UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Actualización de mecanismos de monitoreo y continuidad operativa de sistemas críticos

INFORME DE ACTIVIDADES PROFESIONALES

Que para obtener el título de

Ingeniería en Computación

P R E S E N T A

Ana Laura Morales Guzmán

ASESOR DE INFORME

Fis. Raymundo Hugo Rangel Gutiérrez

Ciudad Universitaria, Cd. Mx., 2019

Contenido

1. Objetivo

Actualizar los mecanismos de monitoreo y continuidad operativa de sistemas críticos interdependientes con requerimientos de alta disponibilidad a fin de:

a. Identificar fallas en el menor tiempo posible.
b. Asegurarse que, ante la materialización de fallas, los sistemas continúen operando a un nivel mínimo aceptable minimizando el tiempo de indisponibilidad.
c. Asegurarse, que al recuperar la operación de los sistemas no exista pérdida de información.
d. Actualizar los protocolos de evaluación de los mecanismos implementados a fin de asegurar su buen funcionamiento.

2. Marco teórico

2.1. Sistemas críticos

Un sistema crítico es aquel que en caso de que ocurra una falla de funcionamiento afecta de manera sustancial el negocio causando pérdidas significativas para el mismo, las cuales pueden ser daños físicos, económicos, legales o reputacionales para el administrador del sistema o para los usuarios del mismo.

Hay tres tipos principales de sistemas críticos:

1. Sistemas de seguridad críticos: Son sistemas cuyo fallo de funcionamiento puede provocar perjuicio, pérdida de vidas o daños graves al medio ambiente. Un ejemplo de un sistema de seguridad crítico es un sistema de control para una planta de fabricación de productos químicos.
2. Sistemas de misión críticos. Son sistemas cuyo fallo de funcionamiento puede provocar errores en algunas actividades dirigidas por objetivos. Un ejemplo de un sistema de este tipo es un sistema de navegación para una nave espacial.
3. Sistemas de negocio crítico. Son sistemas cuyo fallo de funcionamiento puede provocar costes muy elevados para el negocio que utiliza un sistema de este tipo. Un ejemplo de un sistema de negocio crítico es un sistema de cuentas bancarias.

Una de las propiedades más importantes dentro de un sistema crítico es la confiabilidad debido a los siguientes motivos:

- Los sistemas que no son fiables, inseguros o desprotegidos son rechazados a menudo por usuarios. Si los usuarios no confían en un sistema, se negarán a utilizarlo. Es más, también rehusarán comprar o utilizar productos de la misma compañía que produjo el sistema no confiable, puesto que creerán que tendrán la misma característica.
- Los costes de los fallos de funcionamiento del sistema pueden ser enormes, En algunas aplicaciones, como un sistema de control de reactores o un sistema de navegación aérea, el coste de un fallo en el sistema es mayor en varios órdenes de magnitud que el coste de dicho sistema de control.
- Los sistemas no confiables pueden provocar pérdidas de información. La captura y mantenimiento de los datos son muy costosos; algunas veces cuesta más que el sistema

informático que los procesa. Se tiene que hacer un gran esfuerzo e invertir mucho dinero para duplicar los datos importantes a fin de protegerlos de cualquier corrupción.

Dicho término fue propuesto por Laprie en 1995 para hacer referencia a las siguientes propiedades relacionadas de los sistemas: disponibilidad, fiabilidad, seguridad y protección. Estas propiedades están entrelazadas inextricablemente, por lo que se utiliza el término confiabilidad para referirse a cada todas ellas.

La fiabilidad de un sistema es la probabilidad de que el sistema funcione correctamente tal y como se ha especificado. La disponibilidad es la probabilidad de que el sistema esté en disposición de funcionar para proporcionar los servicios a los usuarios que lo soliciten.

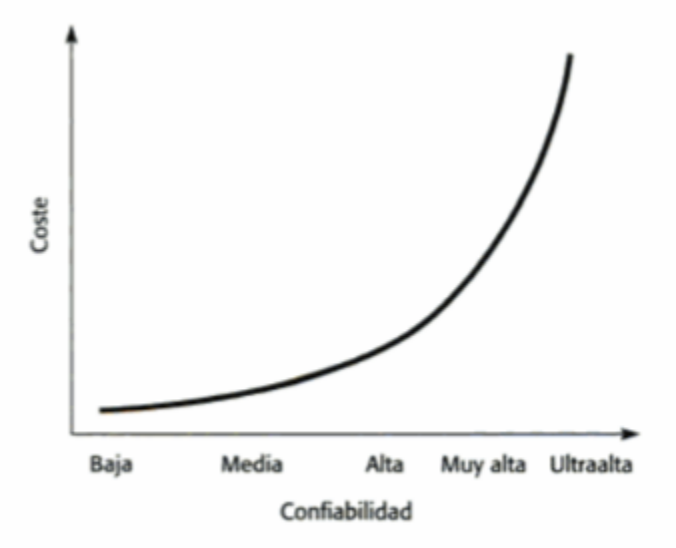


Figura 1. Curva de coste/confiabilidad. Fuente: Summerville 2005

Si bien estas dos propiedades guardan estrecha relación, no se puede deducir que los sistemas fiables estarán siempre disponibles y viceversa. Por ejemplo, algunos sistemas pueden tener como requisito una disponibilidad alta, pero una fiabilidad mucho más baja. Si los usuarios esperan un servicio continuo, entonces los requerimientos de disponibilidad son altos; sin embargo, si las consecuencias de un fallo de funcionamiento son mínimas y el sistema puede recuperarse rápidamente de dichos fallos, entonces el mismo sistema puede tener requerimientos de fiabilidad bajos.

Un ejemplo de un sistema en el que la disponibilidad es más crítica que la fiabilidad es una central telefónica. Los usuarios esperan escuchar un tono cuando descuelgan el teléfono, de forma que el sistema requiere un alto nivel de disponibilidad; sin embargo, si un defecto en el sistema hace que la conexión termine, esta es, a menudo, recuperable. Normalmente, los conmutadores incluyen facilidades para reiniciar el sistema y volver a intentar establecer a conexión. Esto puede realizarse de forma rápida y el usuario puede incluso no darse cuenta de que ha ocurrido un fallo de funcionamiento. Por lo tanto, la disponibilidad es el requerimiento clave en estos sistemas en vez de la fiabilidad.

Una diferencia adicional entre estas características es que la disponibilidad no depende simplemente del sistema en sí, sino también del tiempo necesario para reparar los defectos que hicieron que el sistema dejara de estar disponible. Por ello, si un sistema A falla una vez al año, y un sistema B falla al menos una vez al mes, entonces A es más fiable que B. Si en cambio, un sistema A tarda tres días en recuperarse después de un fallo, mientras que B tarda 10 minutos en reinicializarse, la disponibilidad de B a lo largo del año (120 minutos de tiempo sin servicio) es mucho mejor que la del sistema A (4,230 minutos sin servicio).

El elevado costo de un fallo de funcionamiento en los sistemas críticos implica que se deben utilizar métodos y técnicas confiables en su desarrollo. Como consecuencia, los sistemas críticos generalmente se desarrollan utilizando técnicas que han sido objeto de una extensa experiencia práctica. Uno de los motivos por los cuales se utilizan estas técnicas formales es que ayudan a reducir la cantidad de pruebas requeridas. Para sistemas críticos, los costos de verificación y validación generalmente son muy elevados, generalmente más del 50% del costo total del desarrollo del sistema.

Adicionalmente, a fin de minimizar los costos y tiempos de respuesta ante la materialización de un fallo de funcionamiento de un sistema crítico se requiere contar con mecanismos de monitoreo y atención de incidentes que permitan identificar y atender fallas de dicho sistema en un tiempo corto, así como mecanismos de continuidad operativa.

Existen tres tipos de componentes de un sistema susceptibles de generar un fallo en el sistema:

1. El hardware del sistema puede fallar debido a errores en su diseño, también debido a que los componentes fallan como resultado de errores de fabricación, o debido a que dichos componentes han llegado al final de su vida útil.
2. El software del sistema puede fallar debido a errores en su especificación, diseño o implementación.
3. Los operadores del sistema pueden provocar fallos en el sistema debido a un uso incorrecto del mismo. Si bien el hardware y el software son cada vez más fiables en la actualidad, los fallos derivados de un mal uso del sistema son la principal causa de fallos de funcionamiento en un sistema.

Estos fallos pueden interrelacionarse. Un componente de hardware que deja de funcionar implica que los operadores del sistema tengan que afrontar una situación inesperada y una carga de trabajo adicional. El estrés provocado por dicha carga puede ocasionar que los operadores cometan errores al manipular el software del sistema, provocando una falla. Lo anterior continúa repitiéndose si no existen implementados adecuados procedimientos para atender este tipo de situaciones.

2.2. Disponibilidad en sistemas críticos

Tal como se mencionó en la sección 2.1, la disponibilidad de un sistema computacional se refiere al periodo de tiempo en que un sistema esté en funcionamiento y sea capaz de proporcionar los servicios para los que está destinado. Matemáticamente, la disponibilidad del servicio puede medirse como sigue:

$$Disponibilidad = \frac{TA}{TT}$$

Donde:

TA = Tiempo de actividad del sistema en un periodo determinado.

TT = Tiempo total de operación requerido en un periodo determinado.

Una métrica generalmente utilizada para expresar el nivel de disponibilidad con el que cuenta un sistema es el "número de nueves". Por ejemplo, 526 minutos de indisponibilidad en un año resulta en un 99.9% de disponibilidad o "tres nueves de disponibilidad". La relación entre el número de nueves y el tiempo de indisponibilidad se encuentra reflejada en la siguiente tabla:

Tabla 1. Nivel de disponibilidad y rangos de indisponibilidad de un sistema.

Número de 9's	Nivel de disponibilidad	Periodo de indisponibilidad por año
1	90%%	876 horas
2	99%	88 horas
3	99.9%	9 horas
4	99.99%	50 minutos
5	99.999%	5 minutos
6	99.9999%	30 segundos

Un sistema con disponibilidad "normal" cuenta con al menos tres nueves, mientras que un sistema de alta disponibilidad cuenta con cuatro o cinco nueves de disponibilidad. También existen los sistemas de disponibilidad continua, los cuales alcanzan hasta seis nueves, lo que se traduce en solo unos segundos de disponibilidad por año.

