Propuesta de implementación de un Sistema Gestor de Seguridad de la Información, basados en INTE/ISO/IEC 27001:2014 en el departamento de TI para Almacenes El Rey, en el año 2021
Proposal for the implementation of an Information Security Management System, based on INTE / ISO / IEC 27001: 2014 in the IT department for Almacenes El Rey, in 2021

Ing. Jeffry Herrera Córdoba
Universidad Latina, Costa Rica
jjherrera57@gmail.com

Recibido 16/set/2020
Aprobado 10/nov/2020

Resumen-

Durante este articulo se explica la importancia de las normativas como la INTE/ISO/IEC 27001:2014 y la INTE/ISO/IEC 27002:2016 en el campo de la seguridad informática, se explica el proceso PHVA, las clasificaciones de las diferentes dimensiones de seguridad, las secciones que requiere un SGSI y el proceso que se realizó para la implementación de estas dos normas durante el desarrollo del trabajo final de graduación para optar por el grado de Licenciatura en Seguridad Informática, así como los procesos, alcances y documentos que se consideran básicos y necesarios para dar ese primer paso que debe tomar toda empresa en el mundo de la seguridad de la información que cambia y avanza cada día con mayor rapidez.

Palabras Claves: *normativas, INTE/ISO/IEC 27001:2014, INTE/ISO/IEC 27002:2016.*

Abstract Context:

During this article the importance of regulations such as INTE / ISO / IEC 27001: 2014 and INTE / ISO / IEC 27002: 2016 in the field of computer security is explained, the PHVA process is explained, the classifications of the different dimensions of security, the sections that an ISMS requires and the process that was carried out for the implementation of these two standards during the development of the final graduation project to opt for the Bachelor's degree in Computer Security, as well as the processes, scopes and documents that They are considered basic and necessary to take that first step that every company must take in the world of information security that changes and advances more quickly every day.

Keywords: *normative, INTE/ISO/IEC 27001:2014, INTE/ISO/IEC 27002:2016.*

I. Introducción

Partiendo de los términos seguridad de la información, y es que lo podemos definir como una serie de medidas o técnicas que permiten a las empresas y personas resguardar de diferentes formar un bien o un activo de información, existen diferentes aristas que

deben ser resguardadas a la hora de hablar de seguridad de la información.

Desde la aparición de la tecnología con fines militares hasta hoy día con el uso de tecnología en casi todas nuestras tareas diarias ha pasado un tiempo con un crecimiento exponencial, un crecimiento que ciertamente ha sido para beneficio de muchos también ha crecido la ciberdelincuencia, la facilidad de acceso a los datos, las herramientas están cada día más en línea y estos cambios nos han generado la obligación de difundir la importancia de la seguridad de la información, de los activos de información, de proteger incluso nuestra identidad digital.

II. Normas Internacionales

En temas de seguridad informática la Organización Internacional de Estándar ISO por sus siglas en inglés, en conjunto con la Comisión Electromecánica Internacional formularon una extensa familia denominada ISO/IEC 27000, esta familia está compuesta por una serie de diferentes normas que ayudan a la aplicación de buenas practicas en materia de seguridad de la información en su sitio web la ISO nos indica que

> ISO / IEC 27001 es ampliamente conocido y proporciona requisitos para un sistema de gestión de seguridad de la información (SGSI), aunque hay más de una docena de normas en la familia ISO / IEC 27000. Su uso permite a las organizaciones de cualquier tipo gestionar la seguridad de activos como información financiera, propiedad intelectual, datos de empleados o información confiada por terceros. (Organización Internacional de Estandar, 2021, pár 1).

En contemplación con lo anterior se puede observar que es casi indispensable que toda empresa cuente con un sistema gestor de seguridad de la información (SGSI) con el fin claro de salvaguardar la seguridad de los activos de información propios o de terceros que se encuentren bajo su custodia.

Para que las organizaciones logren de manera efectiva una seguridad de la información, se debe iniciar por crear una cultura de seguridad entre sus colaboradores, proporcionar un marco de trabajo que permita asegurar un norte en la seguridad para todos los colaboradores y socios comerciales.

