# Caso de estudio DRP en la empresa JBSecurity

Barreto Cortes Javier Hernan
Javierbarreto1@hotmail.com
Universidad Piloto de Colombia

*Resumen*— Identificar la viabilidad de la implementación de un Plan de Recuperación de Desastres (DRP) en una empresa en el sector de la tecnología a través de la metodología de Análisis de Negocios Impacto (BIA), Evaluación de Riesgos Estrategia TI y Diseño de Continuidad.

*Abstrac*— Identify the feasibility of implementing a Disaster Recovery Plan (DRP) in a company in the technology sector through the methodology of Business Impact Analysis (BIA), Risk Assessment, TI Strategy and Design of Continuity.

*Índice de Términos*— Amenaza, vulnerabilidad, DRP, BIA, Información, Plataforma, disponibilidad, Incidente, Impacto, Riesgo, Seguridad, Interrupción, Recursos, Plan, Objetivo, RTO, RPO, BCP, Hardware, Software,

## I. INTRODUCCIÓN

La seguridad de la información en la actualidad se considera como uno de los procesos más importantes para la continuidad de las empresas, ya que los activos de información son la base fundamental para su operación y control.

Basado en los fundamentos de la Seguridad de la información (Confidencialidad, Integridad, Disponibilidad, No repudio) son cada vez más las empresas que buscan tener políticas, procedimientos, manuales que les ayuden a mantener correctamente administrados y controlados toda su información y sistemas dependientes a esta.

El plan de recuperación de desastres (DRP) se genera como salvaguardas en cuanto a lo que tiene que ver con el fundamento de la disponibilidad de la información, a partir de conocer en profundidad cada proceso que realiza la empresa y conocer que elementos críticos hay que proteger y saber cómo protegerlos.

La finalidad de un DRP es obtener la información de RPO y RTO de dichos sistemas de información para implementar soluciones que se ajusten a determinados tiempos y así minimizar las pérdidas que se puedan presentar en un incidente de indisponibilidad.

## II. ANTECEDENTES

### IMPACTO DE LA NO DISPONIBILIDAD DE LOS SISTEMAS DE INFORMACIÓN EN LAS ORGANIZACIONES

Existen diferentes riesgos que pueden impactar negativamente las operaciones normales de una organización. Una evaluación de riesgo debería ser realizada para ver que constituye el desastre y a que riesgos es susceptible una empresa específica, así mismo dichos impactos tienen diversas dimensiones.

*IMPACTO FINANCIERO*

Los impactos financieros son cuantificados en términos de la cantidad de dinero que puede llegar a perder y/o dejar de ganar una organización como parte de una interrupción de uno o varios sistemas de información que están soportando los procesos de negocio. Algunos ejemplos de los impactos financieros son la falta de ganancias por tener inhabilitado un proceso comercial, los costos por inactividad de los empleados al no poder utilizar algún sistema de información o al no poder laborar desde cierta instalación, pagos de multas o penalidades con los clientes por la no prestación de los servicios, pagos de multas o penalidades con el Gobierno por el no cumplimiento de requerimientos legales, entre otros.

### PÉRDIDA EN VENTAS

El impacto financiero más obvio que se puede presentar como parte de una interrupción es la inhabilidad de vender o procesar las solicitudes de sus clientes por falta de sus sistemas de información. No se diga si se trata de e-commerce, ya que en ese caso se magnifica el problema, ya que las ventas están íntimamente ligadas a la disponibilidad del Sistema.

Una forma de calcular las pérdidas por ganancias, es revisar las estadísticas de venta en el último año y escoger el rango de fechas en el cual se hayan presentado las mayores ventas. Lo anterior se realiza porque nunca se puede llegar a saber en qué momento en específico se puede presentar una interrupción, entonces por mejores prácticas se escoge el peor de los escenarios, en este caso el periodo de mayores ventas de la empresa.

### PÉRDIDA DE PRODUCTIVIDAD DE EMPLEADOS

Los empleados que dejan de producir para la compañía una o dos horas, significan pérdidas ya que la compañía sigue pagando sus honorarios y salarios, aunque no estén haciendo ninguna actividad. Otros empleados pueden hacer otras actividades; pero el costo no es tan alto. Se puede proyectar el número de horas pérdidas, en caídas de Sistemas de Información anteriores, a fin de determinar cuál es el costo aproximado para una caída del Sistema; esto nos puede dar una idea de cómo lo podemos proyectar en el tiempo y tener una buena base de cálculo.

El camino más común para determinar el costo de la pérdida de productividad es, tomar un periodo de nómina (incluyendo horas trabajadas y prestaciones) del grupo de personas que se vean afectadas por la no disponibilidad de los Sistemas de Información.

### ENTREGAS A DESTIEMPO Y PENALIDADES

Algunas compañías trabajan bajo contratos que incluyen penalizaciones por entregas a destiempo de la mercancía, por lo que también hay que sumar este tipo de penalización al costo de caída de los Sistemas de Información, ya que dependiendo de la industria es la penalización, más los honorarios de los abogados.

