					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P38					Título del documento: **Política de Comunicaciones Seguras y Autenticación Multifactor**							
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**

Aviso legal (derechos de autor y restricciones de uso)

(C) 2025 Clarysec LLC. All rights reserved.

Este documento es propiedad intelectual de Clarysec LLC. Ninguna parte de este documento podrá copiarse, reutilizarse, distribuirse ni modificarse con fines comerciales o de implantación sin autorización previa y expresa por escrito.

El uso no autorizado está estrictamente prohibido y puede dar lugar a acciones legales.

Para cuestiones de licenciamiento, contacte con: info@clarysec.com

Alineación con normas y reglamentos

Norma/Reglamento	Cláusula/Artículo	Comentario
ISO/IEC 27001:2022	5.30, 5.31, 8.24	
ISO/IEC 27002:2022	5.15, 5.17, 5.18, 8.24, 8.28	
NIST SP 800-53 Rev. 5	IA-2, IA-3, IA-5, IA-8, SC-12, SC-13, SC-31	
RGPD de la UE	Art. 32(1)(b)	
Directiva NIS2 de la UE	Art. 21(2)(j)	
DORA de la UE	Art. 9(2)(d), Art. 11	
COBIT 2019	DSS05.04, DSS05.05, DSS05	

1. Propósito

1.1 Definir los requisitos para el uso de soluciones de autenticación multifactor o autenticación continua para el acceso a sistemas, en consonancia con el artículo 21(2)(j) de la Directiva NIS2 de la UE.

1.2 Establecer controles para las comunicaciones seguras de voz, vídeo, texto y emergencia, con el fin de proteger la confidencialidad e integridad de la información.

2. Alcance

2.1 Esta política se aplica a todos los mecanismos de autenticación y sistemas de comunicación (llamadas de voz, videoconferencia, mensajería y sistemas de notificación de emergencias) utilizados por la organización.

2.2 Abarca a todos los empleados, contratistas y terceros que utilicen los canales de comunicación de la organización o accedan a sus redes y sistemas de información.

3. Objetivos

3.1 Garantizar que solo los usuarios debidamente autenticados obtengan acceso a los sistemas, reduciendo el riesgo de acceso no autorizado mediante la implantación de autenticación multifactor.

3.2 Garantizar que las comunicaciones internas y de emergencia se transmitan a través de métodos seguros (por ejemplo, canales cifrados), evitando su interceptación o manipulación.

3.3 Cumplir los requisitos de la Directiva NIS2 de la UE en materia de autenticación robusta y comunicaciones seguras, reforzando la ciberresiliencia general.

4. Funciones y responsabilidades

4.1 Director de Seguridad de la Información / equipos de TI y seguridad: definir y mantener los mecanismos de autenticación multifactor y las herramientas de comunicación segura; garantizar la implantación técnica de esta política.

4.2 Administradores de sistemas: implantar la autenticación multifactor en los sistemas pertinentes, configurar las plataformas de comunicación segura aprobadas y supervisar el cumplimiento.

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

9. Supervisión y auditoría

9.1 Los equipos de TI y seguridad supervisarán de forma continua los registros de autenticación para detectar intentos de inicio de sesión con un único factor o fallos anómalos de autenticación multifactor.

Los registros de los sistemas de comunicación segura, cuando resulte aplicable, también deberán supervisarse para detectar intentos de acceso no autorizado o cambios de configuración.

9.2 La auditoría interna revisará anualmente el grado de implantación de la autenticación multifactor, verificando que todos los sistemas críticos la apliquen, y comprobará que los canales seguros aprobados se utilicen de forma exclusiva para las comunicaciones sensibles. Las conclusiones se comunicarán a la dirección junto con las recomendaciones correspondientes.

10. Revisión y mantenimiento

10.1 Esta política se revisará al menos una vez al año y también tras cualquier incidente grave de seguridad o ante cualquier riesgo recientemente identificado relacionado con la autenticación o las comunicaciones (por ejemplo, nuevos vectores de amenaza contra la autenticación multifactor o detección del uso de comunicaciones inseguras).

10.2 Las revisiones se realizarán cuando sea necesario para responder a la evolución tecnológica (por ejemplo, la adopción de soluciones de autenticación continua más robustas) o para cumplir directrices regulatorias actualizadas, como futuras recomendaciones de ENISA sobre comunicaciones seguras.

11. Políticas relacionadas y vínculos

11.1 P01 – Política de Seguridad de la Información. Establece las salvaguardas de autenticación y comunicaciones en toda la organización.

11.2 P04 – Política de Control de Acceso. Establece la gobernanza de accesos que la autenticación multifactor de la P38 refuerza.

11.3 P11 – Política de Gestión de Cuentas de Usuario y Privilegios. Vincula la autenticación multifactor al ciclo de vida del acceso privilegiado.

11.4 P18 – Política de Controles Criptográficos. Proporciona los mecanismos criptográficos y de gestión de claves aprobados para las comunicaciones seguras.

11.5 P21 – Política de Seguridad de Redes. Protege los canales de transporte utilizados por voz, vídeo y mensajería.

11.6 P22 – Política de Registro y Supervisión. Supervisa los eventos de autenticación y el uso de canales seguros.

11.7 P32 – Política de Continuidad del Negocio y Recuperación ante Desastres. Protege las comunicaciones de emergencia durante las crisis.

11.8 P08 – Política de Concienciación y Formación en Seguridad de la Información. Forma a los usuarios sobre autenticación multifactor y uso seguro de los canales.

12. Referencias

12.1 Directiva NIS2 (UE 2022/2555), artículo 21(2), letra (j) (uso de autenticación multifactor y comunicaciones seguras)

12.2 Reglamento de Ejecución (UE) 2024/2690 de la Comisión, anexo, sección 11 (requisitos de control de acceso, incluida la autenticación multifactor para cuentas privilegiadas)

12.3 ISO/IEC 27001:2022 e ISO/IEC 27002:2022