

# **POLÍTICA CORPORATIVA ANTI-SPAM**

## **PLATAFORMA AV**

### **1. OBJETO**

La presente **Política Corporativa Anti-Spam**, en adelante la “**Política**”, tiene por objeto establecer los principios, obligaciones, prohibiciones, controles y responsabilidades aplicables para prevenir, detectar, controlar y mitigar el envío, recepción, distribución o utilización de comunicaciones electrónicas no solicitadas, masivas, fraudulentas o no autorizadas, denominadas para efectos de esta Política como **spam**.

La Política tiene como finalidad proteger la confidencialidad, integridad, disponibilidad y seguridad de la información, preservar el adecuado funcionamiento de los recursos tecnológicos, garantizar la continuidad de las operaciones y proteger la reputación e intereses de **PLATAFORMA AV**, en adelante la “**Compañía**”.

### **2. ALCANCE Y OBLIGATORIEDAD**

La presente Política es de obligatorio cumplimiento para todos los colaboradores, trabajadores, directivos, contratistas, aprendices, practicantes, proveedores, consultores y demás terceros que, directa o indirectamente, tengan acceso, utilicen o administren recursos tecnológicos, sistemas de información, cuentas corporativas, redes, plataformas, bases de datos o cualquier otro activo de información propiedad de **PLATAFORMA AV** o puesto a su disposición.

El desconocimiento, omisión o interpretación incorrecta de las disposiciones contenidas en esta Política **no exime a ninguna persona de su cumplimiento ni de las consecuencias derivadas de su incumplimiento**.

La aceptación y utilización de los recursos tecnológicos de **PLATAFORMA AV** implica el conocimiento, aceptación y obligación de cumplir integralmente las disposiciones aquí establecidas.

### **3. DEFINICIONES**

Para efectos de la presente Política, se adoptan las siguientes definiciones:

#### **3.1. Spam**

Se entiende por **spam** toda comunicación electrónica no solicitada, no autorizada, masiva, repetitiva o enviada sin una finalidad legítima, independientemente del medio utilizado para su transmisión.

El spam podrá incluir, entre otros, mensajes publicitarios, comerciales, promocionales, fraudulentos, engañosos, repetitivos, cadenas de mensajes o cualquier contenido distribuido de manera indiscriminada o contraria a los intereses, procedimientos y controles establecidos por **PLATAFORMA AV**.

### **3.2. Comunicación electrónica**

Corresponde a cualquier mensaje transmitido mediante correo electrónico, mensajería instantánea, aplicaciones corporativas, plataformas colaborativas, sistemas de información, redes sociales corporativas, formularios electrónicos, herramientas de comunicación o cualquier otro medio tecnológico utilizado en desarrollo de las actividades de la Compañía.

### **3.3. Comunicación masiva**

Es aquella comunicación dirigida simultáneamente a múltiples destinatarios mediante listas de distribución, bases de datos, grupos, sistemas automatizados o cualquier otro mecanismo de difusión.

### **3.4. Usuario**

Toda persona autorizada para acceder o utilizar recursos tecnológicos, sistemas, plataformas, cuentas o activos de información de **PLATAFORMA AV**.

## **4. PRINCIPIOS GENERALES**

Toda comunicación electrónica realizada utilizando recursos tecnológicos de **PLATAFORMA AV** deberá cumplir con los siguientes principios:

- **Legalidad:** Las comunicaciones deberán ajustarse a las disposiciones legales, contractuales y corporativas aplicables.
- **Finalidad legítima:** Todo mensaje deberá responder a una necesidad laboral, institucional, contractual, comercial autorizada o funcionalmente justificada.
- **Necesidad:** Las comunicaciones deberán dirigirse únicamente a los destinatarios que requieran recibir la información.
- **Responsabilidad:** El remitente será responsable por el contenido, los destinatarios y la utilización adecuada de los canales corporativos.
- **Seguridad:** Las comunicaciones no deberán comprometer la seguridad de los sistemas, la información o los activos tecnológicos de **PLATAFORMA AV**.

- **Confidencialidad:** Los usuarios deberán proteger la información y los datos a los que tengan acceso.
- **Uso adecuado de los recursos:** Los recursos tecnológicos deberán utilizarse exclusivamente conforme a las funciones, autorizaciones y necesidades establecidas por la Compañía.