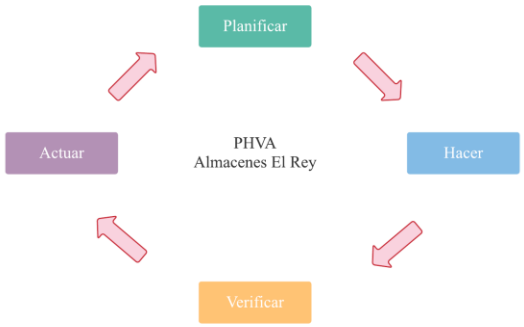
III. Modelo PHVA

Con el objetivo de contar con un marco de trabajo en la seguridad de la información, se le recomienda a la empresa el diseño de un Sistema Gestor de Seguridad de la Información (SGSI), y para esto lo primero que se debe realizar es la identificación de los activos de información.

Para esto se diseño una ficha de registro de activos y una base de datos para mantener de forma centralizada la lista de todos los activos, una vez realizada esa etapa de procedió con la definición de la metodología de trabajo, la cual se tomó como referencia el Ciclo de Deming el cual basa su filosofía en un sistema de mejora continua, también llamada ciclo PHVA (Planificar, Hacer, Verificar, Actuar) así lo menciona en el sitio web especializado en metodologías ISO de la Escuela Europea de Excelencia donde dice que “La metodología PDCA tiene un carácter cíclico, que garantiza la atención continua sobre la mejora de la calidad. Después de la evaluación y aplicación de acciones correctivas, el proceso se reinicia” (Escuela Europea de Excelencia, s.f., pár. 7). Por medio de este ciclo hemos determinado realizar el proceso de mejora continua para el manejo de los activos.

Ilustración 1

Modelo PHVA



Cuando se habla de un sistema gestor de seguridad de la información se debe entender que es parte fundamental la mejora continua el mpdelo PHVA está compuesto por:

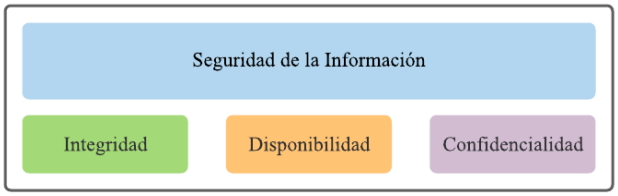
- Planificar: En esta etapa se define el contexto de la organización, se crean las políticas de seguridad, se define la metodología de analisis de riesgo que se va a utilizar, se seleccionan controles y la declaración de aplicabilidad.
- Hacer: En esta segunda face del ciclo se debe implementar el sistema de gestión de la seguridad, se debe hacer la implementación del plan de tratamiento de los riesgos, así como se debe llevar a cabo la implementación de los controles previamente definidos.
- Verificar: Esta estapa nos van a ser de gran ayuda las auditorías internas, se debe monitorear las actividades y hacer revisiones de que los controles y politicas se estén aplicando de manera correcta.
- Actuar: para esta etapa del ciclo, se deben revisar los resultados de las auditorías, tomar acciones correctivas, acciones de mejora, y nos da el banderazo de partida para el reinicio del ciclo.

IV. Dimensiones de Seguridad

Para la realización de la propuesta de un Sistema Gestor de Seguridad de la Información en el departamento de TI de Almacenes El Rey se tomaron como referencia tres pilares de la seguridad expuestos el Instituto Nacional de Ciberseguridad INCIBE, integridad, disponibilidad y confidencialidad, dimensiones sobre las que se aplicaran las salvaguardas.

Ilustración 2

Dimensiones de seguridad



- Integridad: Se refiera a que la información sea correcta, que no haya sido manipulada, cambiada o alterada de forma indebida o por personal no autorizado.
- Disponibilidad: Hace referencia a que la información se encuentre accesible en el momento que se requiera.
- Confidencialidad: Consiste en que la información no sea accedida, leída, o conocida por las personas o autoridades con permisos para esto.

