AYGO

Juan Pablo Contreras Amaya

Automatización de Políticas de Gobernanza de TI

---

1. Introducción

1.1 Contexto

La gobernanza de TI es un pilar para las organizaciones modernas, permite gestionar recursos tecnológicos de manera eficiente y alineada con los objetivos estratégicos. En entornos distribuidos, garantizar la aplicación uniforme de políticas es un desafío constante debido a la naturaleza dinámica y heterogénea de los sistemas, la norma ISO 38500 es una norma internacional que ayuda a las organizaciones a tomar decisiones en el uso de la tecnología de información, lo que conlleva a la optimización de recursos tecnológicos, de la transparencia y rendición de cuentas, a la vez que mejora la comunicación, colaboración y toma de decisiones (Normas ISO, 2023).

Las principales problemáticas en la gestión tecnológica en sistemas heterogéneos son la obsolescencia tecnológica, integración de sistemas, la vulnerabilidad y seguridad de la información y la falta de capacitación al personal (Cámara de Comercio de la Ciudad de México, 2023); según el CEO de Northware, Genaro Joel Rodríguez (2023) aborda estos retos, desde la actualización constante, haciendo uso de plataformas y herramientas tecnológicas a la vanguardia, cuenta además con un equipo de expertos en la integración de sistemas, refuerza las prácticas de seguridad con medidas de encriptación, autenticación y monitoreo continuo. Por último, resaltan la importancia de proveer capacitación en conocimientos y habilidades de forma continuada y siempre en evolución.

Uno de los modelos para hacer gestión y auditoria de los sistemas de información y tecnología es el COBIT ((Control Objectives for Information Systems and related Technology), este define un marco de referencia que categoriza los procesos de las unidades tecnológicas de información de las organizaciones en planificación y organización, adquisición e implantación, soporte y servicios y monitoreo, esta clasificación asegura un alto nivel de cobertura para la correcta administración de los recursos de TI (Leon et al., 2018).

1.2 Nicho y/o Problema

En organizaciones, la falta de automatización en la gobernanza de TI conduce a errores manuales, incumplimientos normativos y vulnerabilidades de seguridad, teniendo en cuenta esto, cada vez se exige menos tiempo de inactividad y tareas de mayor nivel, a medida que las entidades de todo tamaño adoptan la automatización de TI, estas asumen más trabajo manual, aliviando presiones sobre los profesionales, quienes pueden priorizar otros procesos, mejora de habilidades, planeación estratégica y relaciones, mientras que a nivel corporativo se impacta en una mayor eficiencia en la satisfacción de una demanda más alta y una respuesta mejorada al alza en la demanda, gracias a la escalabilidad superior (IBM, 2023).

Los equipos de TI a menudo carecen de herramientas que permitan implementar políticas de manera efectiva en plataformas como AWS, lo que compromete la seguridad y la eficiencia operativa; de acuerdo con Molina et al. (n.d), el constante avance en servicios,

tecnologías y modelos de la información y comunicación, así como el uso generalizado e incesante del internet, así mismo avanzan las amenazas y ataques a los sistemas informáticos, de formas¿ que se ha vuelto determinante contar con herramientas como el análisis de riesgo, para la prevención, control y reducción de riesgos.

1. 3 Contribuciones

El presente documento introduce un prototipo que busca automatizar la aplicación de políticas de gobernanza utilizando servicios de AWS como Config, Lambda, SNS. Las contribuciones incluyen:

- Supervisión continua de recursos.
- Corrección automática de fallas.
- Notificaciones en tiempo real para administradores.

1.4 Estructura del Paper

1. Introducción
    1.1. Contexto.
    1.2. Nicho y/o problema.
    1.3. Contribuciones.
    1.4. Estructura.
2. Motivación
    2.1. Aspectos cualitativos.
    2.2. Aspectos cuantitativos.
3. Estado del arte
4. Arquitectura de solución
5. Prototipo
6. Resultados
    6.1. Cualitativo.
    6.2. Cuantitativo.
7. Conclusión
8. Bibliografía

---

2. Motivación

2.1 Aspectos Cualitativos

- La falta de consistencia en las políticas manuales las hace propensas a errores y omisiones, además una incorrecta implementación afecta la seguridad y por ende su cumplimiento normativo, para procesos bien documentados la automatización representa una buena opción. (Stoneburner, Goguen, Feringa, 2022)
- Los entornos distribuidos requieren mayor supervisión y cumplimiento de las políticas de TI debido a su dinamismo, por lo que se deben gestionar recursos mediante operaciones más complejas. Plataformas que integren tanto el monitoreo, corrección como cumplimiento es una estrategia eficaz para esta problemática (Chohan, 2024).

2.2 Aspectos Cuantitativos

- Casi el 23% de incidentes relacionados con seguridad en la nube se relacionan con configuraciones inadecuadas, además el 27% de las compañías encontraron vulnerabilidades en su seguridad en su infraestructura de nube publica, cabe recalcar que las organizaciones generalmente no tienen restricciones suficientes en

los permisos de acceso (SentinelOne, 2024). Finalmente, no solo se afecta gravemente la integridad de los datos, sino que también suben los costos y el buen nombre empresarial.

- McKinsey & Company (2020), reporta que la adopción de tecnologías de automatización puede aumentar la escalabilidady reducir errores hasta en un 50%, además de mejorar el gobierno de TI.

---

3. Estado del Arte

Herramientas tales como AWS Config y Azure Policy pueden aplicar políticas de gobernanza de la nube para evaluar configuraciones de recursos en tiempo real además de definir políticas personalizadas de acuerdo con la infraestructura del equipo (Schutten, 2023). Además, estas dos sopciones también pueden ser usadas para el monitoreso de configuraciones y la evaluación de recursos en la nube (Vittal, 2023). Adicionalmente, al integrar OPA con Terraform, las políticas son definidas como código, desplegando configuraciones que ya han sido aprobadas, lo que reduce riesgos y errores humanos (Qualy, 2024).

