Propuesta de implantación del «Cyber Security Framework (CSF)» del NIST, usando COBIT, en Honda del Perú

Tesis presentada en satisfacción parcial de los requerimientos para obtener el grado de Magíster en Dirección de Tecnologías de Información por:

Aguilar Araujo, Carlos Eduardo
Lau Alayo, Eduardo Roberto
Olivera Kalinowski, Sandro
Polanco Ramos, Cristian Arthur

Programa Maestría en Dirección de Tecnologías de Información a tiempo parcial 15-1

Lima, 10 de julio de 2017

RESUMEN EJECUTIVO

Maestría en:	Maestría en Dirección de Tecnologías de la Información
Título de la tesis:	*Propuesta de implantación del «Cyber Security Framework (CSF)» del NIST, usando COBIT, en Honda del Perú*
Autor(es):	Aguilar Araujo, Carlos Eduardo Lau Alayo, Eduardo Roberto Olivera Kalinowski, Sandro Polanco Ramos, Cristian Arthur

RESUMEN:

Hoy en día existe una clara tendencia por parte de las organizaciones por lograr un nivel de eficiencia operacional que les permita concretar sus objetivos estratégicos y competir exitosamente en sus respectivas industrias. Conseguir en la actualidad, este nivel de desempeño sin el uso de las Tecnologías de la Información y de la Comunicación —en adelante, TIC— es utópico, dado que las TIC permiten, precisamente, la obtención de mayores niveles de eficiencia y de procesos generadores de valor en la transición de las actividades desde el plano físico hacia el plano digital.

Si bien esta transición es la que permite obtener estos nuevos niveles de eficiencia, los procesos e información que están expuestos a riesgos de seguridad física, una vez trasladados al plano digital, se exponen ahora a riesgos de las TIC.

Es en este punto donde se identifica a la ciberseguridad como la disciplina que permite mitigar y eliminar los nuevos riesgos que implican el uso de las TIC.

Bajo la premisa de analizar la ciberseguridad como un tema de alta relevancia para los procesos de transformación digital que están ocurriendo en los diferentes tipos de organizaciones, la presente tesis busca EVALUAR LOS RESULTADOS DE APLICAR LA GESTIÓN DE LA CIBERSEGURIDAD A UNA EMPRESA PERUANA, PARA LO CUAL SE HA ELEGIDO A HONDA DEL PERÚ— HDP— como objeto de estudio, y al *Cyber Security Framework* (CSF) del *National Institute of Standards and Technology* (NIST), usando COBIT 5, como el marco de referencia a ser aplicado.

Por lo tanto, en el presente trabajo se plantean los siguientes objetivos específicos:

—DETERMINAR los tres componentes principales de la problemática identificada al implantar un framework de ciberseguridad en una empresa peruana.

—SUGERIR estrategias de solución a los tres principales problemas identificados al implantar un framework de ciberseguridad en una empresa peruana.

—PROPONER un plan de acción para la gestión de la ciberseguridad en HDP.

La realización de esta investigación se ha visto motivada por el hecho de que las ciberamenazas no son ajenas al Perú a pesar de la poca difusión existente en los medios de comunicación.

El crecimiento económico que ha experimentado el país y las inversiones de multinacionales extranjeras, atraen la atención de ciberdelincuentes. Precisamente, por esa razón, se ha elegido a Honda del Perú como empresa objeto del estudio, dada su condición de ser una empresa nacional que forma parte de una organización global y que, debido al nivel de vanguardia tecnológica que representa como fabricante mundial de automóviles y motocicletas, requiere que la gestión local comience a considerar a la ciberseguridad como un elemento estratégico dentro de su operación.

En cuanto al marco de trabajo, se determina utilizar el CSF del NIST, debido a su capacidad de ser aplicado a cualquier tipo de organización, independientemente de su tamaño o nivel de madurez, lo cual se comprueba como parte de la ejecución de esta tesis.

