Informe de Políticas de Seguridad: Prevención de Pérdida de Datos (DLP) en la Nube

Fecha: 01 de septiembre de 2025

Elaborado por: Gustavo Rodil

Empresa: CloudwareKnox

1. Introducción

Los servicios en la nube son hoy una de las principales plataformas para almacenar y procesar información dentro de CloudwareKnox. Sin embargo, sin un control adecuado, representan un riesgo importante de fuga de datos o accesos no autorizados.

Este informe propone una política de seguridad de DLP (Data Loss Prevention) aplicando el Principio del Menor Privilegio, para garantizar que cada usuario solo tenga acceso a los datos que necesita para realizar su trabajo.

2. Clasificación de Datos

Para gestionar mejor los permisos y accesos en la nube, la organización clasifica sus datos en tres niveles:

1. Datos Públicos (Baja): Información que puede compartirse abiertamente (ej. comunicados oficiales, material de marketing).

2. Datos Internos (Media): Información para uso exclusivo de la empresa, accesible solo por el personal autorizado (ej. manuales internos, reportes operativos).

3. Datos Sensibles (Alta): Información altamente confidencial (ej. datos financieros, PII de clientes, propiedad intelectual) restringida a personal autorizado bajo estricta necesidad.

3. Acceso y Control (Principio del Menor Privilegio)

- Acceso Restringido: cada empleado accede únicamente a los datos necesarios para sus tareas.
- Revisión Periódica: los permisos se revisan trimestralmente, revocando accesos innecesarios.
- Acceso Temporal: los permisos especiales se conceden con autorización formal y se eliminan al terminar el proyecto.
- Permisos de Edición: solo responsables directos pueden editar datos sensibles; el resto tendrá acceso de solo lectura.

4. Monitoreo y Auditoría

Se implementarán políticas de monitoreo en los servicios en la nube para detectar accesos no autorizados o malas prácticas:

- Registro de Actividades: se usará el log de auditoría del proveedor cloud (ejm: AWS CloudTrail).
- Alertas de Seguridad: notificaciones automáticas ante descargas masivas, accesos desde países no autorizados o compartición externa de documentos sensibles.

- Auditorías Trimestrales: revisión de accesos a datos sensibles y verificación del cumplimiento de las políticas.

5. Prevención de Filtraciones

- Compartición Controlada: deshabilitar la opción de 'cualquier persona con enlace' en documentos sensibles.
- Cifrado: todos los datos sensibles estarán cifrados en tránsito (TLS) y en reposo (AES-256).
- Etiquetas de Seguridad: documentos marcados como 'Confidencial' o 'Solo Interno' tendrán restricciones adicionales (ej. no descarga sin permiso).
- Bloqueo Automático: políticas DLP para impedir el envío de datos sensibles por correo corporativo o herramientas de colaboración.

6. Educación y Concientización

- Capacitaciones Trimestrales: formación obligatoria en el uso seguro de servicios en la nube y manejo de datos sensibles.
- Ejemplos Prácticos: casos de fugas comunes (ej. compartir mal un enlace en la nube) y cómo evitarlos.
- Campañas Internas: recordatorios visuales en la intranet y correos con tips de ciberseguridad.

7. Conclusión

La aplicación del Principio del Menor Privilegio junto con políticas claras de DLP permite proteger la información más sensible de CloudwareKnox en la nube. Con monitoreo continuo, cifrado, controles de acceso y concienciación del personal, se reducen significativamente los riesgos de accesos indebidos o filtraciones.