Bogotá, 28 de agosto del 2025

Mecanismos de Filtrado de SPAM en cumplimiento de la Resolución 1519 de 2020

Este documento se elabora con el propósito de dar cumplimiento al **Anexo 3 de la Resolución 1519 de 2020**, así como a las políticas nacionales de seguridad de la información y al Plan de Seguridad y Privacidad de la Información (SPI) implementado en la Superintendencia de Sociedades. En él se describen los mecanismos de filtrado de correos electrónicos no deseados (SPAM), aplicados tanto en FortiMail como en Microsoft 365 (O365), con el fin de fortalecer la seguridad institucional, prevenir incidentes relacionados con correos electrónicos maliciosos y garantizar la protección de la información de la Entidad.

Tabla de Contenido

FORTIMAIL

Mecanismos de Filtrado para evitar recepción de correos categorizados como SPAM

Tenemos una categoría llamada Seguridad que tiene varios parámetros de configuración entre estos están:

Filtrado URL:

Es una funcionalidad dentro del módulo **Antispam** que permite analizar los enlaces (URLs) incluidos en los correos electrónicos para detectar si apuntan a sitios maliciosos, de phishing o relacionados con spam.

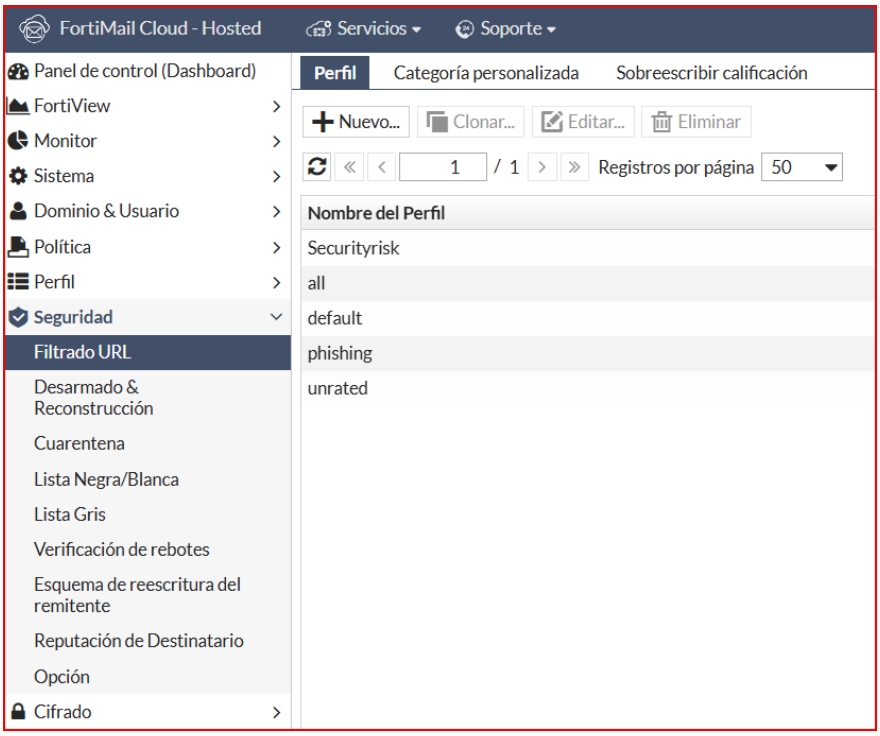


Ilustración 1:Interfaz de usuario FortiMail – Filtrado por URL

Lista Negra/Blanca:

Son mecanismos de control de acceso que permiten **permitir o bloquear** correos electrónicos según el remitente, dominio, IP o incluso contenido específico. Son herramientas clave para reforzar la seguridad y reducir el spam.

