¿POR QUÉ ES NECESARIO AUDITAR SAP GRC ACCESS CONTROL?

En los últimos años, ha aumentado la tendencia de las empresas que implementan la solución SAP GRC Access Control u otras de similares características, con el fin de controlar el otorgamiento de privilegios en SAP ERP y otros aplicativos del entorno tecnológico, como también el provisioning de cuentas de usuario en los sistemas (altas, bajas y mantenciones del maestro de usuario), aplicando análisis de riesgo sobre los conflictos de interés (SoD, por sus siglas en inglés) y/o autorizaciones críticas.

Lo que no están haciendo las organizaciones o muy pocas lo hacen, es auditar el aplicativo SAP GRC Access Control o cualquier otro que cumpla esta función. ¿Por qué habría que auditarlo como parte del plan anual de auditoría? A continuación, les comentaré los 10 principales motivos:

1. Se debe revisar si los **aprobadores de privilegios o dueños de roles** en SAP GRC Access Control, son los que se autorizó en base a la política y/o procedimiento.
2. Se debe revisar que las **reglas de segregación funcional SoD para transacciones conflictivas**, no estén siendo desactivadas. Esta es una forma de mostrarle a los auditores (internos y/o externos) o a la organización de que hay pocos conflictos por incompatibilidades o por asignación de transacciones críticas, siendo que la realidad es otra.
3. Se debe revisar las **reglas SoD para transacciones Y-Z** que han sido creadas ad hoc a la organización y que las mismas estén cumpliendo los fines para los cuales fueron creadas. Se debe aplicar el mismo criterio escéptico del punto anterior. Asimismo, se debe revisar la combinatoria de reglas asociadas a conflictos de transacciones Y-Z con transacciones estándar.
4. Se debe revisar que las **reglas SoD para transacciones o autorizaciones criticas** estén activas, aplicando el mismo criterio escéptico que mencionamos en el número 2.
5. Se debe revisar que los **controles de mitigación denominados "firefighter FF"** estén debidamente asignados, tanto para FF ID como para FF role. Ciertas organizaciones tienden a colocar este tipo de controles de mitigación, para ocultar conflictos reales SoD o autorizaciones críticas.

6. Se debe revisar que los **workflow de aprobación operen de acuerdo a lo estipulado en las políticas y/o procedimientos** de aprobación de otorgamiento de privilegios y cuentas de usuario.
7. Se debe revisar que las **reglas de segregación de funciones SoD**, diseñadas a la medida de la organización o para cubrir verticales del "core business", **estén diseñadas e implementadas a nivel de objetos de autorización primario, secundario y complementario** (3 capas de seguridad de autorizaciones SAP ERP). Esto es por la potencial proliferación de falsos positivos en los reportes que conllevan a ineficiencia y/o ineficacia.
8. Se debe revisar que se **cumpla con los protocolos de control de cambio**, en el sentido que se administre SAP GRC Access Control, cumpliendo con la segregación de ambientes: Desarrollo, Prueba y Productivo, de acuerdo a lo que recomiendan las buenas prácticas.
9. Se debe revisar que la **integración con los sistemas sea integra y que tanto roles como usuarios**, estén siendo analizados de manera exacta y completa, respecto a lo que se administra en ambiente productivo de los sistemas analizados.
10. Se debe revisar que el **diseño e implementación de los controles de mitigación** para los conflictos SoD y asignación de autorizaciones críticas, **sea adecuado y que cubra los riesgos**. En este ámbito, se suele colocar controles que no guardan relación con el riesgo y se pierde visibilidad de los riesgos reales y su exposición.

Una de las herramientas que le permite al auditor (interno y/o externo) hacer auditorias independientes a las reglas tanto de conflictos de interés como de autorizaciones críticas, es la que posee SAP ERP y que menciono en el siguiente post: https://goo.gl/idYvG8 . De esta forma el revisor podrá comparar el resultado de la regla SAP GRC Access Control con el resultado de su prueba de auditoría y verificar si las reglas realmente están operando de acuerdo a los objetivos que fueron diseñadas e implementadas.

Pedro Hernández

GRC Latam (*)

(*) Pedro Hernández es Socio Fundador y CEO de GRC Latam. MAZARS en Perú cuenta con un Acuerdo de Colaboración con GRC LATAM para desarrollar en forma conjunta servicios relacionados con Governance, Risk & Compliance en SAP GRC.