La disponibilidad de un sistema depende de dos factores:

- **Indisponibilidad planeada:** Estos eventos son necesarios a fin de realizar actualizaciones del hardware que aloja los sistemas. De igual forma, muchas actualizaciones de software, incluyendo las actualizaciones de los sistemas operativos, aplicaciones y los manejadores de bases de datos, pueden requerir que el sistema sea detenido. Dependiendo del horario de operación del sistema estas actualizaciones podrían impactar en el nivel de disponibilidad del servicio. Mientras que algunos sistemas cuentan con ventanas

programadas donde se pueden realizar estas actualizaciones, usualmente durante fines de semana o durante la noche para aquellos sistemas que no operan 24x7; para el caso de sistemas de operación continua esta indisponibilidad planeada puede representar un componente importante en la indisponibilidad del sistema, al contar con las referidas ventanas. Asimismo, el riesgo de que las actualizaciones puedan no completarse en tiempo permanece para los sistemas que no operan 24x7. Cabe señalar que dichas ventanas normalmente son programadas en horarios no críticos a fin de minimizar el impacto al servicio.

- **Indisponibilidad no planeada:** Un evento que cause indisponibilidad no planeada requiere una recuperación inmediata del componente que falló o una conmutación a un componente redundante, si se cuenta con uno. A continuación se muestran las causas más comunes de indisponibilidad no planeada en un sistema:

Tabla 2. Causas de indisponibilidad en un sistema. Fuente: Gravic Inc. 2018

Causa de indisponibilidad	%
Errores operativos	41%
Fallas en el software	25%
Desastres naturales	15%
Fallas en el hardware	10%
Fallas en la red de datos	8%
Causas desconocidas	1%

Algunos sistemas críticos, cuyo horario de operación es continuo requieren contar con una arquitectura que permita mantener altos niveles de disponibilidad. A fin de lograrlo, se requiere eliminar los puntos únicos de falla del sistema, lo cual se logra mediante la implementación de redundancia en sus componentes. De igual forma, es necesario asegurar que la información de la operación del sistema se encuentre disponible en dichos componentes.

a. Redundancia en sistemas críticos que requieren alta disponibilidad

La redundancia es un componente esencial para alcanzar alta disponibilidad en un sistema dado que ofrece la oportunidad de recuperar rápidamente el servicio en una unidad operativa en lugar de acumular una indisponibilidad mayor mientras que el componente que falló es revisado, reparado y el servicio es recuperado.

La redundancia consiste en duplicar componentes críticos de un sistema para mejorar su disponibilidad. Cabe señalar que sólo porque unidades idénticas son utilizadas en un sistema, no significa que dichas unidades son redundantes; por ejemplo, aunque ambas alas de un avión son esencialmente idénticas, no son redundantes dado que el avión no volará sin ambas. De acuerdo con Bauer etal 2012 [2], existen dos categorías de redundancia:

- **Redundancia interna:** Considera la redundancia en el hardware y software, la cual es gestionada por una sola instancia del sistema. Por ejemplo, en un automóvil con un motor de seis cilindros, estos se encuentran integrados y parecen como una sola unidad para los usuarios finales y los mecánicos; sin embargo, la ocurrencia de una falla en alguno de los

cilindros resulta en una disminución del poder del motor, no en una falla crítica que causa que el automóvil deje de funcionar.

- **Redundancia externa:** Considera varios sistemas o componentes interrelacionados y configurados para funcionar en conjunto a fin de ofrecer mayor disponibilidad o capacidad a los usuarios finales. Estos sistemas pueden encontrarse en el mismo lugar o en ubicaciones separadas.

Algunas características importantes que considerar al implementar redundancia en un sistema son:

- **Aislamiento:** Los componentes redundantes deben estar aislados entre sí a fin de que, ante la ocurrencia de una falla en el componente principal, el respaldo no se afecte.

- **Dispersión:** Los componentes redundantes deben encontrarse geográficamente separados a fin de que un mismo evento no afecte a ambos simultáneamente.

- **Conmutación:** Un componente redundante es inútil si no puede realizar las tareas de su contraparte afectada, requiriendo como parte de su arquitectura:

    a) mecanismos de detección de fallas,
    b) posibilidad de conmutar a fin de determinar si es más conveniente restaurar el componente afectado o conmutar al respaldo y
    c) verificar que el respaldo está dando el servicio requerido.

    En la medida en que estas capacidades estén automatizadas, la conmutación es más rápida, confiable y menos propensa a errores; sin embargo, en muchos casos una o más de estas capacidades se consideran demasiado complejas de automatizar y la gestión de estos componentes recae en los operadores del sistema. En estos casos, es esencial establecer procedimientos bien documentados y realizar pruebas periódicas de los mecanismos implementados.

b. Replicación en sistemas críticos que requieren alta disponibilidad

Si bien la disponibilidad de un sistema es importante, un sistema con capacidad completa de procesamiento no es funcional si no cuenta con datos correctos para procesar. En algunos casos, también se requiere el acceso a un historial completo de la actividad del sistema.

Existen muchas razones por las cuales información importante puede perderse, desde fallas del sistema hasta fallas del centro de datos. Usualmente, esta información es protegida mediante el respaldo de esta a fin de que en caso de un evento que afecte la fuente principal de información del sistema, los datos puedan recuperarse del último respaldo. Cabe señalar que, en estos casos, la información procesada posterior al último respaldo, se pierde.

Cada sistema tiene diferente importancia para una organización, por lo que la relevancia de contar con la información que el sistema genera, varía dependiendo del tipo de sistema que se trate. Para

el caso puntual de los sistemas críticos de alta disponibilidad, especialmente aquellos con transacciones de alto valor, es necesario que no exista pérdida de datos.

El concepto de replicación se refiere al proceso de respaldar la información generada por un sistema en su nodo principal mediante la copia de dicha información a un nodo secundario. Es importante que al establecer un mecanismo de replicación se asegure la integridad y consistencia de la información en todos los nodos.

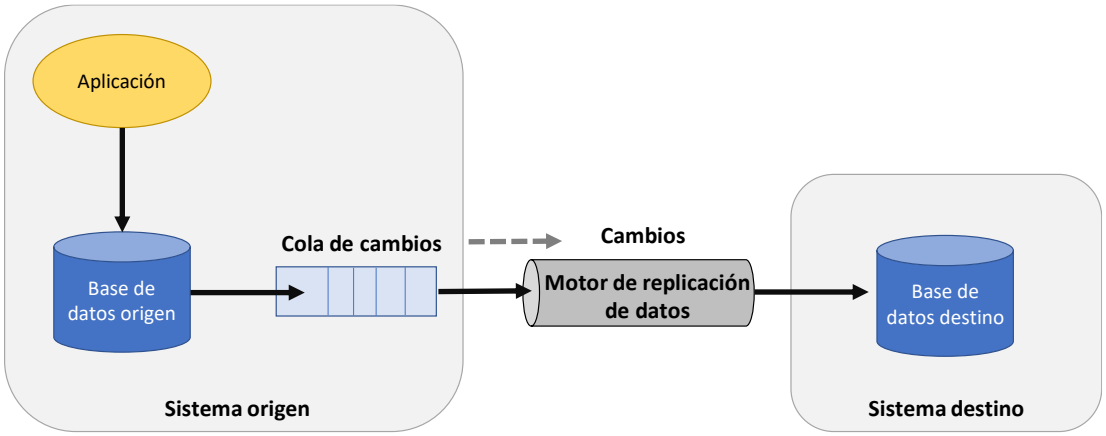


Figura 2. Diagrama conceptual de replicación de datos. Fuente: Gravic Inc. 2018

Dentro de un esquema de replicación, los motores de replicación de datos se encargan de recolectar los cambios realizados en la base de datos principal y los aplica a la base de datos objetivo. Los motores de replicación de datos son categorizados en las siguientes formas:

- **Hardware y software:** La replicación de hardware se implementa a través de los drivers de bajo nivel de los dispositivos, típicamente en el subsistema de almacenamiento. Para el caso de sistemas de alta disponibilidad, el software de alto nivel es el que se encarga de la tarea de replicación. El motor de replicación ejecutándose en los sistemas origen y objetivo, realizan la replicación. Esta es la única forma en la que los sistemas de alta disponibilidad activo-pasivo y activo-activo pueden ser implementados.
  Los motores de replicación de software leen los cambios de una cola y los envían al sistema objetivo para actualizar su base de datos. Mientras las actualizaciones en el sistema objetivo sean hechas en el mismo orden que en el sistema origen, la base de datos objetivo es consistente y puede ser usada por otras aplicaciones. Algunos motores de este tipo son multihilo para mejorar el rendimiento de la replicación.
  La replicación de software puede ser por evento, por transacción o por petición.

- **Síncrona y asíncrona:** Un motor de replicación asíncrona es completamente transparente para las aplicaciones ejecutándose en el nodo origen. Como se muestra en la Figura 3, los cambios a la base de datos origen se extraen hacia una cola y se envían, una vez realizados, a la base de datos objetivo. El resultado es que las bases de datos están sincronizadas, sin embargo, la base de datos objetivo tiene un retraso con respecto a la base origen por un intervalo corto de tiempo. Este intervalo de tiempo se conoce como latencia.

La latencia de una replicación asíncrona representa una posible pérdida de información en caso de una falla de la base de datos origen que debe considerarse al usar esta tecnología.

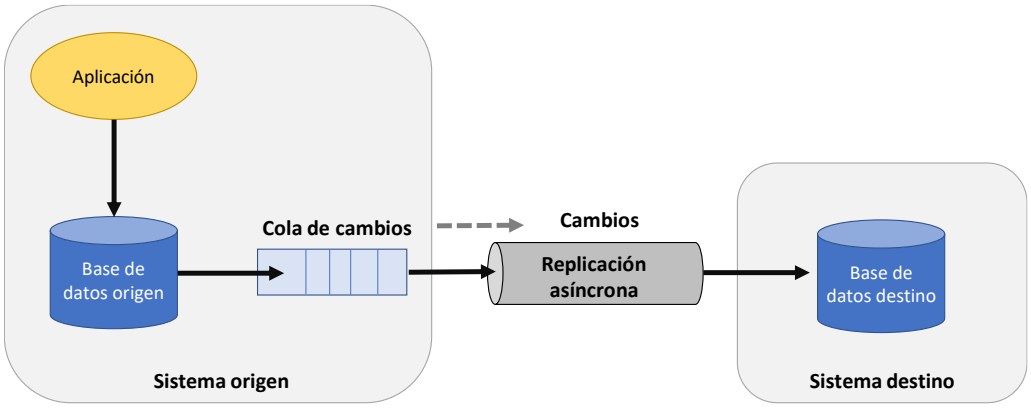


Figura 3. Motor de replicación asíncrona. Fuente: Gravic Inc. 2018

Un motor de replicación síncrona no realiza cambios permanentes a la copia de la base de datos a menos que esos cambios sean aplicados en todas las copias existentes; por lo que, si un nodo o la red fallan, no se pierde información. Con este mecanismo la latencia es cero.

