					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P36					Título del documento: **Política de Redes Sociales y Comunicaciones Externas**							
Versión: 1.0		Fecha de entrada en vigor: 01.01.2025			Propietario del documento:							
X	Política		Norma		Procedimiento		Formulario		Registro		Otro	

Historial de revisiones				
Número de revisión	**Fecha de revisión**	**Cambios**	**Revisado por**	**Propietario del proceso**

Aprobaciones			
Nombre	**Cargo**	**Fecha**	**Firma**

Alineación con normas y reglamentos

Norma/Reglamento	Cláusula/Artículo	Comentario
ISO/IEC 27001:2022	Cláusula 8	Procesos definidos y gobernanza basada en funciones para gestionar las comunicaciones públicas, garantizando la exactitud, los flujos de aprobación y el escalado de incidentes.
ISO/IEC 27002:2022	Controles 5.10, 5.11, 5.35, 5.36	Regula el uso de la información, el uso aceptable, la comunicación externa con autoridades y la notificación de cumplimiento.
NIST SP 800-53 Rev. 5	AC-8, AU-12, PL-4	Normas de comportamiento para el uso de sistemas y comunicaciones, notificaciones a los usuarios y conservación de registros de auditoría.
RGPD de la UE	Artículos 5, 25, 32, 33	Principios del tratamiento de datos, protección de datos desde el diseño, seguridad del tratamiento y obligaciones de notificación de violaciones de seguridad.
Directiva NIS2 de la UE	Artículo 21	Medidas de gestión del riesgo de las TIC, obligaciones en materia de incidentes y comunicaciones públicas relacionadas con riesgos.
DORA de la UE	Artículos 9, 16	Gestión del riesgo de las TIC y estrategia de comunicación para proveedores críticos.
COBIT 2019	APO09, DSS05	Gobernanza de acuerdos de servicio y comunicaciones, así como prácticas seguras de comunicación y gestión de incidentes.

1. Propósito

1.1 Esta política establece normas y responsabilidades obligatorias que rigen el uso de las redes sociales y todas las formas de comunicación externa por parte del personal vinculado a la organización.

1.2 Garantiza que los mensajes públicos, ya sean planificados o espontáneos, sean exactos, respetuosos, seguros, conformes y coherentes con la marca.

1.3 Esta política tiene por objeto minimizar los riesgos asociados al daño reputacional, el incumplimiento normativo, la fuga de propiedad intelectual y las divulgaciones no autorizadas a través de canales expuestos públicamente.

1.4 Asimismo, promueve la responsabilidad proactiva y una gobernanza estructurada en todas las formas de comunicación digital que involucren a la organización o la afecten.

2. Alcance

2.1 Esta política se aplica a todos los empleados, contratistas, becarios y representantes de terceros que:

2.1.1 Se comuniquen en nombre de la organización, ya sea de manera oficial o informal

2.1.2 Hagan referencia o den a entender su vinculación con la organización en un entorno público

2.1.3 Utilicen cuentas personales o corporativas para participar en debates públicos relacionados con la organización

2.2 Los canales de comunicación cubiertos incluyen, entre otros:

2.2.1 Plataformas de redes sociales (p. ej., LinkedIn, X/Twitter, Instagram, TikTok, YouTube, Facebook)

2.2.2 Blogs, wikis, foros y tablones públicos de debate

2.2.3 Correo electrónico o mensajería directa a terceros externos (p. ej., clientes, reguladores, medios de comunicación)

2.2.4 Entrevistas de prensa, paneles de ponentes o apariciones en medios grabados

2.2.5 Participación en comunidades en línea en las que se haga referencia a la organización

2.3 Esta política regula tanto el contenido en tiempo real como el programado con antelación y se aplica a todos los dispositivos y cuentas, personales o corporativos, utilizados para difundir comunicaciones.

3. Objetivos

3.1 Prevenir la divulgación accidental o intencionada de información confidencial, sensible o regulada a través de canales de comunicación externa.

3.2 Garantizar que las declaraciones públicas oficiales y el contenido en redes sociales sean exactos, estén autorizados y alineados con la marca corporativa, la ética y los mensajes estratégicos.

3.3 Prevenir daños reputacionales y garantizar la coherencia de los mensajes entre los departamentos internos y las plataformas externas.

3.4 Cumplir las obligaciones legales aplicables relacionadas con las declaraciones públicas, incluidas, entre otras, las derivadas del RGPD de la UE, la Directiva NIS2 de la UE, DORA de la UE y las normas sectoriales de comunicación.

