Universidad Tecnológica Nacional
AJEA – Actas de Jornadas y Eventos Académicos de UTN
Trabajo Completo Publicado en AJEA – Full Text Published in AJEA
https://rtyc.utn.edu.ar/index.php/ajea/article/view/1c39
Libro de actas de resúmenes DOI: https://doi.org/10.33414/ajea.1640.2024
Colección JIT en AJEA https://rtyc.utn.edu.ar/index.php/ajea/JITs

Jóvenes Investigadores Tecnológicos
Facultad Regional Rafaela 26 y 27 de octubre de 2023

Área: Sistemas de Información e informática / Categoría: Estudiante de Grado / Regional: Facultad Regional Rosario

Análisis de beneficios de la integración de Inteligencia Artificial en la estrategia organizacional para la detección de amenazas internas.

Analysis of benefits of the integration of Artificial Intelligence in the organizational strategy for the detection of insider threats.

Presentación: 17/10/2023

Maximiliano Mansilla
Universidad Tecnológica Nacional Facultad Regional Rosario Argentina
mmansilla02@outlook.com

Ornella Colazo
Universidad Tecnológica Nacional Facultad Regional Rosario Argentina
ornicolazo@gmail.com

Bautista Guerra
Universidad Tecnológica Nacional Facultad Regional Rosario Argentina
bautistaguerra.it@gmail.com

Guillermo Patricio Dolan
Universidad Tecnológica Nacional Facultad Regional Rosario Argentina
guillermopatdolan@gmail.com

Lucía Morena Fabbri
Universidad Tecnológica Nacional Facultad Regional Rosario Argentina
fabbriluciam@gmail.com

Resumen

En el presente trabajo se analizarán algunas de las técnicas basadas en Inteligencia Artificial para su utilización en la detección y análisis del comportamiento de las personas en interacción con los sistemas de la organización y el flujo de actividades internas. El objetivo es incorporarlas como estrategia para la mitigación de riesgos asociados a amenazas internas. Dado que los empleados suelen tener acceso directo a datos sensibles o tenerlos fácilmente a su alcance para su uso diario, suponen un desafío a la seguridad de la información. Es crucial, por lo tanto, considerar estrategias que aborden la prevención de fugas de datos y evaluar la viabilidad y conveniencia de implementar estas técnicas como parte de la estrategia de seguridad de la organización. En este sentido, se analizará la factibilidad de invertir en estas tecnologías como medida preventiva para mitigar fugas de datos.

Palabras clave: Inteligencia Artificial, Amenazas internas, Prevención de Fuga de Datos

Abstract

In this work, we will analyze some of the techniques based on Artificial Intelligence for their use in the detection and analysis of people's behavior when interacting with the organization's systems and the flow of internal activities. The objective is to incorporate them as a strategy for mitigating risks stemming from insider threats. Because of employees often have direct access to sensitive data or easily have it within their reach for daily use, they suppose a challenge to information security. Therefore, it

AJEA – Actas de Jornadas y Eventos Académicos de UTN
Libro de actas de resúmenes DOI: https://doi.org/10.33414/ajea.1640.2024
Texto Completo Publicado en AJEA – Full Text Published in AJEA
https://rtyc.utn.edu.ar/index.php/ajea/article/view/1639

is crucial to consider strategies that address data leakage prevention and evaluate the feasibility and suitability of implementing these techniques as part of the organization's security strategy. In this regard, we will analyze the feasibility of investing in these technologies as a preventive measure to mitigate data leaks.

Keywords: Artificial Intelligence, Insider Threats, Data Leakage Prevention

Introducción

La Inteligencia Artificial (IA) es un tema que en este último tiempo ha sido tendencia, si bien queda mucho por investigar al respecto, se puede decir que su uso en diferentes campos de aplicación genera resultados más que aceptables. En el ámbito de la seguridad de la información, donde las organizaciones se enfrentan diariamente a diversas amenazas que pueden materializar riesgos, la *perspicacia* de la IA nos puede ser de mucha utilidad. En línea con el proyecto al que está vinculado este trabajo (Riva et al., 2022), nos enfocaremos en aquellos riesgos que se puedan materializar sobre activos de información que, en este contexto, serán aquellos activos críticos para la organización que deberá proteger y a partir de los cuales podremos identificar otras categorías de activos relevantes (activos de soporte, hardware, software, etc.). El propósito será mitigar cualquier tipo de amenaza interna que comprometa a dichos activos de manera eficiente y efectiva.

