

PROPUESTA DE PLAN DE PROYECTO PARA DIMINUIR LA BRECHA DE VULNERABILIDAD TECNOLÓGICA EN LOS DISPOSITIVOS DE ALMACENAMIENTO DE LA EMPRESA X

Randall Alvarez Oporta

Hispanic Coalition S.A.

ralvarez@rsr.co.cr

Iván Espinoza Benamburg

Novacom S.A

iespinoza.cr@gmail.com

Resumen: El Departamento de TI de la Empresa X, reconoce la situación de invertir recursos en la búsqueda de una solución viable para disminuir la brecha de vulnerabilidad tecnológica de los dispositivos de almacenamiento digital. El proyecto presenta una propuesta para brindar el conocimiento y las herramientas adecuadas, que permita ampliar la capacidad del departamento al ser su primera aproximación hacia la gestión formal de proyectos. Los resultados permitieron el reconocimiento de la situación actual con la deseable a alcanzar según el marco de trabajo de COBIT®, la identificación de los requerimientos que reduzca la brecha entre ellas y la elaboración de un plan de proyecto basado en las normas internacionales de gestión de proyectos detallados en la guía del PMBOK®.

Abstract: The IT department of Company X, recognizes the situation to invest resources in the search for a viable solution to reduce the technological vulnerability gap of digital storage devices. The project presents a proposal to provide the knowledge and tools in such a way that expands the capacity of the department as their first project formal management approach. The found results allowed the recognition of the current situation together with the one to be reached according to COBIT® standards, identifying the requirements that reduce the gap among them, and elaborating a project plan based on the international guidelines of project management mentioned in the PMBOK® guide.

Palabras claves: Gestión de Proyectos, PMBOK®, Plan para la Dirección de Proyectos, Desastres Tecnológicos, Dispositivos de Almacenamiento Digital.

Introducción

Establecer el valor de la información digital es algo totalmente relativo para cada organización, pues la información constituye un recurso que, en muchos casos, no se valora adecuadamente debido a su intangibilidad, al contrario de los equipos. La información comercial es uno de los activos de mayor importancia para las organizaciones, ya que de ellos generalmente depende el desarrollo de sus operaciones y la creación de valor en su nicho de mercado, por lo que pueden llegar a representar una ventaja competitiva considerable.

Existen diversos lineamientos y mejores prácticas internacionales destinadas a incrementar la capacidad de las organizaciones para reaccionar ante desastres tecnológicos que puedan comprometer la integridad de esta información digital. Para estar conforme a estos lineamientos, es necesario que la organización realice un diagnóstico hacia lo interno y lo externo, para determinar su nivel de preparación y los factores o condiciones que afectan positiva o negativamente los medios de almacenamiento de la información digital.

El Departamento de TI de la Empresa X, ha identificado que sus dispositivos de almacenamiento digital son un factor a considerar ya que presentan vulnerabilidades críticas, que ante un eventual desastre tecnológico que los afecte, se vería comprometida la realización de sus operaciones comerciales, generando una amenaza no aceptable por la alta dirección.

A pesar de reconocer esta necesidad, el departamento, y la organización como tal, carece de la capacidad necesaria para poder realizar un análisis adecuado de los requisitos técnicos a partir de la brecha existente con las

mejores prácticas aceptadas internacionalmente. Adicionalmente, el departamento cuenta con una limitada capacidad para realizar una planeación formal que permita establecer un plan para gestionar la implementación de tales medidas.

El presente trabajo propone un plan de gestión del proyecto que busca disminuir la brecha de vulnerabilidad tecnológica en los dispositivos de almacenamiento digital de la Empresa X, lo que le permitirá a la organización contar con un análisis adecuado de requerimientos y con una herramienta formal basada en lineamientos de administración de proyectos de basta aceptación internacional y de análisis apropiados para la toma de decisiones.

