SEGURIDAD EN LA INFORMACIÓN APLICADA EN PROYECTO DE MIGRACIÓN TECNOLÓGICA

Buitrago Delgado, Liliana Astrid
labd312@gmail.com
Universidad Piloto de Colombia

Abstract— The implementation of any project involving technology in the organization, is so important to achieving strategic objectives that can´t be put aside the information security, so in this article will discuss the integration of each one of the phases of technology migration project of an organization best practices to ensure information security.

Resumen—La implementación de cualquier proyecto que involucre tecnología en la organización es tan importante para el logro de objetivos estratégicos, que no se puede dejar a un lado la seguridad en la información. Por lo tanto, en este artículo se va a hablar de la integración de cada una de las fases del proyecto de migración tecnológica de una organización y las mejores prácticas para garantizar la seguridad en la información.

Índice de Términos— Proyecto, Riesgos, Seguridad en la Información.

I. INTRODUCCIÓN

La gestión de proyectos en la organización es de vital importancia puesto que de esta labor se puede mantener a cualquier organización a la delantera de sus competidores. Con una adecuada gestión de recursos y una correcta planificación de objetivos se pueden alcanzar metas que generen una mejor productividad; en la mayoría de los casos, los proyectos dentro de la organización se encaminan a la optimización de procesos o creación de productos innovadores que de algún modo maximicen los beneficios de la empresa, por lo que es muy importante velar por la seguridad en la información de cada uno de los proyectos que se emprendan en las organizaciones.

Teniendo en cuenta que los proyectos son de vital importancia para la organización, es necesario establecer durante la planeación, ejecución e implementación de los proyectos, las medidas necesarias para mantener la seguridad en la información con el objetivo principal de garantizar la calidad del proyecto y minimizar el riesgo de pérdidas por implementación de proyectos que no cumplen con las expectativas de los usuarios finales porque no cumplen con características mínimas de seguridad para resguardar la confidencialidad, integridad y disponibilidad de la información de la organización.

Para el contexto de este artículo, se hablará sobre la ejecución del proyecto de migración o actualización tecnológica de toda la infraestructura de una organización privada.

II. FASES DE UN PROYECTO

En la actualidad se tienen diversas metodologías para gestión, los proyectos PMI, ITIL, COBIT entre otros, en los cuales siempre coincide que para el éxito de dichos proyectos se deben mantener las siguientes fases:

- Inicio.
- Planificación.
- Ejecución.
- Implementación o Cierre de Proyecto.

A. INICIO

En esta fase, es donde se concibe la idea de implementar un proyecto. Según PMI, se debe realizar un acta de constitución del proyecto donde se define el alcance del mismo y, de igual forma, se nombra el gerente del proyecto quien es el responsable de la planeación, ejecución y cierre del mismo.

Por otra parte, se debe evaluar si el proyecto se

alinea con los objetivos estratégicos de la organización, y validar la competencia del personal líder asignado para la gerencia del proyecto, lo anterior teniendo en cuenta que el líder es la persona responsable de la consecución de los hitos del proyecto.

En este proyecto la migración tecnológica es necesaria para cumplir con la estrategia tecnológica de la organización, lo anterior para mantener la adecuada infraestructura que soporte las aplicaciones misionales.

La migración tecnológica se concibe como necesidad de mantener actualizada la plataforma tecnológica, que soporta la misión crítica de la organización y provee una infraestructura tecnológica de servicios seguros, estables, confiables y eficientes, para apoyar el desarrollo del objeto social organización.

Adicionalmente, uno de los objetivos de la estrategia del departamento de tecnología, es modernizar la plataforma tecnológica; de manera que se ajuste a los retos de la organización, en la consolidación de nuevos productos, aumentando su capacidad instalada de operación y aumentando la eficiencia de los procesos.

La organización realizó la tarea de identificar los riesgos asociados a la planeación, ejecución e implementación del proyecto, para esta actividad se tiene como guía la ISO 31000 que proporciona una lista por orden de preferencia en la forma de abordar el riesgo[1]:

1) Evitar el riesgo al decidir no iniciar o continuar con la actividad que da lugar al riesgo.