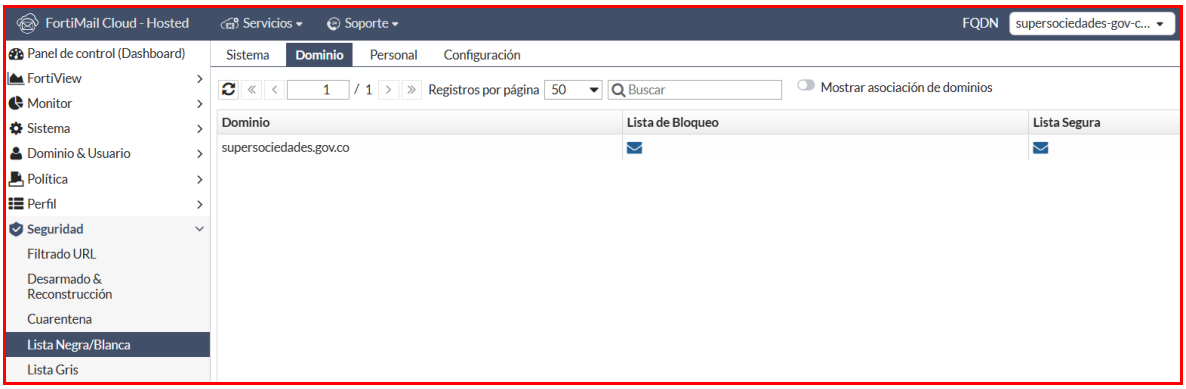


Ilustración 2: Interfaz de usuario FortiMail – Filtrado por Lista negra/blanca

Política IP:

Es una funcionalidad que permite controlar el acceso y tratamiento de correos electrónicos en función de la dirección IP del servidor que los envía. Es una herramienta clave para prevenir spam, ataques y correos no deseados desde fuentes sospechosas o no autorizadas.

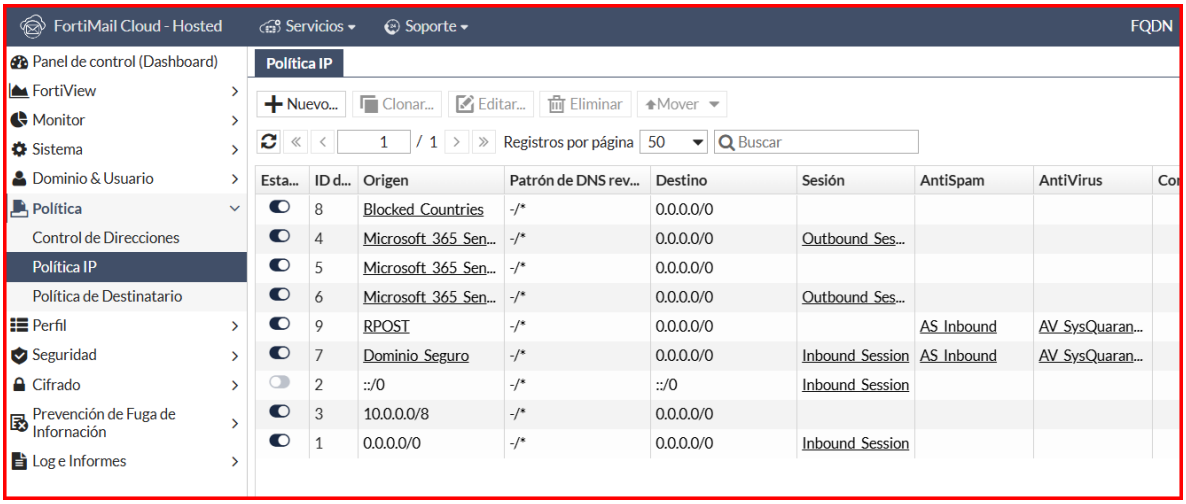


Ilustración 3: Interfaz de usuario FortiMail – Filtrado por Política IP

Perfil:

Otra Categoría es Perfil: es un conjunto de configuraciones que define cómo se deben tratar los correos electrónicos en relación con funciones específicas de seguridad y filtrado. Los perfiles se aplican dentro de las **políticas** (como IP Policy, Recipient Policy, etc.) tenemos en la opción **AntiSpam** varios perfiles para controlar el comportamiento del sistema ante diferentes tipos de tráfico.

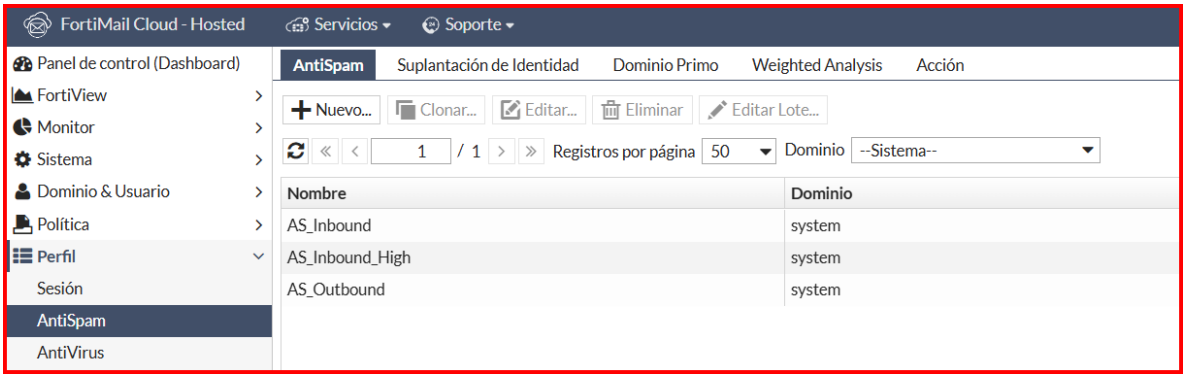


Ilustración 4: Interfaz de usuario FortiMail – Filtrado por Perfil

Monitor:

Otro mecanismo es el de Monitor: es una sección clave que permite a los administradores visualizar en tiempo real el estado y flujo de los correos electrónicos que pasan por el sistema. Es esencial para la gestión operativa, la detección de incidentes y el análisis forense. Dentro de esta categoría tenemos Cuarentena que son correos retenidos por políticas de seguridad, los cuales podemos monitorear y analizar para dar posibilidad de liberarlos, eliminarlos o revisar contenido.

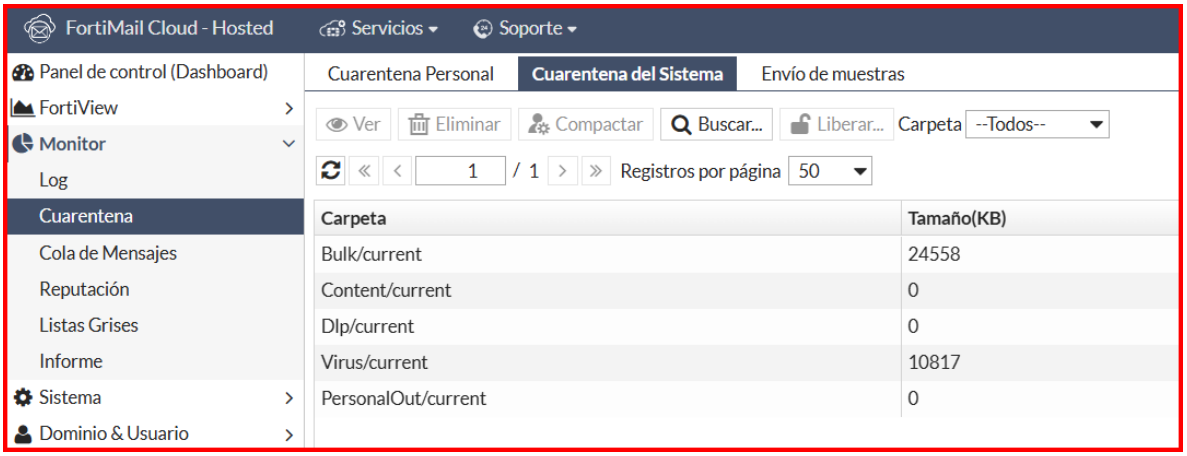


Ilustración 5: Interfaz de usuario FortiMail – Filtrado por Monitor

Microsoft 365 (O365)

Configuración SPAM:

- Esta es la configuración predeterminada de protección contra correo no deseado en Microsoft 365.
- El umbral de spam masivo está establecido en un nivel medio/alto (7).
- Solo se bloquean los mensajes vacíos y se filtran correos masivos.