Situación actual de la organización

Para determinar la situación actual de la organización ante desastres tecnológicos que afecten los dispositivos de almacenamiento digital, se realizó un análisis FODA que permitió identificar los siguientes factores importantes:

Fortalezas

- Nivel profesional de sus empleados.
- Interés y credibilidad de la Gerencia General por los procesos de TI.
- Disponibilidad del personal.
- Tecnologías medianamente actualizadas.
- Rápido acceso a la toma de decisiones.

Oportunidades

- Infraestructura diversa.
- Condiciones del mercado para ser competitivos.
- Infraestructura de telecomunicaciones.

Debilidades

- Falta de capacitación enfocada a procesos y personal insuficiente.
- Procesos de respaldo de información no tan automatizados.
- Falta de redundancia de Bases de Datos.

- No se cuenta con sitios alternos para resguardar la información.
- No se cuenta con equipo de monitoreo.

Amenazas

- Pérdida de confianza en clientes.
- Problemas financieros por información incoherente.
- Robo de información.
- Costos crecientes por licenciamientos de software.
- Riesgos asociados con la sostenibilidad de la actual plataforma.

Brecha actual de vulnerabilidad tecnológica

El análisis FODA despliega datos importantes para determinar la brecha de vulnerabilidad tecnológica que posee actualmente la empresa, según la situación deseable en la que se debería encontrar tomando como referencia lo establecido en el estándar de COBIT®.

Con ello, se identifica que la Empresa X presenta deficiencias en la administración de diversos eventos que pueden suceder en cualquier momento. Se debe fortalecer, en el departamento de Tecnologías de Información, los procedimientos de: respaldos de datos, la búsqueda de una alternativa para salvaguardar la información fuera de la compañía, la migración y actualización del motor de bases de datos, una estandarización en el mantenimiento de los equipos, un sistema de monitoreo ambiental y otro para monitorear el estado de los servidores principales.

Para reducir tal brecha, es necesario entonces satisfacer los siguientes entregables:

- Adquisición e integración de un dispositivo que permita realizar respaldos de la información digital de la empresa.
- Arrendamiento de sitio alternativo con discos en espejo, conexión a internet y acceso seguro a los datos.

- Adquisición y actualización del motor de bases de datos.
- Elaboración de una lista de chequeo y un documento donde se hagan todas las observaciones con respecto al ambiente físico donde se encuentran instalados los equipos activos.
- Adquisición de un sistema autónomo de monitoreo ambiental.
- Adquisición e implementación de un sistema de monitoreo de los servidores.

Con ello, se propone un plan cuyo objetivo es dirigir el proyecto que implementará los entregables que permita satisfacer estos requerimientos. Este plan se encuentra integrado y alineado a la información previamente presentada, y constituye la propuesta de solución al problema planteado por la investigación. El plan está compuesto por cinco planes subsidiarios que integran diversos procesos de planificación.

Gestión de la Integración

Se integran diversos procesos para la dirección del proyecto, según su ciclo de vida: Inicio y Planificación, Ejecución, Seguimiento y Control y Cierre. Cada proceso requiere entradas que, mediante la aplicación de herramientas específicas, se procesan para obtener resultados que consolidan el plan para la gestión del proyecto.

Se establece un Plan para la Gestión de Cambios, donde se detallan tres tipos de cambios soportados: acción correctiva, acción preventiva y reparación de defectos, que pueden ser emitidas por cualquier interesado y deben ser revisadas por el equipo de proyecto para determinar su impacto.

Si el tipo de cambio es “Correctivo”, el director del proyecto realiza la evaluación final y aprueba o rechaza directamente la solicitud de cambio. Para los otros tipos, se integra un Comité de Control de Cambios que debe evaluar

el impacto de la solicitud y comunicar la decisión sobre su implementación.