### IMPACTOS LEGALES

Dependiendo de cómo afectó la caída del sistema en el mercado, el costo legal asociado con el tiempo de la caída, puede ser significante, para darse cuenta de lo anterior basta con mencionar algunos ejemplos:

Si la caída del Sistema contribuyó a la pérdida en las acciones de la Bolsa, los accionistas pueden demandar a la junta directiva por negligencia, por no proteger adecuadamente los recursos vitales de la empresa.

Si dos compañías están asociadas dando un servicio y una de las compañías depende directamente de la disponibilidad de los Sistemas de la segunda compañía, entonces, dependiendo de la estructura legal del contrato, la primera puede demandar a la segunda por la pérdida de ganancias en el tiempo de la caída.

Si la falta de disponibilidad del Sistema hace que una compañía produzca artículos defectuosos, la compañía puede incurrir en costos por productos defectuosos. El ambiente legal es muy complejo, ya que cada caso es una demanda diferente, por lo que se deberá consultar a los especialistas para explorar la posibilidad de incurrir en riesgos que la compañía pueda caer.

### IMPACTO PÉRDIDA DE IMAGEN

Estos impactos son muy difíciles de calcular ya que no pueden ser cuantificados en términos de cantidad de dinero, sin embargo tiene un impacto al negocio muy fuerte a nivel reputacional ya que a un mediano plazo, incluso así ya se haya superado la interrupción, podría generar que los clientes empiecen a dejar de comprar los productos o servicios de la compañía, y se empiecen a pasar a la competencia. En caso que la pérdida de imagen sea muy alta incluso la empresa podría llegar a perder todos sus clientes y podría terminar cerrando su negocio.
Teniendo en cuenta que los impactos de pérdida de imagen no se pueden cuantificar es importante definir niveles de pérdida de imagen con los cuales se pueda llegar a calificar una interrupción (ejemplo: bajo, medio, alto). Generalmente estos niveles se definen en términos de la cantidad de clientes que pueden sentir insatisfacción por el evento de interrupción, teniendo en cuenta que posiblemente estos clientes son los que se podrían llegar a perder.

Las grandes compañías gastan millones de pesos construyendo sus marcas y desarrollando y protegiendo su imagen. Cuando repetidamente tienen caídas de Sistemas, dañan fuertemente su imagen. [3].

## III. ESTÁNDARES Y BUENAS PRÁCTICAS

### DRI INTERNATIONAL

El Disaster Recovery Institute International (DRI International) es una organización internacional encargada de promover mejores prácticas respecto a la implementación de proyectos de continuidad de negocio y recuperación de desastres. A través de sus diez prácticas profesionales indican a los planificadores de continuidad los lineamientos y actividades que deben tener en cuenta para ejecutar los proyectos desde la planeación del proyecto hasta la implementación y ejecución de pruebas.

A pesar que esta articulo sólo abarca ciertas fases de un proyecto de continuidad, a continuación se indica una breve descripción de cada una de estas prácticas profesionales.

### PRÁCTICA PROFESIONAL NO 1: INICIO Y ADMINISTRACIÓN DEL PROGRAMA

El objetivo de esta práctica profesional es establecer la necesidad de implementar un Plan de Continuidad de Negocio / Plan de Recuperación de Desastres con apoyo de la Alta Gerencia de las Organizaciones, durante la implementación y mantenimiento del Plan. Inicio

Como parte de esta práctica profesional se deben definir el alcance y los objetivos del Plan, así mismo las razones legales y los requerimientos en el negocio. Adicionalmente se debe establecer un Comité Directivo del proyecto (roles y responsabilidades), definir los requerimientos de presupuesto del plan, identificar los grupos de planificación y los responsables, desarrollar y coordinar los planes de acción del proyecto y finalmente obtener la aprobación de la Alta Gerencia de la Organización.

### PRÁCTICA PROFESIONAL NO 2: EVALUACIÓN Y CONTROL DE RIESGOS

La fase de evaluación y control de riesgos permite identificar los eventos y situaciones externas e internas que pueden impactar en forma negativa la organización y sus instalaciones como parte de una interrupción.

A partir de esta práctica profesional también son identificados los controles y protecciones que se deben implementar para prevenir y/o mitigar los impactos sobre la organización.

Con el objetivo de ejecutar estas actividades se requiere evaluar y seleccionar una metodología para el Análisis de Riesgos de tal forma que se utilicen las mejores prácticas durante el análisis.

Finalmente, una vez son identificados los eventos de interrupción y los controles, son implementados y evaluados periódicamente para revisar la efectividad de los mismos.

*PRÁCTICA PROFESIONAL NO 3: ANÁLISIS DE IMPACTO DE NEGOCIO*

El objetivo de esta práctica profesional es identificar los impactos que generen una interrupción y las técnicas que pueden ser empleadas para cuantificar y calificar aquellos impactos. Así mismo identificar las funciones críticas, las prioridades de recuperación, los puntos objetivos de recuperación (RPO) y los tiempos objetivos de recuperación (RTO).

Como parte de la metodología utilizada se pueden utilizar cuestionarios, entrevistas, sesiones de trabajo o la combinación, con las diferentes áreas de negocio de la organización para identificar los impactos.