Será importante, entonces, tener en cuenta algunas cuestiones. Por un lado que los activos de información no solamente están expuestos a ciberataques. Como menciona Fabbri en su trabajo sobre recursos humanos (Fabbri and Dolan, 2022), el factor humano desempeña un papel fundamental en la seguridad de la información dentro de una organización, por lo tanto, pueden ser los mismos empleados quienes, intencionalmente o no, se encarguen de exponer los datos. Por otro lado, el crecimiento que han experimentado los datos con los que opera una organización en la era digital es exponencial.

Por lo expuesto hasta aquí será necesario analizar la viabilidad de la implementación de tecnologías de IA en conjunto con técnicas de análisis de grandes volúmenes de datos (Big Data) capaces de advertir respecto de cualquier tipo de comportamiento por parte de los empleados que pueda ser definido como anómalo dentro de una organización.

Amenazas Internas

De acuerdo con la definición propuesta por Schultz (Schultz, 2002), amenaza interna representa *el uso inadecuado e intencional de los sistemas de información por usuarios autorizados a utilizarlos.* En función de esto podemos afirmar que los agentes internos a la organización suponen una amenaza a la seguridad de la información. A los agentes internos se los conoce también con el nombre de *insiders*. Incluso en regiones hispanohablantes, el término insider es ampliamente usado y con el tiempo se ha ido adoptando cada vez más debido a la practicidad y representatividad que demuestra la palabra.

Como ya hemos mencionado, los riesgos en los cuales nos enfocamos son aquellos amenazan contra alguna de las dimensiones de la seguridad de la información (disponibilidad, integridad y confidencialidad). Si bien es una problemática sobre la cual trabajan los especialistas del área de TI, cuando de amenazas internas se habla, no son los únicos actores intervinientes en la prevención o mitigación del impacto de estos riesgos. Conforme a lo que propone Delgado (Delgado, 2021), *el departamento de recursos humanos es una pieza imprescindible en la gestión de amenazas internas al ser la primera línea de defensa de las organizaciones*, quedando en el departamento de RRHH cierta responsabilidad en el tratamiento de dichos riesgos.

El proceso de selección y contratación del personal que será parte de la organización, es uno de los momentos sobre los cuales RRHH deberá prestar especial atención. En estos procesos usualmente se llevan a cabo una serie de verificaciones, para esto, será necesario establecer la sensibilidad y criticidad de la información a la que los aspirantes tendrán acceso, no es lo mismo la selección y contratación de un puesto para personal de limpieza a contratar un DBA (administrador de bases de datos).

AJEA – Actas de Jornadas y Eventos Académicos de UTN
Libro de actas de resúmenes DOI: https://doi.org/10.33414/ajea.1640.2024
Texto Completo Publicado en AJEA – Full Text Published in AJEA
https://rtyc.utn.edu.ar/index.php/ajea/article/view/1639

No obstante, el rol que cumple RRHH en materia de seguridad, no termina en la fase inicial de la contratación, debe perdurar durante todo el ciclo de vida de la relación contractual. Resulta útil, mediante controles periódicos, conocer el nivel de satisfacción y conformidad que tienen los empleados respecto a la organización, para analizar en cierto modo el nivel de pertenencia que se tiene con la misma con el objetivo de detectar y mitigar deslealtades.

Por último, el proceso de finalización de la relación contractual es uno de los considerados de mayor riesgo para la seguridad de la información, es por esto que no se deberá descuidar la atención sobre estos casos durante el período de tiempo que existe entre que se informa la decisión hasta que queda efectivo el fin de la relación contractual. Inmediatamente finalizado el contrato, RRHH deberá encargarse de asegurar el desaprovisionamiento de todo tipo credencial de acceso. Estas medidas, buscan detectar y mitigar cualquier actitud vengativa que pueda tener el empleado que ha sido apartado del puesto de trabajo.

