NORMA ISO/IEC 27001

AUTOR: ANDRADE J. CHÁVEZ C

MAYO: 2018

San Marcos

Introducción

Las normas ISO 27001:2013 e ISO 27002 de Seguridad de la Información, radican en comprobar el cumplimiento de los controles y las exigencias definidas por el estándar, de darse el caso de no cumplimiento de estos controles en general se realiza una auditoria para definir las no conformidades que son presentadas por un informe de un auditor. El proceso de auditoría es sistemático e independiente basándose en la verificación de los objetivos de control de las normas siendo este evidenciado.

Todo plan de seguridad de la información debe estar alineado en las normas ISO 27001:2013 e ISO 27002, en relación a seguridad de los datos, a fin de mantener la confidencialidad, integridad, y disponibilidad, definiendo reglas y procedimientos que aseguren tomar buenas prácticas cuando se presenten incidentes de seguridad, gestionando los riesgos y procedimientos que se realizan en la compañía.

Dado esto, se pasa a retomar la información contenida en la norma ISO/IEC 27001, con la finalidad de dar a conocer las generalidades de la misma.

Contenido

Introducción 1
NORMA ISO/IEC 27001 3
Contenidos de la Norma 3
Sistema de Gestión de Seguridad de la Información (SGSI) 4
Metodología 4
PLANEAR 4
HACER 5
VERIFICAR 5
ACTUAR 5
Conclusiones y recomendaciones 6
Referencias bibliográficas 6

NORMA ISO/IEC 27001

Contenidos de la Norma

A contiuación se incluye los contenidos correspondientes a dicha norma.

A. La política de seguridad: cuyo objetivo es garantizar el soporte y gestión necesarios para la seguridad, alineados a los requisitos institucionales y normativos.

A. La organización de la seguridad de la información: cuyo objetivo es crear un marco de referencia para la implementación y control de la seguridad de la información.

A. La seguridad de los recursos humanos: cuyo propósito es establecer las medidas necesarias para controlar la seguridad de la información, que sea manipulada por los recursos humanos.

A. La gestión de activos: tiene como propósito asegurar los activos de la organización.

A. El control de acceso: Por medio del cual asegura la confidencialidad de los sistemas de información de la empresa.

A. 10 Criptografía: establece reglas para la implementación de claves criptográficas

A. 11 La seguridad física y del ambiente: orientada a proteger a las instalaciones de la organización y a toda la información que manipula.

A. 12 Seguridad en las operaciones: controla la creación de procedimientos de operaciones, implementación y actualización.

A. 13 La gestión de las comunicaciones: ayuda a determinar el procedimiento y responsabilidades de las operaciones que realiza la organización.

A. 14 La adquisición, desarrollo y mantenimiento de los sistemas de información: orientada a organizaciones que desarrollen software internamente o que mantengan un contrato con otra empresa que sea la encargada de desarrollarlo.

A. 15 Relaciones con proveedores: su objetivo es tener un grado de seguridad apropiado en las transacciones con terceros

A. 16 La gestión de incidentes en la seguridad de la información: ejecuta un proceso de mejora constante en la gestión de incidentes de seguridad de la información.

A. 17 La gestión de la continuidad del negocio: Su propósito es asegurar la continuidad operativa de la organización.

A. 18 El cumplimiento: cuyo objetivo es velar que los requisitos legales de seguridad, con respecto al diseño, operación, uso y gestión de los sistemas de información se lleven a cabo.

Sistema de Gestión de Seguridad de la Información (SGSI)

El SGSI, define la implementación de mecanismos de gestión de varios estándares definidos con anterioridad para calificar la seguridad. El objetivo primordial es hallar todos los activos y personal que pertenecen al área tecnológica por medio de un proceso de gestión de riesgos alineados a los procesos y servicios que posee la organización con la ayuda del departamento tecnológico, adicional comprueba si existen controles de seguridad que admitan a las políticas y procedimientos para disminuir los riesgos.

Metodología

Esta metodología describe los cuatro pasos primordiales que se deben de ejecutar de forma secuencial para lograr la mejora continua, entendiendo como tal al mejoramiento continuado de la calidad sean estos la reducción de fallos, incremento de la eficacia y eficiencia, resolución de incidentes, previsión y eliminación de riesgos. El siguiente cuadro menciona los procesos más principales que menciona la norma alineados con las etapas del ciclo PHVA.

PLANEAR

Establecer el contexto.
Alcance y Límites

Definir Política del SGSI
Definir Enfoque de Evaluación de Riesgos
Identificación de riesgos
Análisis y Evaluación de riesgos Evaluar alternativas para el Plan de tratamiento de riesgos Aceptación de riesgos Declaración de Aplicabilidad
Declaración de Aplicabilidad

HACER

Implementar plan de tratamiento de riesgos
Implementar los controles seleccionados
Definir las métricas
Implementar programas de formación y sensibilización
Gestionar la operación del SGSI
Gestionar recursos Implementar procedimientos y controles para la gestión de incidentes de seguridad

VERIFICAR

Ejecutar procedimientos de seguimiento y revisión de controles.
Realizar revisiones regulares de cumplimiento y eficacia de los controles y del SGSI.
Medir la eficacia de los controles y verificación de satisfacción de los requerimientos de seguridad.
Revisión de la evaluación de riesgos periódicamente.
Realizar auditorías internas
Revisión de alcance y líneas de mejoras del SGSI por la Dirección.
Actualizar los planes de seguridad
Registrar acciones que podrían impactar la eficacia y/o eficiencia del SGSI

ACTUAR

Implementar las mejoras identificadas para el SGSI
Implementar las acciones correctivas y preventivas pertinentes.
Comunicar acciones y mejoras a todas las partes involucradas.
Asegurarse que las mejoras logren los objetivos previstos.
Bibliografía

Conclusiones y recomendaciones

En conclusión, toda gestión de seguridad dicta los procedimientos, los procesos y recursos con los que tiene compañía para sostener y tener un mayor control de los procesos así establecer una política de prevención y calidad de los servicios, están regulados por las normas ISO/IEC 27001 y la ISO/IEC 27002, estas establecen mecanismos para constituir, implementar, ejecutar, monitorear, inspeccionar, enriquecer un SGSI, adicional indica los requerimientos para implementar mecanismos de seguridad a través de los requerimientos de las empresas por medio de un proceso determinado o un servicio en base a el SGSI alineado a los objetivos y alcances de la empresaes. Por ello, es vital conocer la norma debido a que esta metodología describe los cuatro pasos primordiales que se deben de ejecutar de forma secuencial para lograr la mejora continua, entendiendo como tal al mejoramiento continuado de la calidad sean estos la reducción de fallos, incremento de la eficacia y eficiencia, resolución de incidentes, previsión y eliminación de riesgos.

Referencias bibliográficas

- Andrade J.C y Chávez E. (2018). Tesis. Recuperado De http://repositorio.ug.edu.ec/handle/redug/32606

San Marcos

www.usanmarcos.ac.cr

San José, Costa Rica