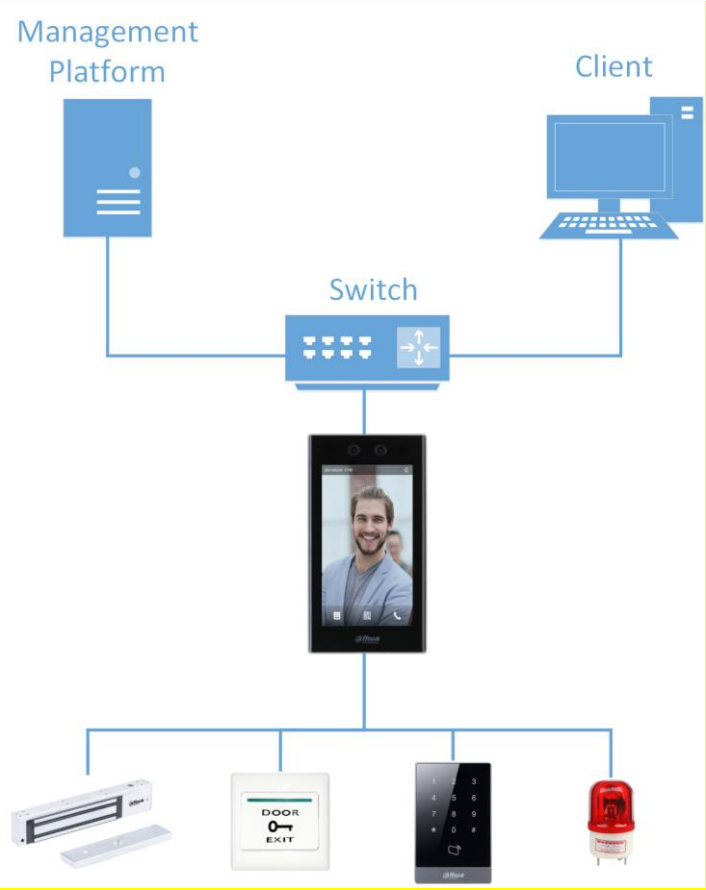
HAC-HFW2249TU-A-LED
2MP Full-color HDCVI Bullet Camera - Fuente: (Dahua, 2024)

10.2.4 Control de acceso:

Un sistema de control de acceso es una solución tecnológica que regula y gestiona la entrada a áreas físicas mediante autenticación de usuarios, como tarjetas, códigos o biometría. Puede incluir funciones como programación de horarios, registro de entradas y salidas, y se utiliza para garantizar la seguridad de personas y activos. Existen básicamente dos tipos:

Sistemas de control de acceso autónomos: Estos sistemas funcionan de manera independiente y no requieren una conexión en red para operar. Por lo general, están diseñados para ser utilizados en entornos más pequeños o donde la integración con otros sistemas no es necesaria. Los sistemas autónomos suelen estar compuestos por una unidad de control central, lectores de tarjetas o dispositivos biométricos, y dispositivos de bloqueo (como cerraduras eléctricas). La programación y administración se realizan localmente en cada dispositivo.

Sistemas de control de acceso en red: Estos sistemas están conectados a una red de computadoras y permiten una gestión centralizada de los accesos. Los dispositivos de control de acceso, como lectores de tarjetas y paneles de control, están interconectados a través de la red y pueden ser controlados y supervisados desde una ubicación remota. Este tipo de sistema es ideal para organizaciones grandes o distribuidas que requieren un control de acceso centralizado y una supervisión más avanzada. Además, los sistemas en red suelen ofrecer características adicionales como integración con otros sistemas de seguridad (como videovigilancia) y generación de informes detallados.



Modelo ASI7213K-W

Módulo de extensión de control de acceso a huellas dactilares

Reconocimiento facial Dahua, Detección de rostros, Deslizamiento de tarjetas,

Controlador de acceso de reconocimiento facial con contraseña

Fuente: (Dahua, 2024)

El módulo de la figura presenta varias opciones de acceso adaptables y combinables, según la necesidad de cada organización.