2) Tomar o aumentar el riesgo con el fin de perseguir una oportunidad.

3) Extracción de la fuente de riesgo.

4) El cambio de la probabilidad.

5) Modificación de las consecuencias.

6) Compartiendo el riesgo con la otra parte o partes (incluidos los contratos y financiación de riesgos).

7) Mantener el riesgo por decisión informada.

La organización se enfrenta al riesgo de falla del hardware de los servidores, puesto que ya cumplieron el tiempo estimado de vida útil y se pueden presentar problemas de incompatibilidad del hardware con las nuevas versiones de software disponibles en el mercado. Adicionalmente, las versiones de software actualmente instaladas ya no cuentan con soporte por parte del fabricante; por lo tanto, si se tuviese algún inconveniente no se encuentran actualizaciones disponibles. Por lo anterior la Junta Directiva de la organización tomó la decisión de apoyar la ejecución del proyecto.

Por otra parte, teniendo en cuenta los riesgos asociados a la ejecución del proyecto, se estimaron los siguientes:

- No aprobación de todo el presupuesto necesario para la ejecución del mismo por parte de la junta.
- Falta de conocimiento de la nueva infraestructura por parte del equipo de trabajo.

Para los riesgos mencionados anteriormente, la gerencia del proyecto tomó la decisión de implementar las siguientes actividades para mitigarlos:

- Solicitud de recursos económicos a la Junta Directiva de la organización, teniendo en cuenta los riesgos asociados a la no implementación del proyecto.
- Capacitación del usuario responsable en la instalación y configuración de los nuevos ambientes SQL Server 2014, IIS 8.0, Windows Server 2012.
- Capacitación en Seguridad de la Información.
- Contratación de servicios profesionales de

personal experto para la migración de la infraestructura de almacenamiento, SAN.

B. PLANEACIÓN

En esta fase se realiza el desglose de cada una de las actividades que se deben ejecutar para el logro de los hitos del proyecto. Luego de esto, se deben planear los tiempos adecuados para cada una de las actividades, lo cual constituye el insumo inicial para la creación del cronograma del proyecto.

En cuanto a la Seguridad de la Información, se deben establecer los roles y responsabilidades asociados al equipo de trabajo que van a ejecutar el proyecto. Es importante tener claro qué recurso humano interno será parte integral del proyecto y establecer si se cuentan con acuerdos de confidencialidad con los empleados, y si se tiene conciencia acerca de las políticas establecidas para la prevención de fugas de información y conocimiento de la importancia de la misma; éste es un punto a tener en cuenta como lo estipula la Norma ISO 27001, en los controles de seguridad en recurso humano.

Para este proyecto los miembros del equipo de tecnología fueron designados como los responsables para la ejecución del proyecto, y se verifica que con todo el equipo se tienen suscritos contratos de confidencialidad.

Se debe realizar el plan de calidad el cual debe contener los lineamientos mínimos de calidad que deben tener los objetos o los hitos claves del mismo, para garantizar el éxito al finalizar. Los siguientes son los hitos claves de la migración tecnológica:

- Adquisición de hardware y software requerido para continuar con los servicios de misión crítica.
- Instalación y configuración de los nuevos ambientes.
- Migración de las aplicaciones misión crítica de ASP.NET 2.0 a 4.0.
- Pruebas de seguridad de los nuevos ambientes.
- Pruebas funcionales de los aplicativos en la nueva infraestructura.
- Configuración de los ambientes de replicación.
- Compra de hardware y software para potenciar ambientes virtualizados.

Como parte primordial de este proyecto es la compra de la nueva infraestructura se debe realizar la evaluación del presupuesto y por lo tanto se debe realizar el plan de compras que incluye lo siguiente:

- Compra de licenciamiento: Microsoft y VMWare.
- Compra de hardware: servidores HP Proliant Gen 9.
- Contratación de consultoría especializada.
- Capacitación del equipo de trabajo.

