# Metodología aplicada para la automatización de Respuesta a Incidentes para la oficina de Seguridad de la Información

Juan José Ochoa Gnecco
*Maestria en Seguridad de la Información*
*Universidad de los Andes*
Bogotá, Colombia
jj.ochoa@uniandes.edu.co

Juan Esteban Vergara Ascencio
*Maestria en Seguridad de la Información*
*Universidad de los Andes*
Bogotá, Colombia
je.vergara@uniandes.edu.co

***Abstract*—Este documento plantea el proceso de construcción para una metodología para la automatización a respuestas para incidentes y reducción de la carga de trabajo para la oficina de la Seguridad de la Información. Con esto se obtiene información critica de Seguridad de la Universidad de los Andes y opciones de respuesta automáticas. Además, se mide su desempeño y se explica su despliegue junto con consejos practicos.**

***Index Terms*—Metodología, Logs, Automatización, Analítica, Seguridad, Respuestas, Patrones, Riesgos.**

## I. Introducción

En el entorno de Seguridad Informática el recurso del tiempo es critico para la correcta respuesta a eventos de riesgo. Lastimosamente la carga de trabajo alta con mucha facilidad puede dificultar el trabajo de aquellos encargados de la Seguridad de la Información en una empresa como la Universidad de los Andes, pero no es una situación sin salida. Las automatizaciones surgen como una herramienta de soporte ideal para reducir significativamente la carga de trabajo de la oficina de Seguridad de la Información.

## II. Problema

Las Universidades, particularmente las de mayor renombre del país, son focos de múltiples ataques de forma diaria. Según la revista La República [1], el sector educativo se encuentra entre los objetivos mas vulnerables de ataques en Colombia. Sin importar la cantidad de medidas preventivas que se tomen, siempre hay un riesgo latente de ataques cada vez mas avanzados y es importante contar con personal capacitado para dar respuesta a estas eventualidades. Según IBM [2], Colombia es el país con mas ciberataques en Latinoamérica, pero en estas condiciones los equipos encargadas de la Seguridad Informática ya cuentan con las manos llenas con el trabajo diario.

En 2023 , Colombia registró aproximadamente 12.000 millones de intentos de ciberataques, según FortiGuard Labs de FortiNet [3]. Aunque esta cifra es menor que la declarada en el 2022, da indicios de un enfoque en ataques mas especializados. Las tecnologías necesarias para que la oficina de Seguridad de la Información sea capaz de defenderse deben estar al filo de lo mas efectivo y en entornos universitarios donde el flujo de peticiones a servicios o usuarios es constante y alto, la seguridad se convierte en un componente fundamental que debe ser lo mas robusto posible.

## III. Propuesta de Solución

### A. Propuesta

Para prevenir los potenciales escenarios de riesgo se propone la recopilación de información sobre las amenazas de Seguridad que enfrenta la oficina de Seguridad de la Información, identificar eventos de interés que puedan ser resueltos por medio de automatizaciones que respondan apropiadamente acorde a las necesidades de la Universidad, estructurar un proceso para la identificación y solución de dichos eventos para finalmente automatizar este procedimiento de respuesta haciendo uso de herramientas para la estructuración de respuestas automáticas vinculadas a reglas de detección. Todo esto en conjunto planteado como una metodología que pueda repetirse de forma periódica para mantener la Universidad de los Andes segura.

### B. Objetivos

*1) Objetivo General:*

- Definir una metodologia replicable y periodica en Microsoft Azure para la gestión de incidentes de seguridad para la Universidad e los Andes, que incluya la identificación, diseño y construcción de programas que permitan automatizar la respuesta a incidentes, mejorar la eficiencia en la mitigación de amenazas, y reducir la carga operativa sobre el equipo de TI de la Universidad.

*2) Objetivos Específicos:*

- Analizar la distribución de Azure Sentinel en la Universidad, comprendiendo su configuración actual y capacidades.
- Identificar principales necesidades y desafíos que la oficina de Seguridad de la Información enfrenta en la gestión de eventos de seguridad.

- Recopilar y analizar datos estadísticos sobre las amenazas generadas para identificar patrones y áreas críticas que requieren atención.
- Diseñar y programar los componentes que se encarguen de la automatización del manejo de los incidentes identificados.
- Desarrollar y ejecutar una PoC para validar la efectividad de las automatizaciones desarrolladas en un entorno controlado antes de su despliegue en la red principal.
- • Desarrollar una metodología que permita a la oficina de Seguridad de la Información crear y adaptar nuevas automatizaciones, para que puedan continuar automatizando la respuesta a incidentes de manera eficiente y autónoma en el futuro.