10.2.5 Mapa de calor.

Captura de imágenes: Las cámaras de seguridad capturan continuamente imágenes de la escena que están siendo monitoreadas.

Procesamiento de imágenes: Estas imágenes son procesadas por algoritmos de IA, que pueden incluir técnicas de visión por computadora y aprendizaje profundo, para detectar objetos, personas u otros elementos de interés en la escena.

Generación de mapa de calor: Con base en la detección de objetos y actividad, el sistema de IA crea un mapa de calor que resalta las áreas de la escena donde se concentra la actividad. Este mapa de calor se genera asignando diferentes colores o intensidades a las áreas de la escena según el nivel de actividad detectado.

Visualización y análisis: El mapa de calor se visualiza en tiempo real, permitiendo a los operadores de seguridad o analistas de datos identificar rápidamente las áreas de alta actividad dentro de la escena. Esto puede ayudar

a priorizar la atención en áreas críticas y a detectar patrones de comportamiento anómalos.

Ajuste y optimización: Suelen ser adaptables, lo que significa que pueden ajustarse y optimizarse para satisfacer las necesidades específicas de seguridad de un entorno particular. Esto puede incluir la configuración de umbrales de actividad, la definición de zonas de interés y la personalización de la visualización del mapa de calor.

10.2.6 Gestión de filas.

La gestión de filas en videovigilancia con inteligencia artificial (IA) es un sistema diseñado para monitorear y gestionar las filas de personas en tiempo real, con el objetivo de reducir el tiempo de espera de los clientes y mejorar la eficiencia del servicio.

Detección de personas: Las cámaras de videovigilancia capturan imágenes de las áreas donde se forman filas, como cajas registradoras, puntos de venta o áreas de servicio al cliente. Los algoritmos de IA procesan estas imágenes para detectar la presencia de personas y rastrear sus movimientos.

Análisis de la actividad: La IA analiza la actividad de las personas detectadas para identificar las filas y determinar su longitud y velocidad de avance. Esto se logra mediante técnicas de visión por computadora y análisis de flujo óptico, que permiten seguir el movimiento de las personas en la escena.

Predicción de tiempos de espera: Basándose en la longitud de la fila y la velocidad de avance, el sistema utiliza modelos predictivos para estimar el tiempo de espera de los clientes en la fila. Estas predicciones pueden ser actualizadas en tiempo real a medida que se producen cambios en la longitud de la fila o en la velocidad de avance.

Optimización del servicio: Con base en las predicciones de tiempo de espera, el sistema puede tomar medidas para optimizar el servicio y reducir los tiempos de espera. Por ejemplo, puede alertar al personal de servicio al cliente para abrir más cajas registradoras cuando se prevé un aumento en la demanda, o dirigir a los clientes hacia áreas con menor congestión.

Monitoreo y ajuste: Se monitorea continuamente la situación de las filas y ajusta sus predicciones y recomendaciones en función de los cambios en la actividad. Esto permite una gestión dinámica y adaptable de las filas para garantizar una experiencia óptima para los clientes.

10.2.7 Integración operación con tarjeta de crédito:

La integración de la operación con tarjeta de crédito realizada en un punto de venta (POS) y la videovigilancia a la hora de buscar una filmación para aclarar una compra con tarjeta de crédito es un proceso que combina tecnologías de transacciones financieras y sistemas de seguridad para facilitar la investigación de posibles fraudes o discrepancias en las transacciones con tarjeta de crédito.

Registro de transacciones: Cuando un cliente realiza una compra utilizando una tarjeta de crédito en un punto de venta (POS), se registra la transacción en el sistema del comerciante. Este registro incluye información sobre la fecha, hora, monto de la transacción y otros detalles relevantes.

