1. OBJETIVO

Establecer los lineamientos técnicos, operativos, legales y disciplinarios que permitan prevenir, detectar y mitigar el envío y la recepción de mensajes no solicitados (spam) a través de la infraestructura y los servicios provistos por CABLE FUTURO TV S.A.S. (en adelante, "la Compañía"), garantizando la protección de nuestros usuarios, el cumplimiento normativo y la reputación de la Compañía.

2. ALCANCE

Esta política aplica a:

Todos los servicios de conectividad y correo electrónico ofrecidos directa o indirectamente por la Compañía.
Todo el personal de planta, contratistas y terceros que utilicen los recursos de red de la Compañía.
Todo el tráfico de salida y de entrada cursado por IPs e infraestructuras asignadas o administradas por la Compañía.

3. MARCO NORMATIVO

Ley 1266 de 2008 (Habeas Data – Información Financiera y Crediticia).
Ley 1273 de 2009 (Delitos informáticos).
Ley 1581 de 2012 y Decreto 1377 de 2013 (Protección de Datos Personales).
Ley 527 de 1999 (Comercio Electrónico).
Resolución CRC 3495 de 2011 y posteriores sobre buenas prácticas de spam.
Recomendaciones CITEL sobre mitigación de spam en redes IP.
Estándares técnicos: RFC 7208 (SPF), RFC 6376 (DKIM), RFC 7489 (DMARC).

4. DEFINICIONES

Término	Definición
Spam	Mensaje electrónico no solicitado, enviado masiva e indiscriminadamente, usualmente con fines comerciales, fraudulentos o maliciosos.
Phishing	Técnica de ingeniería social que busca obtener datos confidenciales simulando ser una entidad legítima.
Spoofing	Suplantación de identidad de dominio, IP o remitente para aparentar legitimidad.

RBL (Realtime Blackhole List)	Listado en tiempo real de direcciones IP o dominios asociados a envío de spam.
Rate Limiting	Restricción del número de correos que un remitente puede enviar en un periodo definido.

5. PRINCIPIOS

1. **Legalidad:** Cumplir la legislación colombiana y estándares internacionales.
2. **Prevención:** Implementar controles que eviten incidentes antes de que ocurran.
3. **Responsabilidad Compartida:** Usuarios y la Compañía comparten la responsabilidad de prevenir el spam.
4. **Transparencia:** Mantener informados a los usuarios sobre prácticas antispam y sus derechos.

6. RESPONSABILIDADES

Dirección Técnica: Diseño, implementación y mantenimiento de controles técnicos antispam.
Dirección Jurídica: Interpretación normativa y actualización de esta política.
Área de Seguridad de la Información (ASI): Monitoreo de listas negras, respuesta a incidentes y generación de reportes.
Usuarios Finales: Uso responsable de los servicios, adhesión a la Política de Uso Aceptable (PUA) y reporte de incidentes.

7. CONTROLES TÉCNICOS

7.1 Correo Saliente

1. **Bloqueo de puerto 25 SMTP saliente**; sólo se habilita el puerto 587 con autenticación TLS.
2. **Autenticación y cifrado obligatorio (STARTTLS).**
3. **SPF, DKIM y DMARC** configurados a nivel de DNS para todos los dominios de la Compañía (política DMARC: p=reject).
4. **Rate Limiting**: máximo 100 correos/hora y 1 000 correos/día por buzón.
5. **Análisis de reputación saliente** con herramientas como **SpamAssassin**, **Rspamd** y verificación contra RBLs (Spamhaus, SORBS).
6. **Sandbox** para detección de malware en adjuntos y URLs.

7.2 Correo Entrante

1. **Filtro antimalware** con doble motor (ClamAV + comercial).
2. **Greylisting** y **RBL checks**.
3. **Desempaquetado de enlaces (URL rewriting)** y verificación en tiempo real.
4. **Puntuación de Spam** (SpamAssassin) con cuarentena automática para puntuación > 6.0.
5. **Quarantine Digest**: Resumen diario para que el usuario libere correos legítimos.

7.3 Infraestructura de Red

1. **NetFlow y sistemas IDS/IPS** para detectar comportamientos de envío masivo.
2. **Bloqueo automático de IPs** que superen umbrales configurados (por ejemplo, > 500 conexiones SMTP en 10 min).
3. **DNS sinkhole** para dominios de spam/phishing.

8. CONTROLES OPERATIVOS

1. **Procedimiento de Alta de Clientes**: validación de documentos y aceptación de la PUA.
2. **Auditorías internas trimestrales** sobre cumplimiento de la política.
3. **Planes de concientización** semestrales (boletines y webinars).
4. **Mesa de Servicio** con canal exclusivo antispam (cablefuturotvsas@gmail.com).

9. PROCEDIMIENTO DE RESPUESTA A INCIDENTES

1. **Recepción** del reporte (usuario, RBL, autoridad).
2. **Clasificación** (spam saliente vs. entrante).
3. **Contención**: suspensión temporal del servicio o filtrado reforzado.
4. **Erradicación**: corrección de configuraciones, eliminación de malware, educación al usuario.
5. **Recuperación**: prueba de envíos, verificación de salida de listas negras.
6. **Lecciones aprendidas** documentadas en Acta de Incidente.

10. SANCIONES Y MEDIDAS DISCIPLINARIAS

Usuarios residenciales: suspensión temporal (24 h) y notificación formal; reincidencia implica suspensión definitiva.
Clientes corporativos: suspensión de rangos IP involucrados y penalidades contractuales según PUA.

Empleados/contratistas: medidas disciplinarias internas conforme al Reglamento Interno de Trabajo y/o terminación de contrato.

11. REGISTRO Y MONITOREO

Logs de SMTP, NetFlow y eventos IDS se conservarán **por 18 meses**.
Reportes mensuales: *tasa de spam detectado*, *IPs bloqueadas* y *listas negras*.
Revisión trimestral por el Comité de Seguridad de la Información.

12. REVISIONES Y ACTUALIZACIONES

Esta política será revisada **anualmente** o cuando existan cambios regulatorios o tecnológicos significativos. Las versiones actualizadas se publicarán en el portal interno.