## IV. Requerimientos

### A. Tecnológicos

- Los programas que se crearán deben ser compatibles con Azure Sentinel dado que esta es la herramienta que actualmente usa la universidad como SIEM.
- Un entorno controlado para realizar pruebas de concepto, es decir un grupo de amenazas controladas que no representen un riesgo en la Universidad para probar la efectividad de la automatización.

### B. Regulatorios

- Cumplimiento normativo, incluyendo el GDPR, para asegurar que el desarrollo e implementación del producto respete las regulaciones pertinentes.

### C. Funcionales

- Extraer de las fuentes de datos relevantes. Con el objetivo de recopilar la información correspondiente a la problemática a solventar.
- Realizar la adecuada analítica sobre los datos obtenidos de las fuentes de información de Microsoft Azure, identificando puntos críticos para la automatización, como patrones de comportamiento sobre los eventos o la construcción de listas negras y blancas acorde al comportamiento de los datos.
- Identificar de eventos de interés cuyas soluciones se definen como una cadena de eventos automatizados que cumplan con los requisitos flexibles de seguridad que necesitan.
- Estructurar estas cadenas de eventos para su apropiada automatización.

### D. No Funcionales

- Dar acceso a la oficina de Seguridad de la Información un rastro de las acciones ejecutadas durante la construcción de las automatizaciones, estos rastros incluyen histórico de información y eventos identificados e histórico de resultados de cada iteración de la automatización.
- Mantener el modelo de solución abierto a posibilidades de escalamiento y flexibilidad, estas métricas se definirán más adelante en el proyecto.

## V. Arquitectura de Alto Nivel

Se plantea una Arquitectura de Alto Nivel cíclica que ejecuta de forma periódica las etapas fundamentales de la metodología. Iniciando con la extracción de los datos disponibles y relevantes de Microsoft Azure, posteriormente la ejecución de la analítica sobre los datos obtenidos con el objetivo de extraer información critica; esto usando métodos como búsqueda de patrones de comportamiento, clustering y frecuencias con las que se repiten eventos. Continuando la metodología, se construye una regla capaz de identificar los eventos asociados a la información obtenida y una respuesta automática que satisfaga las necesidades de la oficina de Seguridad de la Información para posteriormente probar su desempeño.

Esta arquitectura permite repetir esta metodología periódicamente para mantener las automatizaciones vigentes a las necesidades cambiantes del ambiente de Seguridad Informática de la Universidad y responder a posibles fallos en el proceso.


Fig. 1. Arquitectura de alto nivel.

## VI. Capitulo Analítico

### A. Procedimiento para la Analítica

Para una obtención de información valiosa y útil para la solución de necesidades de la Universidad se busca la extracción de los datos mas relevantes para la oficina de Seguridad de la Información. Inicialmente se realiza una indagación exhaustiva sobre las acciones que ejerce el equipo para defender la Universidad y se toman decisiones sobre los datos mas relevantes disponibles en los Logs de Microsoft Azure, ya que la plataforma soporta una gran cantidad de eventualidades y amenazas, es preferible ser selectivo y no acumular datos que no contengan información relevante. Siguiente a la obtención de los datos, por medio de practicas de

búsqueda de patrones y búsqueda de sucesos mas repetidos se identifican características que tiendan a aparecer en amenazas de tipos específicos, como filtración de credenciales, intentos de fuerza bruta, etc. Todo esto con el propósito de construir una regla que sirve como ”malla” que filtra el paso de los eventos de seguridad y retiene aquellos que cumplan con las características identificadas, esto para poder agruparlas y solucionarlas automáticamente.

Para la ejecución de esta analitica se aconseja dividir el proceso en los siguientes pasos:

*1) Extracción de datos de Microsoft Azure:* Debido a que la metodología propuesta gira entorno a los Logs de Seguridad de Microsoft Azure, es fundamental identificar que datos pueden obtenerse de Microsoft Azure, cuales de estos son útiles pson datos que son usados como indicadores para identificacion de incidentes y asegurarse de que puede exportar un volumen de datos que sea representativo temporalmente de forma completa y sin inconsistencias. En el caso de esta metodología se aconseja un mínimo de 6 meses para poder ejecutar los pasos posteriores de forma satisfactoria. En este paso solo se necesita estar familiarizado con las herramientas disponibles en Microsoft Azure.