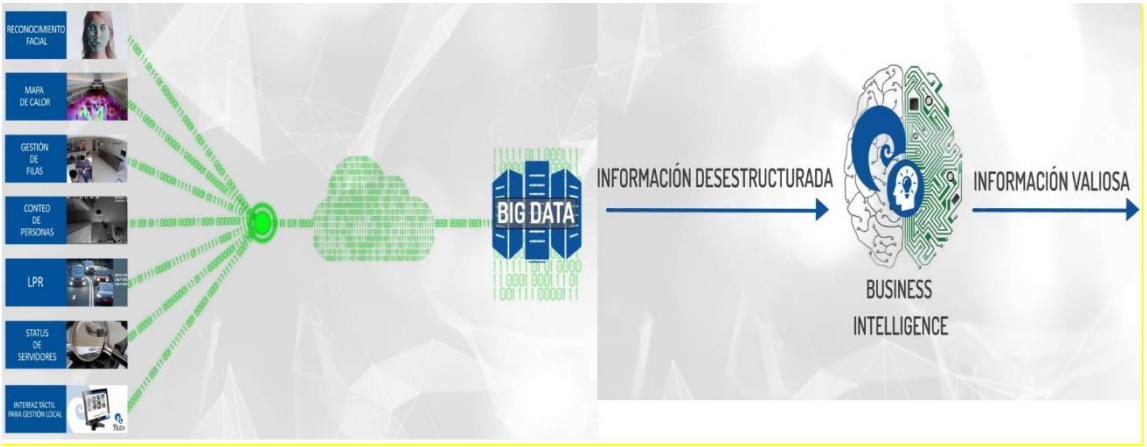
Asociación con datos de videovigilancia: Al mismo tiempo que se registra la transacción en el POS, se puede asociar automáticamente esta información con las grabaciones de videovigilancia correspondientes al momento de la transacción. Esto se logra mediante sistemas integrados que vinculan los datos del POS con los sistemas de videovigilancia del establecimiento.

Almacenamiento de datos: Tanto los datos de transacción del POS como las grabaciones de videovigilancia se almacenan de manera segura en sistemas de gestión de datos. Esto permite que los datos estén disponibles para su análisis posterior en caso de que surjan discrepancias o reclamaciones relacionadas con la transacción.

Búsqueda y recuperación de grabaciones: Cuando se necesita investigar una transacción específica, el personal autorizado puede utilizar la información de la transacción registrada en el POS para buscar y recuperar las grabaciones de videovigilancia correspondientes al momento de la compra. Esto se puede hacer utilizando herramientas de búsqueda que permiten filtrar las grabaciones por fecha, hora y ubicación en el establecimiento.

Análisis de evidencia: Una vez que se recuperan las grabaciones de videovigilancia, el personal de seguridad o los investigadores pueden analizar las imágenes para verificar la autenticidad de la transacción y buscar cualquier actividad sospechosa o irregular que pueda haber ocurrido durante la compra. Esto puede incluir la verificación de la identidad del titular de la tarjeta, la confirmación de la cantidad de productos comprados y la identificación de cualquier actividad fraudulenta.

10.2.8 Información accesible:



La gran cantidad de información generada está disponible de manera fácil y simple para ser visualizada por usuarios autorizados de perfil no técnicos.

La transformación de la gran cantidad de información generada por la videovigilancia con inteligencia artificial (IA) desde el big data de información desestructurada hasta la generación de información valiosa que es fácilmente accesible y comprensible para usuarios no técnicos a través de la inteligencia empresarial (Business Intelligence) implica varios pasos clave:

Captura y almacenamiento de datos: Las cámaras de videovigilancia capturan continuamente datos de video que contienen una gran cantidad de información, como imágenes de personas, vehículos, movimientos y eventos. Estos datos se guardan en sistemas de almacenamiento de big data diseñados para manejar grandes volúmenes de información desestructurada.

Procesamiento de datos con IA: Los algoritmos de inteligencia artificial analizan los datos de video para identificar patrones, detectar eventos específicos y extraer información relevante. Esto puede incluir la identificación de personas, el reconocimiento de actividades, el seguimiento de objetos y la detección de anomalías.