El CSF está compuesto por tres elementos: *Core, Tiers y Profiles*.

El *Core* está conformado por las cinco funciones del ciclo de vida de la gestión de los riesgos de la ciberseguridad de una organización: IDENTIFICAR, PROTEGER, DETECTAR, RESPONDER Y RECUPERAR, donde cada una se compone, a su vez de actividades, resultados y controles.

El segundo componente denominado *Tiers,* asiste en conducir la evaluación y planeamiento de las actividades de la ciberseguridad, y contiene los atributos a considerar para la creación de los PERFILES ACTUAL y OBJETIVO.

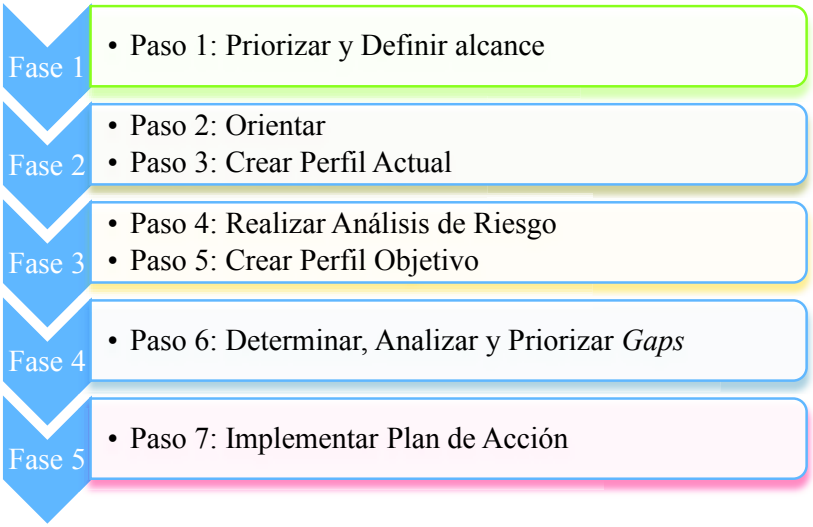
El tercer componente o *Profiles* son dos: ACTUAL y OBJETIVO, los que representan los resultados basados en las necesidades del negocio, que identifican las oportunidades de mejora en la postura de la ciberseguridad de una organización.

El CSF ofrece la posibilidad, además, de utilizar los controles propuestos por diferentes marcos de trabajo para la gestión de TI y de la seguridad de la información como COBIT 5, ISO 27001, ISA 62443-2-1:2009, entre otros.

Para la presente tesis, se determina utilizar el *framework* de COBIT 5, debido a que los valores del enfoque basado en riesgos para permitir la obtención de resultados

rápidos que utiliza el CSF, son muy cercanos a los principios de gestión y gobierno embebidos dentro del framework de COBIT 5. Adicionalmente, la disponibilidad de recursos definidos en COBIT 5, como el uso de los Catalizadores y los Escenarios de riesgos, permiten un mejor entendimiento respecto de cómo llevar a cabo la implementación del CSF, al ofrecer un enfoque bastante práctico respecto a los resultados a obtener y cómo deben ser medidos.

La metodología del CSF, basado en COBIT 5, que se utiliza en la presente tesis está compuesta por siete pasos, los cuales se muestran a continuación:



En la presente investigación, aplicar el CSF a HDP involucró un desarrollo exhaustivo de los componentes principales de cada fase, para lo cual se hizo uso de los recursos y las herramientas de COBIT 5, utilizándose sus prácticas e instrumentos de gobierno y gestión más relevantes. También fue necesario crear herramientas particulares de análisis en la gestión de los riesgos, para adaptar la realidad y contexto actual de HDP, dentro de la metodología de trabajo de aplicación del CSF bajo COBIT 5.

Como resultado final, el desarrollo del paso 7 en la Fase 5, propone los tres proyectos de ciberseguridad más relevantes, de acuerdo a la urgencia en la operación y a los beneficios estratégicos que ofrecen a HDP, a fin de que la organización apruebe la idoneidad de su ejecución, en base a los argumentos suministrados.