*2) Búsqueda y extracción de Información:* Con los datos previamente exportados en el paso anterior se debe realizar una exploración exhaustiva de los mismos. Para esta tarea existen múltiples herramientas y métodos para el análisis de datos, entre las opciones que pueden contemplar se encuentra Power BI, Tableau, incluso Excel. Sin embargo, para poder realizar un análisis mas profundo y manipular los datos de forma mas directa en esta sección se aconseja la construcción de notebooks desarrollados en el ambiente Jupyterlab y con la incorporación de la librería Pandas disponible en Python en conjunto con librerías de apoyo que soportan actividades extra en el análisis.

Con el uso de de estos notebooks o de las otras herramientas se puede iniciar una exploración y búsqueda de información en los datos de Microsoft Azure, inicialmente se deben buscar datos relacionados con los indicadores de eventos mas recurrentes y características mas repetidas en ventanas de tiempo.

Posterior a esta búsqueda inicial se deben buscar patrones de riesgo en los datos. Un porcentaje grande de los datos de Seguridad en Microsoft Azure que tienen una antigüedad mayor a 15 días cuentan con una etiqueta que identifica los eventos como riesgos reales o descartados, haciendo uso de esto se pueden buscar los patrones con mayor facilidad; Se puede hacer una revisión individual de parámetros para evaluar su comportamiento, agrupación de parámetros e incluso recorrer los datos en búsqueda de patrones con algoritmos de fuerza bruta. Pero una opción mucho mas avanzada es la búsqueda de patrones usando modelos de Clustering, esta ultima opción puede revelar patrones de riesgo mas específicos y mas sutiles que las demás formas de identificación pueden pasar por alto. Nuevamente estos indicadores deben seguir en toda la medida de lo posible información que indique la mayor cantidad de ocurrencias.

*3) Selección de información de patrones de riesgo:* Por ultimo, de toda la información extraída se debe consultar con la oficina de Seguridad de la Información si esta misma es útil, representativa y no es información que solo representa una ocurrencia aislada en vez de un patrón constante. Cabe aclarar que esto no es una comunicación de toma de decisiones unilaterales, la información que se encuentra se debe consultar con la oficina de Seguridad de la Información pero también presentar como hallazgos y discutir su veracidad.

La información resultante es el resultado final de todo el capitulo analítico y el pilar sobre el que se construyen los apoyos automáticos de respuesta.

## VII. Construcción de apoyo automático de respuesta

### A. Diseño y Construcción del Playbook

La implementación de playbooks automatizados en plataformas de seguridad permite gestionar incidentes de manera eficiente, reduciendo el tiempo de respuesta y minimizando el impacto en las operaciones. Este proyecto se enfoca en diseñar una solución automatizada que responde de forma proactiva ante eventos clasificados como riesgosos, utilizando una metodología estructurada para la identificación, análisis y resolución de incidentes.

Un playbook típico puede incluir múltiples flujos de acción. Entre las respuestas automatizadas más comunes se encuentran el cambio forzoso de contraseñas en cuentas comprometidas, el bloqueo de cuentas ante amenazas críticas y el descarte de eventos clasificados como falsos positivos. Estas acciones se desencadenan a partir de eventos detectados por sistemas de monitoreo, los cuales analizan patrones de actividad en las cuentas de usuario.

Para una implementación efectiva, se utiliza un enfoque basado en análisis de datos, donde se identifican patrones de riesgo en los registros de actividad. Estos datos son procesados para generar reportes detallados, los cuales son revisados y aprobados antes de activar las acciones automatizadas. Posteriormente, el sistema notifica a los usuarios afectados, brindándoles la posibilidad de confirmar si reconocen las actividades sospechosas. En caso de inacción o falta de respuesta, el sistema aplica medidas de protección adicionales, como el cambio automático de credenciales y la invalidación de sesiones activas.

El diseño de este playbook incluye mecanismos para realizar consultas avanzadas, filtrar datos relevantes y ejecutar acciones específicas de mitigación. Además, se propone una estructura modular que facilita la adaptabilidad y la integración con otras soluciones de seguridad. Esta metodología puede ser aplicada en diversos entornos organizacionales, con el fin de buscar una respuesta más rápida y efectiva a incidentes de seguridad, mientras se optimizan los recursos disponibles y se mejora la capacidad de detección y mitigación de amenazas.

## VIII. Despliegue en un entorno real

Finalmente, después de la construcción completa de la automatización, se debe pasar un tiempo en un entorno de

pruebas para asegurarse de que el desempeño de las automatizaciones mejora los tiempos de respuesta y cumple con la meta inicial de reducir la carga de trabajo de la oficina de Seguridad de la Información. Para un despliegue en un entorno real completo se deben realizar estas pruebas; Por esto se aconsejan seguir los siguientes pasos.