PRÁCTICA PROFESIONAL NO 4: ESTRATEGIA DE CONTINUIDAD DE NEGOCIO

La información recolectada durante el BIA y la evaluación de riesgos permite identificar la estrategia de continuidad más apropiada. Esta debe estar expresada en términos de los Tiempos Objetivos de Recuperación (RTO) y los Puntos Objetivos de Recuperación (RPO). Adicionalmente se requiere de un análisis costos beneficio para entender que la estrategia está alineada con las necesidades de la organización.

PRÁCTICA PROFESIONAL NO 5: RESPUESTA Y OPERACIÓN DE EMERGENCIA

El profesional de continuidad durante esta práctica desarrolla las aptitudes para desarrollar e implementar el plan de respuesta a emergencias que pueda afectar la integridad de los empleados, visitantes o activos de la organización. Entre otras actividades se tiene la identificación de regulaciones aplicables, identificación de escenarios y tipos de emergencia, identificación de las capacidades necesarias para sobrellevar la emergencia, revisión de procedimientos de respuesta a la emergencia y elaboración de recomendaciones sobre los planes de emergencia y sobre los procedimientos que se tienen implementados.

PRÁCTICA PROFESIONAL NO 6: PLANES DE CONTINUIDAD DE NEGOCIO

El Plan de Continuidad de Negocio es un conjunto de procesos y procedimientos que permiten dar continuidad a los procesos críticos definidos por la organización. Durante esta práctica de continuidad el profesional diseña, desarrolla e implementa la estrategia de continuidad. Diseña el marco de trabajo para la documentación del plan, coordina la documentación de los procedimientos dentro de la organización y publica el plan a todos los interesados.

PRÁCTICA PROFESIONAL NO 7: PROGRAMAS DE CAPACITACIÓN Y CONCIENTIZACIÓN

Una vez documentado el Plan de Continuidad dentro de la organización el siguiente paso es realizar la respectiva capacitación y concientización a los funcionarios involucrados en algún rol dentro del plan. Entre las actividades que se tienen está el establecimiento de los objetivos de las capacitaciones y concientizaciones, la identificación de los requerimientos de las capacitaciones y concientizaciones, identificar la audiencia tanto interna como externa, desarrollar una metodología de entrenamiento e identificar herramientas necesarias para estas actividades, entre otras.

PRÁCTICA PROFESIONAL NO 8: PLAN DE PRUEBAS DE CONTINUIDAD DE NEGOCIO, AUDITORÍA Y MANTENIMIENTO

El principal objetivo en esta práctica profesional es establecer un programa de pruebas, mantenimiento y auditoría del plan de continuidad de negocio dentro de la organización. Todo esto con el fin que el Plan este actualizado respecto a los cambios que se vayan presentando en la organización. Finalmente, como parte de la comunicación del plan a toda la organización, se realiza la divulgación a los interesados de los resultados de las pruebas, las auditorías y los procesos de mantenimiento que se realicen.

PRÁCTICA PROFESIONAL NO 9: COMUNICACIÓN EN CRISIS

La comunicación en crisis antes, durante y después de un evento de interrupción es indispensable para que los usuarios internos, cliente, familiares estén enterados de la situación actual del desastre sin necesidad de generar pánico. Para esto el profesional debe diseñar, desarrollar e implementar un Plan de Comunicación en Crisis, comunicar a los patrocinadores de la organización sus roles dentro del Plan y realizar pruebas en Crisis.

El Plan de Comunicación en Crisis debe estar actualizado de acuerdo a los cambios que vaya sufriendo el negocio.

PRÁCTICA PROFESIONAL NO 10: COORDINACIÓN CON AGENCIAS EXTERNAS

Finalmente, la décima práctica profesional hace referencia la necesidad establecer políticas y procedimientos para casos de emergencia, continuidad y recuperación con las agencias externas, ya sean locales, regionales o nacionales. [2].

B. MAGERIT

Magerit es una metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica del Gobierno Español. La creación de esta metodología partió de la evolución que han tenido las tecnologías de la información y por ende la necesidad de estar evaluando constantemente los riesgos a los que están siendo sometidos.

1. Magerit persigue los siguientes objetivos (tomado textualmente de la metodología):
2. Concienciar a los responsables de los sistemas de información de la existencia de riesgos y de la

necesidad de atajarlos a tiempo
3. Ofrecer un método sistemático para analizar tales riesgos
4. Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control
5. Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso

Como parte de la metodología se realiza una caracterización de los activos de información que están involucrados en la prestación de los servicios informáticos, la relación de cómo las amenazas están afectando estos activos de información y la valoración de los salvaguardas o controles que se tienen implementados, mitigando de esta forma la materialización del riesgo.

Entre los activos de información que se contemplan dentro de la metodología se encuentran [1].

1. Servicios
2. Datos / Información
3. Aplicaciones (Software)
4. Equipos informáticos (Hardware)
5. Redes de comunicaciones
6. Soporte de información
7. Equipamiento auxiliar
8. Instalaciones
9. Personal

## IV. CASO DE ESTUDIO

### DESCRIPCIÓN DE LA EMPRESA DE ESTUDIO Y LA NECESIDAD DEL PROYECTO

No es fácil entender y calcular el costo real por la no disponibilidad de los Sistemas de Información que soportan los procesos de negocio de nuestras organizaciones, ya que estamos tan inmersos en las operaciones del día a día, que no nos permiten darnos cuenta del valor real de nuestra información y de tener disponible nuestros Sistemas de Información para servirle oportunamente a nuestros clientes o proveedores.