Existen dos métodos para implementar la replicación síncrona: escrituras duales y confirmaciones coordinadas. Al utilizar escrituras duales, la aplicación debe esperar cada actualización de la base de datos origen para poder completar la copia en la base de datos destino. Es necesario esperar a que la transacción sea confirmada tanto localmente como en el nodo replicado para poder informar que la transacción está completa y continuar con el procesamiento. Este retraso está en función principalmente de la latencia en la comunicación entre nodos, la cual se relaciona con la distancia que separa los nodos y el tamaño de la transacción. Por lo tanto, los nodos deben estar ubicados cerca el uno del otro (en la misma ubicación o área geográfica) y conectados a través de un medio rápido (por ejemplo, fibra óptica).

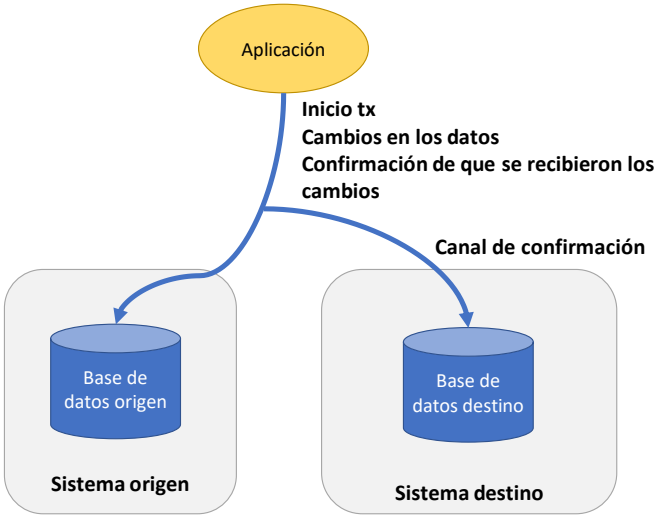


Figura 4. Esquema de replicación con escrituras duales. Fuente: Gravic Inc. 2018

Un motor de replicación de confirmaciones coordinadas es una combinación de técnicas de replicación síncrona y asíncrona, en donde el motor de replicación actúa como un miembro de la base de datos origen. Los cambios realizados por la aplicación son enviados a la base de datos destino asíncronamente a fin de no impactar en el funcionamiento de la aplicación, tal como se realiza en la escritura dual. El motor de replicación debe esperar sólo un tiempo de confirmación para verificar si la base de datos destino recibió toda la información de la transacción y pueda votar "Sí" para confirmar la transacción.

Por lo tanto, la técnica de confirmaciones coordinadas impone una latencia del periodo de confirmación con la base de datos destino, pero sólo al momento de la confirmación. Incluso si los nodos se encuentran separados por miles de kilómetros, la latencia con este método puede ser tan pequeña como decenas de milisegundos. La Figura 5 muestra un ejemplo de esquema de replicación de este tipo.

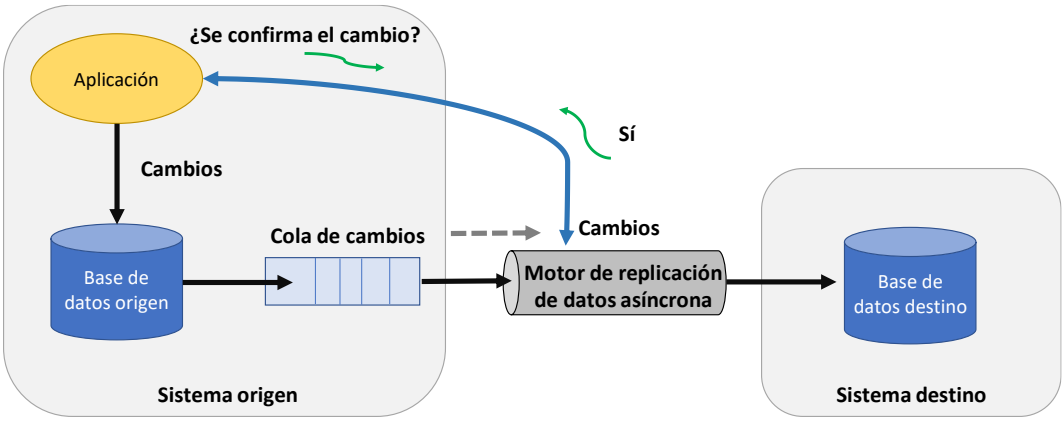


Figura 5. Esquema de replicación con confirmaciones coordinadas. Fuente: Gravic Inc. 2018.

- **Unidireccional y bidireccional:** Un motor de replicación unidireccional replica información de una base de datos origen a una base de datos destino. Las figuras 3, 4 y 5 son ejemplos de una replicación de este tipo. La replicación unidireccional es frecuentemente utilizada para mantener un sistema de respaldo pasivo sincronizado con un sistema activo. Esta configuración se denomina configuración activa-pasiva.
  Los sistemas con una configuración activa-pasiva tienen un tiempo de recuperación mucho mayor a los sistemas configurados como activo-activo.

  Un motor de replicación bidireccional replica la información entre dos bases de datos en ambas direcciones y actúa tanto como base de datos origen como destino. Dado que cada que se realiza un cambio en la información se refleja en todas las bases de datos, cada componente del sistema cuenta con la información necesaria para continuar operando.

  En la figura 6 se muestra el esquema de un motor de replicación bidireccional asíncrona. Es importante mencionar que los motores de replicación no son independientes, si no que

cuentan con una configuración que asegura que un cambio recibido no se envíe nuevamente a replicar al nodo del que se recibió.

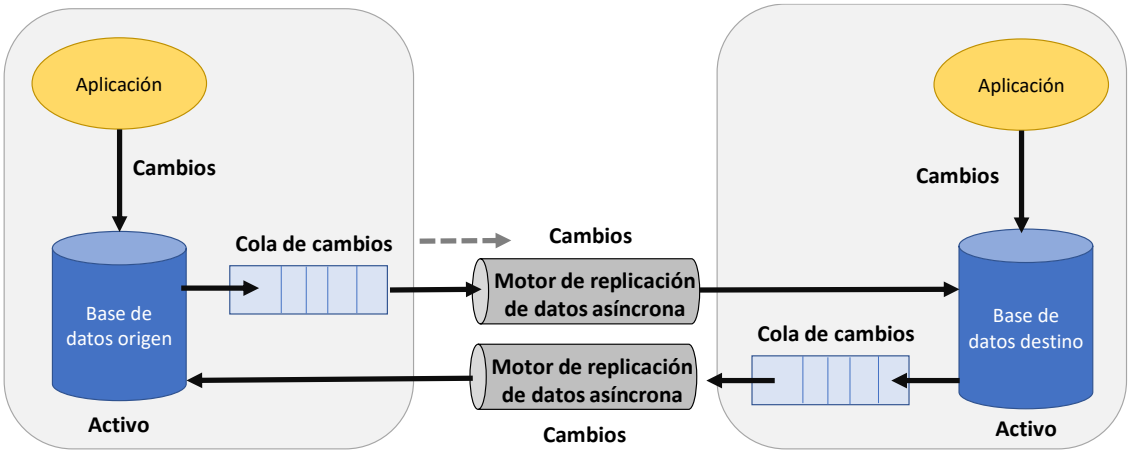


Figura 6. Ejemplo de motor de replicación bidireccional asíncrona. Fuente: Gravic Inc. 2018

Un inconveniente de la replicación bidireccional asíncrona es que es posible cambiar el mismo dato en cada una de las bases de datos durante su intervalo de latencia, por lo que los dos cambios se replican y sobrescriben el cambio realizado originalmente en ambas bases de datos. Como consecuencia, las bases de datos son diferentes entre sí y cuentan con datos erróneos. Este evento es conocido como “colisión de datos”.

En un sistema con replicación bidireccional síncrona se evitan por completo las colisiones de datos dado que el motor de replicación debe contar con candados en todas las copias de la información previo a que se realice algún cambio a fin de que sólo sea posible escribir un cambio en un dato específico por una aplicación a la vez. Un motor de replicación bidireccional síncrona puede ser implementado utilizando dos motores de replicación con confirmaciones coordinadas, tal como se muestra en la figura 7.

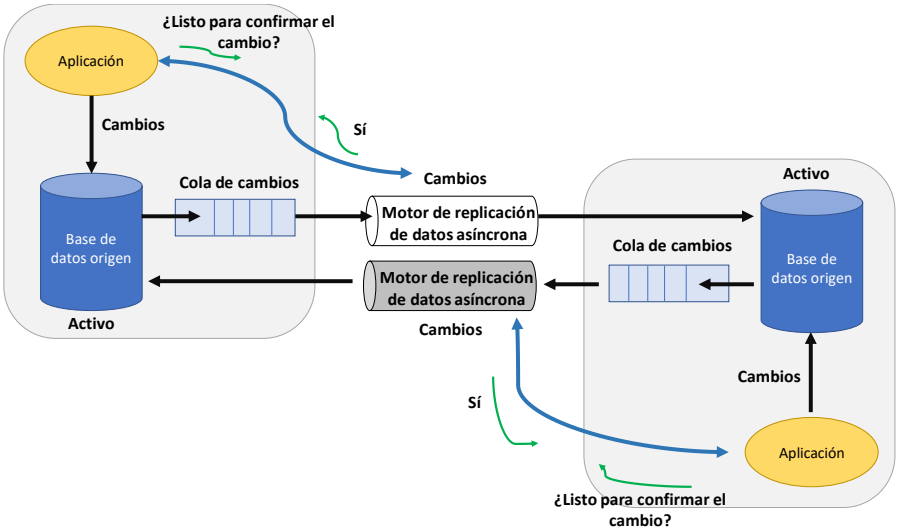


Figura 7. Ejemplo de un motor de replicación bidireccional síncrona. Fuente: Gravic Inc. 2018

c. Ventajas de sistemas con arquitecturas Activo-Activo

A continuación, se describen las principales ventajas de contar con un sistema activo-activo:

- Existe una menor afectación de usuarios en caso de una falla. En una arquitectura activo-pasivo cuando el nodo activo falla, el sistema completo se detiene; mientras que, en un sistema activo-activo, sólo los usuarios conectados al nodo que falló presentan una afectación.
- La conmutación de los usuarios afectados por una falla es más rápida, lo que permite cumplir con un tiempo de recuperación objetivo de unos cuantos segundos, ya que sólo es necesario enrutar las transacciones al nodo que continúa operando.
- El proceso de conmutación es más sencillo desde la perspectiva de que todos los nodos operan diariamente y, por lo tanto, su funcionamiento es probado constantemente. En los sistemas activo-pasivos se tiene el riesgo de que al momento de hacer la conmutación existan fallas en el funcionamiento de los componentes no probados constantemente o en el procedimiento que se debe seguir para lograrlo, retrasando la recuperación y ocasionando que no se puedan cumplir los tiempos objetivo de recuperación establecidos.
- El tiempo de indisponibilidad por mantenimientos en el sistema puede reducirse dado que, en caso de requerirlo, es posible dar de baja controladamente un nodo y mantener el/los otro(s) operando.
- El sistema se vuelve escalable en términos de la capacidad, ya que, para incrementarla, sólo es necesario añadir más nodos al sistema.
- Es más sencillo balancear la carga del sistema mediante el enrutamiento de las transacciones a diferentes nodos.