### A. Pruebas de desempeño de la automatización

Antes de un despliegue sin limitaciones de los componentes de la automatización en la red objetivo, se necesita tener 2 grupos de cuentas con el único objetivo de ser usadas para pruebas por un lapso de tiempo y posterior eliminación de las credenciales. Teniendo estos grupos en su poder, elegir cualquiera de los 2 arbitrariamente como el equipo A de medición de automatización y el otro como equipo B espejo para comparación.

Luego, debe añadir un filtro en el factor analítico que ejecuta la automatización para que solo busque automatizar las respuestas de los eventos generados por las cuentas del equipo A de medición de automatización. De esta forma puede tener la automatización encendida sin afectar el desempeño de los sistemas objetivo.

Posteriormente, tome todas las cuentas de ambos grupos y busque levantar los eventos de riesgo identificados en el capitulo analítico sobre TODAS estas cuentas de forma simultanea y cada cierto tiempo, ya sea con el uso de VPNs, simulaciones de ataques de fuerza bruta, etc. De esta forma el equipo A de cuentas será manejado por la automatización y el equipo B será manejado por la oficina de Seguridad de la Información como en un escenario normal. Ya que la mitad de las cuentas serán manejadas como eventos de riesgo directamente por el equipo de Seguridad de la Información es recomendable que la cantidad de cuentas sea moderada.

Esto debe mantenerse por una semana y medir diferentes parametros para calcular KPIs, los que se desean medir deben estar relacionados a tiempo de respuesta y efectividad de la respuesta. De esta forma para el final de la semana de pruebas se tiene información suficiente para comparar el desempeño de la automatización con el equipo de Seguridad de la Información.

### B. Análisis de resultados de pruebas

Con los resultados obtenidos de las pruebas, se debe establecer un margen que se considere exitoso en la comparación entre equipo A y B. Tenga en cuenta que tiempos de respuesta similares o resultados similares en la comparación no son necesariamente negativos, esto también puede concluir que la automatización cumple su propósito de dar respuesta de forma efectiva y reducir la carga de trabajo de la oficina de Seguridad de la Información. Por esto debe elegirse un margen considerando los objetivos del proyecto y no buscando escenarios ideales.

Si bajo los margenes seleccionados las respuestas del equipo A son satisfactorias respecto al equipo B, se considera la automatización como un éxito y se le da una vigencia de 6 meses. Esta vigencia se establece ya que los patrones de riesgo pueden cambiar por motivos completamente impredecibles.

En el caso contrario, se debe indagar sobre los motivos del desempeño negativo y decidir si son motivos solucionables para volver a iniciar el capitulo de construcción de automatización o descartar la información del capitulo de analitica e iniciar de nuevo desde ”Busqueda y extracción de Información” descartando las conclusiones ya encontradas de ese capitulo con tal de encontrar nuevas.

### C. Despliegue y practicas posteriores recomendadas

Luego de las pruebas, todo lo que se necesita para desplegar la automatización es remover el filtro de cuentas de prueba y hacer un seguimiento de un mes de las respuestas generadas por la misma. Esto debido a que el usuario siempre puede encontrar escenarios no previstos y afectar negativamente el desempeño de la Solución.

Como practicas posteriores se recomienda continuar con la exportación de datos de forma paralela al despliegue de la automatización con el objetivo de proyectarse para la siguiente iteración de la metodología, para repetirla y reemplazar las automatizaciones previas con nuevas y adaptadas a las necesidades del momento futuro.

## IX. Conclusiones

Para finalizar, los resultados obtenidos demostraron ser prometedores e incentivaron a la producción de la metodología como un servicio con los productos incluidos para soportar la analítica. Una ejecución correcta con un volumen adecuado de datos puede dar resultado a una reducción de carga de trabajo considerable para la oficina de Seguridad de la Información. Esperamos que nuestro trabajo sea de suma utilidad y cumpla con el propósito de ayudar a la Universidad y proteger a su comunidad.

## References


[1] Gutierrez Núñez, “Las empresas que han sido blanco de ciberataques en Colombia en el último año” Disponible en https://www.larepublica.co/empresas/epm-y-afinia-entre-las-companias-que-han-sido-victimas-de-ciberataques-en-el-ano-3510742, 2023.

[2] Gartner, “Predicts 2024: Network Security and Automation” www.gartner.com, 2021.

[3] Vanguardia, “En Colombia se reportaron 12.000 millones de intentos de ciberataques en 2023” Disponible en https://www.vanguardia.com/mundo/tecnologia/2024/04/01/en-colombia-se-reportaron-12000-millones-de-intentos-de-ciberataques-en-2023-que-esta-pasando/, 2023.