JBSecurity es una empresa nacional cuya misión es comercializar infraestructura tecnológica y ofrecer servicios de administración y monitoreo de la infraestructura tecnológica y sistemas de información de sus clientes.

La comercialización de infraestructura tecnológica consiste en identificar o conocer los requerimientos de los clientes en términos de infraestructura tecnológica, realizar diseños de arquitectura tecnológica y de comunicaciones, comprar infraestructura tecnológica a los fabricantes (ejemplo: fabricantes de servidores, sistemas de almacenamientos, switches de comunicación), y venderla junto con el diseño a sus clientes buscado un margen representativo sobre la compra y venta de la infraestructura tecnológica.

Los servicios de administración y monitoreo de la infraestructura tecnológica y sistemas de información están asociados a garantizar que los sistemas de información de los clientes se encuentren disponibles, con base en acuerdo de niveles de servicio definidos previamente con los clientes. Para lograr esto, JBSecurity utiliza un grupo de especialistas en cada uno de los aspectos de tecnología de la información (ejemplo: sistemas operativos, servidores y sistemas de almacenamiento, bases de datos, seguridad y conectividad y aplicaciones ERP) y una herramienta de monitoreo y administración que permite automatizar y optimizar las tareas que realizan estos especialistas. Actualmente todos los clientes de JBSecurity despliegan sus sistemas de información sobre infraestructura tecnológica implementada en sus Centros de Cómputo, sin embargo la infraestructura tecnológica donde están implementadas las aplicaciones de administración y monitoreo de JBSecurity si se encuentran desplegadas sobre el Centro de Cómputo de JBSecurity.

Actualmente los clientes de JBSecurity están distribuidos en las principales ciudades del País tanto para la comercialización de la infraestructura tecnológica como para la prestación de los servicios de administración y monitoreo.

Como se presentó anteriormente, los servicios de administración y operación de los sistemas de información, JBSecurity tiene comprometidos Acuerdos de Niveles de Servicios con la mayoría de sus clientes, relacionados con la disponibilidad que deben tener estos sistemas de información.

Como antecedentes uno de los incidentes que más preocupación generó para el Comité Directivo de JBSecurity fue un conato de incendio que se presentó en el Centro de Cómputo. Afortunadamente este conato de incendios se presente en horarios laborarles, periodo durante el cual estaban varios trabajadores en la oficina, y por tal motivo fue controlado rápidamente por los mismos. Como resultado del conato de incendio se evidenciaron varias vulnerabilidades a nivel del sistema de detección de incendios del Centro de Cómputo, la presencia de objetos inflamables y los deficientes mecanismos para contrarrestar la materialización de estas amenazas.

Debido a la atención de este conato de incendio por parte de los funcionarios de JBSecurity, hubo la necesidad de apagar los servidores del Centro de Cómputo por un periodo de cuatro horas. Durante estas dos horas toda la compañía quedó sin comunicaciones internas ni externas, sin brindar servicios de File Server, Correo electrónico, sistema de relaciones con los clientes (CRM) gestión documental, servicios de nómina y facturación, y lo más crítico los sistemas que permiten la administración y operación de los sistemas de información de los clientes de JBSecurity.

Teniendo en cuenta los Acuerdos de Niveles de Servicio con los clientes y los frecuentes eventos de interrupción presentados, JBSecurity ha decido realizar un estudio para definir e implementar un Plan de Recuperación de Desastres que le permita a JBSecurity tener tranquilidad de dar continuidad a sus sistemas de información y a lo de sus

clientes en caso que se genere un evento de interrupción.

## V. ALCANCE

Así las prácticas profesionales del DRII apliquen tanto para Planes de Continuidad de Negocio (BCP) como para Planes de Recuperación de Desastres (DRP), durante este estudio sólo se incluirá alcance sobre el Plan de Recuperación de Desastres enfocada a la continuidad operativa de los Sistemas de Información.

Respecto a los servicios de JBSecurity, este estudio tendrá alcance sobre los procesos críticos de esta organización, es decir sobre:

- Servicios de comercialización de infraestructura tecnológica con los clientes
- Servicios de administración y operación de los sistemas de información de los clientes
- Por consiguiente sólo tendrá alcance sobre los sistemas de información que están apoyando a estos procesos críticos de negocios, en este caso los siguientes sistemas de información:
- Sistema de gestión de relación con los clientes (CRM)
- Repositorio Archivos (File Server)
- Sistema de administración y monitoreo de JBSecurity
- Correo electrónico
- El estudio se realizará para las siguientes prácticas profesionales del DRII:
- Evaluación de Riesgos y Control
- Análisis de Impacto de Negocio
- Estrategia de continuidad de negocio (aplicado a Plan de Recuperación de Desastres)

El estudio se realizará solo para la sede principal de la empresa, teniendo en cuenta que y se basará en los sistemas de información que soportan los procesos de negocio de las áreas Comercial (Comercialización de Infraestructura TI) y de Operaciones de TI (Administración y Operación de Sistemas de Información), consideradas como las áreas críticas de JBSecurity.

