CUMPLIMIENTO

INTRODUCCIÓN Y ANTECEDENTES

Es una prioridad el buen cumplimiento de los requisitos legales para evitar las violaciones a cualquier ley y cualquier requerimiento de seguridad. La identificación de la legislación aplicable debe estar bien definida. El cumplimiento de los requisitos legales se aplica también a la protección de los documentos de la organización, protección de datos y privacidad de la información personal, prevención del uso indebido de los recursos de tratamiento de la información, y a regulaciones de los controles criptográficos. Los sistemas de información deben estar bajo monitoreo y deben chequearse regularmente para ver y garantizar el cumplimiento de los estándares de implementación de la seguridad. Las actividades y requerimientos de auditoría que involucran chequeos de los sistemas operacionales deben ser planeados y acordados cuidadosamente para minimizar el riesgo de interrupciones en los procesos. También se requiere protección para salvaguardar la integridad y evitar el mal uso de las herramientas de auditoría. Se deben definir explícitamente, documentar y actualizar todos los requerimientos legales para cada sistema de información y para la organización en general.

OBJETIVOS

El objetivo es cumplir con las disposiciones normativas y contractuales a fin de evitar sanciones administrativas a la organización y a los empleados que tengan responsabilidad civil o penal como resultado de incumplimientos. Se debe revisar la seguridad de los sistemas de información periódicamente a efectos de garantizar la adecuada aplicación de la política, normas y procedimientos de seguridad, sobre las plataformas tecnológicas y los sistemas de información. Se debería buscar asesoría sobre los requisitos legales específicos de los asesores jurídicos de la organización o de abogados practicantes calificados.

CUMPLIMIENTO DE LOS REQUISITOS LEGALES Y CONTRUACTALES

Evitar el incumplimiento de cualquier ley que está establecida en la empresa, como las leyes o reglas que se establezcan en el reglamento que tenga dicha empresa y cualquier requisito de la seguridad. El diseño, la operación y la gestión de los sistemas de información pueden estar sujetos a requisitos de seguridad reglamentaria. Por lo que se debería de buscar asesoría sobre los requisitos específicos y legales de los asesores jurídicos de la empresa o bien de los abogados con los que cuente. La empresa garantice el cumplimento de todas las normas que establece o bien de los contratos externos que se tienen además de tener resguardada la información para que terceras personas no se enteren de los detalles de algún contrato.

Identificación de la legislación aplicable. La organización para cumplir estos requisitos se deberían definir explícitamente, documentar y mantener actualizados para cada sistema de información y para la organización.

Derechos de propiedad intelectual (DPI). Se deberían implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso del material con respecto al cual pueden existir derechos de propiedad intelectual y sobre el uso de productos de software patentados.

Protección de los registros de la organización. Los registros importantes se deberían proteger contra pérdida, destrucción y falsificación, de acuerdo con los requisitos estatutarios, reglamentarios, contractuales y del negocio.

Protección de datos y privacidad de la información personal. Se debería desarrollar e implementar una política de protección y privacidad de los datos. Esta política se debería comunicar a todas las personas involucradas en el procesamiento de información personal.

Regulación de los controles criptográficos. Se deberían utilizar controles criptográficos o bien cifrados u ocultos, que cumplan todos los acuerdos, las leyes y los reglamentos pertinentes.

REVISIONES DE LA SEGURIDAD DE LA INFORMACIÓN

Se deberían realizar revisiones regulares de la seguridad de los sistemas de información. Las revisiones se deberían realizar según las políticas de seguridad apropiadas y las plataformas técnicas y sistemas de información deberían ser auditados para el cumplimiento de los estándares adecuados de implantación de la seguridad y controles de seguridad documentados. Alinee los procesos de auto-evaluación de controles de seguridad con el auto-evaluación de gobierno corporativo, cumplimiento legal y regulador. Complementados por revisiones de la dirección y verificaciones externas de buen funcionamiento. Deberían existir controles para proteger los sistemas en activo y las herramientas de auditoría durante el desarrollo de las auditorías de los sistemas de información.

Revisión independiente de la seguridad de la información. Se debería revisar el enfoque de la organización para la implementación como los controles, las políticas, los procesos y procedimientos para la seguridad de la información, en base a revisiones independientes e intervalos planificados o cuando tengan lugar cambios significativos en la empresa.

Cumplimiento de las políticas y normas de seguridad. Los directores deberían garantizar que todos los procedimientos de seguridad dentro de sus áreas de responsabilidad se llevan a cabo correctamente para lograr el cumplimiento con las políticas y las normas de seguridad.

Comprobación de cumplimiento. Los sistemas de información se deberían verificar periódicamente para determinar el cumplimiento con las normas de implementación de la seguridad. La verificación del cumplimiento se debería realizar bien sea manualmente por un ingeniero de sistemas con experiencia y con la ayuda de herramientas automáticas que generan un informe técnico para la interpretación posterior por parte del especialista técnico.

FUENTES DE BIBLIOGRAFICAS

- http://isoedith18.blogspot.com/2015/06/15-cumplimiento.html
- https://www.welivesecurity.com/la-es/2013/04/17/importancia-cumplimiento-requisitos-legales-gestion-informacion/
- https://www.pmg-ssi.com/2016/06/la-norma-iso-27002-complemento-para-la-iso-27001/