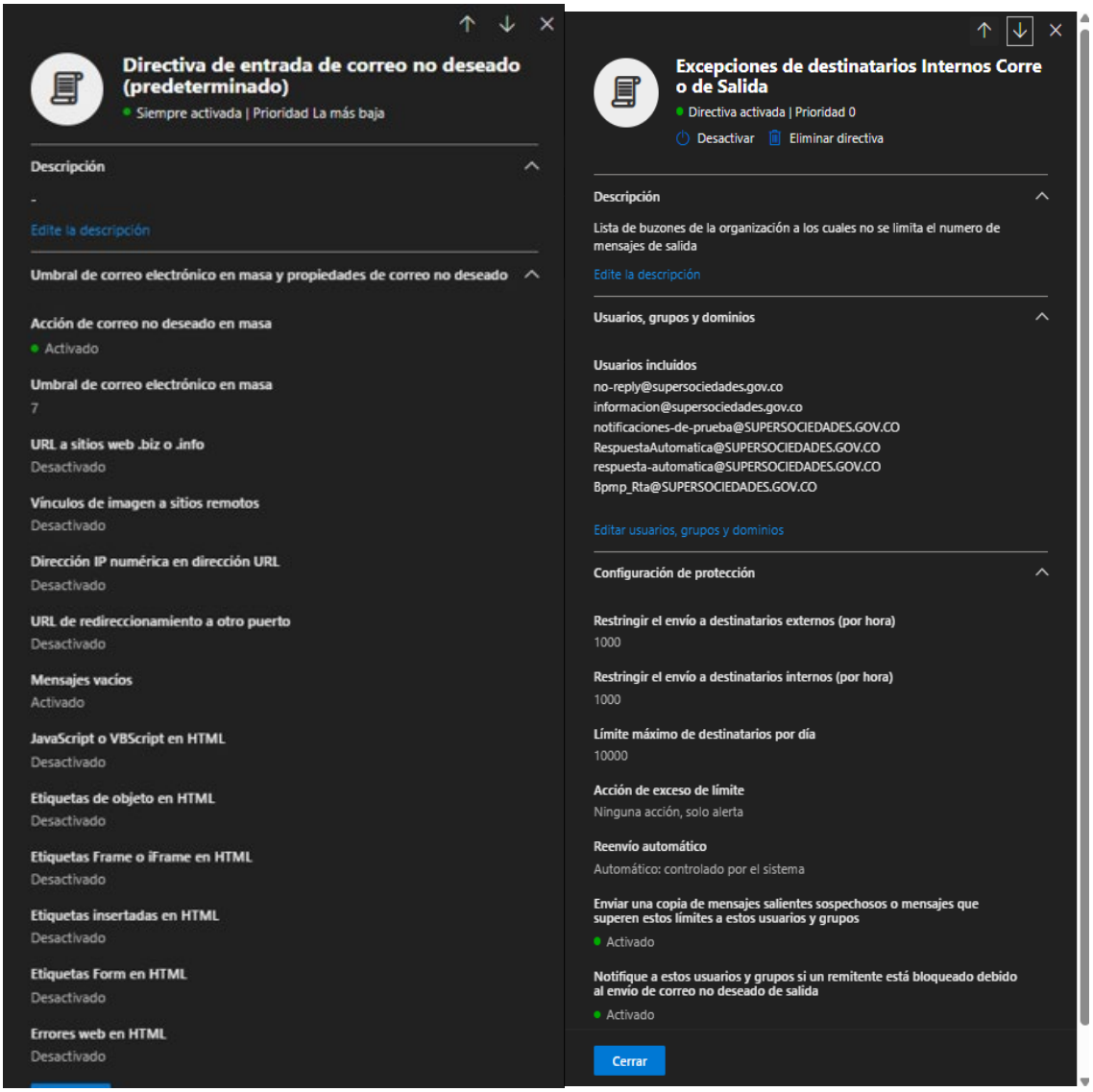
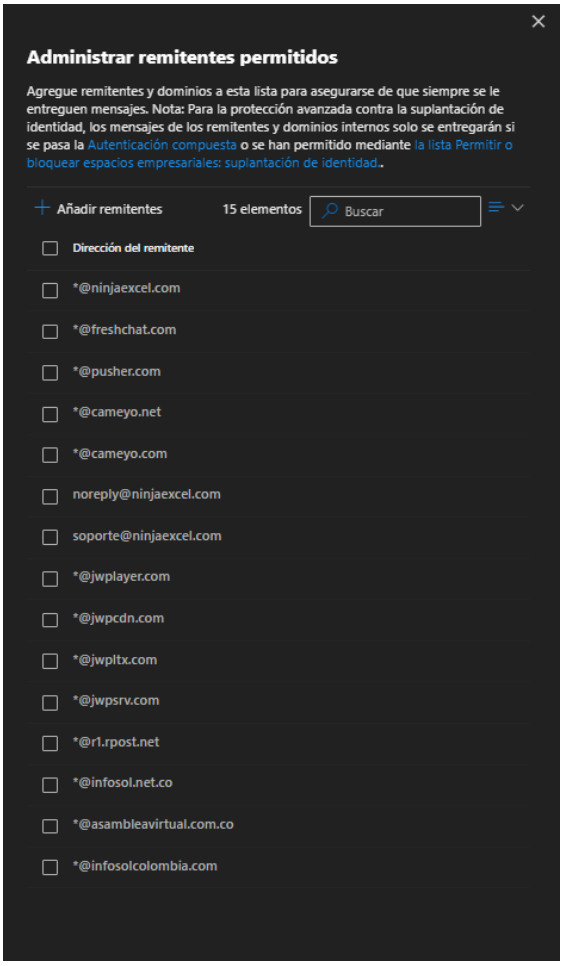
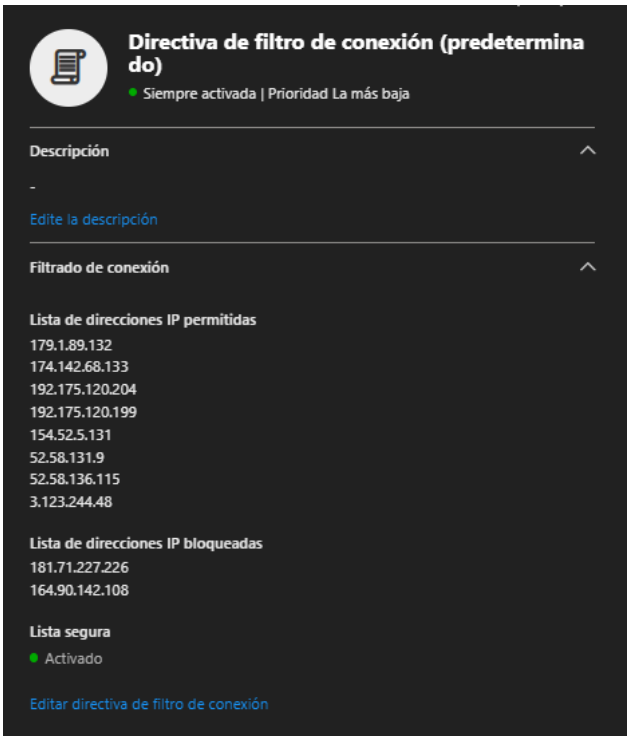