## 5. OBLIGACIONES DE LOS USUARIOS

Todo usuario de los recursos tecnológicos de **PLATAFORMA AV** deberá:

1. Utilizar las cuentas, sistemas y medios de comunicación corporativos exclusivamente para fines autorizados y relacionados con las actividades de la Compañía.
2. Verificar, antes del envío de una comunicación masiva, que exista una finalidad legítima y una necesidad objetiva para contactar a los destinatarios.
3. Limitar las comunicaciones únicamente a las personas, áreas o grupos que requieran recibir la información.
4. Abstenerse de utilizar bases de datos, listas de distribución o información de contacto para fines personales, comerciales o no autorizados.
5. Cumplir con los procedimientos internos establecidos para la realización de campañas, comunicaciones masivas o envíos automatizados.
6. Reportar de manera inmediata cualquier mensaje sospechoso, fraudulento, no solicitado o identificado como posible spam, a través de los canales definidos por **PLATAFORMA AV**.
7. Acatar las medidas técnicas, administrativas y de seguridad implementadas para prevenir, filtrar, bloquear o controlar comunicaciones no autorizadas.
8. Abstenerse de realizar acciones destinadas a evadir, alterar, deshabilitar o interferir con los mecanismos de seguridad y filtrado implementados por la Compañía.
9. Proteger las credenciales de acceso y evitar cualquier uso indebido de las cuentas corporativas que pueda facilitar el envío de comunicaciones no autorizadas.

## 6. CONDUCTAS EXPRESAMENTE PROHIBIDAS

Queda expresamente prohibido a todos los usuarios:

**6.1.** Enviar, distribuir, retransmitir o facilitar el envío de mensajes considerados como spam utilizando recursos, cuentas, dominios, sistemas o infraestructura tecnológica de **PLATAFORMA AV**.

**6.2.** Utilizar cuentas corporativas para el envío de publicidad, promociones, campañas, cadenas de mensajes o contenidos ajenos a las funciones autorizadas.

**6.3.** Realizar envíos masivos sin contar con la autorización correspondiente, cuando esta sea exigida por los procedimientos internos de la Compañía.

**6.4.** Utilizar listas de distribución, bases de datos o directorios corporativos para fines diferentes a aquellos para los cuales fueron creados o autorizados.

**6.5.** Recolectar, copiar, extraer, compartir, comercializar o utilizar datos de contacto sin la autorización correspondiente.

**6.6.** Utilizar mecanismos técnicos, automatizados o manuales para evadir filtros anti-spam, controles de seguridad, restricciones de envío o mecanismos de monitoreo establecidos por **PLATAFORMA AV**.

**6.7.** Suplantar, falsificar, ocultar o manipular la identidad del remitente, la dirección de correo electrónico, el dominio, la información de origen o cualquier otro elemento relacionado con una comunicación electrónica.

**6.8.** Distribuir mensajes que contengan enlaces, archivos, solicitudes o contenidos fraudulentos, engañosos o que puedan comprometer la seguridad de los usuarios, los sistemas o la información de la Compañía.

**6.9.** Reenviar de manera indiscriminada mensajes, cadenas, promociones, campañas o contenidos que no cuenten con una finalidad laboral, institucional o corporativa legítima.

**6.10.** Utilizar los recursos tecnológicos de **PLATAFORMA AV** para afectar, directa o indirectamente, la disponibilidad, integridad, confidencialidad o reputación de los sistemas, usuarios o terceros.

## **7. CONTROLES Y MEDIDAS DE SEGURIDAD**

**PLATAFORMA AV** podrá implementar, modificar, actualizar o fortalecer, en cualquier momento, las medidas técnicas y administrativas que considere necesarias para prevenir, detectar y controlar el spam y demás comunicaciones no autorizadas.

Entre dichas medidas podrán incluirse, sin limitarse a:

- Filtros de correo electrónico.

- Bloqueo de dominios, remitentes o direcciones identificadas como riesgosas.
- Restricciones sobre el volumen o frecuencia de envío de mensajes.
- Sistemas de detección y prevención de amenazas.
- Monitoreo de actividades relacionadas con las cuentas corporativas.
- Bloqueo temporal o definitivo de cuentas.
- Restricción de acceso a sistemas o servicios.
- Análisis e investigación de eventos o incidentes de seguridad.

La Compañía podrá adoptar medidas preventivas o correctivas cuando identifique comportamientos que puedan representar un riesgo para sus activos de información, infraestructura tecnológica, operaciones o reputación.

## **8. REPORTE Y GESTIÓN DE INCIDENTES**

Todo usuario que identifique o reciba una comunicación que considere sospechosa, fraudulenta, no solicitada o potencialmente peligrosa deberá reportarla de manera inmediata al **Área de Tecnología, Seguridad de la Información, Mesa de Ayuda o al área que PLATAFORMA AV determine oficialmente**.

