

	PROCEDIMIENTO Y LINEAMIENTOS DE IMPLEMENTACIÓN DE DLP EN CORREO ELECTRÓNICO.	Clasificación:
		Versión: 2.0
		Fecha de Actualización: 22-septiembre-2024

1. OBJETIVO

Crear reglas para controlar el contenido que se maneja al interior de la compañía, Es decir los usuarios que tengan cuentas corporativas de correo electrónico y que manejen información en la nube mediante plataforma de Google.

2. ALCANCE

Dicho procedimiento va a tener un control aplicado en las plataformas de correo electrónico, así evitar fuga de información que posiblemente sea sensible para la compañía para todas las personas que manejen cuenta de correo corporativa y con alcance a servicios propios de la plataforma como lo son Drive, Gmail, actividades de calendarios, Grupos, Meet y Registros de usuarios.

3. DEFINICIONES

DLP (PREVENCIÓN DE PERDIDA DE DATOS):

La Reglas DLP (Prevención de Pérdida de Datos) de Google WorkSpace, son políticas de seguridad que ayudan a proteger información sensible como datos personales o información confidencial, de ser compartida o expuesta de manera no intencionada o no autorizada, estas reglas permiten a los administradores de Google WorkSpace establecer controles para detectar o bloquear la divulgación de datos críticos dentro de correos electrónicos de Gmail y archivos de Google Drive.

PRINCIPALES FUNCIONES DE LAS REGLAS DLP:

1. Detección de información sensible: La reglas DLP pueden detectar números de Tarjeta de crédito, Números de Cedula, Datos Financieros, Información médica entre otros tipos de información.
2. Acciones de Protección: Una vez detectada la información sensible, las reglas DLP pueden realizar acciones como bloquear el envío del correo, compartir del archivo, notificar al usuario o administrador.
3. Personalización: Los administradores pueden crear Reglas DLP personalizadas en necesidades específicas, definiendo que tipo de contenido debe ser monitoreado y las acciones a tomar cuando se detecte una posible violación-

Estas reglas son especialmente Útiles para evitar fugas de información accidental o mal intencionada dentro de RST ASOCIADOS PROJECT

LINEAMIENTOS

En Gmail, las reglas DLP (Prevención de Pérdida de Datos) permiten a RST ASOCIADOS PROJECT proteger información sensible al controlar cómo se manejan los correos electrónicos que contienen datos confidenciales. Las principales reglas DLP en Gmail se enfocan en detectar y gestionar ciertos tipos de datos críticos, como información personal o financiera.

	PROCEDIMIENTO Y LINEAMIENTOS DE IMPLEMENTACIÓN DE DLP EN CORREO ELECTRÓNICO.	Clasificación:
		Versión: 2.0
		Fecha de Actualización: 22-septiembre-2024

A continuación, se definen las reglas a implementar en la plataforma de Gmail para establecer controles en el envío y recepción de información sensible y prevenir la pérdida de datos:

1. Detección de información financiera

- Números de tarjetas de crédito o cuentas bancarias.
- Propósito: Evitar que los colaboradores envíen por error información financiera sensible fuera de la organización.
- Acción: rechazar el envío de correos con estos datos, o modificar mensaje.

2. Detección de información personal identificable

- Números de Seguro Social, números de identificación nacional, direcciones de correo físico.
- Propósito: Proteger la información personal del colaborador o de los clientes.
- Acción: Marcar el correo para revisión o bloquear el envío a destinatarios no autorizados.

3. Detección de información de salud protegida

- Datos médicos o relacionados con seguros de salud.
- Propósito: Cumplir con la protección de información sensible de la ley 100 y regímenes especiales de Salud en Colombia.
- Acción: Alertar al administrador de seguridad y evitar la exposición de estos datos.

4. Detección de patrones personalizados

- Creación de reglas específicas para detectar frases o patrones únicos de RST ASOCIADOS PROJECT SAS (contratos, Compras, datos de proyectos confidenciales).
- Propósito: Adaptarse a las necesidades específicas de la empresa en cuanto a seguridad de datos.
- Acción: Bloquear, poner en cuarentena o enviar una advertencia a los remitentes.

