MNEMO

Anexo 18

CUMPLIMIENTO LEGAL

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

A5.31	Requisitos legales, estatutarios, reglamentarios y contractuales
Objetivo	Los requisitos legales, estatutarios, regulatorios y contractuales relevantes para la seguridad de la información y el enfoque de la organización para cumplir con estos requisitos deben identificarse, documentarse y mantenerse actualizados.
Principios	Garantizar el cumplimiento de los requisitos legales, estatutarios, reglamentarios y contractuales relacionados con la seguridad de la información. El diseño, operación, uso y gestión de los sistemas de información pueden ser objeto de requisitos estatutarios, reguladores y de seguridad contractuales. Los requisitos legales específicos deberían ser advertidos por los asesores legales de la organización o por profesionales adecuadamente cualificados. Los requisitos que marca la legislación cambian de un país a otro y pueden variar para la información que se genera en un país y se transmite a otro país distinto (por ej., flujos de datos entre fronteras).
Información	Obtenga asesoramiento legal competente, especialmente si la organización opera o tiene clientes en múltiples jurisdicciones. Los requisitos externos, incluidos los legales, estatutarios, reglamentarios o contractuales, deben tenerse en cuenta a la hora de a) el desarrollo de políticas y procedimientos de seguridad de la información

A5.31	Requisitos legales, estatutarios, reglamentarios y contractuales
	b) el diseño, la aplicación o la modificación de los controles de seguridad de la información c) clasificar la información y otros activos asociados como parte del proceso para establecer los requisitos de seguridad de la información para las necesidades internas o para los acuerdos con los proveedores d) la realización de evaluaciones de los riesgos para la seguridad de la información y la determinación de las actividades de tratamiento de los riesgos para la seguridad de la información e) determinar los procesos junto con las funciones y responsabilidades relacionadas con la seguridad de la información f) determinar los requisitos contractuales de los proveedores pertinentes para la organización y el alcance del suministro de productos y servicios.
Medición	Número de cuestiones o recomendaciones de cumplimiento legal, agrupadas y analizadas por su estado (cerradas, abiertas, nuevas, retrasadas) e importancia o nivel de riesgo (alto, medio o bajo). Porcentaje de requisitos externos clave que, mediante auditorías objetivas o de otra forma admisible, han sido considerados conformes.

A5.32	Derechos de propiedad intelectual
Objetivo	La organización debería implementar procedimientos apropiados para proteger los derechos de propiedad intelectual.
Principios	Garantizar el cumplimiento de los requisitos legales, estatutarios, reglamentarios y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos patentados.

A5.32	Derechos de propiedad intelectual
	El diseño, operación, uso y gestión de los sistemas de información pueden ser objeto de requisitos estatutarios, reguladores y de seguridad contractuales. Los requisitos legales específicos deberían ser advertidos por los asesores legales de la organización o por profesionales adecuadamente cualificados. Los requisitos que marca la legislación cambian de un país a otro y pueden variar para la información que se genera en un país y se transmite a otro país distinto (por ej., flujos de datos entre fronteras).
Información	Obtenga asesoramiento legal competente, especialmente si la organización opera o tiene clientes en múltiples jurisdicciones. Los derechos de propiedad intelectual incluyen los derechos de autor de los programas informáticos o los documentos, los derechos de diseño, las marcas comerciales, las patentes y las licencias de código fuente. Los productos de software propietario suelen suministrarse bajo un acuerdo de licencia que especifica los términos y condiciones de la misma, por ejemplo, limitando el uso de los productos a máquinas específicas o limitando la copia a la creación de copias de seguridad únicamente. Véase la serie ISO/IEC 19770 para más detalles sobre la gestión de activos informáticos. Los datos pueden adquirirse de fuentes externas. Por lo general, estos datos se obtienen bajo los términos de un acuerdo de compartición de datos o un instrumento legal similar. Estos acuerdos de compartición de datos deben dejar claro qué tratamiento se permite para los datos adquiridos. También es aconsejable que se indique claramente la procedencia de los datos. Véase la norma ISO/IEC 23751, para más detalles sobre los acuerdos de intercambio de datos.

A5.32	Derechos de propiedad intelectual
Medición	Número de cuestiones o recomendaciones de cumplimiento legal, agrupadas y analizadas por su estado (cerradas, abiertas, nuevas, retrasadas) e importancia o nivel de riesgo (alto, medio o bajo). Porcentaje de requisitos externos clave que, mediante auditorías objetivas o de otra forma admisible, han sido considerados conformes.