Transformación en información estructurada: La IA procesa los datos de video para convertirlos en información estructurada y contextualizada. Esto implica etiquetar los objetos detectados, asociar eventos con metadatos relevantes (como fecha, hora y ubicación), y organizar la información de manera que sea fácilmente accesible y comprensible para su análisis posterior.

Integración con herramientas de inteligencia empresarial: La información estructurada generada por la IA se integra con plataformas de inteligencia empresarial que permiten visualizar, analizar y compartir datos de manera intuitiva y accesible para usuarios no técnicos. Estas herramientas suelen incluir

paneles de control interactivos, informes personalizados y herramientas de visualización de datos.

Acceso y visualización para usuarios autorizados: Los usuarios autorizados, como gerentes de seguridad, supervisores de operaciones o analistas de negocios, pueden acceder a la información procesada y visualizada a través de las herramientas de inteligencia empresarial. Estas herramientas les permiten explorar los datos, generar informes personalizados, establecer alertas y tomar decisiones informadas basadas en la información proporcionada.

11. Conclusión:

La video vigilancia con inteligencia artificial (IA) enfrenta diversos desafíos y presenta soluciones innovadoras, para mejorar la seguridad y eficiencia de los sistemas de vigilancia. Entre los desafíos se encuentran la necesidad de gestionar grandes volúmenes de datos de manera eficiente, la identificación precisa de eventos relevantes en tiempo real, y la protección de la privacidad de los individuos.

Sin embargo, las soluciones basadas en IA ofrecen avances significativos, como la detección y seguimiento automático de objetos y personas, análisis avanzado de comportamientos, sistemas de alerta temprana para situaciones de riesgo. Además, la integración de tecnologías como el reconocimiento facial y la detección de anomalías permite una vigilancia más proactiva y precisa. A pesar de los desafíos, el desarrollo continuo de la video vigilancia con IA promete mejorar la seguridad pública, la prevención del delito y la eficiencia en una variedad de entornos, desde ciudades inteligentes hasta instalaciones industriales y comerciales.

El delicado equilibrio entre la seguridad pública y la privacidad de las personas es un tema de gran relevancia en la era moderna, donde la tecnología, especialmente en la video vigilancia con inteligencia artificial, ofrece herramientas poderosas para garantizar la seguridad, pero también plantea preocupaciones sobre la invasión de la privacidad. Por un lado, la implementación de sistemas de vigilancia avanzados puede ayudar a prevenir y resolver delitos, proteger instalaciones críticas y aumentar la sensación de seguridad en comunidades y espacios públicos.

Sin embargo, estas tecnologías también tienen el potencial de violar la privacidad individual, especialmente cuando se utilizan para el reconocimiento facial o el monitoreo continuo de actividades cotidianas. El acceso indebido a datos de video, el seguimiento sin consentimiento y la recopilación masiva de información pueden socavar las libertades individuales y generar preocupaciones sobre el uso indebido de datos por parte de gobiernos o entidades privadas. Por

lo tanto, es crucial establecer regulaciones claras y mecanismos de control para garantizar que la video vigilancia se utilice de manera ética y responsable, protegiendo simultáneamente los derechos fundamentales de privacidad y libertad de las personas.

Esto implica el desarrollo de políticas transparentes sobre el uso de la tecnología de vigilancia, la limitación del acceso a los datos recopilados, el anonimato de los individuos cuando no sea necesario su identificación, y la rendición de cuentas de las autoridades encargadas de la vigilancia. Al encontrar un equilibrio entre la seguridad pública y la privacidad de las personas, se puede maximizar el potencial beneficio de la video vigilancia mientras se salvaguardan los derechos individuales y se construye una sociedad más segura y justa para todos.