En este punto de las compras es importante establecer los acuerdos de niveles de servicio con el objeto de cumplir con los estándares de calidad sobre los productos o servicios contratados. Lo anterior, aplicando los controles de la norma ISO 27001:2013, con lo estipulado en el apartado de la relación con los proveedores.

En la mayoría de los casos los proyectos de tecnología incluyen manipulación y/o transformación de información que forma parte de la misión de la organización. Cuando se requiere entregar información o recursos tecnológicos de la organización a proveedores o consultores, se deben establecer acuerdos de confidencialidad que velen por esta misma y por la integridad de la información que se manipule durante la ejecución del contrato y hasta después del cierre del proyecto, siguiendo con la aplicación de los controles establecidos en la norma.

Como este proyecto es de actualización tecnológica se requiere la compra de software y hardware, y se debe velar por adquirir dichos productos con la garantía de los fabricantes y así evitar pérdidas por compras de equipos obsoletos que no cumplan con las últimas actualizaciones que garanticen el cumplimiento de los objetivos del proyecto.

La finalidad de la seguridad en la información, en los proyectos, es garantizar que cuando el producto o servicio se entregue a los usuarios finales, cuente con el nivel de seguridad apropiado que le permita asegurar los principios fundamentales de la seguridad en la Información:

- *Confidencialidad*: Hace referencia a que la información se tratará de forma adecuada, es decir, si la información debe ser clasificada como privada se debe velar por no publicar dicha información. Por lo anterior, se debe realizar la validación y clasificación de la información para declarar si la información es pública, confidencial o de reserva de la compañía. Esta labor se debe realizar por el gerente del proyecto según los lineamientos establecidos por el área de seguridad.

- *Integridad*: Hace referencia a que la información permanezca completa e inalterada desde su creación y origen.

- *Disponibilidad*: hace referencia a que el producto o servicio debe ser accesible por todos los usuarios finales en cualquier momento que lo requiera para su uso.

Al realizar el diseño de la infraestructura que cumpla con los principios descritos anteriormente, para este hito se debe tener en cuenta lo siguiente:

- Control de acceso.
- Seguridad en redes y comunicaciones.
- Segmentación de las redes con el fin de administrar de manera organizada el tráfico de red.
- Aseguramiento de los objetos que componen la infraestructura tecnológica.
- Asegurar el menor privilegio, mantener únicamente activos los servicios o puertos necesarios para la misión de cada objeto.
- Mantener la continuidad de los servicios del negocio.
- Mantener el principio de la defensa en profundidad.
- Minimizar las brechas de seguridad.

Para este proyecto se trabajó con el equipo de tecnología el cronograma de actividades en conjunto y se estableció el plan de trabajo, en el cual se dividió en 3 fases la actualización total de la plataforma.

- Fase 1, actualización de la infraestructura misional.
- Fase 2, actualización de la infraestructura virtualizada.
- Fase 3, Contratación de servicios Cloud.

C. EJECUCIÓN, SEGUIMIENTO Y CONTROL

Siguiendo con la dinámica de este artículo, que es resaltar los puntos clave de la implementación de seguridad en la información en cada una de las fases del proyecto, en la fase de ejecución es importante ejecutar las actividades de compra de hardware y software, para ello es muy importante el trabajo en conjunto del área jurídica y el área tecnológica de la organización, con el objetivo de realizar las compras necesarias que cumplan con las expectativas de la organización.

Se debe garantizar que los contratos suscritos con los proveedores incluyan pólizas de cumplimiento, garantías de servicio y adicionalmente, si se puede obtener, servicio post-venta en el caso del hardware.

Para la contratación de servicios profesionales de consultoría, se deben identificar los niveles de servicio para mantener el nivel apropiado de seguridad de la información y la entrega de los servicios contratados en línea con los acuerdos de entrega de servicios de terceros.

La organización debe verificar que se implementen adecuadamente los acuerdos, y realizar seguimiento y control para validar su correcto cumplimiento, teniendo en cuenta las normas vigentes, para asegurar que los servicios sean entregados correctamente y de esta forma satisfacer todos los requerimientos acordados con terceras personas.