Con el fin de comprender mejor la dimensión de esta problemática, se presentan los resultados de un estudio realizado por el Instituto Ponemon (Ponemon Institute, 2020), un reconocido instituto de investigación y educación estadounidense. En éste fueron incluidas 204 organizaciones alrededor del mundo y más de 960 especialistas de TI pertenecientes a las mismas. Es importante tener en cuenta que fue realizado sobre organizaciones empresariales con una planta global de 1000 (mil) o más empleados, por lo tanto ese es el tipo de empresas a la cual se hará referencia en lo que resta del trabajo. Estos números afectan directamente en el análisis que se va a realizar en secciones posteriores, por esto la importancia de saber que los números que se presentarán no reflejan la realidad de todas las organizaciones.

El reporte muestra que, de un total de 4716 incidentes asociados a insiders, aproximadamente un 23% corresponden a insiders considerados maliciosos, un 14% refieren al robo de credenciales y un 63% ocurren debido a negligencia humana. A su vez, informa que el 60% de las organizaciones encuestadas, presentaron en promedio, más de 20 incidentes referidos a amenazas internas en el año 2019. Haciendo referencia a los costos los cuales las organizaciones se ven expuestas, según el reporte, la empresa que menos gasto tuvo en relación a estos incidentes, gastó US$ 0.43 millones y la que mayor gasto tuvo fue de US$ 26.99 millones. Así mismo, US$ 10.80 millones representa más del 50% de las organizaciones. En promedio el gasto fue de US$ 11.45 millones.

IA en el ámbito de la Seguridad de la Información

La IA ha experimentado un crecimiento vertiginoso en los últimos años y ha demostrado ser una herramienta invaluable para las organizaciones en el ámbito de la ciberseguridad. De acuerdo con los lineamientos establecidos para este proyecto, analizaremos algunos de los sistemas que pueden ser implementados dentro de una organización y que pueden ayudar a detectar posibles amenazas internas que atenten contra la seguridad de la información desde cualquiera de sus dimensiones. En particular, se expondrán la Analítica de Vídeo Inteligente y el Análisis de Comportamiento basado en Datos.

Analítica de Video Inteligente.

La analítica de video tradicionalmente se basaba en reglas decretadas por cada programador, con parámetros fijos para cada situación que el sistema debía reconocer. La IA viene a cambiar este paradigma y propone el desarrollo de algoritmos que realmente aprendan de los objetos que están viendo, sus relaciones y comportamientos. Esto le permitirá identificar elementos y clasificar situaciones, como así también analizar si el comportamiento es el esperado o no, para notificar en caso de que alguno resulte fuera de lo esperado (Montes, 2021). A los algoritmos de análisis de vídeo basados en IA se los conoce también como "visión artificial". En general, un algoritmo de visión artificial, podemos resumir y decir que realiza tres procesos principales: *detección*, *rastreo* y *razonamiento*.

El proceso de **detección** se encargará de clasificar lo que ve en una imagen y además identificar la posición espacial, es decir las coordenadas que ocupa ese objeto. Por ejemplo, será el proceso encargado de detectar que en una imagen hay personas, animales y edificios especificando dónde se encuentran cada uno y qué tipo de animal particular es.

AJEA – Actas de Jornadas y Eventos Académicos de UTN
Libro de actas de resúmenes DOI: https://doi.org/10.33414/ajea.1640.2024
Texto Completo Publicado en AJEA – Full Text Published in AJEA
https://rtyc.utn.edu.ar/index.php/ajea/article/view/1639

En cuanto al **rastreo**, a partir de los objetos identificados en la detección, se encargará de individualizarlos y lograr hacer un seguimiento de ellos en cada frame del vídeo, uniendo los resultados para obtener la trayectoria del objeto en el vídeo.

Por último, el **razonamiento**, representa la "capa lógica" que, se encargará de darle valor para el negocio a los resultados obtenidos anteriormente.

Análisis de Comportamiento Basado en Datos.