Si no es posible mantener una configuración activo-activo por completo, es recomendable que, si bien un nodo es el encargado de todo el procesamiento del sistema, se cuente con una arquitectura en donde exista redundancia tanto en los nodos de cómputo como de telecomunicaciones y que se mantenga la información replicada en cada uno de ellos. De esta manera, no es necesario realizar procesamiento distribuido; sin embargo, se reduce el tiempo de indisponibilidad del sistema al recuperar el sistema después de una falla.

2.3. Mecanismos de monitoreo para sistemas críticos

Las métricas, monitoreo y alertamiento son conceptos interrelacionados que forman parte de un sistema de monitoreo y permiten proveer visibilidad del estado del software y de la infraestructura que lo soporta para asegurar la confiabilidad y estabilidad de los servicios.

Las métricas representan las medidas de la utilización de recursos o comportamiento que es observado en un sistema. Pueden ser un resumen de utilización a bajo nivel provisto por los sistemas operativos, o puede ser información de alto nivel atada a una funcionalidad específica de un componente, como peticiones realizadas por segundo en un conjunto de servidores web. Algunas métricas son representadas con relación a una capacidad total, mientras que otras son representadas como una proporción que indica qué tan ocupado está un componente.

Mientras las métricas representan la información en un sistema, el monitoreo es el proceso de recolectar, conjuntar y analizar esos valores para mejorar el conocimiento que se tiene del comportamiento y características de los sistemas. La información de diferentes partes del sistema se conjunta en un sistema de monitoreo, el cual es responsable de almacenar, analizar, visualizar e iniciar respuestas automáticas cuando los valores cumplen con ciertos requerimientos.

El alertamiento es el componente de un sistema de monitoreo que ejecuta acciones con base en cambios en métricas definidas. Para definir una alerta se requieren dos componentes:

1) una condición basada en una métrica o un umbral definido,
2) una acción que se deberá ejecutar una vez que los valores alcancen condiciones inaceptables.

Uno de los principales beneficios de un sistema de monitoreo es permitir a los administradores definir qué situaciones específicas se requiere gestionar, mientras que el monitoreo sigue ejecutándose de forma pasiva a fin de identificar los cambios en el estado del sistema. Si bien el objeto principal del alertamiento es que un ser humano preste atención al cambio de estado de un sistema; el contar con procesos automáticos de respuesta es un mecanismo importante para asegurar que las notificaciones hacia los seres humanos únicamente se activan en situaciones donde se requiere tomar decisiones que no se tenían previamente consideradas. La alerta misma debe contener información sobre cuál es el error o la alarma y sobre el lugar donde el administrador puede obtener más información, ya sea una función en un código o un equipo de cómputo en donde se activó la alarma.

a. Elementos por monitorear en un sistema

Los tipos de valores que se monitorean y la información que se rastrea cambia cada que se realizan actualizaciones al sistema o a la infraestructura que lo aloja. Dado que los sistemas normalmente funcionan de forma jerárquica, es útil que las métricas que se definan para el monitoreo consideren los siguientes niveles.

- Servidores en donde se aloja el sistema/servicio

En el fondo de la jerarquía de las métricas primitivas se encuentran las métricas enfocadas en evaluar el desempeño de un equipo individual, sin importar qué aplicaciones o servicios aloja. Las métricas más comunes en este nivel son:

1) utilización de CPU,
2) utilización de memoria,
3) utilización de espacio en disco y,
4) estado de los procesos que se están ejecutando en la máquina.

- Aplicaciones

Estas métricas están relacionadas con unidades de procesamiento que dependen en el nivel de recursos que posea la máquina que aloja el sistema o servicio. Los tipos específicos de métricas a elegir dependen del servicio que se provee, sus dependencias y los componentes con los que

interactúa. Las métricas en este nivel son indicadores del desempeño o la carga de una aplicación y te permiten determinar si una aplicación está funcionando correctamente y con eficiencia:

1) indicadores de error o éxito,
2) fallas del servicio o reinicios
3) desempeño y latencia en las respuestas y,
4) utilización de recursos.

- Conectividad entre las redes de comunicación

En general para todos los tipos de infraestructura, los indicadores de conectividad entre los equipos son medidores importantes de la disponibilidad y son esenciales para asegurar que los servicios son accesibles a otras máquinas para sistemas que abarquen más de un equipo. Es necesario monitorear el buen funcionamiento de las redes de comunicación, así como el desempeño de estas enfocándose en: 1) la conectividad entre equipos; 2) indicadores de errores y pérdida de paquetes; 3) latencia y 4) utilización de ancho de banda.

- Conjunto de servidores

Cuando un sistema cuenta con infraestructura escalable horizontalmente, otra capa que es necesario monitorear es el conjunto de servidores. Si bien las métricas individuales son útiles, a gran escala un servicio es mejor representado como la capacidad de un conjunto de equipos de cómputo de ejecutar las instrucciones definidas y responder adecuadamente a las peticiones realizadas. Este tipo de métricas es una extrapolación a un nivel más alto de las métricas de los servidores y de las aplicaciones mencionadas anteriormente. La información que se requiere identificar en este nivel es:

1) utilización de recursos en conjunto,
2) indicadores de ajuste de escala y,
3) degradación de servicio en las instancias.

- Dependencias externas

Otras métricas que pueden ser incorporadas a un sistema de monitoreo son las relacionadas con dependencias externas. Frecuentemente los servicios proveen visores de estado o una interfaz gráfica para identificar fallas en el servicio; sin embargo, incorporar el rastreo de estas fallas dentro del sistema de monitoreo, así como las interacciones que tiene un servicio, puede ayudar a identificar problemas con las dependencias que pudieran afectar las operaciones. Algunos elementos que monitorear en este nivel son:

1) estado del servicio y disponibilidad,
2) indicadores de error y éxito,
3) indicadores de ejecución y costos operacionales y,
4) agotamiento de los recursos.

b. Factores por considerar al implementar un sistema de monitoreo

En los párrafos anteriores se expusieron los niveles que es recomendable considerar en un sistema de monitoreo; sin embargo, existen múltiples factores que pueden intervenir en cuáles niveles se determinará monitorear para un servicio dado. A continuación, se mencionan los factores a considerar para definir qué elementos de un sistema se monitorearán:

A. **Recursos disponibles para monitorear.** Es importante considerar la infraestructura, presupuesto y recursos humanos con los que se cuenta a fin de delimitar el alcance del sistema de monitoreo.
B. **La complejidad y objetivo del servicio a monitorear.** La complejidad de las aplicaciones y sistemas utilizados para proveer un servicio pueden tener un impacto alto en los elementos que se determina monitorear. Los elementos que pueden ser críticos para algunos sistemas pueden no serlo para otros.
C. **El ambiente en el que se ejecutan los sistemas y aplicaciones.** El contar con un monitoreo robusto es relevante tanto en los sistemas productivos, como en los ambientes de prueba, aunque los umbrales de monitoreo pueden variar entre ambos.
D. **La probabilidad de que las métricas sean útiles.** Uno de los factores más importantes en la determinación de monitorear o no un elemento del sistema está relacionado con el potencial que este puede tener en el futuro. Cada métrica incrementa la complejidad del sistema de monitoreo y consume sus recursos. Adicionalmente, la necesidad de información puede cambiar en el tiempo, requiriendo reevaluar los elementos a monitorear en intervalos regulares.

c. Características importantes de un sistema de monitoreo

Si bien existen múltiples tipos de sistemas de monitoreo, a continuación, se describen las características con las que todos deberían contar:

- **Ser independientes de la infraestructura del servicio monitoreado.** Uno de los requerimientos básicos de un sistema de monitoreo adecuado es que sea externo a otros servicios. Mientras que en ocasiones es útil agrupar servicios, las responsabilidades principales del sistema de monitoreo y su capacidad de diagnosticar problemas hacen que este tipo de sistemas requieran ser accesibles en todo momento. Los sistemas de monitoreo necesariamente tendrán un efecto en los sistemas monitoreados; sin embargo, este efecto debe ser mínimo a fin de reducir la posibilidad de afectar el desempeño del sistema monitoreado e incrementar la confiabilidad del monitoreo implementado ante la ocurrencia de fallas en este.

- **Ser confiables.** Dado que un sistema de monitoreo es responsable de recabar, almacenar y proveer acceso a información de alto valor, es importante poder confiar en que dicho sistema funcionará de la manera esperada diariamente. Las fallas en estos sistemas o alertamientos equivocados pueden tener un impacto dañino en la capacidad de gestionar la infraestructura de forma efectiva.

- **Que faciliten el uso de resúmenes o vistas detalladas.** La capacidad de desplegar resúmenes de alto nivel y poder requerir mayor detalle de la información a demanda es una característica importante para asegurar que los datos de las métricas son útiles para los operadores. El diseño de tableros que presenten la información más vista de una forma simple y entendible ayuda a los usuarios a entender cuál es el estado general del sistema en un vistazo. De igual importante es la capacidad de poder mostrar el detalle de un elemento específico, por ejemplo, el ajustar la escala de una gráfica, eliminar métricas innecesarias y subrayar información de múltiples sistemas es útil para realizar investigaciones o análisis de causas raíz de incidentes.