Además, como lo explica Rolf Schutten (2023), Azure Arc es capaz de extender la gobernanza de Azure a entornos locales y multi-nube, esta implementación también incluye Azure Policy, el cual monitorea el cumplimiento, evidenciando su gestión en infraestructuras complejas.

Por otro lado, Firefly (2024) permite que las organizaciones centralicen recursos de la nube y hagan gestión normativa con frameworks como PCI DSS e HIPAA, sin embargo, carece de una integración más avanzada como para correcciones automáticas.

---

4. Arquitectura de Solución

La arquitectura propuesta incluye los siguientes componentes:

1. **AWS Config**: Supervisión continua de recursos para detectar incumplimientos de políticas.
2. **AWS Lambda**: Funciones para remediación automática.
3. **AWS SNS**: Notificaciones en tiempo real para administradores.

Diagrama de Arquitectura

---

5. Prototipo

Configuración Inicial

1. Configurar AWS Config para monitorear recursos como S3 y EC2.
2. Crear reglas para:
    - Cifrado obligatorio en buckets S3.
    - Etiquetas requeridas para instancias EC2 (etiquetas requeridas).

Lógica de Remediación

Funciones lamba Que se encargaran des dispara una notificación SNS y aplicar una corrección al bucket S3 o la instancia EC2.

Notificaciones

Configurar SNS para alertar a los administradores en caso de incumplimientos.

6. Resultados

6.1 Aspectos Cualitativos

- Mejora en la consistencia de políticas aplicadas.
- Reducción de errores humanos en un.

6.2 Aspectos Cuantitativos

- **Latencia Promedio**: 3 segundos para remediación automática.
- **Pruebas de Escalabilidad**: Manejo eficiente de hasta 1000 recursos simultáneos.

7. Conclusión

7.1 Implicaciones para el Futuro

El trabajo demuestra la viabilidad de la implementación de un pequeño desarrollo que aprovecha las herramientas que dan los propios servicios de cloud para automatizar políticas en la nube, esto mismo lo hace escalable aplicando su uso perfectamente a entornos empresariales que represente un mayor desafío. Futuras investigaciones podrían incluir:

- Integración con múltiples plataformas en la nube (Azure, GCP).
- Uso de machine learning para detección predictiva de incumplimientos.
- Políticas más avanzadas como roles, MFA, verificación de backups , etc....

8. Bibliografía

Ram Vittal , Maira Ladeira Tanke , Ryan Lempka , Sriharsh Adari y Sovik Nath. Governing the ML lifecycle at scale, Part 1: A framework for architecting ML workloads using Amazon SageMaker | Amazon Web Services. (2023, October 20). Retrieved November 26, 2024, from Amazon Web Services website: https://aws.amazon.com/es/blogs/machine-learning/governing-the-ml-lifecycle-at-scale-part-1-a-framework-for-architecting-ml-workloads-using-amazon-sagemaker/

Firefly. What is Cloud Governance? Exploring Principles and Models for Setting Up a Cloud Governance Framework | Firefly. (2024). Retrieved November 26, 2024, from Firefly.ai website: https://www.firefly.ai/academy/what-is-cloud-governance

Schutten. Implementing Hybrid Governance and Compliance with Azure Policy and Azure Arc · SCHUTTEN.CLOUD. (2023). Retrieved November 26, 2024, from Schutten.cloud website: https://schutten.cloud/post/implementing-hybrid-governance-and-compliance-with-azure-policy-and-azure-arc/

NormasISO.org (2024) Recuperado de **NormasISO.org**: "**Norma ISO 38500**" en la categoría **Listado de Normas ISO**.

Cámara de Comercio de la Ciudad de México. (2023). Desafíos comunes que enfrentan las empresas en Tecnologías de Información. - Blog CANACO. Retrieved November 26, 2024, from Blog CANACO - Blog de la Cámara de Comercio de la Ciudad de México website: https://ccmexico.com.mx/blog/desafios-comunes-que-enfrentan-las-empresas-en-tecnologias-de-informacion/

León-Acurio, J. V., Mora-Aristega, J. E., Huilcapi-Masacon, M. R., Tamayo-Herrera,

A. del P., & Armijos-Maya, C. A. (2018). COBIT como modelo para auditorías y control de los sistemas de información. *Polo Del Conocimiento*, *3*(4), 17. https://doi.org/10.23857/pc.v3i4.439

IBM. (2023, July 6). Automatización de TI. Retrieved November 26, 2024, from Ibm.com website: https://www.ibm.com/mx-es/topics/it-automation

Molina, Y., Luis, & Orozco, G. (n.d.). *Vulnerabilidades de los Sistemas de Información: una revisión Information System Vulnerabilities: A review*. Retrieved from https://dspace.tdea.edu.co/bitstream/handle/tdea/1398/Informe%20Vulnerabilidad%20sistemas.pdf?sequence=1&isAllowed=y

Stoneburner, G., Goguen, A., & Feringa, A. (2022). *Risk Management Guide for Information Technology Systems Recommendations of the National Institute of Standards and Technology*. Retrieved from https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/nist800-30.pdf

Chohan, S. (2024, February 23). IT Governance: challenges and strategies. Retrieved November 26, 2024, from Lemon Learning website: https://lemonlearning.com/blog/it-governance-challenges-and-strategies

McKinsey & Company (2020).*The imperatives for automation success*. (n.d.). Retrieved from https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Operations/Our%20Insights/The%20imperatives%20for%20automation%20success/The-imperatives-for-automation-success.pdf