El análisis de comportamiento es una disciplina que forma parte del análisis de datos y, en particular, nos permite examinar todas las acciones que los usuarios realizan mientras interactúan en entornos digitales. Por ejemplo, cuando un usuario utiliza una computadora, además de los datos generados por la ejecución de tareas específicas, también se generan datos de uso que abarcan desde los clics efectuados y el movimiento del ratón hasta los archivos abiertos y los sitios web visitados, entre otros. Estos datos se recopilan y se organizan cronológicamente para cada usuario, formando lo que comúnmente se conoce como el *viaje o flujo del usuario*. Para poder inferir respecto del comportamiento de los usuarios dentro de la organización, existen algoritmos que ayudan a cumplir este objetivo:

- **Aprendizaje Automático supervisado:** este método utiliza conjuntos de datos etiquetados para su entrenamiento, aquellos que incluyen ejemplos de comportamientos normales y anómalos. A partir de estos datos, el modelo aprende a distinguir entre comportamientos y determinar si son anómalos o no.
- **Aprendizaje Automático no supervisado:** a diferencia del método supervisado, este enfoque aprende a partir de datos no etiquetados, esto implica que no se especifica si el comportamiento es anómalo o no. En su lugar, analiza los datos de comportamiento para identificar patrones de uso y determinar si están dentro de los parámetros esperados o presentan desviaciones atípicas que puedan representar una amenaza.
- **Procesamiento del lenguaje natural:** esta herramienta permite analizar texto y convertirlo en valores numéricos para que pueda ser procesado por modelos analíticos que generalmente trabajan con variables numéricas. Esto facilita la obtención de información a partir del texto analizado.

Como recurso para aplicar este tipo de análisis, se tomarán como referencia las herramientas UEBA (por sus siglas en inglés, User and Entity Behavior Analytics), basadas en el aprendizaje automático no supervisado. Estas herramientas, están destinadas al análisis de comportamiento de los usuarios conectados a una red organizacional y los equipos o entidades dispuestos para ser usados para el trabajo diario. Para la implementación de este sistema dentro de una organización, se propone la siguiente estrategia (Angulo Cárdenas, 2023):

1. **Recopilación de la información:** la herramienta debe recopilar datos de comportamiento e interacción sobre las entidades de los usuarios dentro de la organización. Esto le permitirá "aprender" cuáles son los parámetros de comportamiento esperados de cada usuario para luego poder advertir respecto de desviaciones.
2. **Detección de amenazas:** una vez que la herramienta haya adquirido los datos necesarios y los haya analizado, comienza la puesta en marcha para el cumplimiento de su función, la detección de amenazas internas. Las herramientas UEBA permitirán a la organización: detectar amenazas basadas en acciones de los usuarios en tiempo real, generar una lista de prioridad de alerta, mejorar la eficiencia de detección de ataques maliciosos.
3. **Creación de perfiles de comportamiento:** es importante que sean permeables al cambio. Los perfiles de comportamiento permiten a las herramientas UEBA establecer una línea base de como el usuario interactúa con la red y las posibles desviaciones que este comportamiento puede tener.
4. **Generar alerta temprana:** permitirá la detección temprana de posibles incidentes asociados a mal comportamiento de insiders.

AJEA – Actas de Jornadas y Eventos Académicos de UTN
Libro de actas de resúmenes DOI: https://doi.org/10.33414/ajea.1640.2024
Texto Completo Publicado en AJEA – Full Text Published in AJEA
https://rtyc.utn.edu.ar/index.php/ajea/article/view/1639

5. **Prevenir amenazas internas:** las herramientas UEBA pueden generar una escala de puntaje de riesgos sin la necesidad que intervenga un encargado de seguridad. Organiza la escala en función del perfil de comportamiento, patrones de ataques internos, privilegios del usuario sobre los datos o sistemas.
6. **Actualizar perfiles con regularidad:** es importante que la herramienta siempre siga aprendiendo sobre lo que sucede en la organización, al tratarse de un ambiente donde generalmente se producen muchos cambios en materia de recursos humanos.

Integración de la IA en la estrategia de mitigación de amenazas internas

En función de las herramientas y tecnologías presentadas en secciones anteriores, el objetivo ahora es ver la manera en que pueden ser integradas en la estrategia organizacional para la mitigación de riesgos provenientes de amenazas internas. Una de las ventajas que tiene la inclusión de IA en la estrategia de seguridad de la información es lograr que estas cuestiones dejen de tener una dependencia tan alta del factor humano. Si bien es cierto que ninguna de las tecnologías presentadas tiene las habilidades necesarias para tomar decisiones operativas sobre la organización de manera autónoma en su totalidad, su implementación descongestiona y agiliza el trabajo humano y también permite que se hagan controles en tiempo real en todo momento sin perder eficiencia.

Incorporación de Analítica de Vídeo Inteligente.