5. Detección de adjuntos no seguros o confidenciales

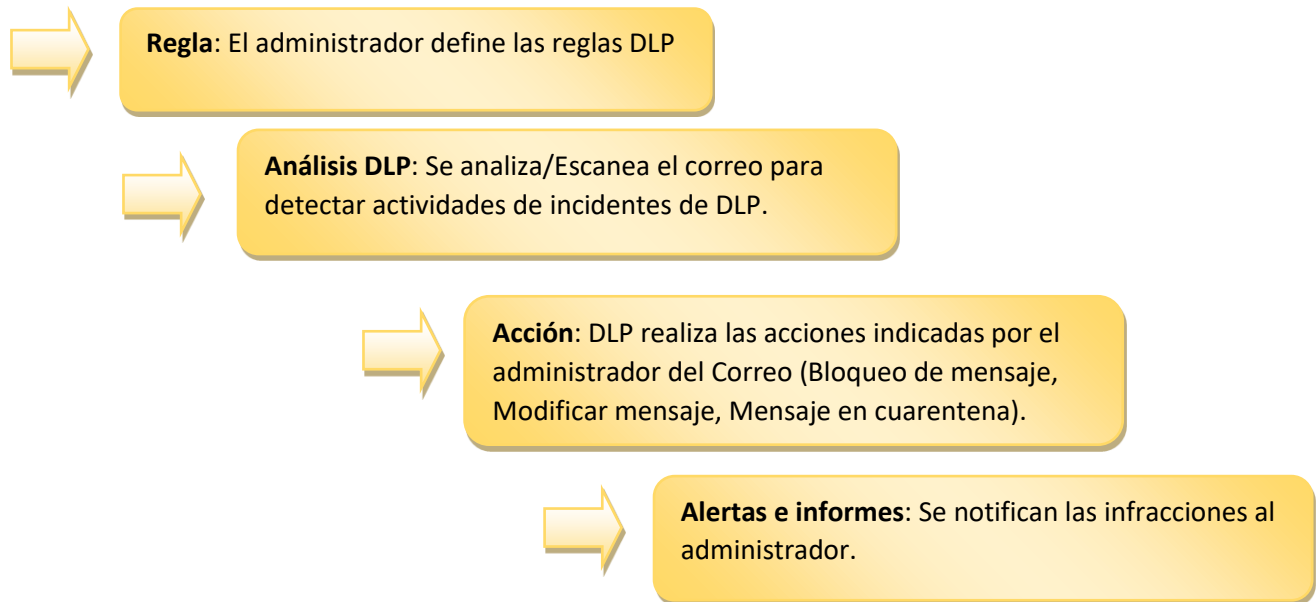
- Adjuntos con datos sensibles (archivos Excel con listas de clientes o informes financieros).
- Propósito: Evitar que archivos con información crítica se filtren fuera de la organización.
- Acción: Prevenir el envío de correos con adjuntos, o limitar el acceso a destinatarios autorizados.

6. Control de datos compartidos externamente

- Ejemplo: Restricción de correos electrónicos que contienen datos confidenciales enviados a dominios externos a la organización.
- Propósito: Evitar la fuga de información fuera de la empresa.

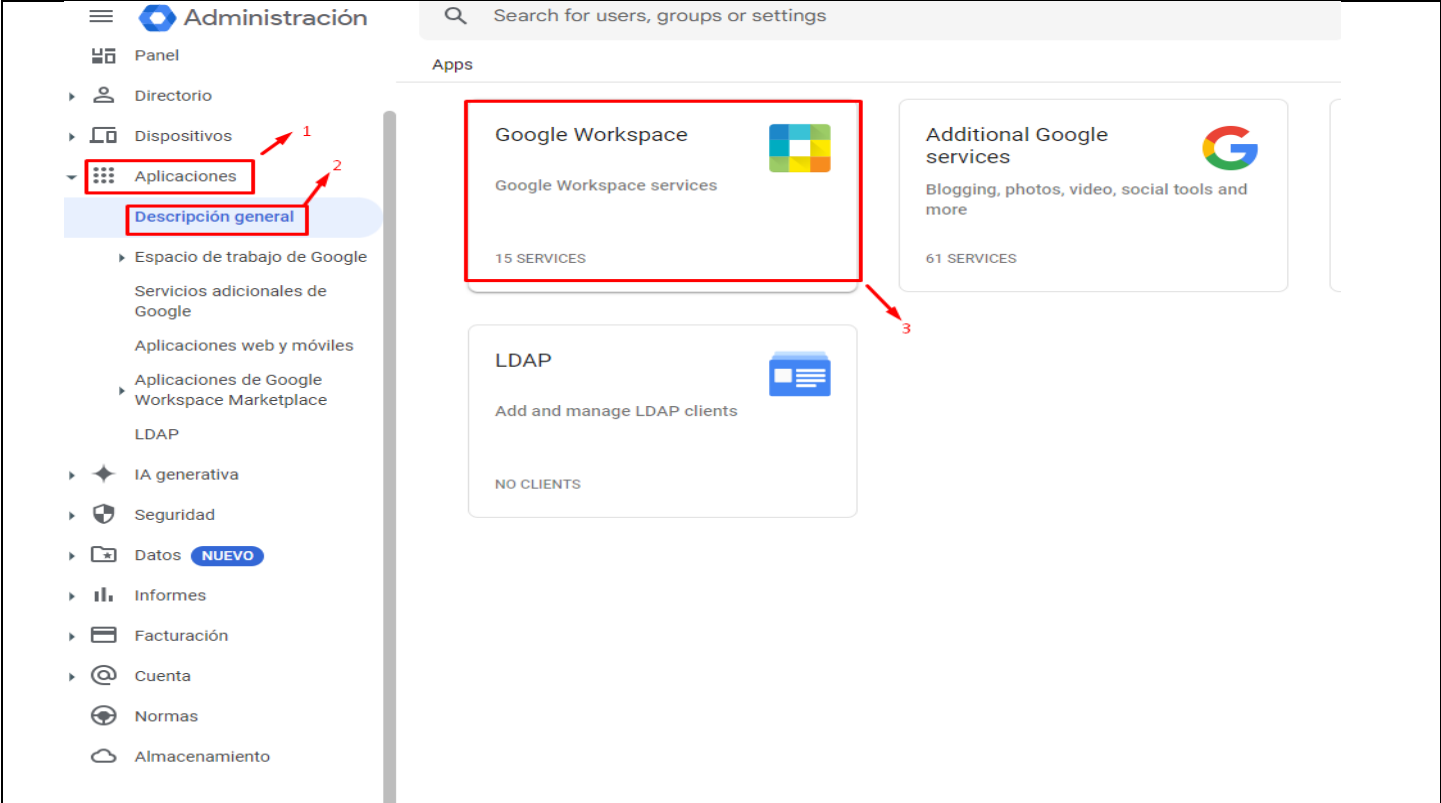
	PROCEDIMIENTO Y LINEAMIENTOS DE IMPLEMENTACIÓN DE DLP EN CORREO ELECTRÓNICO.	Clasificación:
		Versión: 2.0
		Fecha de Actualización: 22-septiembre-2024