V. Sistema Gestor de Seguridad de la Información

Se dice que un Sistema Gestor de Seguridad de la Información (SGSI) es un conjunto de guías, procedimientos y protocolos orientados a el fortalecimiento de los pilares de seguridad,

integridad, disponibilidad y confidencialidad. El SGSI es la joya de la corona de la norma ISO/IEC 27001, y está compuesta por una serie de documentos ente los que se pueden listar:

- Alcance del SGSI referenciado en el apartado 4.3 de la norma.
- Políticas y objetivos de seguridad de la información, apartados 5.2 y 6.2.
- Metodología de evaluación y tratamiento de los riesgos, apartado 6.1.2.
- Declaración de aplicabilidad, apartado 6.1.3 d.
- Plan de tratamiento del riesgo, apartado 6.1.3 e y 6.2

A lo largo de toda la norma se van estipulando una serie de requisitos para conformar el sistema gestor, entre los que se pueden encontrar documentos obligatorios y documentos recomendados.

VI. Propuesta realizada

A lo largo del proyecto se realizó un levantamiento de activos de información por medio de una ficha, luego se procedió a realizar la clasificación de los activos por categorías, se realizó una codificación de todos y cada uno de los activos.

Ya con los activos identificados y clasificados se procedió a realizar la valoración de los activos según los tres pilares de seguridad, se valoró de la siguiente manera:

- Confidencialidad

  Público: Toda persona dentro y fuera de la organización puede acceder a la información.

  Intermedio: Es accesible a cualquier miembro de la organización, pero no externos.

  Restringido: Accesible para las gerencias, coordinaciones y personal especificado.

  Confidencial: Acceso restringido solo a alta gerencia y propietarios de la información.

- Integridad

  No clasificada: Activos de información a la espera de ser clasificados.

  Baja: Activos cuya perdida de completitud o exactitud pueden generar un impacto tolerable para la organización.

  Media: Activos cuya perdida de completitud o exactitud pueden generar un impacto negativo, de carácter legal o económico tolerable para la organización.

  Alta: Activos cuya pérdida de completitud o exactitud pueden generar un impacto negativo, de carácter legal, económico, o de imagen no tolerable para la organización.

- Disponibilidad

  No clasificada: Activos de información a la espera de ser clasificados.

  Baja: La no disponibilidad del activo puede afectar la operación normal de la organización, pero no genera pérdidas legales, económicas o de imagen ante externos.

  Media: La no disponibilidad del activo puede conllevar a perdidas de tipo económico, legal, o incluso de imagen aceptables para la organización.

  Alta: La no disponibilidad del activo puede conllevar a perdidas de tipo económico, legal, o incluso de imagen no tolerables para la organización.

Ya con los activos valorados, se procedió a realizar un análisis de amenazas y vulnerabilidades, a determinar si en la actualidad existe implementado algún tipo de control, todo esto para poder proceder a la determinación de los activos, basados en la norma INTE/ISO/IEC 27002:2016 se procedió a definir controles a cada una de las amenazas con la clara intención de minimizar el riesgo.

Como lo mencionamos anteriormente en el modelo PHVA, en la etapa de planificación es fundamental la identificación de los activos, el establecimiento de controles y la creación de políticas de seguridad, ya en este punto se cumple con las dos primeras partes, se cuenta con el inventario de activos y los controles seleccionados, seguido a formular el SGSI (Sistema Gestor de Seguridad de la Información).

Para el postulado del SGSI en Almacenes El Rey se partió por la redacción del alcance del SGSI, para la política general de seguridad se tomó solo las partes requeridas, los objetivos, el alcance, el compromiso de cumplimiento y el compromiso de mejora continua. Seguido se estipuló la metodología para la evaluación y tratamiento del riesgo, la cual se basó en un método cualitativo apoyado por el marco de trabajo de Magerit y se realizó de la siguiente manera:

- Determinar los activos que son relevantes para la organización.
- Determinar el modelo valor de los activos.
- Determinar las amenazas a las que se encuentran expuestos los activos.
- Determinar que salvaguardas existen y que tan eficientes son frente al riesgo.
- Estimar el impacto.
- Estimar el riesgo (impacto por ocurrencia).