- **Contar con una estrategia efectiva para mantener información histórica.** Un sistema de monitoreo es mucho más útil cuando cuenta con información que permite establecer tendencias, patrones y consistencias a lo largo de un periodo de tiempo. Mientras que idealmente, toda la información puede ser almacenada en su granularidad original, las restricciones de costos y recursos pueden causar que sea necesario eliminar la información más vieja. Los sistemas de monitoreo que cuentan con la flexibilidad de trabajar tanto con información resumida como con el detalle completo, proveen una amplia gama de opciones para gestionar una cantidad aún mayor de información.
  Una característica que se puede incorporar a los sistemas de monitoreo es la facilidad de importar grupos de datos existentes. Si reducir la densidad de la información histórica no es una opción, el cargar fuera de línea la información vieja en una solución de almacenamiento a largo plazo, es una mejor alternativa. De esta forma, no se requiere mantener toda la información en el sistema, pero puedes cargarla nuevamente cuando se requiera realizar un análisis particular.

- **Capacidad de correlacionar información de diferentes fuentes.** Un sistema de monitoreo es responsable de proveer una vista de la infraestructura en general, por lo que requiere mostrar información relacionada, incluso si esta información es de diferentes sistemas o tiene diferentes características. Los administradores deben ser capaces de conjuntar la información de sus sistemas a voluntad y conocer el estado general de la infraestructura. El poder asegurar que los diferentes sistemas estén sincronizados es un prerrequisito para poder correlacionar información proveniente de distintos sistemas de forma confiable.
- **Facilidad de incorporar nuevas métricas o infraestructura.** Con el objeto de que el sistema de monitoreo cuente con una representación precisa del sistema que se está monitoreando, es necesario contar con la capacidad de realizar ajustes cuando los equipos e infraestructura cambian, se actualizan o se eliminan. En este último caso, se requiere mantener la información generada por el equipo que se dará de baja.
  De igual forma, es necesario poder definir nuevas métricas dentro del sistema. Lo anterior depende de la forma en la que se configuran dichas métricas en el sistema de monitoreo, así como en la variedad y calidad de mecanismos disponibles para enviar información al sistema.
- **Alertamiento flexible y robusto.** Uno de los aspectos más importantes a evaluar de un sistema de monitoreo son sus capacidades de alertamiento. Adicional a que se requieren requerimientos de confiabilidad estrictos, el alertamiento necesita ser suficientemente flexible para notificar a los operadores a través de distintos medios y suficientemente robusto para activar las respuestas de notificación de acuerdo con los umbrales definidos. Al definir los parámetros para las alertas se debe considerar el no sobre alertar a los

operadores, para lo cual se necesita contar con un análisis de los comportamientos del sistema a fin de diferenciar comportamientos momentáneos, de aquellos que son repetitivos.

Los sistemas de monitoreo son implementados para todo tipo de servicios y sistemas, sin embargo, cobran especial importancia cuando los sistemas a monitorear son sistemas de misión crítica.

2.4. Sistemas de gestión de continuidad de negocio

La continuidad de negocio es la disciplina de desarrollar, implementar y mantener estrategias y procedimientos que permitan identificar las amenazas potenciales a una organización, los impactos a los procesos críticos del negocio si dichas amenazas se materializan, así como el detalle de las actividades a realizar a fin de construir un marco de resiliencia con la capacidad de contar con una respuesta efectiva que salvaguarde los intereses y reputación de cualquier organización.

A fin de contar con un marco de continuidad de negocio sólido, las mejores prácticas recomiendan implementar un sistema de gestión. Los componentes de un Sistema de Gestión de Continuidad de Negocio (SGCN) de acuerdo con la norma ISO 22301, la cual define los requerimientos para implementar un SGCN, son los siguientes:

1. **Alcance.** Establece qué servicios o productos formarán parte del sistema de gestión considerando la misión y objetivos de la organización; así como sus requerimientos normativos y regulatorios.
2. **Política.** Establece un marco para definir los objetivos de continuidad de negocio, determina la tolerancia al riesgo, define los roles y responsabilidades dentro del sistema de gestión, así como el compromiso de contar con una mejora continua del sistema.
3. **Objetivos de continuidad de negocio.** Estos objetivos deben ser consistentes con la política definida; tomar en consideración el nivel mínimo de productos y servicios que requiere la organización para lograr sus objetivos, ser medibles, ser evaluados y actualizados conforme se requiera.
4. **Análisis de riesgos.** Identifica las potenciales amenazas a las que está expuesta una organización con el propósito de establecer controles o mecanismos para mitigar el impacto que dichas amenazas podrían causar a la organización en caso de materializarse con respecto a la probabilidad de ocurrencia.
5. **Análisis de impactos al negocio (BIA)[1].** Es la base para definir las estrategias de continuidad de negocio que se implementarán. Identifica las actividades críticas para proveer los servicios o productos; evalúan los impactos en el tiempo de no realizar dichas actividades; fijan tiempos para la recuperación de estas actividades críticas a un nivel mínimo aceptable, tomando en cuenta el tiempo en el que el impacto de no recuperar la operación se convierte en inaceptable; e identifica las dependencias y recursos necesarios para realizar cada una de las actividades.
6. **Estrategias de continuidad de negocio.** Definición de las estrategias a implementar para asegurar que ante la materialización de algún evento que cause una disrupción, la provisión

[1] Por sus siglas en inglés Business Impact Analysis.

de los productos y servicios continúe a un nivel mínimo aceptable con base en los resultados obtenidos de los análisis de riesgos y de impactos al negocio.

7. **Planes para atención de incidentes.** Establece las actividades y responsables de atender la ocurrencia de cualquier evento que pudiera derivar en una afectación a la provisión de los productos y servicios, considerando la evaluación del origen y alcance del incidente y de su impacto potencial; la activación del protocolo de comunicación interno y externo; así como, la activación de alguno de los mecanismos de continuidad implementados, en caso de ser necesario.
8. **Planes de continuidad de negocio.** Detalle de las actividades a realizar para cada una de las estrategias de continuidad de negocio definidas, incluyendo los roles y responsabilidades asignados al personal involucrado, así como los requerimientos con los que se requiere contar para la activación de cada estrategia.
9. **Planes de regreso a la operación normal.** Detalle de las actividades a realizar una vez que el incidente fue solucionado para regresar el servicio a su operación normal, incluyendo los roles y responsabilidades involucrados.
10. **Planes de pruebas.** Establecen los lineamientos para ejercitar periódicamente las estrategias y planes implementados considerando el cumplimiento de los objetivos del SGCN a fin de identificar áreas de oportunidad.
11. **Planes de evaluación periódica.** Establecen los lineamientos para la realización de revisiones internas a fin de identificar actualizaciones o áreas de mejora en los componentes del SGCN.

3. Trayectoria profesional

Desde hace cinco años me encuentro laborando en una institución financiera, en un área dedicada a la administración, pruebas, operación y soporte de los sistemas que la misma institución desarrolla y a través de los cuales ofrece sus servicios. Mis primeros tres años de carrera, fui analista de continuidad y mis actividades principales eran:

1. Actualización del Sistema de Gestión de Continuidad de Negocio.
2. Elaboración y seguimiento del calendario anual de pruebas internas y externas de los mecanismos de continuidad implementados.
3. Coordinación y monitoreo de los mantenimientos a la infraestructura en la que se alojan los sistemas que administramos.
4. Seguimiento a los incidentes operativos suscitados y a la implementación de las acciones correctivas y preventivas.

Durante los últimos dos años, he desempeñado el puesto de Jefe de Operación de los sistemas que administra el área X. Si bien en mi puesto anterior, tuve la oportunidad de actualizar, e incluso, implementar nuevos mecanismos de continuidad, en mi puesto actual coordino la ejecución de dichos mecanismos ante la ocurrencia de un incidente y conozco más a fondo los sistemas administrados en el área. A continuación, se describen mis principales funciones:

1. Asegurar que se ejecuten los procesos requeridos para el buen funcionamiento de los sistemas en tiempo y forma.
2. Coordinar la gestión de los incidentes operativos.

3. Coordinar la ejecución de los procedimientos de continuidad implementados, si es que se determina su activación.
4. Participar en la liberación de nuevas versiones de los sistemas al ambiente productivo.
5. Participar en la ejecución de las actividades operativas necesarias ante la realización de mantenimientos a la infraestructura donde se alojan los sistemas.

4. Antecedentes y problemática

Algunas instituciones financieras administran sistemas críticos entre cuyas funciones principales se encuentran:

A. Administrar los recursos de los cuentahabientes y permitir la transferencia de estos al sistema B a fin de que pueda cumplir con sus obligaciones financieras.
B. Proveer la infraestructura necesaria para procesar transferencias en diferentes divisas.
C. Proporcionar recursos adicionales a los cuentahabientes en el sistema B a través de operaciones a un plazo establecido que involucran valores gubernamentales.
D. Procesar la parte en moneda nacional de operaciones cambiarias realizadas con instituciones financieras del extranjero mediante la utilización del sistema B.

Estos sistemas se consideran críticos dado en caso de que ocurra una indisponibilidad del servicio existiría una afectación económica importante para los cuentahabientes toda vez que estarían en riesgo de incumplir obligaciones financieras por montos relevantes. Otro punto por destacar es que existen interdependencias entre los sistemas mencionados, lo cual agrega un grado adicional de complejidad en la administración de la infraestructura y los procesos que deben ejecutarse, ya que de no ejecutarse de forma correcta esta falla podría convertirse en un riesgo sistémico. Por ejemplo, en caso de que el sistema A sufra una afectación que imposibilite la transferencia de los recursos al sistema B, este último no podría procesar transferencias y a su vez, afectaría el buen desempeño del sistema C y D al no ser posible entregar los recursos a los cuentahabientes derivados de las operaciones realizadas.

Dado lo anterior, se requiere contar con mecanismos de monitoreo que permitan verificar el buen funcionamiento de los procesos de cada sistema en tiempo real, así como con mecanismos de alertamiento que notifiquen a los administradores del sistema respecto a una falla en la ejecución de los procesos o en la infraestructura de cómputo y telecomunicaciones en la que se aloja. Cabe señalar que también es necesario definir umbrales que permitan a los administradores prevenir la materialización de fallas o en caso de que estas sean inevitables, permitan poner en marcha procedimientos de continuidad operativa para corregir el problema o recuperar el servicio.