Así mismo el estudio se realizará exclusivamente para los Sistemas de Información que están apoyando a los procesos de negocio de las áreas Comercial y de Operaciones de TI.

## VI. DESARROLLO DE LA METODOLOGÍA

### ANÁLISIS DEL IMPACTO SOBRE EL NEGOCIO (BIA)

¿Cuál es el costo de tener fuera de operación a la compañía por tres horas? El Análisis de Impacto de Negocio es el camino para responder a esta pregunta del negocio.

Para evaluar el impacto de la indisponibilidad, las compañías deben considerar todos los costos que la constituyen y como cada uno de ellos puede ser afectados por una falla en el Sistema, incluyendo no solamente la pérdida de las ganancias en ese momento, sino también las posibles pérdidas en las ganancias futuras, pérdida de productividad, pérdida por ocupación de espacio por empleado, pérdida o desajuste del inventario; costos de pérdidas por falta de ganancias y recuperación de la información, pérdidas por no entregar las mercancías a tiempo, pérdidas de oportunidad de negocios, pérdida de clientes y pérdida del valor en la forma de compartir la depreciación, demandas de los clientes, reputación y quién sabe cuántas cosas más, haya que facturar en el transcurso de la caída del Sistema.

Como la gran mayoría de las compañías se vuelven más independientes por unidades de negocio, así como por la cadena de suministros, el impacto de la caída del Sistema escala rápidamente, afectando no solamente al Negocio Principal, sino a cada uno de las componentes de la cadena de suministros.

El análisis del impacto sobre el negocio (BIA) es uno de los aspectos más importantes a considerar en el desarrollo de un Plan de Recuperación de Desastres. Se trata pues, de identificar los impactos que puede generar un evento de interrupción sobre los sistemas de información, adicionalmente los requerimientos para el Diseño del Plan de Recuperación de Desastres (DRP).

Durante este capítulo se desarrollarán los siguientes aspectos:

- Descripción de la estructura organizacional de JBSecurity.
- Descripción de los sistemas de información de JBSecurity que tendrán alcance en este estudio
- Alineamiento entre los procesos de negocio críticos de JBSecurity y los Sistemas de Información
- Plan de ejecución del BIA incluido cuestionario BIA
- Definición de requerimientos para la implementación del Plan de Recuperación de Desastres (DRP)
- Presentación de los resultados del BIA

## VII. ESTRUCTURA ORGANIZACIONAL DE JBSECURITY

JBSecurity es una empresa de 80 empleados y con oficinas en las principales ciudades del País: Bogotá (sede principal), Medellín y Cali. Su estructura organizacional está descrita como se indica en la siguiente figura:

Grafico 1. Organigrama de la empresa
Fuente: El autor.

De acuerdo con el organigrama indicado en la figura anterior, la Gerencia General y las Direcciones se encuentran ubicadas en la sede principal (Bogotá). Para dar cobertura sobre las diferentes ciudades donde JBSecurity tiene presencia, se cuenta con Ejecutivos de Cuenta y Arquitectos TIC en todas

las sedes de JBSecurity (Bogotá, Medellín, Cali y Barranquilla). Todos los especialistas TIC están ubicados en la Sede Principal, donde realizan la administración y operación de los sistemas de información de los clientes de JBSecurity desde un centro de operaciones centralizado (NOC). Finalmente los Analistas de Talento Humano, Asistentes financieros y de Contabilidad se encuentran en la sede principal.

## VIII. SISTEMAS DE INFORMACIÓN DE JBSECURITY

En la siguiente tabla se obtiene la lista de los sistemas de información que posee JBSecurity en sus instalaciones y se determina cuáles de ellos están relacionados de manera directa o indirecta con el servicio de TI.

| SISTEMA DE INFORMACION | CONCEPTO |
|---|---|
| CRM | Este sistema de información es utilizado por el área comercial para la comercialización de infraestructura tecnológica y de servicios de administración y monitoreo. Por medio de esta aplicación se puede registrar los aspectos básicos de cada una de las oportunidades de negocio (datos del cliente, productos y/o servicios ofrecidos, monto esperado de venta, etc), así como la trazabilidad del estado en el cual se encuentran. A pesar que este sistema CRM lleva dos años con la organización, se ha convertido en una aplicación muy crítica para el área comercial ya que a través del sistema se optimizan todos los procesos comerciales, de arquitectura TIC y de comunicación con los clientes. |
| Repositorio Archivos (File Server) | Es una computadora conectada a una red que tiene el objetivo principal de proporcionar una ubicación para el acceso al disco compartido. Sobre este repositorio de archivos actualmente los ejecutivos de cuenta, arquitectos de TIC, especialista de TIC y asistentes administrativos y financieros; almacenan los archivos de trabajo tales propuesta de comercialización, diseño de arquitectura, reportes de administración y monitoreo, informes administrativos y financieros, etc. |
| Sistema de administración y monitoreo de Technoservices | Este sistema es un desarrollo propio de Technoservices que es utilizado por los especialistas de TIC de Technoservices para administrar y monitorear los sistemas de información de los clientes. Cuenta con un sistema de alarmas que informa a los especialistas cuando existan errores o fallas tanto en la infraestructura tecnológica como en los sistemas de información. Este sistema de información está conectado con la infraestructura tecnológica de los clientes que se desea administrar y monitorear, a través de enlaces de comunicación dedicados o enlaces de internet. |
| Correo electrónico | Es un servicio de red que permite a los usuarios enviar y recibir mensajes y archivos rápidamente (también denominados mensajes electrónicos o cartas electrónicas) mediante sistemas de comunicación electrónicos. |

Tabla 1. Sistemas de Informacion JBSecurity
Fuente: El autor.