Gestión del Alcance

El alcance del proyecto está comprendido por los siguientes entregables a nivel de proyecto:

- Acta de Constitución del Proyecto
- Registro de Interesados
- Plan de Gestión de la Integración
- Plan de Gestión del Alcance
- Plan de Gestión del Tiempo
- Plan de Gestión del Costo
- Plan de Gestión de las Comunicaciones
- Plan de Gestión del Riesgo
- Solicitudes de Cambio
- Reporte de desempeño
- Lecciones aprendidas

Y por los siguientes entregables a nivel de producto:

- **Sistema de Monitoreo Ambiental RSE-WeatherGoose®:** Sistema autónomo de monitoreo ambiental con sensores internos de temperatura, flujo de aire, intensidad de luz y sonido, tres sensores de contactos secos y cámara web.
- **NAS POWERVAULT® NX3600:** Almacenamiento de información digital de forma compartida, propio sistema operativo y servidor interno.
- **Motor de base de Datos SQL Server 2008 R2:** Migración del motor de bases de datos SQL Server® 2000 a SQL Server® 2008 R2.
- **Sistema Applications Manager:** Monitoreo de servidores para asegurar que la utilización sus recursos sea adecuada.
- **Servidor dedicado en TicoServer:** Arrendamiento de servidor dedicado “en la nube” con administración de un panel de control remoto.
- **Manual para el Mantenimiento de los Equipos:** Herramienta de apoyo para los

procesos de mantenimiento de los equipos activos.

Gestión del Tiempo

Para desarrollar los entregables del proyecto se consideran 65 actividades y 25 puntos de control o hitos. Para las tareas de seguimiento y control que implican la elaboración de informes de desempeño del proyecto, las reuniones para la revisión de estos informes y de las solicitudes de cambio, se establece realizarlas semanalmente durante la fase de ejecución del proyecto.

El proyecto requiere la utilización de 9 recursos de trabajo, como se detalla en la **Tabla 1**.

Tabla 1. Recursos de trabajo

Nombre del recurso	Capacidad máx.
Gerente General	25%
Gerente Financiero	50%
Gerente de Operaciones	25%
Gerente de TI	100%
Arquitecto de Base de Datos	75%
Analista/Programador de Sistemas	100%
Soporte de Sistemas	75%
Director de Proyecto	100%
Misceláneo	75%

Además, se estima el uso de 11 recursos materiales y de costo fijo, como se detalla en la **Tabla 2**.

Tabla 2. Recursos materiales y de costo fijo

Nombre del recurso	Tipo
NAS POWERVAULT NX3600	Material
Instalación NAS	Costo
Capacitación NAS	Costo
Sistema RSE-WeatherGoose	Material
Instalación RSE	Costo
Capacitación RSE	Costo
Sistema SQL Server 2008 R2	Material
Capacitación SQL Server	Costo
Sistema Applications Manager	Material
Capacitación Applications Manager	Costo
Servidor Dedicado TicoServer	Material

El tiempo de duración estimado se determinó mediante tres valores, para cada actividad se estimó un tiempo de duración pesimista, más

probable y optimista, aplicando posteriormente la fórmula PERT con estos tres valores. Por juicio experto, parte de estos valores se estimaron incluyendo una reserva o aplicando un redondeo de horas, para que el desarrollo de la actividad completara unidades de tiempo de fácil manejo.

Con ello fue posible establecer el cronograma del proyecto, considerando rubros laborales (días y período laboral), días no laborales, capacidad máxima de los recursos asignados y la secuencia adecuada de las actividades. Se estima un esfuerzo total de 963,5 horas distribuidas en 55 días laborales.

Gestión del Costo

El presupuesto para desarrollar el proyecto consiste en la suma de los salarios requeridos según los recursos de trabajo, el costo de los equipos y las licencias de software que se deben adquirir, los costos de instalaciones y capacitaciones por parte de los proveedores, así como el uso de otros materiales comunes. En la **Tabla 3** se detalla el presupuesto estimado del proyecto.

Tabla 3. Presupuesto del proyecto

Rubro	Costo Total
Salarios	\$6.919,5
Equipos	\$11.055,24
Licencias y Servicios	\$12.730,00
Instalaciones	\$400,00
Capacitaciones	\$4.500,00
Presupuesto Total	\$35.604,74

Gestión de las Comunicaciones

Cada interesado del proyecto posee una expectativa de la información que desea recibir del proyecto, según el papel que desempeña dentro del mismo.

