					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P36S					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 aplicables

Norma/Reglamento	Cláusula/Artículo	Comentario
ISO/IEC 27001:2022	Cláusulas 5.1, 5.2, 6.1, 8	Liderazgo, gestión de riesgos y control operacional de las comunicaciones externas
ISO/IEC 27002:2022	Controles 5.10, 5.11	Uso aceptable y seguridad de la información en las comunicaciones
RGPD de la UE	Artículos 5, 32, 33	Principios de protección de datos, seguridad y notificación de violaciones de seguridad de los datos personales con impacto en la comunicación pública
Directiva NIS2 de la UE	Artículo 21(2)(e), 21(2)(f)	Políticas para el uso de sistemas y gestión de riesgos de la cadena de suministro y de las comunicaciones públicas
DORA de la UE	Artículo 14(4)	Obligaciones de comunicación tras incidentes
NIST SP 800-53 Rev. 5	PL-4, AU-7, IR-6, AC-22	Normas de conducta, auditoría, notificación de incidentes y gestión del contenido público y de los accesos

1. Propósito

1.1. Esta política establece directrices obligatorias para toda comunicación expuesta al público, incluido el uso de redes sociales, la relación con la prensa y el contenido digital externo, cuando haga referencia a la empresa, su personal, sus clientes, sus sistemas o sus prácticas internas.

1.2. Esta política contribuye a proteger la reputación de la empresa, mantener el cumplimiento legal y normativo y reducir el riesgo de fuga de datos, desinformación o incidentes de seguridad.

1.3. Permite que el personal y los socios participen de forma positiva y responsable en debates en línea, evitando al mismo tiempo divulgaciones accidentales o tergiversaciones.

1.4. Esta política refuerza la preparación de la PYME para la certificación ISO/IEC 27001 al abordar el control de la información puesta a disposición del público o de partes interesadas externas.

2. Alcance

2.1. Esta política se aplica a todas las personas vinculadas a la organización, incluidas:

2.1.1. Personas trabajadoras y contratistas

2.1.2. Profesionales autónomos, consultores y proveedores externos

2.1.3. Becarios o personal a tiempo parcial implicado en la prestación de servicios a clientes o con acceso a sistemas

2.2. Esta política se aplica a todas las formas de comunicación externa que hagan referencia a la organización, incluidas:

2.2.1. Publicaciones en redes sociales (LinkedIn, X, TikTok, Instagram, Facebook, etc.)

2.2.2. Entradas de blog, foros en línea, reseñas de clientes y hilos de debate

2.2.3. Intervenciones públicas (por ejemplo, conferencias, seminarios web, pódcast)

2.2.4. Correos electrónicos o mensajes dirigidos a periodistas, representantes gubernamentales o personas influyentes

2.2.5. Capturas de pantalla, fotografías o vídeos compartidos públicamente desde entornos de trabajo

2.3. Esta política también se aplica cuando dicha comunicación se realice:

2.3.1. Desde dispositivos personales o cuentas personales

2.3.2. Fuera del horario laboral habitual

2.3.3. Sin intención maliciosa; incluso los comentarios accidentales o informales están dentro del alcance si hacen referencia a la empresa

3. Objetivos

3.1. Protección de la reputación: prevenir daños a la imagen de la empresa derivados de comunicaciones públicas no autorizadas o inadecuadas.

3.2. Seguridad de la información: evitar la exposición no intencionada de datos sensibles, sistemas internos o información de clientes a través de redes sociales o canales públicos.

3.3. Cumplimiento legal y normativo: garantizar que todo contenido público que haga referencia a la empresa cumpla la normativa aplicable en materia de protección de datos y comunicaciones empresariales.

3.4. Conducta profesional: promover una participación responsable en debates en línea e interacciones con medios, incluso desde cuentas personales.

3.5. Preparación ante incidentes: proporcionar pasos claros y aplicables en caso de divulgaciones accidentales o incumplimientos de esta política.

4. Funciones y responsabilidades

4.1. Director General (DG)

4.1.1. Es el responsable de esta política y la aprueba.

4.1.2. Revisa y autoriza cualquier declaración pública, relación con la prensa o entrevista con medios.

4.1.3. Garantiza que esta política se comunique claramente a todas las personas trabajadoras y a terceros.

4.1.4. Investiga y responde a cualquier incumplimiento de esta política, en coordinación con los procedimientos de respuesta a incidentes.

4.2. Persona designada o responsable de comunicación (si se hubiera asignado)

4.2.1. Apoya al DG revisando el contenido antes de su publicación externa (por ejemplo, entradas de blog o temas de ponencias).

4.2.2. Mantiene registros de la actividad en medios aprobada o de publicaciones en redes sociales de alto riesgo aprobadas.

4.2.3. Supervisa las menciones conocidas de la empresa en línea para identificar riesgos reputacionales o de seguridad, en la medida en que la capacidad operativa lo permita.