A5.33	Protección de registros
Objetivo	Los registros deben protegerse contra pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada.
Principios	Garantizar el cumplimiento de los requisitos legales, estatutarios, reglamentarios y contractuales, así como las expectativas de la comunidad o de la sociedad relacionadas con la protección y la disponibilidad de los registros. El diseño, operación, uso y gestión de los sistemas de información pueden ser objeto de requisitos estatutarios, reguladores y de seguridad contractuales. Los requisitos legales específicos deberían ser advertidos por los asesores legales de la organización o por profesionales adecuadamente cualificados. Los requisitos que marca la legislación cambian de un país a otro y pueden variar para la información que se genera en un país y se transmite a otro país distinto (por ej., flujos de datos entre fronteras).
Información	Obtenga asesoramiento legal competente, especialmente si la organización opera o tiene clientes en múltiples jurisdicciones. La organización debe adoptar las siguientes medidas para proteger la autenticidad, fiabilidad, integridad y utilidad de los documentos

A5.33	Protección de registros
	de archivo, ya que el contexto empresarial y los requisitos para su gestión cambian con el tiempo: a) emitir directrices sobre el almacenamiento, el manejo de la cadena de custodia y la eliminación de los registros, que incluyan la prevención de la manipulación de los mismos. Estas directrices deben estar en consonancia con la política específica de la organización en materia de gestión de registros y otros requisitos de los mismos; b) Elaborar un calendario de conservación que defina los registros y el periodo de tiempo que deben conservarse. El sistema de almacenamiento y manipulación debe garantizar la identificación de los registros y su período de conservación, teniendo en cuenta la legislación o la normativa nacional o regional, así como las expectativas de la comunidad o la sociedad, si procede. Este sistema debe permitir la destrucción adecuada de los registros después de ese período si la organización no los necesita. Puede ser necesario conservar algunos registros de forma segura para cumplir con los requisitos legales, reglamentarios o contractuales, así como para apoyar las actividades empresariales esenciales. Las leyes o reglamentos nacionales pueden establecer el periodo de tiempo y el contenido de los datos para la conservación de la información. Puede encontrar más información sobre la gestión de registros en la norma ISO 15489.
Medición	Número de cuestiones o recomendaciones de cumplimiento legal, agrupadas y analizadas por su estado (cerradas, abiertas, nuevas, retrasadas) e importancia o nivel de riesgo (alto, medio o bajo). Porcentaje de requisitos externos clave que, mediante auditorías objetivas o de otra forma admisible, han sido considerados conformes.

A5.34	Privacidad y protección de la Información de identificación personal PII
Objetivo	La organización debe identificar y cumplir con los requisitos relacionados con la preservación de la privacidad y la protección de la PII de acuerdo con las leyes y regulaciones aplicables y los requisitos contractuales.
Principios	Garantizar el cumplimiento de los requisitos legales, estatutarios, reglamentarios y contractuales relacionados con los aspectos de seguridad de la información de la protección de la Información Personal PII. El diseño, operación, uso y gestión de los sistemas de información pueden ser objeto de requisitos estatutarios, reguladores y de seguridad contractuales. Los requisitos legales específicos deberían ser advertidos por los asesores legales de la organización o por profesionales adecuadamente cualificados. Los requisitos que marca la legislación cambian de un país a otro y pueden variar para la información que se genera en un país y se transmite a otro país distinto (por ej., flujos de datos entre fronteras).
Información	Obtenga asesoramiento legal competente, especialmente si la organización opera o tiene clientes en múltiples jurisdicciones. La organización debe establecer y comunicar a todas las partes interesadas una política específica sobre privacidad y protección de la Información Personal PII. La organización debe desarrollar e implementar procedimientos para la preservación de la privacidad y la protección de la IIP. Dichos procedimientos deberán comunicarse a todas las partes interesadas pertinentes que participen en el tratamiento de la información personal identificable. El cumplimiento de estos procedimientos y de toda la legislación y los reglamentos pertinentes relativos a la preservación de la privacidad y la protección de la IIP requiere funciones,

A5.34	Privacidad y protección de la Información de identificación personal PII
	responsabilidades y controles adecuados. A menudo, la mejor manera de lograrlo es designando a una persona responsable, como un funcionario de privacidad, que debe orientar al personal, a los proveedores de servicios y a otras partes interesadas sobre sus responsabilidades individuales y los procedimientos específicos que deben seguirse. La norma ISO/IEC 29100 proporciona un marco de alto nivel para la protección de la IPI en los sistemas de TIC. En la norma ISO/IEC 27701 se puede encontrar más información sobre los sistemas de gestión de la información sobre la privacidad. La información específica sobre la gestión de la información sobre la privacidad para las nubes públicas que actúan como procesadores de la IPI se puede encontrar en la norma ISO/IEC 27018.
Medición	Número de cuestiones o recomendaciones de cumplimiento legal, agrupadas y analizadas por su estado (cerradas, abiertas, nuevas, retrasadas) e importancia o nivel de riesgo (alto, medio o bajo). Porcentaje de requisitos externos clave que, mediante auditorías objetivas o de otra forma admisible, han sido considerados conformes.