Teniendo en cuenta lo anterior, la organización

realiza la firma de acuerdos de confidencialidad y acuerdo de buen uso de los recursos tecnológicos para iniciar el proceso de contratación.

Como parte fundamental de este proyecto se estableció que se debe contar con el personal capacitado en la nueva infraestructura contratada, por lo anterior, se ejecutaron planes de capacitación a los responsables de cada proceso; adicionalmente, se solicitó capacitación en seguridad de la información, puesto que es necesario que el equipo de trabajo se encuentre consciente de la necesidad de implementar las mejores prácticas en cuanto a los controles de seguridad que se establecerán durante la ejecución del proyecto. Por lo anterior se realizaron sesiones de capacitación abarcando los siguientes aspectos:

- Introducción a la Seguridad de la Información.
- Importancia del cumplimiento en las políticas de Seguridad de la Información.
- Uso responsable de los recursos tecnológicos.
- Seguridad de la Información y Legislación.
- Ingeniería Social y Robo de identidad.
- Seguridad en Dispositivos Móviles. Uso de conexiones inalámbricas.
- Generalidad de marcos de referencia en torno a la Gestión de la Seguridad de la Información aplicable a las organizaciones.
- Casos reales de Colombia y el mundo asociados a incidentes de seguridad.

Para el diseño de una infraestructura tecnológica que cumpla con los lineamientos mínimos de seguridad, se establece realizar o analizar las vulnerabilidades sobre los objetos que lo componen,

- Servidores.
- Firewall.
- Sistema Operativo.
- Canales de Comunicación.

Por lo anterior y teniendo en cuenta los resultados iniciales de los análisis de vulnerabilidades, para la fase 1 del proyecto se establecieron actividades para garantizar que la infraestructura contratada cumpla con los requerimientos de seguridad, para tal tarea se recomendó trabajar las guías de mejores prácticas de configuración que se encuentra en la página https://benchmarks.cisecurity.org/. Como la plataforma que se quiere implementar es Microsoft se tienen en cuenta las guías para:

- IIS 8.0.
- SQL SERVER 2014.
- Windows Server 2014.

Para el aseguramiento de los servidores se establece el principio del menor privilegio, por lo anterior se inician las labores necesarias teniendo en cuenta el rol de cada servidor y cerrando las brechas de seguridad, es decir, lo servicios que no hacen parte de la razón de ser de cada uno de ellos.

En cuanto al aseguramiento de los servidores de aplicaciones se establece que se debe exigir host-headers, lo anterior es importante de utilizar puesto que en producción se tienen aplicaciones publicando por IP y puerto, esta información puede ser utilizada para comprometer la disponibilidad de las aplicaciones según las guías mencionadas anteriormente, se pueden evitar ataques de DNS-Rebinding e IP-scan. Adicionalmente, al publicar las aplicaciones en varios sitios del mismo servidor se abrirán varios puertos, tantos como aplicaciones, lo cual aumentará la probabilidad de ataques e intrusiones de usuarios internos o externos.

Este elemento de seguridad, al implementarlo en la plataforma actual, permite que el usuario final no puede establecer la dirección IP del servidor así como tampoco los puertos abiertos del mismo. Adicionalmente, es más fácil de administrar puesto que solo se tiene un puerto abierto para publicación en este caso el 80 y en ocasión de alguna falla, se configura en un nuevo servidor el host-header y se configura en el FQDN y el cambio es trasparente para el usuario.

De igual forma se realiza la inhabilitación del listado de directorios, esta configuración de seguridad es básica, pero en algunas ocasiones en

las aplicaciones revisadas se permite el acceso al directorio raíz. Por lo anterior se debe documentar y establecer como política esta recomendación y ejecutar la política, puesto que los usuarios internos y externos pueden tener acceso a todo el directorio de las aplicaciones y podrían llegar a archivos de configuración que permitan alteración de la aplicación provocando fallas de disponibilidad e integridad de las aplicaciones.

Al definir esta práctica de seguridad, como lineamiento dentro de la organización para la configuración y creación de sitios, tendríamos asegurados los ambientes de producción, pruebas y replicación; evitando ataques de directorio trasversal, Shell injection, entre otros.