En la actualidad, existen dos soluciones principales posibles para incorporar analíticas de vídeo al sistema de seguridad por videovigilancia de una organización. La implementación de uno u otro dependerá del presupuesto que disponga la organización, infraestructura disponible y la necesidad que busca satisfacer con la incorporación de estas tecnologías. A su vez, se pueden presentar ecosistemas que planteen un esquema híbrido entre ambas soluciones.

La primera de ellas es adquiriendo cámaras IP que tengan la analítica integrada. Esta solución tiende a ser más costosa ya que requiere que la cámara disponga, entre otras cosas, de un microprocesador, memoria RAM y demás componentes electrónicos con la potencia y capacidad necesarias para la ejecución del software que realiza la analítica.

La segunda consiste en implementar un entorno de analítica de vídeo basado en la nube, donde el vídeo es capturado por las cámaras y enviado al servidor para que sea procesado. Esta solución requiere de una conexión lo suficientemente veloz y estable para poder compartir el gran volumen de datos que una cámara de vídeo genera, en caso de requerirse que la analítica se haga sobre vídeos en vivo. Tiene la ventaja de que el hardware disponible para ejecutar la analítica probablemente sea más potente al que una cámara puede ofrecer.

Como se comentó al comienzo de esta sección, es posible plantear esquemas híbridos, lo que supone que la cámara comparta las tareas de análisis con el software que la integra. Este software puede ser provisto por la empresa fabricante o bien, puede ser un desarrollo personalizado. Para poder hacer esto la cámara necesariamente debe ser de tipo IP y ser compatible con el protocolo ONVIF (del inglés, “foro abierto de interfaz de vídeo en red”). Las cámaras de videovigilancia que incorporan este protocolo tienen la capacidad de generar el mismo streaming de vídeo permitiendo la interoperabilidad entre los dispositivos de seguridad IP, como cámaras de seguridad, plataforma de gestión de vídeo, software y sistemas de control de acceso (Castro Arteaga, 2023). A continuación, se darán dos ejemplos que facilitarán la comprensión de cómo puede ser implementado un sistema de análisis de vídeo en función de las dos soluciones presentadas.

Cámaras con Tecnología IVA 8.10.

Nos centraremos en este ejemplo en las cámaras de videovigilancia con tecnología IVA 8.10 desarrolladas por la reconocida empresa alemana Bosch. En particular nos enfocaremos en los modelos IP 7000-9000 que son aquellos que integran la tecnología “Intelligent Video Analytics 8.10” (IVA 8.10) y que además están adecuadas al protocolo ONVIF.

AJEA – Actas de Jornadas y Eventos Académicos de UTN
Libro de actas de resúmenes DOI: https://doi.org/10.33414/ajea.1640.2024
Texto Completo Publicado en AJEA – Full Text Published in AJEA
https://rtyc.utn.edu.ar/index.php/ajea/article/view/1639

La tecnología IVA 8.10 trae consigo mucho potencial que puede ser aprovechado en la detección temprana de posibles amenazas internas. Según declara la empresa en su reporte (Bosch Security Systems, 2021), algunas de las funcionalidades que las cámaras traen consigo son: detección de posicionamiento de objetos, detección de remoción de objetos, conteo de personas, detección de intrusos, detección de merodeo en una determinada área y detección de multitudes en zonas específicas. Las funciones mencionadas anteriormente son solo algunas de todas las posibilidades que ofrece el amplio catálogo presentado por la marca. Todas las funcionalidades de las cámaras son fácilmente configurables y combinables. Además, el sistema ofrece un entorno de desarrollo donde se pueden adicionar hasta 8 tareas extras de analítica definidas por el usuario.

Estos dispositivos tienen un punto en contra y es su precio. De acuerdo con lo publicado en el sitio web “B&H Photo Audio", distribuidor oficial de Bosch, tienen un precio que va, aproximadamente, desde los US$ 2799 (modelo NDP-7512-Z30 7000i), llegando a valores de US$ 32 999 (modelo MIC IP fusion 9000i).

Cámaras Dahua Imou.

La compañía Imou, propiedad de Dahua Technology, es una empresa de origen chino. El modelo que tomaremos de ejemplo en particular es “Imou Bullet 2 Pro". Estas cámaras presentan un muy buen rendimiento en relación con su precio, que es de aproximadamente US$ 100. La principal diferencia respecto de las anteriores está en que la analítica de vídeo que incorporan es de las más sencillas y no es nativo a la cámara, depende del software que se encargue de ejecutar estas tareas.