Ilustración 6 Interfaz de Admin Office 365 – Filtrado por Directivas AntiSpam.





- Esta lista es un filtro adicional contra spam y phishing dirigido.
- Es útil para bloquear emisores específicos que ya intentaron enviar correos no deseados o fraudulentos.
- Las IPs permitidas saltan controles de antispam: debes revisar periódicamente que realmente correspondan a proveedores confiables.
- Las IPs bloqueadas indican que ya se detectaron orígenes maliciosos y se detuvo el correo.
- La lista segura activada ayuda a reducir falsos positivos con grandes proveedores de correo.

Política de Exchange Online Protection (EOP)

Esta política en **Exchange Online Protection (EOP)** controla el comportamiento cuando un usuario o aplicación de la organización **intenta enviar correo masivo o sospechoso**.

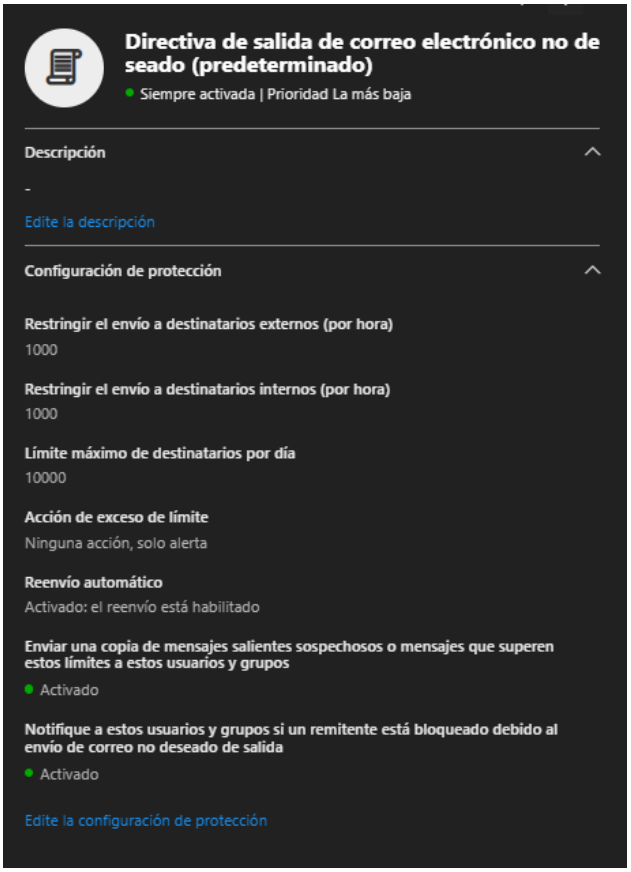


Ilustración 7 Interfaz de Admin Office 365 – Filtrado por política en Exchange Online Protection.

Tabla 1. Cuadro de control			
Versión	**Fecha**	**Instancia de Aprobación**	**Descripción**
01	28/08/2025	DTIC/GIDAA	Primera Versión del Documento.