El Gerente General, como promotor del proyecto, es el principal receptor de información del proyecto, por lo que es fundamental que reciba oportunamente todos los informes de seguimiento y control que se generen con el proyecto. El Gerente de TI, como principal

experto técnico del proyecto, debe contar con canales de comunicación desde y hacia todos los miembros del equipo de proyecto, dada la interacción que los demás miembros tienen en los procesos o equipos del Departamento de TI.

Entre las demás gerencias, deben existir canales de comunicación ya que se espera su participación activa en los procesos de evaluación de cambios y de seguimiento del proyecto. Así mismo, al formalizar las relaciones entre los interesados, se busca que las expectativas de cada uno estén alineadas al objetivo del proyecto.

Según el análisis de requisitos de comunicaciones realizado, para contar con un adecuado esquema de comunicaciones, es necesario establecer 36 canales de comunicación distribuidos entre los partidos interesados en el proyecto.

En estos canales, se planifica el uso de los siguientes recursos:

- **Tecnologías de Comunicación:** Correo electrónico, proyector, teléfono, computadora portátil, conferencias remotas.
- **Reportes:** Minuta de Reunión, Reporte de Desempeño, Solicitud de Cambio.
- **Reuniones:** Equipo de proyecto, Comité de Control de Cambios, Revisión del desempeño y riesgos del proyecto.

Gestión de los Riesgos

Para realizar una adecuada gestión de riesgos, se deben considerar los siguientes factores:

- **Identificación de los riesgos:** La identificación de los riesgos, tanto negativos como positivos, debe ser un proceso continuo realizado durante todo el ciclo de vida del proyecto. Conforme se vayan considerando nuevos riesgos, se debe actualizar el registro base de riesgos presente en este plan subsidiario.

- **Evaluación de los riesgos:** Para la evaluación de los riesgos, se establecer la probabilidad e impacto de los riesgos, así como la asignación de su prioridad y los requisitos para realizar una acción de evaluación. A cada riesgo se le debe asignar además una categoría acorde su naturaleza: Gestión del Proyecto, Organización, Técnico o Externo.
- **Roles y responsabilidades:** El director del proyecto es el encargado de documentar formalmente los riesgos identificados y evaluarlos junto al equipo de proyecto. Para cada estrategia de respuesta planificada para los riesgos aplicables, se debe asignar un único responsable encargado de velar que la acción considerada se lleve a cabo. Ciertas estrategias de respuesta ante los riesgos no tienen una acción asociada (por ejemplo, aceptar una amenaza), por lo que no se considera un responsable.
- **Comunicación:** En caso de identificar y evaluar nuevos riesgos, se deben incluir la información de referencia dentro de la minuta de reunión levantada en la sesión de trabajo.

Inicialmente, se identificaron para el proyecto 14 riesgos negativos, entre ellos los siguientes:

- Estimaciones realizadas en la planificación previa al inicio del proyecto pueden no estar acorde al contexto actual de ejecución.
- Atraso en la adquisición de los equipos, sistemas o servicios por contención en la entrega de los recursos financieros necesarios.
- Insatisfacción en la expectativa de los interesados por especificaciones inadecuadas en los equipos adquiridos.
- Mal pronóstico del crecimiento de la demanda de almacenamiento digital de la empresa, produciría que el alcance del proyecto sea insuficiente.

- Limitado aseguramiento del funcionamiento de los nuevos equipos y sistemas adquiridos, al implementarse en conjunto con los nuevos equipos de monitoreo.
- Daños en los equipos nuevos debido a una inadecuada limpieza.
- Inadecuada instalación de los equipos y sistemas adquiridos.
- Inadecuada configuración y utilización de los equipos y servicios adquiridos.

Así mismo, se identificaron tres riesgos positivos:

- Disponibilidad del personal del departamento para documentar el proceso de mantenimiento de los equipos existentes y del cuarto de servidores.
- Descuentos en la adquisición de los equipos por contratación de instalación y capacitaciones.
- Adelantos en la ejecución del proyecto por incremento en la disponibilidad de los recursos para el proyecto.