Los profesionales de la seguridad informática son una pieza clave para el desarrollo, implementación y seguimiento de las tecnologías de videovigilancia con IA, implementando normas internacionales como ISO 27000 entre otros estándares de seguridad. Su experiencia y conocimientos en ciberseguridad les permiten evaluar y mitigar los riesgos asociados con el uso de la inteligencia artificial en sistemas de videovigilancia. Además, pueden garantizar el cumplimiento de las regulaciones de privacidad y protección de datos, asegurando que la información capturada por las cámaras de vigilancia se maneje de manera ética y conforme a las leyes vigentes. Su labor contribuye a proteger la privacidad de las personas y a evitar posibles vulneraciones de seguridad que podrían comprometer la integridad de los sistemas de videovigilancia. En un mundo cada vez más digitalizado, su papel es fundamental para garantizar la seguridad y la confianza en el uso de la tecnología de inteligencia artificial aplicada a la videovigilancia.

Bibliografía inicial

U. o. -. C. N. d. I. Biotecnológica, «Sistema de reconocimiento facial
1] rápido y preciso utilizando MORSCMs-LBP en circuitos integrados,» 2023. [En línea]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9299277/. [Último acceso: 2023].

M. S. Elías, «PRIVACIDAD Y PROTECCIÓN DE DATOS
2] PERSONALES,» CABA, 2022.

S. Maksymenko, «Deep Learning-based Real-time Video Processing,»
3] 2023. [En línea]. Available: https://www.kdnuggets.com/2021/02/deep-learning-based-real-time-video-processing.html. [Último acceso: 2023].

Cameralyze, «How Deep Learning Helps With Real-Time Video
4] Processing,» 2022. [En línea]. Available: https://www.cameralyze.co/blog/how-deep-learning-helps-with-real-time-video-processing. [Último acceso: 2023].

C. Europea, «Union europea,» 2023. [En línea]. Available: https://digital-
5] strategy.ec.europa.eu/en/policies/cybersecurity-act. [Último acceso: 2023].

GBHackers, «Las 50 mejores herramientas gratuitas de inteligencia contra
6] amenazas cibernéticas – 2023,» 2023. [En línea]. Available: https://gbhackers.com/cyber-threat-intelligence-tools/. [Último acceso: 2023].

R. Valbuena, «Redes Neuronolaes Artificiales Recurrentes,» de
7] *Inteligencia Artificial Investigación Científica Avanzada Centrada en Datos*, 2021, p. 345.

E. Villarrubia, «Aprendizaje por refuerzo: área menos conocida del
8] machine learning,» 2023. [En línea]. Available: https://esi.uclm.es/index.php/2022/06/13/aprendizaje-por-refuerzo-area-menos-conocida-del-machine-learning/. [Último acceso: 2023].

D. H. A. M. Silver, «Dominar el juego de Go con redes neuronales
9] profundas y búsqueda de árboles.,» 2016. [En línea]. Available: https://doi.org/10.1038/nature16961. [Último acceso: 2023].

E. e. AlphaStar, «Google DeepMind,» 2019. [En línea]. Available:
10] https://www.deepmind.com/blog/alphastar-mastering-the-real-time-strategy-game-starcraft-ii. [Último acceso: 2023].

INTEL, «INTEL,» 2023. [En línea]. Available:
11] https://www.intel.es/content/www/es/es/internet-of-things/computer-vision/convolutional-neural-networks.html. [Último acceso: 2023].

IBM, «IBM RNN,» 2023. [En línea]. Available: https://www.ibm.com/es-
12] es/topics/recurrent-neural-networks. [Último acceso: 2023].

RAE-Intimidad, «Real Academia Española,» 2024. [En línea]. Available:
13] https://dle.rae.es/intimidad.

RAE-Privacidad, «Real Academia Española y Asociación de Academias
14] de la Lengua Española,» 2024. [En línea]. Available: https://dle.rae.es/privacidad.

INFOLEG, «PROTECCION DE LOS DATOS PERSONALES,» [En
15] línea]. Available: https://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm.

I. D. 1558/2001, «Decreto 1558/2001 PROTECCION DE LOS DATOS
16] PERSONALES,» [En línea]. Available: https://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70368/norma.htm.

INFOLEG, «Normas Constitucionales.,» [En línea]. Available:
17] https://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/804/norma.htm.