Otra de las políticas de configuración adoptadas es deshabilitar la depuración de las aplicaciones, puesto que en la mayoría de los casos los desarrolladores no tienen la consciencia de la seguridad y establecen parámetros para poder visualizar la depuración de las aplicaciones en los exploradores, en el caso que no se establezca la configuración adecuada y recomendada en la guía, el usuario final puede ver información detallada de las aplicaciones que puede ser utilizada para ejecutar ataques que atenten contra la integridad y disponibilidad de la aplicación.

Al configurar dentro del archivo de configuración el parámetro de compilación en estado *"false"*, se asegura en primer lugar el rendimiento de las aplicaciones puesto que este tipo de compilación se realizaría desde cada usuario conectado a la aplicación y podría presentarse indisponibilidad por capacidad de procesamiento del servidor, y mantendríamos la información detallada de la aplicación y de la plataforma a salvo de usuarios malintencionados.

Como trabajo para mantener las configuraciones de seguridad se establecen las siguientes políticas adicionales a las actuales para aprobación de la dirección:

Política de Actualizaciones de sistema operativo: Para el paso de servidores a ambiente productivo se deben mantener las actualizaciones no mayores a 30 días de la fecha paso a producción, lo anterior con el objeto de garantizar la estabilidad del sistema operativo y de los programas propios del servidor.

Política de Configuración Firewall de Windows: Se debe mantener el firewall en estado *ON* para todos los servidores y de esta forma asegurar que los servicios configurados en cada servidor sean los necesarios.

Se deben configurar las reglas de entrada que están por defecto de la siguiente forma en cuanto a la gestión de Servicios, teniendo en cuenta que Se realizará aseguramiento sobre los servicios que deben quedar habilitados por el objeto del servidor y para facilitar al administrador la función diaria.

- IPv6: Se deben bloquear todas las conexiones IPv6, lo anterior teniendo en cuenta que la red de la organización no está configurada en este protocolo. Dado el caso que la organización implemente las redes con el protocolo IPv6, se realizará la activación en las reglas de entrada.

- Echo Request (ICMP): Permite realizar ping sobre el servidor, sobre este protocolo se debe gestionar que únicamente los administradores puedan realizar esta acción.

  Se establece que se deben bloquear los accesos públicos a este servicio y solamente se permiten las peticiones de los equipos de los administradores.

- Remote Desktop (RPC – Puerto 389): Se debe permitir conexión únicamente por protocolo TCP, sobre el dominio y gestionar sobre los equipos de los administradores del servidor, es decir, permitir únicamente el acceso por este protocolo a los equipos permitidos.

- SNMP Trap Service (UDP In): Se debe permitir conexión únicamente por protocolo UDP, sobre el dominio y gestionar sobre los

equipos encargados del monitoreo del servidor.

- World Wide Web Services (HTTP Traffic-In - 80): Este servicio se deja habilitado únicamente por el puerto 80 para los servidores con rol de Aplicaciones.

  Para los servidores de bases de datos, dominio, monitoreo y de aplicaciones que no requieren publicación el servicio se bloqueará para evitar intentos de ingreso al servidor por métodos no permitidos.

- World Wide Web Services (HTTPS Traffic-In- 443): Este servicio se deja habilitado únicamente en el puerto 443 para los servidores con rol de Aplicaciones y que sean implementados con certificados de seguridad.

  Para los servidores de bases de datos, aplicaciones, de dominio y de monitoreo que no requieren publicación, el servicio se bloquea para evitar intentos de ingreso al servidor por métodos no permitidos.

Los demás servicios que no se mencionaron y que se encuentren dentro de las reglas de entrada del firewall de sistema operativo se dejarán en estado bloqueado, puesto que no son necesarios para el correcto funcionamiento de las aplicaciones en la plataforma tecnológica.

Política de asignación de rol de administrador: Se establece que dependiendo de la misión de cada servidor se configurará el acceso remoto al servidor y el rol de administrador del mismo.

- Bases de datos: se asignara únicamente el permiso al administrador o DBA designado.

