MNEMO

Anexo 5

POLÍTICA DE SEGURIDAD

Dentro de esta área se localizan los siguientes objetivos y principios, controles y posibles mediciones asociadas:

A5.1	Política de Seguridad de la información
Objetivo	La política de seguridad de la información y las políticas de temas específicos deben ser definidas, aprobadas por la gerencia, publicadas, comunicadas y reconocidas por el personal relevante y las partes interesadas relevantes, y revisadas a intervalos planificados y si ocurren cambios significativos.
Principios	Garantizar la idoneidad, adecuación y eficacia continuas de la dirección y el apoyo a la seguridad de la información de acuerdo con los requisitos empresariales, legales, reglamentarios y contractuales. La Dirección debería establecer una política clara y en línea con los objetivos del negocio y demostrar su apoyo y compromiso con la seguridad de la información mediante la publicación y mantenimiento de una política de seguridad de la información para toda la organización.
Información	Piense en términos de un manual o wiki de políticas de seguridad de la información que contenga un conjunto coherente e internamente consistente de políticas, normas, procedimientos y directrices. Determine la frecuencia de revisión de la política de seguridad de la información y las formas de comunicación a toda la organización. La revisión de la idoneidad y adecuación de la política de seguridad de la información puede ser incluida en las revisiones de la dirección.
Medición	Cobertura de la política (es decir, porcentaje de secciones de ISO/IEC 27001:2022 / 27002:2022, para las cuales se han especificado, escrito, aprobado y publicado políticas y sus normas, procedimientos y directrices asociadas. Grado de despliegue y adopción de la política en la organización (medido por auditoría, gerencia o autoevaluación).