CUMPLIMIENTO DE NORMAS Y REGULACIONES

Cumplimiento de los requisitos legales y contractuales

Tiene como objetivo el evitar brechas entre las obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con seguridad de la información y cualquier requisito de seguridad.

Identificación de la legislación aplicable y de los requisitos contractuales

Todos los requisitos legales estatutarios, reglamentarios y contractuales pertinentes, así como el enfoque de la organización para cumplirlos, deberían ser explícitamente identificados, documentados y actualizados para cada sistema de información y la organización

Deberían definirse y documentarse los controles específicos y las responsabilidades individuales para cumplir con los requisitos anteriores.

Los administradores deberían identificar toda la legislación aplicable a su organización a fin de cumplir con los requisitos para su tipo de negocio. Si la organización realiza negocios en otros países, los administradores deberían considerar el cumplimento en todos los países pertinentes.

Derechos de propiedad intelectual

Se deberían implementar procedimientos apropiados para asegurarse del cumplimiento de los requisitos legales, reglamentarios y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software propietario.

Deberían considerarse las siguientes directrices para proteger cualquier material que pueda ser considerado propiedad intelectual, para lo cual hay que:

a) publicar una política de cumplimiento de los derechos de propiedad intelectual que defina el uso legal de los productos de software e información;

b) adquirir software sólo de fuentes conocidas y de buena reputación, para asegurarse de que los derechos de propiedad intelectual del software no han sido violados;

c) mantener la concientización de las políticas de protección de los derechos de propiedad intelectual y tomar nota para adoptar medidas disciplinarias contra el personal que los incumpla;

d) mantener un registro apropiado de activos, e identificar todos los activos con requisitos de protección del derecho de propiedad intelectual;

e) mantener los documentos de prueba y evidencia de la propiedad de licencias, discos maestros, manuales, entre otros;

f) implementar controles para asegurarse de que no se sobrepase el número máximo de usuarios permitidos de la licencia;

g) llevar a cabo revisiones de que solo sean instalados productos de software autorizados y con licencia;

h) establecer una política de mantenimiento de las condiciones adecuadas de licencia;

i) establecer una política de eliminación de software o de su transferencia a terceros;

j) cumplir con los términos y condiciones del software y de la información obtenidos de redes públicas;

k) no duplicar, ni convertir a otro formato o extraer información de las grabaciones comerciales (película, audio) con excepción de lo permitido por los derechos de propiedad intelectual;

l) no copiar total o parcialmente, libros, artículos, informes u otros documentos, con excepción de lo permitido por los derechos de propiedad intelectual.

Protección de los registros
Se debería proteger los registros contra pérdida, destrucción, falsificación, acceso no autorizado y la divulgación no autorizada, de conformidad con los requisitos legales, reglamentarios, contractuales y de negocio.

Al decidir sobre la protección de los registros específicos de la organización, debería considerarse la correspondiente clasificación de la organización basada en el esquema de clasificación de la organización. Los registros deberían estar categorizados en tipos de registro, como, por ejemplo: registros contables, registros de bases de datos, registros de bitácoras de transacciones, de auditoría y procedimientos operativos, cada uno de los cuales, con los detalles de plazos de retención y medios de almacenamiento permisibles, como, por ejemplo, papel, microfichas, medios magnéticos u ópticos. Cualquier llave criptográfica y programa asociado con archivos cifrados o firmas digitales, debería también guardarse para permitir el descifrado de los registros durante el tiempo en que sean retenidos.

Debería considerarse la posibilidad de deterioro de los medios utilizados para almacenar los registros.

Deberían implantarse procedimientos para su almacenamiento y utilización de acuerdo con las recomendaciones del fabricante.

Cuando se elige utilizar medios de almacenamiento electrónico, deberían establecerse procedimientos para asegurarse de la capacidad para acceder a los datos (tanto al medio como a la lectura de los formatos) a través de todo el período de retención, para salvaguardarlos contra su pérdida debida a un cambio futuro de tecnología.
Deberían elegirse sistemas de almacenamiento tales que los datos requeridos puedan recuperarse de manera aceptable en un marco de tiempo y formato, dependiendo de los requisitos a satisfacer.

El sistema de almacenamiento y utilización debería asegurar la identificación de los registros y de su período de retención según lo definido por la legislación, las regulaciones nacionales o regionales, si fuera aplicable. Este sistema debería permitir la destrucción apropiada de los registros tras dicho período si ya no los necesita la organización.
Para alcanzar los objetivos de salvaguardar los registros, deberían seguirse los siguientes pasos dentro de una organización:

a) deberían emitirse directrices sobre la retención, almacenamiento, manejo y eliminación de los registros y de la información;

b) debería diseñarse un calendario de retenciones que identifique los registros y los períodos de tiempo en que deberían ser retenidos;

c) debería mantenerse un inventario de las fuentes de información clave.

Privacidad y protección de datos personales
Debería asegurarse la privacidad y la protección de los datos personales según lo dispuesto en la legislación y la reglamentación pertinente cuando sea aplicable.

Debería desarrollarse e implementarse una política de protección y de privacidad de los datos personales de la organización. Esta política debería ser comunicada a todas las personas implicadas en el procesamiento de datos personales.