Estas cámaras son compatibles con el software llamado “Imou life” que se encarga de llevar a cabo tareas básicas de analítica como la detección de humanos. Para garantizar la seguridad de los datos que se manejan, cuenta con certificación ISO 27001 (estándar de seguridad de la información) y cumple con los lineamientos dispuestos por la GDPR (General Data Protection Regulation).

Adicionalmente se ofrece un servicio de procesamiento en la nube, denominado “Imou Protect”, que se paga con una suscripción mensual, donde uno de los beneficios que se adquieren es una mayor potencia y mejor servicio de detección por IA. Sin embargo, gracias a que integran el protocolo ONVIF, es posible conectarse fácilmente al streaming de vídeo generado por la cámara desde cualquier software que esté desarrollado para realizar una analítica más compleja, pudiendo llegar a igualar la potencia de análisis que presentan las cámaras Bosch.

Incorporación Herramientas UEBA.

Para la incorporación de las herramientas UEBA en una organización, tomamos como referencia a la empresa Securonix, especializada en brindar servicios de seguridad basados en la analítica de datos. Securonix UEBA es una solución de SaaS (del inglés, software como servicio) que puede implementarse rápidamente, lo cual permite obtener un tiempo más rápido para demostrar valor para la detección y la respuesta. Por su parte, Securonix, propone la integración de estas herramientas en la organización de una manera medianamente sencilla, sin la necesidad de hacer una inversión en infraestructura que las soporte ya que el servicio que ofrecen está completamente integrado en la nube, por lo tanto el procesamiento de los datos no es local. No obstante, se puede optar por una opción híbrida (procesamiento local y en la nube). Cuenta con modelos de amenazas listos para usar, casos de uso preconfigurados y conectores en la nube integrados que permiten una rápida implementación y procesar datos desde más de cien fuentes distintas.

Comprender la diferencia entre el comportamiento normal y anormal es esencial para la detección de amenazas internas. La solución de Securonix se sustenta en tres tipos de análisis:

- **Análisis Conductual:** gracias a los sofisticados algoritmos basados en aprendizaje automático desarrollados por Securonix, alertan de las amenazas que se desvían de las líneas de base de comportamiento establecidas.

AJEA – Actas de Jornadas y Eventos Académicos de UTN
Libro de actas de resúmenes DOI: https://doi.org/10.33414/ajea.1640.2024
Texto Completo Publicado en AJEA – Full Text Published in AJEA
https://rtyc.utn.edu.ar/index.php/ajea/article/view/1639

- **Análisis de Pares:** el análisis de pares se dedica a examinar el comportamiento de usuarios individuales y a compararlo con el de sus colegas dentro de la misma organización.
- **Análisis de Rareza de los Eventos:** detecta aquellos eventos que no son usuales en la organización y suponen una amenaza.

Al momento de analizar el costo de inversión que conlleva la implementación de estas herramientas en una organización, se ha consultado el portal oficial de "Amazon Web Services". En dicho sitio, el paquete denominado "SNYPR -UEBA_1K_ID", se ofrece a un precio de US$ 48 094 por un período de 12 meses.

Conclusiones

En vista de lo expuesto, queda claro que las amenazas internas no deben subestimarse en ningún aspecto dentro de las organizaciones. Su potencial impacto es significativo y, a menudo, son difíciles de detectar debido a la limitación humana en la monitorización constante que puede verse afectada por factores como la fatiga. Resulta esencial recordar que incluso el personal encargado de la seguridad es en sí mismo un insider, por lo tanto una posible amenaza, lo que agrega una capa adicional de complejidad. En este contexto, los beneficios de la IA emergen como una solución para optimizar la gestión de estos riesgos, ofreciendo la capacidad de efectuar controles constantes y eficientes, sin verse afectada por la fatiga.

En este sentido, teniendo en cuenta los costos asociados a amenazas internas a los cuales se ven expuestas, la inversión en tecnologías como la analítica de video inteligente y las herramientas UEBA, se ve más que justificada cualquiera sea la opción que se elija, dado el precio de estas tecnologías en comparación con los beneficios que ofrecen.