El horario de operación de los sistemas A y B es 24x7 y el nivel de disponibilidad esperado supera el 99.9%, por lo que es de suma importancia contar con procedimientos de continuidad eficientes que consideren la evaluación tanto del servicio afectado como de sus interdependencias, para poder determinar las acciones a realizar para recuperar la funcionalidad esperada.

Adicional a que se requiere que la funcionalidad de los sistemas se recupere en el menor tiempo posible, otra característica importante a considerar en la definición de los mecanismos de continuidad operativa para los sistemas A, B, C y D ante la ocurrencia de algún tipo de fallo, es definir

un punto objetivo de recuperación que asegure que no existe pérdida de información. El perder información durante una falla, dada la criticidad de los sistemas A, B, C y D, podría significar pérdidas monetarias tanto para la institución financiera como para sus cuentahabientes dado que registros de transferencias que fueron procesadas previo al incidente, podrían borrarse o su finalidad quedar en duda, obligando a los cuentahabientes a realizarlas nuevamente a través del mismo sistema o en caso de que estas representen el pago de alguna obligación con fechas límite, a realizarlas por algún medio alterno.

Respecto de sistemas críticos implementados en los sistemas financieros, el Banco de Pagos Internacionales (BIS[2]) publicó los Principios para las Infraestructuras del Mercado Financiero [1], en donde se establecen los lineamientos que deben cumplir las Infraestructuras del Mercado Financiero para asegurar una adecuada gestión de riesgos. Si bien estos principios están enfocados en infraestructuras centrales con implicaciones sistémicas en el funcionamiento de una economía, estas prácticas pueden ser igualmente utilizadas para establecer un estándar para la administración, control y monitoreo de sistemas críticos en el ámbito de operaciones financieras independientemente de si estas son o no Infraestructuras del Mercado Financiero. Relativo a la gestión de riesgos operacionales, los principios establecen que es necesario que una organización que administra sistemas con finalidades de administración de recursos cuente con:

1. Políticas, controles internos y procedimientos para mitigar y gestionar sus fuentes de riesgos. A fin de asegurar el buen funcionamiento de dichos controles se recomienda alinear los procesos operativos a las mejores prácticas publicadas; así como medir y evaluar el desempeño de los controles implementados, para identificar y corregir deficiencias.

   Las evaluaciones de los controles internos y procedimientos se deben realizar periódicamente y a fin de evitar el riesgo de que las actividades de las pruebas interfieran con la operación normal, es recomendable que las pruebas se ejecuten en un ambiente de pruebas, el cual debe, en la medida de lo posible, replicar el ambiente de producción, incluyendo los controles de seguridad.

2. Objetivos de confiabilidad sobre el servicio y políticas establecidas diseñadas para alcanzar estos objetivos, los cuales sirven para evaluar la eficiencia, efectividad y desempeño de los controles implementados.

3. Procedimientos bien documentados para identificar, reportar, analizar, resolver y evaluar los incidentes en la operación de los servicios.

4. Un sistema de gestión de continuidad de negocio con objetivos bien establecidos que permitan una recuperación oportuna del servicio. Entre los objetivos definidos se deben considerar el tiempo objetivo de recuperación y el punto objetivo de recuperación.

De acuerdo con lo establecido anteriormente, la institución financiera para la que laboro estableció sistemas de monitoreo en tiempo real a nivel infraestructura de cómputo y telecomunicaciones,

[2] Bank of International Settlement, por sus siglas en inglés.

considerando umbrales relativos al desempeño de los equipos, tales como monitoreo de uso de memoria, espacio en disco, utilización del CPU. Por otro lado, se implementaron sistemas de alertamiento y monitoreo en donde, de acuerdo con el horario de operación de cada uno de los sistemas, se verifica que los procesos que conforman cada sistema se encuentren activos y funcionando correctamente. En caso de la ocurrencia de una falla, se tienen configuradas alertas vía correo electrónico dirigidas tanto a personal técnico como operativo, en donde entre otras cosas se informa el componente de infraestructura que presenta la alerta, el nombre del proceso y si este se encuentra activo o inactivo.

Se realizó un análisis de riesgos y de impactos al negocio a fin de implementar una política de continuidad de negocio que permitiera mitigar los principales riesgos y cumplir con los niveles de disponibilidad establecidos. Se definió un tiempo objetivo de recuperación de dos horas para los sistemas A, B, C, D; así como un punto objetivo de recuperación de cero minutos tomando como base las recomendaciones de los PFMI.

Se implementó un protocolo de gestión de incidentes alineado a las buenas prácticas de ITIL, el cual considera la intervención de una mesa de ayuda, quien es la principal encargada de monitorear los sistemas a nivel infraestructura y procesos, para realizar el diagnóstico inicial de cualquier tipo de incidente y brindar el primer nivel de atención. Asimismo, se establecieron grupos de segundo nivel de atención, con mayor experiencia en el funcionamiento de los sistemas y sus interdependencias.

A fin de llevar un seguimiento puntual de los casos presentados, se adquirió una herramienta de registro de incidentes en donde se definieron los grupos encargados de la atención, la clasificación de la criticidad de cada incidente, así como los niveles de servicio esperados de acuerdo con dicha clasificación.

Entre los mecanismos de continuidad operativa que se implementaron se encontraba el contar con un sitio operativo secundario con suficientes recursos, capacidades y funcionalidades para continuar con la operación en caso de la ocurrencia de un incidente que afectara el sitio principal; así como contar con un centro de datos alterno con infraestructura de respaldo.

Entre los centros de datos, se implementó infraestructura de telecomunicaciones redundante y configurada en alta disponibilidad. Adicionalmente, como parte de la arquitectura de los sistemas se implementó infraestructura de cómputo de respaldo en espejo a la de producción en dicho centro de datos secundario, con una configuración activo-pasivo y una replicación síncrona entre los distintos componentes.

Se establecieron procedimientos técnicos y operativos para recuperar la operación de cada sistema en la infraestructura de respaldo ante la falla de la infraestructura principal. Estos procedimientos contenían el detalle de las actividades a realizar por el personal una vez que se determinaba activar este mecanismo de continuidad.

A fin de poder evaluar periódicamente tanto el funcionamiento de los propios sistemas como los mecanismos de continuidad operativa implementados, se implementó un ambiente de pruebas con infraestructura con la misma capacidad que la que opera en producción. Esta infraestructura es de

uso tanto interno como externo, es decir, los cuentahabientes pueden conectarse a este ambiente a fin de simular la operación de un día normal.

Adicionalmente, se estableció un esquema de pruebas internas anuales del procedimiento de traslado de la operación a infraestructura de respaldo a fin de evaluar, principalmente, al ejecutarse el procedimiento se cumplía con el tiempo y punto objetivo de recuperación definidos y si las actividades documentadas eran suficientemente claras y completas para el personal que debía realizarlas.

Si bien la institución financiera contaba con un marco de continuidad de negocio sólido, se requería realizar una evaluación a fin de verificar si dicho marco cumplía con las recomendaciones del estándar internacional ISO 22301:2012; así como realizar la actualización y pruebas periódicas de los componentes del sistema de gestión de continuidad de negocio.

5. Evaluación de la adopción del ISO 22301:2012 Sistemas de Gestión de Continuidad de Negocio

El esquema de continuidad del área responsable de la administración de los sistemas A, B, C y D, en adelante Área X, se encontraba alineada a la norma BS 25999, la cual, en su momento, representaba las mejores prácticas relativas a la gestión de continuidad de negocio, principalmente enfocada a la recuperación de los recursos que permiten el funcionamiento normal de un negocio en caso de la ocurrencia de un desastre.

Durante 2012, la BS 25999 fue reemplazada por el ISO 22301: Requerimientos de un Sistema de Gestión de Continuidad de Negocio, el cual es un estándar aceptado mundialmente que provee un marco de referencia para gestionar la continuidad de negocio en una organización, el cual si es implementado correctamente, disminuye la posibilidad de ocurrencia de un incidente disruptivo y, en caso de que este llegue a materializarse, asegura que la organización está preparada para responder en forma adecuada y, de esta forma, reducir el daño potencial del incidente.

Dado lo anterior, el Área X determinó realizar una evaluación para determinar qué tan alineado se encontraba su marco de continuidad con el ISO 22301, el cual fue un proyecto en el que participé como miembro del equipo de continuidad y las actividades principales de realizar la evaluación quedaron a mi cargo. Dicha evaluación consistió en dos fases:

1) Autoevaluación con respecto al estándar
2) Atención de áreas de oportunidad identificadas

5.1. Autoevaluación con respecto al estándar ISO 22301

Elaboramos un plan de trabajo, el cual se enfocaba en realizar un inventario de la información con la que se contaba, la cual incluía, entre otras cosas, el análisis de riesgos, el análisis de impactos al negocio, los planes de continuidad, los planes de pruebas; así como los resultados de las pruebas realizadas y en evaluar si dicha información contenía los componentes clave establecidos por el estándar, detallados en la sección 2.4 del presente documento. A continuación, se listan los principales hallazgos identificados de la autoevaluación que realizamos utilizando como base la documentación existente de la norma, así como la documentación generada por el área X durante los años pasados:

1. Si bien los objetivos de continuidad de negocio del Área X, así como los responsables de la gestión de continuidad y la tolerancia al riesgo eran conocidos por las áreas técnicas y operativas encargadas del funcionamiento de los sistemas A, B, C y D, no se contaba con documentación que definiera el alcance, política y objetivos del SGCN implementado.

2. Con respecto al análisis de riesgos, confirmamos que el Área X contaba con una evaluación de riesgos que calificaba los riesgos de acuerdo con su criticidad e indicaba los controles o estrategias de continuidad implementados para mitigar su ocurrencia. Cabe señalar que era necesario realizar una actualización a la documentación con la que se contaba a fin de reflejar la metodología utilizada para identificar y cuantificar los riesgos a los que estaba expuesta el Área X. Adicionalmente, como parte del ciclo de actualización periódica era necesario evaluar nuevamente los riesgos y los controles implementados.