J. Dibbell, «A Rape in Cyberspace,» 1993. [En línea]. Available:
18] https://en.wikipedia.org/wiki/A_Rape_in_Cyberspace.

T. N. Y. Times, «Clases de ética para la tecnología,» [En línea]. Available:
19] https://www.nytimes.com/es/2018/02/19/espanol/etica-tecnologia-computacion-silicon-valley.html.

R. O. Mason, «Four Ethical Issues of the Information Age,» [En línea].
20] Available:

https://www.researchgate.net/publication/242705009_Four_Ethical_Issues_of_the_Information_Age.

ISO, «ISO,» 2024. [En línea]. Available: https://www.iso.org/home.html.

21]

G. Solutions, «Global Solutions,» [En línea]. Available:

22] https://www.globalsuitesolutions.com/es/cambios-norma-iso-27002-2022/. [Último acceso: 2023].

A. (. N. S. Institute), «ANSI,» 2023. [En línea]. Available:

23] https://blog.ansi.org/iso-iec-27002-2022-information-security-controls/?utm_term=&utm_campaign=Performance+Max-48+br&utm_source=adwords&utm_medium=ppc&hsa_acc=9208454611&hsa_cam=21001946636&hsa_grp=&hsa_ad=&hsa_src=x&hsa_tgt=&hsa_kw=&hsa_mt=&hsa_net=adwor.

A. Saeckel, «DQS Argentina,» 2024. [En línea]. Available:

24] https://www.dqsglobal.com/es-ar/aprenda/blog/revision-de-la-norma-iso-27002-estos-son-los-cambios.

I. 31000:2018, «ISO 31000:2018 Gestión del riesgo — Directrices,» 2024.

25] [En línea]. Available: https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es.

A. Marugán, «Antena 3,» [En línea]. Available:

26] https://www.antena3.com/noticias/sociedad/hackers-difunden-mas-200-videos-sexuales-grabados-camaras-seguridad-viviendas_20240415661d457e8e66020001648c3a.html. [Último acceso: 04 2024].

E. Burgos, «INFOBAE,» [En línea]. Available:

27] https://www.infobae.com/america/mundo/2021/03/10/un-grupo-de-hackers-tuvo-acceso-a-150-mil-camaras-de-seguridad-espiaron-a-tesla-y-a-otras-empresas-hospitales-y-carceles/. [Último acceso: 04 2024].

Fortinet, «Fortiguard Lab,» 2023. [En línea]. Available:

28] https://www.fortiguard.com/threat-signal-report/5152. [Último acceso: 2024].

Ekoparty, «Ekoparty,» 2023. [En línea]. Available:
29] https://ekoparty.org/eko2023-agenda/sadprotocol-goes-to-hollywood-hijacking-an-ip-camera-stream-as-seen-in-the-movies/. [Último acceso: 2024].

Ezviz, «Ezviz,» 2023. [En línea]. Available:
30] https://www.ezviz.com/es/data-security/security-notice/detail/827. [Último acceso: 2024].

ZOSI, «Sistema de cámaras de seguridad 4K PoE,» 2024. [En línea].
31] Available: https://www.zositech.com/collections/4k-poe-security-camera-system/products/c182-4k-4-camera-poe-camera-system-person-vehicle-detection-4tb-hard-drive.

SCATI, «SISTEMAS AVANZADOS DE VIDEOVIGILANCIA PARA
32] HOTELES Y CASINOS,» 04 2024. [En línea]. Available: https://www.scati.com/en/video-surveillance-solutions-hotels-casinos/. [Último acceso: 04 2024].

B. n. d. C. Chile, «Biblioteca Congreso Chile (BCN),» 2023. [En línea].
33] Available: https://www.bcn.cl/observatorio/asiapacifico/noticias/ley-proteccion-informacion-personal-japon.

ISACA, «Cumplimiento de la Ley de Privacidad del Consumidor de
34] California (CCPA),» 2020. [En línea]. Available: https://www.isaca.org/es-es/resources/isaca-journal/issues/2020/volume-2/healthcare-organizations-compliance-with-the-ccpa.