En resumen, la IA y estas tecnologías son esenciales para fortalecer la seguridad y la resiliencia de las organizaciones contra las amenazas internas, proporcionando una monitorización constante y eficaz, análisis avanzados y respuestas rápidas ante posibles amenazas.

Agradecimientos y Reconocimientos

El presente trabajo fue realizado en el contexto del proyecto: TOECRO0008583 – 'Modelización de un Sistema de Diagnóstico de Riesgos de Seguridad de la Información para su Integración a Sistemas de Gestión de Calidad' de la Universidad Tecnológica Nacional radicado en la Facultad Regional Rosario (Universidad Tecnológica Nacional – Facultad Regional Rosario, 2023).

Agradecemos a nuestro equipo de Investigación conformado por docentes y alumnos que siempre están para las dudas que nos van surgiendo y para asesorarnos con la experiencia que ellos poseen. Como así también al especialista Juan Manuel Rodríguez Guerrero quien puso a disposición su tiempo para brindarnos información respecto de la implementación de sistemas de videovigilancia.

Referencias bibliografías

Angulo Cárdenas, W. X. (2023). Propuesta de estrategia para evitar la fuga de información en empresas constructoras utilizando detección por comportamiento (UEBA) CASO DE ESTUDIO: SCMI INC (USA). Tesis de maestría, Universidad Tecnológica Israel, Quito, Ecuador.

Bosch Security Systems. (2021). Intelligent Video Analytics 8.10. Bosch. Disponible en [https://resources-boschsecurity-cdn.azureedge.net/public/documents/DS_IVA_7.10_Data_sheet_esES_69630079883.pdf].

AJEA – Actas de Jornadas y Eventos Académicos de UTN
Libro de actas de resúmenes DOI: https://doi.org/10.33414/ajea.1640.2024
Texto Completo Publicado en AJEA – Full Text Published in AJEA
https://rtyc.utn.edu.ar/index.php/ajea/article/view/1639

Castro Arteaga, R. A. (2023). Evaluación de un prototipo de un sistema de vigilancia bajo protocolo ONVIF perfil D, para una empresa de seguridad. Tesis de doctorado, Universidad de Guayaquil. Facultad de Ingeniería Industrial. Carrera de Lic. en Sistemas de Información.

Delgado, A. (2021). El enemigo en casa: la gestión de las amenazas internas. Revista SIC: ciberseguridad, seguridad de la información y privacidad, 30(146), 148-150.

Fabbri, L. M., & Dolan, G. (2022). Los recursos humanos como eje fundamental en la mitigación de riesgos de seguridad de la información en las organizaciones. En memorias: CONAIISI 2022. 10mo Congreso Nacional de Informática e Ingeniería en Sistemas de Información. UTN Facultad Regional Concepción del Uruguay. Publicación online - ISBN 978-950-42-0218-9.

Montes, G. R. (2021). Inteligencia Artificial en la Seguridad de TI. INF-FCPN-PGI Revista PGI, páginas 99-101.

Ponemon Institute. (2020). 2020 Cost of Insider Threats: Global study. IBM Security.

Proyecto: Modelización de un sistema de riesgos de seguridad de la información (SDRSI) para su integración a sistemas de gestión de calidad. Código: TOE-CRO0008583 Vigencia: Del 1/4/2023 al 31/03/2025. Universidad Tecnológica Nacional – Facultad Regional Rosario.

Riva, F. M., Maenza, R. R., Pereira, N., Font, G., Martin, V., Fabbri, L., Dolan, G., Butti, J., & Bidart, F. (2022). Modelización de un sistema de Riesgos de Seguridad de la Información (SDRSI) para su integración a Sistemas de Gestión de Calidad. En memorias: CONAIISI 2022. 10mo Congreso Nacional de Informática e Ingeniería en Sistemas de Información. UTN Facultad Regional Concepción del Uruguay. Publicación online - ISBN 978-950-42-0218-9.

Schultz, E. E. (2002). A framework for understanding and predicting insider attacks. Computers & Security, 21(6), 526-531.

Securonix. (2023). User and Entity Behavior Analytics. Documento técnico proporcionado por el fabricante. Disponible en [https://www.securonix.com/wp-content/uploads/2021/12/Datasheet_UEBA-1.pdf].