

SKYTEL	Alerta de DLP Google Workspace		
	Fecha de Creación:	Creado por: SkyTel Procesos	Versión del Documento:
	Fecha de Modificación:	Modificado por:	Aprobado por:

SKYTEL

Alerta de DLP Google Workspace

Tabla de Contenidos

ALERTA DE DLP GOOGLE WORKSPACE 1

1 ALERTA DE DLP GOOGEL WORKSPACE 2

1.1 ALERTA DE DLP GOOGLE WORKSPACE 3

1.1.1 ELEMENTOS DEL PROCESO 3

1.1.1.1 Inicio 3

1.1.1.2 Google Rule 3

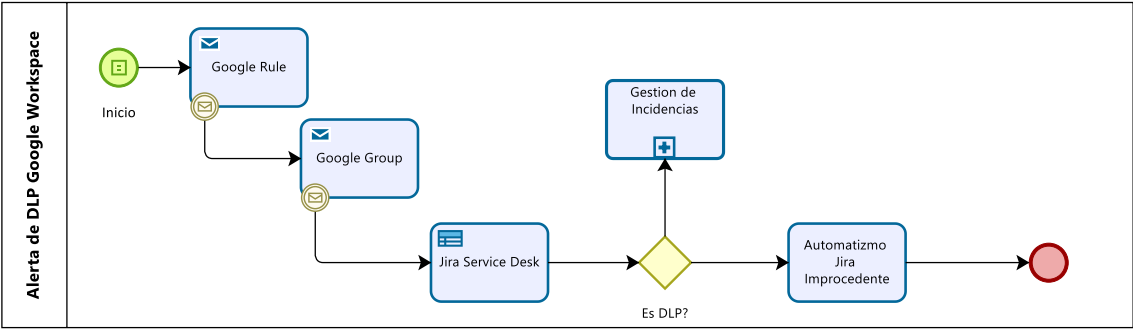
1.1.1.3 Google Group 4

1.1.1.4 Jira Service Desk 4

1.1.1.5 Gestion de Incidencias 5

1.1.1.6 Automatizmo Jira Improcedente 5

1 ALERTA DE DLP GOOGEL WORKSPACE



Powered by
bizagi
Modeler

Descripción

Dicho proceso determinará los pasos de una alerta de Data Loss Prevention dentro de la plataforma de Google Workspace

Versión: 1.0

Autor: Juan Manuel Lacy

1.1 ALERTA DE DLP GOOGLE WORKSPACE

1.1.1 ELEMENTOS DEL PROCESO

1.1.1.1 Inicio

Descripción

El alerta se inicia en base a una condición configurada en la regla <https://admin.google.com/ac/dp/rules/policies%2Fakajj264ao57zff6dm>

Dicha condición se base en la posibilidad de compartir números de tarjetas de crédito y/o números de cuenta.

Condiciones

Todo el contenido

Coincide con el tipo de datos: "Internacional: Número de tarjeta de crédito"

Todo el contenido

Coincide con el tipo de datos: "Internacional: Número de cuenta bancaria (IBAN)"

Todo el contenido

Coincide con el tipo de datos: "Internacional: Número de cuenta bancaria (SWIFT)"

Todo el contenido

Coincide con el tipo de datos: "Estados Unidos: Número de ruta de ABA"

Todo el contenido

Coincide con el tipo de datos: "Estados Unidos: CUSIP"

Todo el contenido

Coincide con la expresión regular: "TC"

1.1.1.2 Google Rule

Descripción

La misma regla establece las acciones, que en este caso consisten en:

1. Enviar al Centro de Alertas de Google un evento en prioridad alta
2. Notificar al Grupo <https://groups.google.com/a/skytel.tech/g/pci.dss> para la pronta notificación.

Alertas

Cuando un evento cumple con los criterios de esta regla (su alcance, sus apps y sus condiciones), el evento se informa en el panel de seguridad y en el Centro de alertas (si corresponde). Elige el nivel de gravedad con el que se informará el evento.

Alta

☒ Enviar al Centro de alertas

Las alertas del Centro de alertas incluyen información detallada adicional que te permite abordar problemas y colaborar con otros administradores de tu dominio para resolverlos. Te recomendamos que habilites este parámetro de configuración. [Más información](#)

Enviar notificaciones por correo electrónico

☐ Todos los administradores avanzados

Agregar destinatarios de correo electrónico

pci.dss@skytel.tech



[AGREGAR DESTINATARIOS](#)

Implementación

Servicio Web

1.1.1.3 Google Group

Descripción

El Grupo de Google esta configurado para que le reenvie los correos a los miembro y uno de los miembros es el correo de JIRA dlp@skytel.atlassian.net que transformara dicho correo en una incidencia.

Implementación

Servicio Web

1.1.1.4 Jira Service Desk

Descripción

Jira recibe el correo y en base a la condicion del contenido,

1. Contaco = pci.dss@skytel.tech
2. Asunto contine " Impedir el uso compartido de información financiera (Internacional)"

1.1.1.5 *Gestion de Incidencias*

Descripción

Crea un comentario en el TK

"REVISAR CON OPERACIONES LA ALARMA DE DLP POR EL USO DE TARJETAS DE CREDITO EN GOOGLE WORKSPACE"

Agrega una etiqueta "DLP" y mueve la prioridad a CRITICA

1.1.1.6 *Automatizmo Jira Improcedente*

Descripción

Mueve el TK a IMPROCEDENTE