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

9. Requisitos de revisión y actualización

9.1. Revisión anual

9.1.1. Esta política debe revisarse al menos una vez al año por el Director General (DG).

9.1.2. La revisión debe garantizar la alineación con las obligaciones legales actualizadas, las tendencias del sector en materia de comunicación y los cambios internos en la organización.

9.2. Revisiones basadas en desencadenantes

9.2.1. Esta política debe actualizarse inmediatamente después de:

9.2.1.1. Un incidente significativo en redes sociales o un problema reputacional

9.2.1.2. Un cambio en los proveedores externos que gestionan las comunicaciones

9.2.1.3. Nueva legislación u obligaciones regulatorias relacionadas con la comunicación en línea, los medios o la marca

9.3. Documentación de cambios

9.3.1. Todas las actualizaciones deben registrarse, incluyendo la fecha de revisión, el resumen de los cambios y la aprobación del DG.

9.3.2. Debe conservarse un historial de versiones con fines de auditoría y certificación.

9.4. Distribución de actualizaciones

9.4.1. Todo el personal y los contratistas deben ser informados de cualquier cambio en la política.

9.4.2. Las versiones actualizadas deben compartirse por correo electrónico o a través de portales internos.

9.4.3. Todo proveedor de comunicaciones públicas debe aceptar los términos actualizados antes de continuar prestando sus servicios.

10. Políticas relacionadas y vinculaciones

10.1. Esta política opera en coordinación con las siguientes políticas de la PYME:

10.1.1. P3S – Política de Uso Aceptable: define el comportamiento aceptable al utilizar plataformas de comunicación, incluido el acceso a redes sociales durante el horario laboral.

10.1.2. P8S – Política de Concienciación y Formación en Seguridad de la Información: garantiza que el personal esté formado para identificar los riesgos de divulgación excesiva de información, phishing o amenazas reputacionales en línea.

10.1.3. P17S – Política de Protección de Datos y Privacidad: garantiza que los datos personales y de clientes no se compartan en comunicaciones externas, en alineación con el RGPD de la UE y otros requisitos legales.

10.1.4. P30S – Política de Respuesta a Incidentes: regula la respuesta ante divulgaciones públicas accidentales, amenazas en línea o ataques reputacionales derivados del uso indebido de redes sociales.

10.1.5. P37S – Política de Cumplimiento Legal y Normativo: establece las obligaciones legales y contractuales más amplias de la organización cuando comparte contenido públicamente.

10.2. Estas políticas deben aplicarse de forma conjunta para mantener una presencia externa segura, respetuosa y conforme a derecho.

11. Normas y marcos de referencia

11.1. ISO/IEC 27001

11.1.1. Cláusula 5.1 – Liderazgo y compromiso: requiere supervisión por parte de la dirección de los riesgos reputacionales y de información.

11.1.2. Cláusula 6.1 – Gestión de riesgos: incluye exposiciones al riesgo relacionadas con las comunicaciones.

11.1.3. Cláusula 8.1 – Control operacional: cubre las reglas sobre cómo se comunica externamente la información.

11.2. ISO/IEC 27002

11.2.1. Control 5.10 – Uso aceptable de la información y de los activos

11.2.2. Control 5.11 – Seguridad de la información en las comunicaciones

11.3. NIST SP 800-53 Rev. 5

11.3.1. PL-4 – Normas de conducta: regula la conducta adecuada en el uso de los recursos de información.

11.3.2. AU-7 – Reducción de auditoría y generación de informes: da soporte a la supervisión del uso público de los sistemas.

11.3.3. IR-6 – Notificación de incidentes: exige respuesta ante brechas reputacionales y de comunicación.

11.3.4. AC-22 – Contenido accesible públicamente: garantiza el control sobre publicaciones externas y accesos.

11.4. RGPD de la UE (2016/679)

11.4.1. Artículo 5 – Principios relativos al tratamiento de datos personales (exactitud, integridad, responsabilidad proactiva)

11.4.2. Artículo 32 – Seguridad del tratamiento: exige salvaguardas en torno a la difusión pública.

11.4.3. Artículo 33 – Notificación de una violación de la seguridad de los datos personales: se activa si los datos personales quedan expuestos a través de una comunicación externa.

11.5. Directiva NIS2 de la UE (2022/2555)

11.5.1. Artículo 21(2)(e) – Políticas sobre el uso de sistemas de información, incluidas las plataformas de comunicación

11.5.2. Artículo 21(2)(f) – Políticas para gestionar los riesgos de ciberseguridad en la cadena de suministro y en las plataformas públicas

11.6. DORA de la UE (2022/2554)

11.6.1. Artículo 14(4) – Obligaciones de comunicación a clientes, terceros y autoridades tras incidentes operativos

11.7. COBIT 2019

11.7.1. APO09 – Gestionar los acuerdos de servicio: cubre la supervisión de proveedores y terceros relacionados con la comunicación.

11.7.2. DSS05 – Gestionar los servicios de seguridad: incluye la protección de activos digitales expuestos al público.

11.7.3. EDM03 – Garantizar la optimización del riesgo: hace hincapié en la gestión de riesgos reputacionales y de cumplimiento relacionados con la comunicación.