## IX. ALINEAMIENTO ENTRE PROCESO DE NEGOCIO Y SISTEMAS DE INFORMACIÓN DE JBSECURITY.

Con el objetivo de definir cómo los sistemas de información de JBSecurity apoyan a los procesos de negocio de la organización, a continuación se indica el alineamiento entre estos, la cual permitirá posteriormente conocer los impactos sobre el negocio que puede generar un evento de interrupción.

En la siguiente tabla se obtiene la lista de los sistemas de información que posee JBSecurity en sus instalaciones y se determina cuáles de ellos están relacionados de manera directa o indirecta con el servicio de TI.


Tabla 2. Alineamiento de TI al proceso de negocio
Fuente: El autor.

## X. CUESTIONARIO BIA

Uno de los aspectos principales al momento de identificar los impactos que pueda generar un evento de interrupción es la elaboración y ejecución de un cuestionario BIA, de tal forma que se permitan identificar los impactos financieros. Este cuestionario es elaborado teniendo como base el alineamiento entre los procesos de negocio y los sistemas de información. Adicionalmente, por medio del cuestionario BIA se busca conocer los requerimientos del DRP de los usuarios.

Las preguntas del BIA están enfocadas en interrupciones de los sistemas de información por un periodo de dos (2) meses, teniendo en cuenta que este sería el peor de los escenarios de interrupción.

| PREGUNTA BIA | RESPUESTA |
|---|---|
| ¿En el último año, cuáles han sido las mayores ventas de comercialización de infraestructura TIC (indicar los dos meses consecutivos con mayores ventas)? | $ 4.000.000.000, en los meses de octubre y noviembre |
| En caso que no se contara con el CRM para realizar la gestión de comercialización de infraestructura TIC por un periodo de dos meses, qué porcentaje de oportunidades de negocio se dejarían de ganar? | 30% |
| Cuál es el porcentaje de rentabilidad promedio en los negocios de comercialización de infraestructura TIC en Technoservices? | 20% |
| En caso que no se contara con el CRM para realizar la gestión de comercialización de infraestructura TIC por un periodo de dos meses, cuántas horas extras de ejecutivos de cuenta se tendría que involucrar para cumplir con la atención de las oportunidades de negocio? | 800 horas |
| Cuál es el costo promedio por una hora extra de un ejecutivo de cuenta para Technoservices? | $ 60.000 |
| En caso que se perdiera la información del repositorio de archivos, cuántas horas extras de arquitectura TIC se tendrían que trabajar para recuperar la información perdida de los diseños? | 1.500 horas |
| Cuál es el costo promedio por una hora extra de un arquitecto TIC para Technoservices? | $ 90.000 |
| Existen propuestas de comercialización de infraestructura TIC que deben ser presentadas exclusivamente a través de correo electrónico corporativo de Technoservices? | Si |
| Cuál es la utilidad de las propuestas de comercialización de infraestructura TIC que son presentadas exclusivamente a través de correo electrónico corporativo de Technoservices por un periodo de dos meses? | $ 85.000.000 |

| PREGUNTA BIA | RESPUESTA |
|---|---|
| En caso que se presentará un evento de interrupción de los sistemas de administración y monitoreo, existe un proceso de contingencia para realizar estas actividades? | Si, los especialistas de TIC se pueden desplazar a las oficinas de los clientes para realizar la administración y operación directamente sobre sus infraestructuras tecnológicas. |
| En caso de contar con un proceso contingente cuánto tiempo se tardaría en restablecer el proceso de administración y monitoreo? | Para el 20% de los clientes en 12 horas y para el 80% restante de los clientes se tendría que esperar hasta que se consigan nuevos especialistas de TI para que puedan desplazarse a las oficinas de los clientes, es decir entre 2 y 3 semanas. |
| Cuál sería el costo de la implementación del proceso de contingencia para las actividades de administración y monitoreo por un periodo de dos meses? | $ 140.000.000: Nuevas contrataciones de especialistas TIC para que atiendan desde las oficinas de los clientes las actividades de administración y operaciones.<br>$ 30.000.000: Otros gastos administrativos y logísticos |
| Del total de los clientes que actualmente se les está presentando los servicios de administración y monitoreo, cuál porcentaje se vería altamente molestos por la interrupción de los servicios de administración y monitoreo? | 80% |
| En caso que se presentará una interrupción de 24 horas de los sistemas de información de los clientes como consecuencia de la interrupción de los procesos de administración y monitoreo de Technoservices, cuáles serían los valores de las multas que tendría que pagar Technoservices como parte de este incidente? | $ 350.000.000 |
| **PREGUNTA BIA** | **RESPUESTA** |
| Como parte de la interrupción de los sistemas de administración y monitoreo de Technoservices y teniendo en cuenta que se cuentan con cláusulas de cancelación de contratos con los clientes por incumplimiento de los acuerdo de niveles de servicio, cuál sería el porcentaje del número de clientes que cancelarían sus contratos con Technoservices? | 50% |
| En caso que el porcentaje de clientes que cancelará sus contratos con Technoservices se diera, cuál serían las utilidades que dejaría de percibir Technoservices como parte de la cancelación de estos servicios? | $ 500.000.000 |

Tabla 3. Cuestionario BIA.
Fuente: El autor.