- Acción: Bloquear el envío a dominios o destinatarios externos no autorizados.

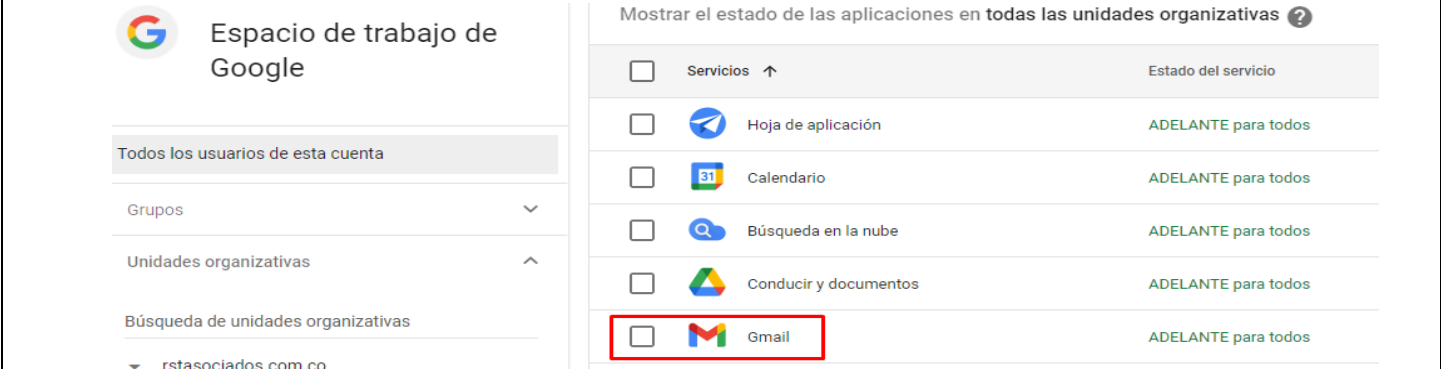


- Procedimiento desde consola Workspace:
- Para realizar este procedimiento y configuración de reglas DLP se deben seguir los siguientes pasos, ingresamos a la plataforma Workspace de Google entramos por 1. Aplicaciones, 2. Descripción General, 3. Google Workspace, tal como se muestra en la siguiente imagen:

	PROCEDIMIENTO Y LINEAMIENTOS DE IMPLEMENTACIÓN DE DLP EN CORREO ELECTRÓNICO.	Clasificación:
		Versión: 2.0
		Fecha de Actualización: 22-septiembre-2024



- A continuación, elegimos la plataforma donde vamos a realizar las reglas DLP en este caso es Gmail:



- Dentro de la opción de Gmail vamos a elegir la opción cumplimiento donde vamos a configurar las opciones.