El usuario deberá abstenerse de realizar acciones que puedan incrementar el riesgo o comprometer los sistemas, la información o los recursos tecnológicos de la Compañía.

**PLATAFORMA AV** podrá investigar los eventos reportados y adoptar las medidas necesarias para contener, corregir, mitigar y prevenir la repetición de incidentes similares.

## **9. MONITOREO, VERIFICACIÓN Y CONTROL**

Con el propósito de garantizar el cumplimiento de esta Política y proteger sus recursos tecnológicos, **PLATAFORMA AV** podrá realizar actividades de monitoreo, revisión, análisis, auditoría y control sobre el uso de sus sistemas, redes, cuentas y canales corporativos, de conformidad con la normatividad aplicable y las disposiciones internas vigentes.

Los usuarios reconocen que los recursos tecnológicos proporcionados por la Compañía están destinados al desarrollo de actividades autorizadas y podrán estar sujetos a controles de seguridad, monitoreo y verificación.

## **10. RESPONSABILIDADES**

### **10.1. De los usuarios**

Cumplir integralmente con las obligaciones y prohibiciones establecidas en esta Política y reportar oportunamente cualquier incumplimiento o situación que represente un riesgo para **PLATAFORMA AV**.

### **10.2. De los líderes y responsables de área**

Promover el cumplimiento de la presente Política dentro de sus equipos y adoptar las medidas necesarias para evitar la utilización inadecuada de los recursos tecnológicos bajo su responsabilidad.

### **10.3. Del Área de Tecnología y Seguridad de la Información**

Implementar, administrar, supervisar y actualizar los controles técnicos y administrativos destinados a prevenir, detectar y mitigar comunicaciones no autorizadas o potencialmente riesgosas.

### **10.4. De las áreas de Talento Humano, Jurídica, Cumplimiento o las que hagan sus veces**

Apoyar, según sus competencias y responsabilidades, la evaluación de los incumplimientos y la aplicación de las medidas disciplinarias, contractuales, administrativas o legales que correspondan.

## **11. INCUMPLIMIENTO Y CONSECUENCIAS**

El incumplimiento de las disposiciones establecidas en la presente Política será considerado una conducta contraria a las obligaciones, normas y procedimientos internos de **PLATAFORMA AV**.

Dependiendo de la naturaleza, gravedad, impacto, recurrencia y circunstancias particulares de cada caso, la Compañía podrá adoptar las medidas que correspondan conforme al Reglamento Interno de Trabajo, contratos, políticas corporativas, procedimientos disciplinarios y demás disposiciones aplicables.

Las medidas podrán incluir, entre otras y según corresponda:

- Llamados de atención.
- Restricciones o suspensión de acceso a recursos tecnológicos.
- Acciones disciplinarias.
- Terminación de autorizaciones o permisos de acceso.

- Aplicación de medidas contractuales frente a contratistas o terceros.
- Inicio de las actuaciones internas o externas que resulten procedentes.

Cuando la conducta pueda constituir una infracción legal o genere perjuicios para **PLATAFORMA AV** o terceros, podrán adelantarse las acciones legales correspondientes.

## **12. INVESTIGACIÓN DE INCUMPLIMIENTOS**

Todo presunto incumplimiento de esta Política podrá ser objeto de revisión, análisis e investigación por parte de las áreas competentes de **PLATAFORMA AV**.

Los usuarios deberán colaborar con los procesos de verificación e investigación y suministrar la información requerida dentro de los límites establecidos por la normatividad aplicable.

La obstrucción, ocultamiento, alteración o suministro deliberado de información falsa relacionada con una investigación podrá constituir una falta adicional y ser evaluada conforme a las disposiciones internas vigentes.

## **13. EXCEPCIONES**

Cualquier excepción a las disposiciones contenidas en esta Política deberá contar con autorización previa, expresa y documentada por parte del responsable o área autorizada por **PLATAFORMA AV**.

Las excepciones serán evaluadas de acuerdo con el nivel de riesgo, la necesidad operativa y los controles de seguridad requeridos.

Ninguna autorización verbal, práctica habitual o tolerancia frente a un incumplimiento podrá interpretarse como una modificación o excepción permanente a esta Política.

## **14. DIVULGACIÓN Y CUMPLIMIENTO**

La presente Política será comunicada a las personas sujetas a su cumplimiento mediante los canales definidos oficialmente por **PLATAFORMA AV**.

Todos los usuarios deberán conocer, comprender y cumplir las disposiciones establecidas en este documento.

La utilización continuada de los recursos tecnológicos corporativos implica la aceptación de las condiciones, obligaciones y restricciones aplicables al uso de dichos recursos.