El cumplimiento de esta política y de toda la legislación y reglamentaciones pertinentes a la protección de la privacidad de las personas y de los datos personales requiere una apropiada estructura de gestión y control. A menudo, este objetivo suele alcanzarse con mayor facilidad designando una persona responsable, por ejemplo, un oficial de protección de la privacidad, que oriente a los administradores, usuarios y proveedores de servicios sobre sus responsabilidades individuales y sobre los procedimientos específicos que deberían seguirse. La responsabilidad de manejar la información personal y de asegurar la toma de conciencia de los principios de privacidad debería establecerse de acuerdo con la legislación y las reglamentaciones pertinentes. Deberían implementarse medidas técnicas y organizacionales apropiadas para proteger la información personal.

Regulación de los controles criptográficos
Se deberían utilizar controles criptográficos en cumplimiento con todos los acuerdos, leyes, y regulaciones pertinentes.

Los siguientes ítems deberían considerarse para el cumplimiento de los acuerdos, las leyes, y las reglamentaciones pertinentes:

a) restricciones en la importación o en la exportación de hardware y de software para ejecutar funciones criptográficas;

b) restricciones en la importación o en la exportación de hardware y de software que se diseña para tener funciones criptográficas adjuntas;

c) restricciones en el uso de cifrado;

d) métodos mandatorios o discrecionales de acceso por parte de las autoridades de los países a la información encriptada en hardware o software para proporcionar la confidencialidad del contenido. Mediante el asesoramiento jurídico debería intentarse asegurar el cumplimiento de leyes y regulaciones pertinentes. Antes de que la información cifrada o los controles criptográficos sean trasladados a través de fronteras jurisdiccionales, también debería tenerse en cuenta el asesoramiento jurídico.

CUMPLIMIENTO DE NORMAS Y REGULACIONES

Revisión de seguridad de la información

Tiene como objetivo el asegurar que la seguridad de la información sea implementada y opere de acuerdo con las políticas y procedimientos de la organización.

Revisiones independientes de la seguridad de la información

El enfoque de la organización para la gestión de seguridad de la información y su implementación (por ejemplo, los objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) deberían ser revisados de forma independiente a intervalos planificados o cuando se produzcan cambios significativos.

La dirección debería iniciar la revisión independiente. Tal revisión independiente es necesaria para asegurar la conveniencia, adecuación y eficacia continuas del enfoque de la organización para gestionar la seguridad de la información. La revisión debería incluir oportunidades de evaluación para la mejora y la necesidad de cambios en el enfoque de seguridad, incluyendo la política y los objetivos de control.

Dicha revisión debería realizarse por personas independientes del área bajo revisión, por ejemplo, la función de auditoría interna, un administrador independiente o una organización de tercera parte especializada en ese tipo de revisiones. Las personas que llevan a cabo estas revisiones deberían tener las habilidades y experiencia apropiadas.

Los resultados de una revisión independiente deberían registrarse y comunicarse a la dirección que la inició. Estos registros deberían conservarse.

Si la revisión independiente identifica que el enfoque de la organización y la implementación para gestionar la seguridad de la información son inadecuadas, por ejemplo, los requisitos y objetivos documentados no se cumplen o no cumplen con la dirección de seguridad de la información establecida en las políticas de seguridad de la información, la dirección debería considerar las acciones correctivas.

Cumplimiento con las políticas y normas de seguridad

Los administradores deberían revisar periódicamente el cumplimiento del procesamiento de la información y procedimientos dentro de su área de responsabilidad con las políticas de seguridad, las normas y otros requisitos de seguridad.

Los administradores deberían identificar cómo revisar si se cumplen los requisitos de seguridad de la información definidos en las políticas, normas y en otras regulaciones aplicables. Deberían considerarse herramientas de medición automática y de informes para una revisión periódica eficiente.

Si algún incumplimiento se encuentra como resultado de la revisión, los directores deberían:

a) identificar las causas del incumplimiento;

b) evaluar la necesidad de tomar medidas para lograr el cumplimiento;

c) implementar las acciones correctivas apropiadas;

d) revisar la acción correctiva tomada para comprobar su eficacia e identificar las deficiencias o debilidades.

CUMPLIMIENTO DE NORMAS Y REGULACIONES

Los resultados de las revisiones y de las acciones correctivas realizadas por los directores deberían registrarse y estos registros deberían mantenerse. Los administradores deberían reportar los resultados a las personas que realizan las revisiones independientes cuando la revisión independiente se realice en el área de su responsabilidad.

Revisiones del cumplimiento técnico
Los sistemas de información deberían ser revisados regularmente para el cumplimiento de las políticas y las normas de seguridad de la información de la organización.

El cumplimiento técnico debería revisarse preferentemente con la ayuda de herramientas automatizadas que generen un informe técnico para su posterior interpretación por parte de un especialista técnico. Alternativamente, un ingeniero de sistemas experimentado podría realizar revisiones manuales (con el apoyo de herramientas de software apropiadas, si es necesario).

Si se utilizan pruebas de intrusión o evaluaciones de vulnerabilidad, debería tenerse cuidado pues estas actividades podrían comprometer la seguridad del sistema. Tales pruebas deberían planificarse, documentarse y repetirse.

Cualquier revisión del cumplimiento técnico debería realizarse solamente por las personas competentes, autorizadas, o bajo supervisión de tales personas.