## XI. RESULTADOS BIA

Teniendo en cuenta las respuestas al cuestionario BIA se realizó un consolidado de los impactos financieros que podría generar una interrupción de los sistemas de información por un periodo de dos (2) meses, teniendo en cuenta que este sería el peor de los escenarios de interrupción.

Los resultados son presentados separadamente para el proceso de comercialización de infraestructura tecnológica y para el proceso de administración y monitoreo de los sistemas de información de los clientes.

## XII. PROCESO DE COMERCIALIZACIÓN DE INFRAESTRUCTURA TECNOLÓGICA

Con el objetivo de presentar los resultados consolidados de los impactos financieros a continuación se describen cada uno de los aspectos que se tuvieron en cuenta:

Utilidad negocios: Este impacto financiero se representa por la pérdida de utilidades de negocios que se pudieron haber percibido pero que por la falta del CRM no se pudieron concretar. El cálculo es el producto de (las mayores ventas de comercialización de infraestructura TIC) X (el porcentaje de oportunidades que se dejaría de ganar si no se contara con el CRM) X (el porcentaje de rentabilidad promedio en los negocios de comercialización de infraestructura TIC)

Productividad ejecutivos de cuenta: Este impacto financiero se representa por la cantidad de dinero que JBSecurity debe pagar a sus ejecutivos de cuenta para que se pueda cumplir con la atención de las oportunidades de negocio. El cálculo es el producto de (las horas extras que los ejecutivos de cuenta deben trabajar para cumplir con la atención de las oportunidades de negocio) X (el costo promedio por una hora extra de un ejecutivo de cuenta para JBSecurity).

Productividad arquitectos TIC: Este impacto financiero se representa por la cantidad de dinero que el JBSecurity debe pagar a sus Arquitectos de TIC para recuperar la información pérdida de los diseños en caso que se llegará a perder la información del repositorio de archivos. El cálculo es el producto de (las horas extras de arquitectura TIC que se tendrían que trabajar para recuperar la información pérdida de los diseños) X (el costo promedio por una hora extra de un arquitecto TIC para JBSecurity).

Utilidad negocios por correo electrónico: Este impacto financiero se representa por la pérdida de utilidades de negocios que se pudieron haber percibido pero que por la falta del correo electrónico no se pudieron presentar.

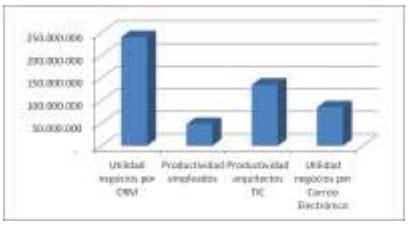

Grafico 2. Impacto financiero.
Fuente: El autor.

## XIII. RPO Y RTO

Una vez conocidos los resultados del Análisis de Impacto de Negocio por parte de la Alta Gerencia de JBSecurity, se definieron los tiempos máximos de pérdida de información (RPO) y los tiempos máximos de interrupción (RTO) que puede tolerar la organización.

Los resultados se indican en la siguiente tabla:

| SISTEMA DE INFORMACION | RPO | RTO |
|---|---|---|
| Sistema de Gestión de Relación con Clientes (CRM) | 5 días | 2 días |
| Repositorio Archivos (File Server) | 5 días | 2 días |
| Sistema de administración y monitoreo de Tecnoservices | 1 día | 12 horas |
| Correo electrónico | 1 días | 12 horas |

Tabla 4. RTO y RPO
Fuente: El autor.

## XIV. JUSTIFICACIÓN DEL RETORNO DE INVERSIÓN

El retorno de la inversión es una medida crítica, ya que se utiliza para hacer la justificación de inversiones que ayuden al

desempeño de la compañía. Si hay un proyecto en puerta que justifique el presupuesto de inversión; pero significa riesgo para la empresa y existe un proyecto para mejorar la disponibilidad de los Sistemas, el cual ayude a la empresa a mejorar y contribuir a no tener impactos financieros, legales o de pérdida de imagen; pero no se sabe vender a la alta dirección, les aseguro que se decidirán por el proyecto riesgoso. Por lo tanto se debe hacer un estudio de costo – beneficio a fin de mostrar las bondades de lo que significa el no tener un Plan de Contingencias Empresarial o una solución de alta disponibilidad de información.

Los proyectos de tecnología de la información deben tener un beneficio directo a los resultados de las aplicaciones críticas que se usan en el manejo y administración de los negocios.