3. En relación con el análisis de impactos al negocio, identificamos que, si bien se contaba con servicios críticos definidos, se requería documentar cuáles eran los procesos críticos dentro de cada servicio; así como las interdependencias que existían entre cada uno de ellos. Cabe señalar que para cada servicio crítico se contaba con un análisis de cuál era el impacto hacia los participantes con respecto a la duración del incidente.

4. El área X contaba con las siguientes estrategias de continuidad implementadas aplicables a los sistemas A, B, C y D:
    a. Imposibilidad de operar desde las instalaciones principales debido a factores externos.
    b. Indisponibilidad del personal encargado de la operación para asistir a las instalaciones de la organización.
    c. Indisponibilidad de la infraestructura de cómputo en donde se alojan los sistemas A, B, C y D.

    Considerando los riesgos identificados en el análisis realizado previamente, así como los controles ya implementados, las estrategias de continuidad estaban bien enfocadas a asegurar una respuesta adecuada ante un incidente.

5. Con respecto al plan de atención a incidentes, con base en la información recopilada con ayuda del personal de la mesa de ayuda, identificamos que si bien existía una relación bien documentada entre la atención del primer y segundo nivel, no había un responsable de la evaluación del impacto del incidente considerando el tiempo estimado de solución con respecto al tiempo objetivo de recuperación a fin de determinar si era posible esperar a que

el área técnica pudiera resolver el incidente, o si se debería iniciar con los preparativos de activación de alguno de los mecanismos de continuidad implementados.

Dado que, ante la ocurrencia de un incidente, los grupos de atención nivel 1 y 2 se encuentran enfocados completamente en intentar resolver el incidente, identificamos que era necesario contar con un tercer grupo que se encargara de la evaluación del impacto del incidente y de dar seguimiento a las acciones realizadas por todos los involucrados.

6. Identificamos que las estrategias de continuidad se encontraban documentadas en el plan de continuidad de negocio y que para cada una de ellas se tenían establecidos objetivos de recuperación, los cuales eran consistentes con los RTO definidos; procedimientos para la implementación de la estrategia; roles y responsabilidades; protocolos de comunicación y actuación una vez activada la estrategia; requerimientos mínimos necesarios para la implementación de la medida; así como, dependencias internas y externas identificadas.

7. Confirmamos que dentro del plan de continuidad de negocio se encontraba identificados los procedimientos a seguir para realizar el regreso a la operación normal para cada una de las estrategias de continuidad, una vez que se determina que el incidente ha concluido, indicando las actividades a seguir, así como a los equipos responsables de las mismas.

8. Identificamos que la organización contaba con un calendario de actividades de continuidad de negocio donde se reflejaban las pruebas programadas de las estrategias de continuidad de negocio. Adicionalmente, se contaba con evidencia que respaldaba las pruebas realizadas y la documentación de las áreas de oportunidad identificadas.

5.2. Atención de áreas de oportunidad identificadas

Una vez concluida la autoevaluación, presentamos los resultados a los directivos del área X, así como las líneas de acción que debíamos seguir para la atención de los hallazgos identificados y un plan de trabajo a fin de dar seguimiento a dicha atención. La presente sección explica dichas mejoras enmarcadas en la documentación que se generó:

a. Alcance, política y objetivos del SGCN

En primera instancia, documenté las actividades principales realizadas por el Área X:

- Dirigir el diseño, implantación y seguimiento de las políticas necesarias para el correcto desarrollo, funcionamiento y operación de los sistemas A, B, C y D.
- Dirigir y establecer los procedimientos necesarios para asegurar la calidad en el diseño, desarrollo, implantación, operación y atención a usuarios de los sistemas A, B, C y D, así como los sistemas de soporte requeridos para el correcto funcionamiento de los anteriores, buscando, entre otras características, costo óptimo, alto desempeño, seguridad y continuidad operativa.
- Dirigir proyectos de actualización tecnológica, innovación, mejores prácticas y tendencias actuales en materia de sistemas de transferencias financieras, con el fin de profundizar

conocimientos, presentar iniciativas e incorporar nuevas funcionalidades a los sistemas existentes.

En conjunto con los directivos del área X, determinamos que el alcance del SGCN incluiría la operación de los sistemas A, B, C y D, así como los activos críticos necesarios para la prestación de dichos sistemas y al personal del Área X. Si bien el Área X, cuenta con un equipo de desarrollo interno, es otra área en la organización la responsable de la administración de los equipos de cómputo y telecomunicaciones, lo que la convierte en la principal proveedora de servicios y por tanto, se encuentra incluida dentro del alcance del SGCN.

Se definieron los siguientes objetivos de continuidad del SGCN:

- Garantizar la continuidad operativa y mitigar el posible impacto negativo en los sistemas de transferencias financieras administrados por el Área X, ante la materialización de un evento disruptivo, mediante la implementación de controles y procedimientos eficientes y eficaces que aseguren su pronta recuperación y buen funcionamiento una vez restaurado el servicio.
- Validar el funcionamiento y en su caso, mejorar los procedimientos de continuidad implementados mediante programas de capacitación, campañas de concientización y ejercicios de las medidas de continuidad operativas establecidas.
- Validar el funcionamiento y en su caso mejorar los planes de respuesta y recuperación ante incidentes que afecten la operación de los sistemas administrados por el Área X.

Adicionalmente, como parte de la política, participé en la definición de los lineamientos para realizar una evaluación periódica de los componentes del SGCN, la cual incluía presentar:

1)un informe de resultados de la revisión integral realizadas,
2)un informe de resultados de los ejercicios de las estrategias de continuidad efectuadas, indicando las áreas de oportunidad identificadas y su seguimiento,
3) un informe de los incidentes presentados, los cuales derivaron en la ejecución de algún procedimiento de continuidad y,
4)un informe de resultados del seguimiento al cumplimiento de las acciones correctivas establecidas ante la ocurrencia de un incidente.

b. Análisis de riesgos

Participé en la documentación del proceso de Gestión de Riesgos para el Área X, el cual se describe en el siguiente diagrama:

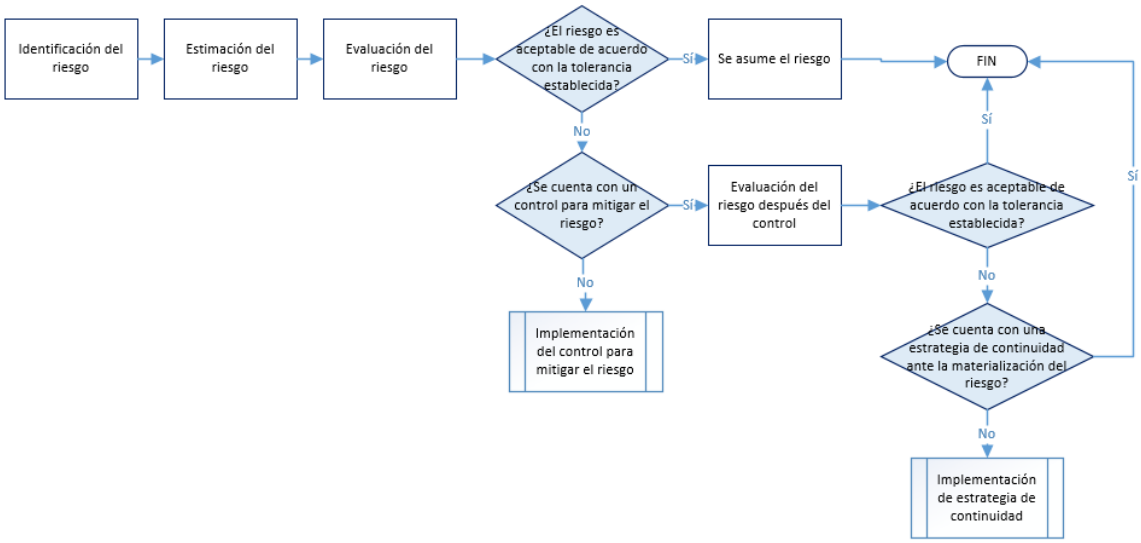


Diagrama 1. Proceso de gestión de riesgos.

- **Identificación del riesgo:** Es el proceso mediante el cual se reconoce que existe una amenaza que podría causar una afectación a los servicios provistos.
- **Estimación del riesgo:** Es el proceso mediante el cual se determina la posibilidad de ocurrencia y el impacto a la organización en caso de que se materialice la amenaza. El impacto es el factor estimado en función de los procesos críticos que se verían afectados en el caso de que el sistema o servicio dejara de funcionar de acuerdo con los siguientes niveles y conforme a la disponibilidad requerida del sistema:

Tabla 3. Niveles de impacto de un incidente.

Factor	Nivel de impacto	Posible periodo de interrupción (minutos)
1	Leve	0-4
2	Bajo	5-14
3	Medio	15- 29
4	Alto	30-60
5	Muy alto	> 60

La posibilidad de ocurrencia está determinada por el número de veces que puede materializarse una amenaza en un año:

Tabla 4. Clasificación de posibilidad de ocurrencia de una amenaza

Número de veces durante el año que se presenta una amenaza	Posibilidad de ocurrencia
De 0 a 1	Poco frecuente
De 2 a 5	Frecuente
Más de 6	Muy frecuente

- **Evaluación del riesgo:** La evaluación del riesgo consiste en determinar si el riesgo identificado es tolerable o no con base en su impacto y probabilidad de ocurrencia. El Área X estableció la siguiente clasificación:

Tabla 5. Clasificación de riesgos en el Área X.

Clasificación	Repercusión en la operación
Aceptable	Se requiere del uso de algunos recursos alternos y se puede cumplir en tiempo y forma con las obligaciones pactadas.
Moderado	Se requiere del uso de recursos alternos para la mayor parte de las actividades y se puede cumplir en tiempo y forma con las obligaciones pactadas.
No aceptable	Se requiere del uso de recursos alternos para la realización de actividades y existe una afectación en tiempo o forma.

Adicionalmente, utilizamos el mapa de riesgos presentado en la Figura 8 a fin de que visualmente fuera sencillo identificar en qué cuadrante se encontraba cada riesgo considerando su nivel de impacto y su clasificación de probabilidad de ocurrencia.