3.5 Definir responsabilidades claras, usos permitidos y protocolos de aplicación para todo el personal que participe en actividades expuestas públicamente.

4. Funciones y responsabilidades

4.1 Director de Marketing o Comunicación / Responsable de Relaciones Públicas

4.1.1 Aprueba todos los mensajes oficiales de la empresa para su publicación externa

4.1.2 Mantiene los calendarios de contenido en redes sociales y las directrices para garantizar la coherencia de la marca

4.1.3 Supervisa las menciones en línea y la exposición mediática relacionadas con la organización

4.2 Director de Seguridad de la Información (CISO) / equipo de seguridad

4.2.1 Supervisa las plataformas digitales para detectar indicadores de fuga de datos, suplantación de identidad o intentos de phishing

4.2.2 Se coordina con los equipos de respuesta a incidentes en caso de ataques o violaciones de seguridad originados a través de redes sociales

[... Las secciones 4.3–8 no están incluidas en esta vista previa. Adquiera el documento completo para acceder al contenido íntegro. ...]

9. Aplicación y cumplimiento

9.1 Esta política es obligatoria para todo el personal incluido en su alcance y para terceros. El incumplimiento podrá dar lugar a:

9.1.1 Advertencias formales

9.1.2 Revocación temporal o permanente del acceso a plataformas o sistemas

9.1.3 Medidas disciplinarias, incluido el cese

9.1.4 Acciones legales, si la comunicación externa da lugar a daño reputacional, una violación de seguridad de los datos o incumplimiento normativo

9.2 Medidas disciplinarias

9.2.1 Los incumplimientos internos (p. ej., filtración de datos confidenciales o difamación de la organización) darán lugar a la intervención de Recursos Humanos, una investigación formal y la documentación en el expediente del empleado.

9.2.2 Cuando proceda, Asuntos Jurídicos emprenderá acciones civiles o notificará a las autoridades actividades delictivas (p. ej., suplantación o filtraciones relacionadas con operaciones con información privilegiada).

9.3 Supervisión del cumplimiento

9.3.1 Los equipos de Seguridad y Comunicación deben realizar una supervisión continua de:

9.3.1.1 Las menciones de la marca en las principales plataformas

9.3.1.2 El uso no oficial de imágenes o marcas comerciales de la empresa

9.3.1.3 Los riesgos conocidos (p. ej., empleados descontentos o intentos de suplantación)

9.3.2 La supervisión debe cumplir la legislación y la normativa sobre privacidad de los empleados, y todos los casos señalados deben ser verificados por una persona revisora.

9.4 Denuncias y notificación de uso indebido

9.4.1 Se anima a cualquier empleado que sospeche un incumplimiento de esta política a comunicarlo al equipo de seguridad de la información, a Asuntos Jurídicos o de forma anónima a través del portal del canal de denuncias.

9.4.2 Las represalias contra denunciantes están estrictamente prohibidas y darán lugar a medidas disciplinarias inmediatas.

10. Requisitos de revisión y actualización

10.1 Esta política debe revisarse anualmente, o antes si:

10.1.1 Se producen cambios significativos en los requisitos regulatorios (p. ej., nuevas normas de la UE sobre comunicaciones digitales)

10.1.2 Se adoptan nuevas plataformas sociales o canales de comunicación

10.1.3 Se produce un incidente significativo o incumplimientos reiterados que indiquen deficiencias en el proceso

10.1.4 Se produce un cambio estructural o de liderazgo en las funciones de relaciones públicas, asuntos jurídicos o seguridad

10.2 La revisión debe realizarse conjuntamente por:

10.2.1 El Responsable de Marketing / Relaciones Públicas

10.2.2 El Director de Seguridad de la Información o el responsable de riesgos de seguridad

10.2.3 Los responsables jurídicos y de cumplimiento normativo

10.3 Las actualizaciones deben documentarse en el Registro de Cambios de Políticas y comunicarse a través de los canales internos de concienciación. Cuando se produzcan cambios materiales, todo el personal afectado deberá volver a confirmar la aceptación de la política.

11. Políticas relacionadas y vinculaciones

11.1 Esta política está respaldada por los siguientes componentes del Sistema de Gestión de la Seguridad de la Información (SGSI) de la organización y se interrelaciona con ellos:

11.1.1 P1 – Política de Seguridad de la Información: establece los principios generales para proteger la información, lo que incluye garantizar que las comunicaciones no den lugar a divulgaciones no autorizadas.