Según la evaluación del riesgo, se determinó una estrategia de respuesta mediante un plan de acción. Entre las principales estrategias se encuentran:

- Asignar recursos para llevar a cabo una validación inicial de los fundamentos y estimaciones realizadas para la planificación del proyecto.
- Considerar un tiempo promedio de adquisición de los equipos, sistemas o servicios según las compras históricas de este tipo realizadas por la empresa.
- Capacitar al personal misceláneo sobre la forma correcta en que se deben limpiar los nuevos equipos.
- Contratar a los proveedores para que realicen la instalación de los equipos adquiridos.
- Contratar a los proveedores para capaciten al personal interno en la

configuración, uso y mantenimiento de los equipos o sistemas adquiridos.

- Aumentar los criterios de aceptación de todos los entregables para incluir suficientes detalles de validación, con lo que se pretende acercar el funcionamiento esperado del equipo a la expectativa de los interesados.
- Ampliar el alcance del proyecto para incluir a los equipos existentes y al cuarto de servidores dentro de los procesos de mantenimiento y limpieza a documentar.

Validación de propuesta

Una vez completado el plan para la dirección del proyecto, se procedió a validar la factibilidad del proyecto propuesto y el nivel de satisfacción obtenido por parte del Gerente General, como patrocinador del proyecto, y del Gerente de TI, como principal figura técnica dentro del equipo de proyecto.

Entre los principales puntos se obtuvo que:

- El proyecto se encuentra alineado a la estrategia de la organización.
- Satisface los objetivos planteados.
- Su desarrollo es factible considerando planes de inversión.
- El plan es de fácil lectura y comprensión.
- Las prioridades planteadas adecuadamente.
- Se reduce la probabilidad de fracaso.
- Se identifica los problemas de mayor criticidad.
- Se desea que exista un interés común entre los departamentos, esfuerzos coordinados para lograr implementar nuevas fases para la gestión de proyectos.
- El alcance propuesto se encuentra aprobado por Gerente de TI.

Conclusiones

1. Entre las principales fortalezas y oportunidades, se encuentra el interés de

la alta gerencia en su plataforma tecnológica y su personal con disponibilidad y disposición para aprender nuevos procesos, así como factores adecuados para la inversión en mejoras a procesos de TI.

2. Entre las principales debilidades y amenazas, se encuentra la falta de capacitación enfocada para los procesos de respaldo y recuperación de la información digital, procesos sin un nivel adecuado de automatización, falta de equipos de respaldo, sitios alternos de almacenamiento y procesos de monitoreo que aseguren el correcto funcionamiento de los recursos de TI.
3. Han ocurrido una considerable cantidad de eventos negativos que impactaron el manejo de la información digital de la organización, por lo que se vuelve un factor importante entre los casos de soporte que atiende el departamento de TI.
4. Según el análisis de precedencia, la instalación de los equipos nuevos se debe realizar antes de la instalación de los sistemas de monitoreo, para que tales procesos de monitoreo incluyan el funcionamiento de los nuevos dispositivos.
5. El Gerente General, como promotor del proyecto, es el principal receptor de información del proyecto, por lo que es fundamental que reciba oportunamente todos los informes de seguimiento y control que se generen con el proyecto.
6. El Gerente de TI, como principal experto técnico del proyecto, debe contar con canales de comunicación desde y hacia todos los miembros del equipo de proyecto, dada la interacción que los demás miembros tienen en los procesos o equipos del Departamento de TI.
7. Se debe valorar constantemente el desarrollo y los cambios producidos con el proyecto, para identificar nuevas amenazas u oportunidades, y gestionar

adecuadamente los riesgos que se materialicen. Para el proyecto se define el proceso para identificar, evaluar, asignar y comunicar los riesgos del proyecto.

8. El proyecto presentado es entendible, viable, factible y soluciona el problema expuesto, según los resultados obtenidos del proceso de validación realizado con el patrocinador y el experto técnico principal.