	PROCEDIMIENTO Y LINEAMIENTOS DE IMPLEMENTACIÓN DE DLP EN CORREO ELECTRÓNICO.	Clasificación:
		Versión: 2.0
		Fecha de Actualización: 22-septiembre-2024

 Gmail

Estado
ON para todos

Seguridad
Configurar funciones de seguridad de correo electrónico y spam

Configuración
Configurar funciones de configuración

Acceso de usuario final
Configurar las funciones de acceso del usuario final

Spam, phishing y malware
Configurar funciones de spam, phishing y malware

Cumplimiento
Configurar funciones de cumplimiento

	PROCEDIMIENTO Y LINEAMIENTOS DE IMPLEMENTACIÓN DE DLP EN CORREO ELECTRÓNICO.	Clasificación:
		Versión: 2.0
		Fecha de Actualización: 22-septiembre-2024

- Se debe habilitar la opción OCR el cual va a inspeccionar archivos adjuntos de correo electrónico



Gmail

Estado

ON para todos

Unidades organizativas

Búsqueda de unidades organizativas

▼ rstasociados.com.co

Mostrando configuraciones para usuarios en rstasociados.com.co

Cumplimiento

Para comprobar cómo estas configuraciones afectan la entrega de correo electrónico y solucionar posibles problemas, vaya a [Búsqueda en el registro de correo electrónico](#)

ENTIENDOC

Eliminación automática de correo electrónico y chat

Elimina automáticamente los mensajes de correo electrónico y chat de todos los usuarios. [Más información](#)

Applied at 'rstasociados.com.co'

No elimine automáticamente mensajes de correo electrónico ni de chat.

La configuración de eliminación automática se aplica a los mensajes de correo electrónico y de chat en la bandeja de entrada del usuario y a los mensajes archivados. No se aplica a los mensajes en la carpeta Papelera, que se eliminan de forma permanente después de la cantidad de días especificada.

Reconocimiento óptico de caracteres (OCR)

[Más información](#)

Applied at 'rstasociados.com.co'

☒ Habilitar OCR para archivos adjuntos de correo electrónico

La configuración de reconocimiento óptico de caracteres (OCR) se aplica solo a usuarios con licencia con la oferta de Google Workspace adecuada.

Most changes take effect in a few minutes. [Learn more](#)

You can view prior changes in the [Audit log](#)

1 unsaved change

CANCELAR

AHORR

- Hacia abajo vamos a encontrar la opción cumplimiento de contenido y le vamos a dar en la opción configurar.



Gmail

Estado

ON para todos

Unidades organizativas

Búsqueda de unidades organizativas

▼ rstasociados.com.co

Restringir la entrega

Restrinja los dominios con los que sus usuarios pueden intercambiar correo electrónico.

[CONFIGURAR](#)

La mayoría de los cambios surten efecto en unos minutos. [Más información](#)

Puede ver los cambios anteriores en el [registro de auditoría](#)

Cumplimiento de contenido

Configure filtros de contenido avanzados basados en palabras, frases o patrones.

La mayoría de los cambios surten efecto en unos minutos. [Más información](#)

Puede ver los cambios anteriores en el [registro de auditoría](#)

[CONFIGURAR](#)

En la opción Cumplimiento de contenido se realiza Creación de las reglas y condiciones

Finalmente, la infracción de la regla mostrara un mensaje como el de la siguiente Imagen

 Gmail

Estado

ON para todos

Unidades organizativas

Búsqueda de unidades organiza...

▼ rstasociados.com.co

La mayoría de los cambios surten efecto en unos minutos. [Más información](#)

Puede ver los cambios anteriores en el [registro de auditoría](#)

Cumplimiento de contenido

Descripción	Estado	Fuente	Coi
Detección de información financiera RST	Activado	Aplicado localmente	Edi
Detección de información personal identificable y sensible	Activado	Aplicado localmente	Edi
Detección de información de salud protegida	Activado	Aplicado localmente	Edi
Detección de patrones personalizados	Activado	Aplicado localmente	Edi
Detección de adjuntos no seguros o confidenciales	Activado	Aplicado localmente	Edi
Control de datos compartidos externamente	Activado	Aplicado localmente	Edi

 Mail Delivery Subsystem <mailer-daemon@googlemail.com>
para mí ▼

12:31 (hace 16 minutos) ☆

Traducir al español

×

 El mensaje se ha bloqueado

Tu mensaje para **gestiondecalidad@rstasociados.com.co** se ha bloqueado. Consulta más información en los siguientes datos técnicos.

La respuesta fue:

Su correo ha sido rechazado, por políticas de SI no es posible enviar este mensaje, para mayor información comuníquese con el administrador correo a través de la plataforma de **gestión de tickets** de RST ASOCIADOS

FIN.		
CONTROL DE CAMBIOS		
VERSIÓN	DESCRIPCIÓN DE LA MODIFICACIÓN	FECHA ACTUALIZACIÓN
1.0	Emisión inicial	13- Agosto-2024