Por ejemplo, aumentando las ganancias y disminuyendo las pérdidas en el negocio, ya que automatizan la producción, reducen el manejo de papel y contribuyen en gran parte a la reducción de costos de operación por disminuir el exceso de empleados. Si se conduce un proyecto de Plan de Contingencias o alta disponibilidad de los sistemas críticos y se omiten los costos de los que hablamos anteriormente, de nada servirá cualquier esfuerzo que se realice, ya que nunca se sabrá el beneficio que se obtendrá de hacer un buen Plan de Contingencias o tener una solución de alta disponibilidad.

Como parte de esta justificación se realizó el Análisis de Impacto de Negocio para identificar cuál podría llegar a ser la pérdida financiera como parte de una interrupción. Los resultados evidenciaron lo siguiente:

| Impacto financiero | Valor |
|---|---|
| Utilidad negocios por CRM | $ 240.000.000 |
| Productividad empleados | $ 48.000.000 |
| Productividad Arquitectos TIC | $ 135.000.000 |
| Utilidad Negocios por Correo Electrónico | $ 85.000.000 |
| **TOTAL** | **$ 508.000.000** |

Tabla 5. Resumen Impactos Comercialización Infraestructura
Fuente: El autor.

| Impacto financiero | Valor |
|---|---|
| Implementación contingencia | $ 170.000.000 |
| Multas por interrupción | $ 350.000.000 |
| Utilidades por cancelación de contratos | $ 500.000.000 |
| **TOTAL** | **$ 1.020.000.000** |

Tabla 6. Resumen Impactos Administración y Monitoreo Sistemas de Información
Fuente: El autor.

Sumando los dos procesos de negocio, una interrupción de los sistemas de información, en el peor de los escenarios representaría pérdidas financieras para JBSecurity por el orden de $1.528.000.000.

Como parte del diseño de la estrategia de continuidad se identificaron los costos de la implementación del Plan de Recuperación de Desastres. Los resultados fueron los siguientes:

| Activos de información | Inversión inicial (CAPEX) | Gasto operativo (OPEX) |
|---|---|---|
| **TOTAL** | **$ 350.000.000** | **$ 4.000.000** |

Tabla 7. Relación CAPEX – OPEX del DRP
Fuente: El autor.

Suponiendo un ciclo de vida del proyecto a 5 años (60 meses), los gastos operativos serían de $ 240.000.000. Sumado este valor a la inversión inicial estaríamos hablando de una inversión de $590.000.000.

Comparando las pérdidas financieras que puede generar una interrupción versus la inversión que se requiere para implementar el Plan de Recuperación de Desastres, encontramos que la inversión es de aproximadamente el 38% de los impactos financieros que se pueden generar.

El anterior análisis permite concluir que financieramente es mucho mejor invertir en la implementación de un Plan de Recuperación de Desastres, que tomar el riesgo de soportar una interrupción prolongada de los sistemas de información. Adicionalmente sin contar los impactos negativos de pérdida de imagen que podrían representar el cierre definitivo de las operaciones de JBSecurity.

## XV. CONCLUSIONES

Hoy en día los sistemas de información se han convertido en uno de los principales activos de información en una organización teniendo en cuenta que la mayoría de procesos de negocio “Core” se han automatizado a través de los mismos.

Sin embargo, lastimosamente todavía la mayoría de las empresas ven la tecnología simplemente como un gasto y no se dan cuenta de lo importante que son para su negocio hasta que no la tienen.

En la mayoría de los casos las compañías empiezan a pensar en la implementación de planes de recuperación de desastres como parte de alguna interrupción que hayan tenido y donde empiezan a evidenciar la criticidad de los sistemas de información.

Como parte de este estudio se concluye la necesidad de realizar un Análisis de Impacto de Negocio y una Evaluación de Riesgos de TI de una manera preventiva y no de una forma reactiva cuando probablemente sea muy tarde.

Para el caso de estudio de JBSECURITY se evidencio que el costo de la implementación del Plan de Recuperación de Desastres es mucho menor que los impactos financieros que puede representar un evento de interrupción grave.

Es claro que todas las organizaciones no son iguales y por ende pueden tener impactos diferentes, por tal motivo es importante realizar este tipo de estudios para saber cuál debe ser la estrategia a implementar. Incluso, de acuerdo a las mejores prácticas es importante volver a realizar este análisis de forma periódica teniendo en cuenta que los negocios son cambiantes y lo que para hoy era un sistema de información no tan crítico, en uno o dos años si puede serlo.

REFERENCIAS

[1] Magerit: Metodología de análisis y gestión de Riesgos [Online].available: http://administracionelectronica.gob.es

[2] Disaster Recovery Institute International. Prácticas Profesionales de Continuidad de Negocio [Online]. Available: https://www.drii.org/

[3] Disaster Recovery Journal. [Online]. Available: http://www.drj.com

**Autor**
**Javier Hernan Barreto Cortes**
Ingeniero de sistemas de información Universidad Nacional a Distancia, certificado en soluciones Microsoft en cuanto a Infraestructura, Correo electrónico y Comunicaciones unificadas, así como de plataformas de virtualización Vmware y sistemas de replicación para DRP Double Take.