Recomendaciones

1. Mantener actualizado los planes de continuidad de TI orientados al negocio.
2. Planear capacitaciones constantes y, en especial, cuando se den cambios en los planes de continuidad o en los entregables, que se definieron como planes necesarios para la continuidad del negocio y para cerrar la brecha tecnológica con respecto a los dispositivos de información digital.
3. Planear los mantenimientos respectivos de la información en la nube, con monitores constantes y verificación de reportes o bitácoras de la administración de del espacio arrendado.
4. Realizar listas de chequeo para garantizar que TI cumpla con la garantía de la información crítica y confidencial de la empresa que la misma se mantenga salvaguardada u oculta contra quienes no deban de tener acceso a ella.
5. Realizar bitácoras autorizadas para el desecho de la información, que la misma sea validada por la auditoría interna de la compañía.
6. Informar mediante un reporte a la Gerencia General de cómo está conformado el contenido de la información en el equipo PowerVault® y en la nube, así como de la información que sea eliminada.

7. Realizar los planes de mantenimiento físico de todos los equipos de la sala de servidores, con su debida coordinación y autorización de la de Gerencia de TI.
8. Realizar esfuerzos focalizados en miembros claves de la organización para proyectar la cultura de proyectos hacia los demás miembros.
9. Ampliar el análisis de los escenarios de desastres tecnológicos para tomar en cuenta otras posibles vulnerabilidades y no sólo la de los equipos de almacenamiento de información digital.
10. Considerar otros dominios de COBIT® para ampliar el análisis de la brecha de vulnerabilidad tecnológica en otros procesos críticos de la organización.
11. Establecer un repositorio central para la información de los proyectos, lo que permitirá crear una carpeta donde se almacene toda la información relacionada al proyecto como tal.
12. Ampliar el proyecto en una nueva o nuevas fases, donde se incluyan los demás planes subsidiarios y procesos de planificación detallados en la guía del PMBOK®, con el fin de abarcar otros ámbitos y consideraciones e ir madurando gradualmente la gestión de proyectos de la organización.

Bibliografía

- Chiavenato, I., & Sapiro, A. (2011). *Planeación Estratégica: Fundamentos y Aplicaciones* (Segunda ed.). (P. Mascaró, Trad.) McGRAW-HILL/INTERAMERICANA EDITORES, S.A. de C.V.
- Freeman, R. E., Harrison, J. S., & Wicks, A. C. (2008). *Managing for Stakeholders : Survival, Reputation, and Success*. New Haven, CT, USA : Yale University Press.
- Gómez, M. (2009). *Introducción a la metodología de la investigación científica* (2da ed.). Córdoba: Editorial Brujas.
- IT Governance Institute. (2007). *COBIT 4.1*. US: ISACA.
- MAPCAL. (1995). *El diagnóstico de la empresa*. España: Ediciones Díaz de Santos.
- MAPCAL S.A. (2007). *El diagnóstico de la empresa*. Madrid, España: Ediciones Díaz de Santos.
- Naghi Namakforoosh, M. (2000). *Metodología de la investigación* (2da ed.). México: Editorial Limusa.
- Niño Rojas, V. M. (2011). *Metodología de la investigación: diseño y ejecución*. Bogotá: Ediciones de la U.
- Project Management Institute. (2008). *Guía de los fundamentos para la dirección de proyectos (guía del PMBOK®)* (4ta ed.). Newtown Square, PA: Project Management Institute.
- Project Management Institute. (2008). *The Standard for Portfolio Management* (2da ed.). Newtown Square, PA: Project Management Institute.
- Rojas López, M. D., & Medina Marín, L. J. (2011). *Planeación estratégica: fundamentos y casos*. Colombia: Ediciones de la U.
- Sallenave, J.-P. (2002). *La gerencia integral: no le temas a la competencia, témale a la incompetencia*. Bogotá: Grupo Editorial Norma.

SYMANTEC ENTERPRISE. (2009). *Disaster Recovery Report*. Recuperado el 15 de 05 de 2012, de Disaster Recovery Global Data - Survey Results: http://www.symantec.com/content/en/us/about/media/2009_disaster_report.pdf