11.1.2 P3 – Política de Uso Aceptable: define los comportamientos aceptables para plataformas y tecnologías digitales, que regulan directamente el uso personal y profesional de los canales sociales.

11.1.3 P6 – Política de Gestión de Riesgos: proporciona el marco de riesgos para evaluar las amenazas relacionadas con la comunicación pública y la exposición reputacional.

11.1.4 P8 – Política de Concienciación y Formación en Seguridad de la Información: establece programas de concienciación para formar al personal sobre prácticas seguras de comunicación y amenazas de ingeniería social.

11.1.5 P13 – Política de Clasificación y Etiquetado de Datos: orienta al personal sobre qué constituye información restringida o confidencial que no debe divulgarse externamente.

11.1.6 P30 – Política de Respuesta a Incidentes: define cómo gestionar incidentes relacionados con comunicaciones públicas, incluidas fugas de datos, suplantación e incumplimiento normativo.

11.1.7 P33 – Política de Supervisión, Auditoría y Cumplimiento: regula los procesos de auditoría que validan los controles de redes sociales, los sistemas de supervisión y el cumplimiento de las políticas de comunicación externa.

12. Normas y marcos de referencia

12.1 ISO/IEC 27001:

12.1.1 Cláusula 8.1 – Planificación y control operacional: exige procesos definidos y gobernanza basada en funciones para gestionar las comunicaciones públicas, garantizando la exactitud, los flujos de aprobación y el escalado de incidentes relacionados con riesgos de datos o reputacionales.

12.2 ISO/IEC 27002:2022:

12.2.1 Control 5.10 – Uso de la información: regula la difusión autorizada y ética de comunicaciones internas o externas.

12.2.2 Control 5.11 – Uso aceptable de la información y de otros activos asociados: refuerza las prácticas aceptables para compartir contenido mediante activos corporativos o cuentas personales.

12.2.3 Control 5.35 – Contacto con las autoridades: exige una comunicación externa estructurada y autorizada con organismos reguladores y entidades públicas.

12.2.4 Control 5.36 – Cumplimiento de políticas, normas y estándares de seguridad de la información: exige la aplicación coherente de las políticas internas en todos los escenarios de comunicación.

12.3 NIST SP 800-53 Rev. 5:

12.3.1 PL-4 – Normas de comportamiento: exige normas formales para el uso de sistemas y comunicaciones, incluidos los criterios de divulgación pública.

12.3.2 AC-8 – Notificación de uso del sistema: respalda avisos obligatorios y advertencias de contenido en plataformas expuestas externamente.

12.3.3 AU-12 – Generación de registros de auditoría: se aplica a la conservación de registros e historial de comunicaciones con fines de revisión de incidentes y auditoría.

12.4 RGPD de la UE (2016/679):

12.4.1 Artículo 5 – Principios relativos al tratamiento: prohíbe el intercambio no autorizado de datos personales mediante comunicación pública.

12.4.2 Artículo 25 – Protección de datos desde el diseño y por defecto: exige salvaguardas de privacidad en las herramientas de comunicación y en los flujos de contenido.

12.4.3 Artículo 32 – Seguridad del tratamiento: aplica procesos de cifrado, control de acceso y aprobación de contenido.

12.4.4 Artículo 33 – Notificación de una violación de la seguridad de los datos personales: exige la notificación oportuna de fugas de datos personales a través de canales públicos.

12.5 Directiva NIS2 de la UE (2022/2555):

12.5.1 Artículo 21 – Medidas de gestión del riesgo de las TIC: incluye protocolos de comunicación y obligaciones durante incidentes y mensajes públicos sobre riesgos.

12.6 DORA de la UE (2022/2554):

12.6.1 Artículo 9 – Gestión del riesgo de las TIC: se aplica a riesgos de comunicación activados externamente, como suplantación, desinformación y alteración reputacional.

12.6.2 Artículo 16 – Estrategia de comunicación: exige que los proveedores críticos financieros o de servicios gestionen los riesgos de comunicación y sus respuestas en escenarios de crisis.

12.7 COBIT 2019:

12.7.1 APO09 – Acuerdos de servicio gestionados y comunicación: exige una gobernanza estructurada de las comunicaciones internas y externas.

12.7.2 DSS05 – Gestionar los servicios de seguridad: garantiza que las actividades de comunicación no introduzcan riesgos adicionales ni menoscaben los procesos de gestión de incidentes.