- Aplicaciones: se asignara únicamente el permiso al administrador de los aplicativos.

- Administrador de Dominio: únicamente el permiso al administrador de la plataforma.

Como la organización debe disponer de los servicios activos en los horarios laborales se mantendrá el acceso remoto al administrador de la plataforma o de dominio en caso que algún administrador anteriormente designado falte a la organización.

Política de nombramiento de servidores: para implementar las mejores prácticas de configuración para el nombramiento de servidores, se estableció que estos no deben ser nombrados por su misión sino por un nombre estándar como por ejemplo: ríos, mares, o departamentos.

Política de segmentación de red: Se estableció que se realiza la separación de los segmentos de red de los equipos de los usuarios internos que utilizaran el segmento 192.168.1.x y los usuarios externos que utilizaran el segmento 172.16.1.x, lo anterior para evitar problemas de tráfico de red y asegurar la correcta disponibilidad de las aplicaciones.

Para validar la consistencia de las configuraciones y políticas establecidas, se solicitó análisis de vulnerabilidades y evaluación de instalación y configuración del sistema operativo. El resultado fue que la plataforma cumple con los niveles de seguridad apropiados para su paso a producción.

Una vez se tienen los ambientes de producción migrados a una nueva plataforma, se deben iniciar las labores para el mantenimiento de los ambientes de pruebas y lo más importante, el ambiente de replicación del cual se hace referencia en el DRP y en plan de continuidad de la organización.

Por último y como complemento de la actualización de la plataforma se realizaron actividades de pruebas con los usuarios finales para asegurar que las funciones y los servicios que se prestan en la plataforma actual, se cubran de igual forma con la actualización tecnológica.

D. IMPLEMENTACIÓN

Una vez se hayan realizado las actividades de

pruebas y éstas resulten satisfactorias, se procede a realizar el plan de actualización y el paso a producción de la plataforma tecnológica.

Para esta actividad se debe garantizar que las políticas y guías de configuración realizadas durante la fase de ejecución, sean las mismas en las cuales los usuarios realizaron las pruebas.

En cuanto a la necesidad de mantener la seguridad de la información en la organización, y teniendo en cuenta que este proyecto de la migración y/o actualización de la plataforma tecnológica es uno de los pilares estratégicos, la gerencia del proyecto toma la iniciativa para realizar la documentación de las políticas anteriormente mencionadas y se solicita la aprobación del comité de calidad para que sean implementadas en adelante en las configuraciones de nuevos ambientes tanto productivos, pruebas o de replicación y de esta forma mantener ambientes seguros.

III. CONCLUSIONES

La seguridad en la información es de vital importancia para la organización, por lo que se debe integrar desde el inicio de la gestión de los proyectos para definir los requerimientos de seguridad que mitigarán los riesgos que se pueden presentar al ser implementado en un ambiente de producción.

Tanto el gerente de proyecto como los colaboradores que hacen parte de la planeación, ejecución e implementación del proyecto, deben recibir capacitación en normatividad legal vigente en seguridad de la información y acerca de las mejores prácticas para que sean sus pilares y las puedan implementar en sus labores diarias asignadas en el proyecto.

El área de seguridad de la información debe tener un rol de acompañamiento continuo sobre todos los proyectos que se realicen en la organización con el objeto principal que proporcionen lineamientos y mejores prácticas de seguridad, con el objetivo primordial de que los proyectos emprendidos no se encuentren en contravía de la misión de la organización, de igual forma, mantenerla blindada de riesgos de tipo reputacional por no cumplir con las normas vigentes.

Para el proyecto, en la actualidad, solo se ha culminado la fase 1 de migración de plataforma tecnológica y se están ejecutando las siguientes fases que culminarán en el segundo semestre del año en curso. Es importante resaltar que el éxito y culminación de la primera fase fue gracias a la implementación de los controles y políticas que se mencionaron durante el artículo de seguridad de la información.

IV. REFERENCIAS

[1] Portal de ISO2700 en Español. [Online] Disponible: http://www.iso27000.es.

[2] Center for Internet Security Guide. [Online] Disponible: https://benchmarks.cisecurity.org.