Como resultado de la evaluación realizada es posible concluir lo siguiente:

—Los componentes principales de la problemática identificada en el proceso de implantación de un framework de ciberseguridad son:

- La cultura organizacional, por la fuerte resistencia al cambio que produce la formalización de los procesos de gestión de la ciberseguridad y por la aún presente actitud reactiva de la Alta Dirección frente a posibles incidentes de ciberseguridad.
- A nivel estratégico, se percibe a la ciberseguridad como un gasto más de TI, debido a la dificultad en traducir las inversiones en ciberseguridad hacia ahorros o beneficios económicos tangibles.
- A nivel de recursos, el personal de TI adolece de los conocimientos técnicos y de gestión necesarios, que les permitan hacer más entendibles para el negocio los riesgos empresariales que implican las ciberamenazas.

—Respecto al CSF es posible concluir que es un *framework* de ciberseguridad que puede ser aplicado en empresas del rubro comercial como HDP, independientemente de su tamaño, madurez o sofisticación en conocimientos de ciberseguridad. Se debe tener presente que la aplicación exitosa del CSF debe incluir:

- La adaptabilidad del CSF mediante un análisis holístico de la organización que incluya sus objetivos estratégicos y su actual gestión de riesgos. Un segundo paso para la adaptación del framework, es la elección de los *Tiers* de implementación correctos, que representen la postura actual y objetiva de la organización respecto a la ciberseguridad.
- La utilización de *frameworks* complementarios que estructuren mejor los controles a ejecutar. En el caso particular de COBIT 5, el uso de herramientas como la *Cascada de metas, los Criterios de evaluación PAM*, y los *Escenarios de riesgo*, permiten reducir el nivel de complejidad en la aplicación del CSF.
- La complementación del uso de COBIT 5 con el desarrollo de herramientas de análisis y diagnóstico particulares. El desarrollo de la presente tesis incluye la preparación de una herramienta propia de calificación de los riesgos basada en los escenarios de riesgos de ciberseguridad de COBIT 5.
- Las organizaciones que deseen implementar el CSF de forma más extensiva deben hacer uso de otros estándares y referencias como el

ISO/IEC 27001:2013 o el *CIS Critical Security Controls for Effective Cyber Defense*.

—La correcta aplicación de un marco de gestión de la ciberseguridad es mucho más asequible de realizar en organizaciones que cuentan con procesos de gestión de riesgos maduros (aunque no sean necesariamente de ciberseguridad), pues ello permite la reutilización de su actual estructura organizacional y de toma de decisiones para ese fin. En este trabajo, la disponibilidad del ERM de HDP agiliza la puesta en marcha del CSF (Paso 1), a la vez que sirve como insumo para la realización de la Evaluación de Riesgos de TI.

A partir de la experiencia adquirida en este ejercicio de implantación, es posible recomendar las siguientes acciones:

—PROMOVER el cambio de actitud de las organizaciones frente a la ciberseguridad exponiendo los riesgos de ciberseguridad de la organización en términos más comprensibles para el negocio.

—EMPLEAR herramientas proporcionadas por otros marcos de referencia como COBIT 5, facilita el proceso de implementación y la obtención de resultados que permitan una asociación más concreta entre los riesgos de negocio y los riesgos de las TIC, y que se cuente con mejores argumentos para articular el valor de la ciberseguridad hacia la Alta Dirección.

—CONCEBIR las soluciones de ciberseguridad considerando no solo los aspectos técnicos, sino también de estructura y cultura organizacional, trabajándose en la sensibilización de todo el personal bajo el acompañamiento y liderazgo de la Alta dirección.

—ACOMPAÑAR la presentación de los Proyectos de Ciberseguridad con los respectivos casos de negocio que incluyan el análisis monetario del riesgo derivado de la no acción.

Resumen elaborado por los autores.