Se realizó la declaración de aplicabilidad, la cual consiste en una tabla donde se enumeran los activos, las amenazas, los riesgos, los controles y las personas que van a estar a cargo de la implementación de cada control sugeridos y tomados de el INTE/ISO/IEC 27002:2016. Posterior a la declaración de aplicabilidad fue necesario realizar la definición de funciones y responsabilidades de seguridad, este documento consta de dos secciones primordiales, la lista de controles que se van a aplicar y los roles que juega cada uno de los miembros del equipo respecto a cada control.

Como requisito del SGSI también se tiene el inventario de los activos el cual debe mantenerse adjunto y actualizado, seguido se redactó la política de uso aceptable de los equipos, esta es una de las políticas más importantes, esta política debe ser revisada y firmada por todos los colaboradores a la hora de ser contratados, ya que la seguridad de la información es un trabajo en equipo y todos debemos ser parte, junto a esta política se debió redactar la política de control de acceso partiendo del principio básico de que el acceso a cualquier sistema, información, u oficina a la cual no se le fuere concebido un acceso entonces estaba por defecto prohibido.

Para los SGSI se requiere una serie de documentos adicionales los cuales no fueron contemplados en el alcance de la propuesta ya que como objetivo de tiene abarcar la etapa de planificación, posteriormente las gerencias deberán dar el aval para proceder con el resto de las etapas las cuales consisten en aplicar, monitorear y mejorar los protocolos, procedimientos y políticas para una seguridad eficiente.

VII. Recomendaciones

Para lograr mantener un Sistema Gestor de Seguridad de la Información de calidad es necesario mantener el ciclo de mejora continua, para las políticas, procedimientos, documentación y muy importante la cultura de seguridad entre los colaboradores de la empresa y socios comerciales, para el presente trabajo se recomienda lo siguiente:

- Se implementen protocolos para la gestión de los activos de información.
- Se mantengan actualizados los activos con sus respectivas amenazas para así poder gestionar los riesgos de manera oportuna.
- Se promueva a lo interno de la empresa la importancia de la seguridad de la información, incluso cuando se utilicen equipos propiedad del colaborador para las funciones propias de su relación contractual.
- Capacitar al personal en uso de metodologías internacionales, normas y controles.
- Ampliar el alcance de la gestión de seguridad de la información a todos los activos de la empresa.
- Se establezca una política general de seguridad de la información.
- Establecer políticas de uso aceptable de los activos.
- Establecer procedimientos para gestión de incidentes.
- Implementar procedimientos para la continuidad del negocio.
- Implementar programas de auditoría interna.

VIII. Conclusión

Las normas, estándares son de vital importancia para el éxito de las empresas, en cuanto a la seguridad de la información la familia de normas INTE/ISO/IEC 27000 continua siendo desarrollada con el fin de facilitar marcos de trabajo en temas de seguridad de la información, este tipo de normas pueden ser aplicadas con la intención de dar claridad a las empresas sobre responsabilidades, procedimientos y hasta en donde enfocar mayor esfuerzo para salvaguardar la seguridad de los activos de información.

Como ya lo decíamos cuando se trata de seguridad de la información es un tema que compete a todos los colaboradores de la empresa, y es con el esfuerzo de cada uno de ellos que puede hacerse efectivo un SGSI, es necesario que los usuarios incorporen buenas prácticas para prevenir la materialización de los riesgos y no ser parte del grupo de victimas de los ataque informáticos que cada día se tornan más frecuentes, más complejos, y cada día se encuentran cambiando, colocando en el foco de los ciberdelincuentes las empresas pequeñas que se les suele complicar la implementación de sistemas de seguridad por costos, complejos o difíciles de mantener con el personal que cuentan.

IX. REFERENCIAS

Escuela Europea de Excelencia. (s.f.). Obtenido de https://www.escuelaeuropeaexcelencia.com/2020/07/en-que-consiste-el-ciclo-pdca-para-la-mejora-continua/

Organización Internacional de Estandar. (2021). *ISO*. Obtenido de https://www.iso.org/isoiec-27001-information-security.html