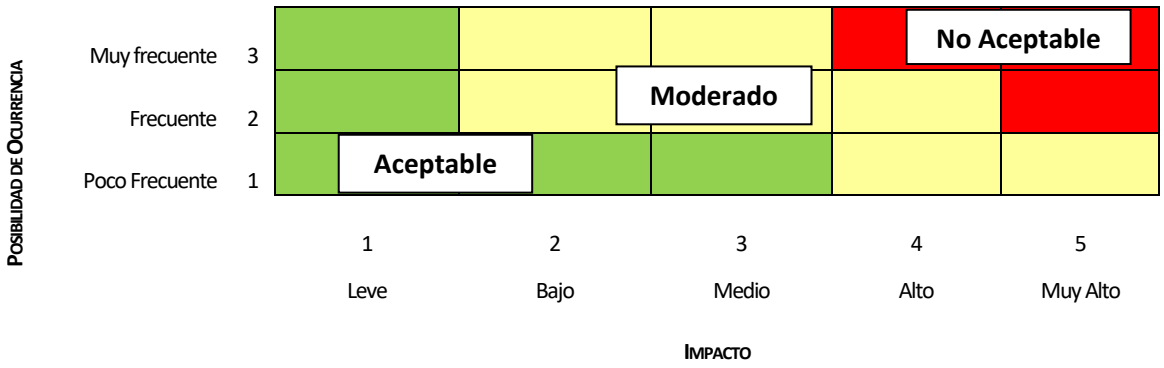


Figura 8. Mapa de calor para identificar los riesgos identificados.

Donde:

- La zona de riesgo en **color verde** indica un umbral de riesgo aceptable dado que la posibilidad de ocurrencia y el impacto es entre Leve y Medio.
- La zona de riesgo en **color amarillo** indica que el umbral de riesgo es moderado, ya que la posibilidad de ocurrencia y el impacto son mayores, por lo que se requiere darles mayor prioridad para implementar controles que disminuyan su impacto.
- La zona de riesgo en **color rojo** indica los riesgos de más alta prioridad para los que se requiere implementar controles y medidas de contingencia. En caso de que no sea posible reducir el riesgo, se requiere contar con estrategias de continuidad para asegurar que, ante su ocurrencia, se cuenta con actividades definidas para recuperar el servicio en el menor tiempo posible.

La tolerancia al riesgo del Área X es baja, ya que busca asumir únicamente riesgos con clasificación Aceptable y para aquellos con clasificación Moderada y No aceptable busca implementar controles que mitiguen la materialización del riesgo y, adicionalmente, contar con estrategias de continuidad eficientes que aseguren la operación de los servicios que administra ante la presencia de incidentes.

Una vez documentada la metodología, dirigimos una nueva evaluación de los riesgos identificados a fin de determinar su clasificación. Se dividieron los riesgos en tres categorías:

1. **Equipamiento y tecnologías de la información:** Referente a cualquier falla o intrusión a los equipos y servicios con los que cuenta la institución: suministro de energía eléctrica, instalaciones, servidores, equipos de telecomunicaciones, entre otros.
2. **Humanos:** Se refiere a los aspectos relacionados con el personal que realiza alguna actividad relacionada al desarrollo, gestión u operación de los sistemas.
3. **Externo:** Se refiere a los factores ajenos a la organización, los cuales pueden causar afectaciones a las actividades diarias del personal.

En la siguiente tabla se presentan algunos de los riesgos identificados indicando su impacto, posibilidad de ocurrencia, su clasificación y, en su caso, los controles implementados.

Tabla 5. Ejemplos de riesgos identificados para el Área X.

Amenaza	Categoría	Posibilidad de ocurrencia	Impacto	Clasificación del riesgo	Control implementado	Clasificación después del control implementado	Estrategia de continuidad relacionada
Falla de algunos de los elementos de hardware en la infraestructura de cómputo que soporta los sistemas	Equipamiento y tecnologías de la información	Frecuente	Muy alto	No Aceptable	Redundancia en la infraestructura de cómputo. Mecanismo de replicación síncrona bidireccional implementado entre centros de respaldo. Sistema de monitoreo en tiempo real del funcionamiento de los elementos de HW y SW de los servicios.	Moderado	Traslado de la operación de los sistemas a la infraestructura de respaldo.
Falla de acceso a la información en el nodo de cómputo principal.	Equipamiento y tecnologías de la información						
Falla en la infraestructura de telecomunicaciones entre el sitio principal y de respaldo	Equipamiento y tecnologías de la información	Frecuente	Muy alto	No Aceptable	Redundancia en infraestructura de telecomunicaciones.	Aceptable	
Falla en la infraestructura de telecomunicaciones de los usuarios de los servicios	Equipamiento y tecnologías de la información						
Omisión accidental de actividades por parte del personal que opera, administra o da soporte a un sistema	Humano	Frecuente	Alto	Moderado	Procedimientos de control operativo implementados para asegurar la correcta ejecución de las actividades.	Aceptable	
Uso inapropiado de los sistemas por parte de los operadores o administradores que puedan derivar en afectaciones al sistema.	Humano	Poco frecuente	Muy alto	Moderado	Esquema de separación de tareas para la ejecución de actividades críticas.	Aceptable	
Imposibilidad de operar desde las instalaciones principales	Externo	Muy frecuente	Medio	Moderado			Se cuenta con un sitio alterno dispuesto con los recursos necesarios para continuar con la operación de los sistemas.
Indisponibilidad del personal encargado de la operación para asistir a las instalaciones de la organización.	Externo	Poco frecuente	Alto	Moderado			Se cuenta con esquemas de trabajo a distancia para personal crítico.

c. Análisis de impactos al negocio

Dentro del Análisis de Impactos al Negocio del área X identificamos los procesos críticos dentro de cada uno de los servicios provistos; las interdependencias entre los servicios; los tiempos y puntos objetivo de recuperación para cada uno; la prioridad de recuperación de acuerdo con el horario de operación y los activos críticos, es decir, los recursos mínimos requeridos para poder continuar con la operación de los servicios;

La siguiente tabla muestra los servicios principales provistos por el área X, sus procesos relacionados, su nivel de criticidad y el sistema que soporta su funcionalidad.

Tabla 6. Nivel de criticidad de los procesos que soportan la funcionalidad del servicio.

Servicio	Procesos	Nivel de criticidad del servicio	Sistema que lo soporta
1. Administrar los recursos de los cuentahabientes y permitir la transferencia de estos hacia otros sistemas administrados por X	1.1. Apertura del sistema.	Alta	A
	1.2. Envío de transferencias hacia el sistema B.	Alta	
	1.3. Envío de transferencias entre cuentahabientes.	Media	
	1.4. Recepción de transferencias del sistema B.	Media	
	1.5. Cierre del sistema.	Alta	
2. Proveer la infraestructura necesaria para procesar transferencias en diferentes divisas	2.1. Apertura del sistema.	Alta	B
	2.2. Recepción de transferencias provenientes del sistema A.	Alta	
	2.3. Transferencias en diferentes divisas dentro del sistema.	Alta	
	2.4. Recepción de información sobre operaciones procesadas en el sistema C.	Alta	
	2.5. Envío de transferencias al sistema A.	Media	
	2.6. Recepción de información para procesar las transferencias del sistema D.	Alta	
	2.7. Envío de información al sistema D sobre el resultado del procesamiento de las operaciones.	Alta	
	2.8. Cierre del sistema	Alta	
3. Proporcionar recursos adicionales a los cuentahabientes a través de operaciones a un plazo establecido que involucran valores gubernamentales	3.1. Apertura del sistema	Alta	C
	3.2. Operaciones de compra de valores gubernamentales	Alta	
	3.3. Operaciones de venta de valores gubernamentales	Alta	
	3.4. Envío de información sobre el resultado de las operaciones al sistema B.	Alta	
	3.5. Cierre del sistema	Alta	
	4.1. Apertura del sistema	Alta	D

Servicio	Procesos	Nivel de criticidad del servicio	Sistema que lo soporta
4. Procesar la parte en moneda nacional de operaciones cambiarias realizadas con instituciones financieras del extranjero	4.2. Recepción de información sobre operaciones cambiarias proveniente de instituciones financieras del extranjero.	Alta	
	4.3. Envío de información al sistema B para el procesamiento de las operaciones.	Alta	
	4.4. Recepción de información del sistema B sobre el resultado del procesamiento de las operaciones.	Alta	
	4.5. Envío de resultado del procesamiento de las operaciones a instituciones extranjeras.	Alta	
	4.6. Cierre del sistema.	Media	

Como parte de las mejoras implementadas documentamos las interdependencias de los servicios con base en la información proporcionada por el área operativa.

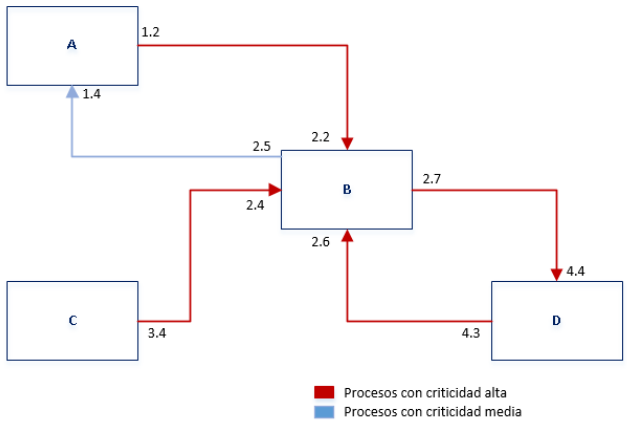


Diagrama 2. Interdependencias en los servicios administrados por el área X.

Como se puede observar, la mayor parte de los procesos que soportan las interdependencias entre los servicios tienen criticidad alta. Lo anterior se debe a que cada uno de los servicios necesita insumos provenientes de dichas interdependencias para continuar con la provisión del servicio. Por ejemplo, el proceso 1.2 Envío de transferencias hacia el sistema B tiene criticidad alta dado que, sin él, el sistema B no contaría con los recursos necesarios para poder realizar transferencias dentro del sistema. De igual forma, el sistema D necesita que el sistema B esté funcionando correctamente a fin de que puedan procesarse sus operaciones y pueda enviar la confirmación de este procesamiento a la institución extranjera de la que provino la operación.

Con base en las interdependencias identificadas entre los sistemas, establecimos la siguiente secuencia de recuperación ante la ocurrencia de un incidente con el objeto de asegurar que conforme se vayan recuperando los sistemas cuenten con la funcionalidad mínima para proveer el servicio a un nivel mínimo aceptable:

Tabla 6. Prioridad de recuperación de los sistemas.

Prioridad de recuperación	Sistema
1	B
2	C
3	D
4	A

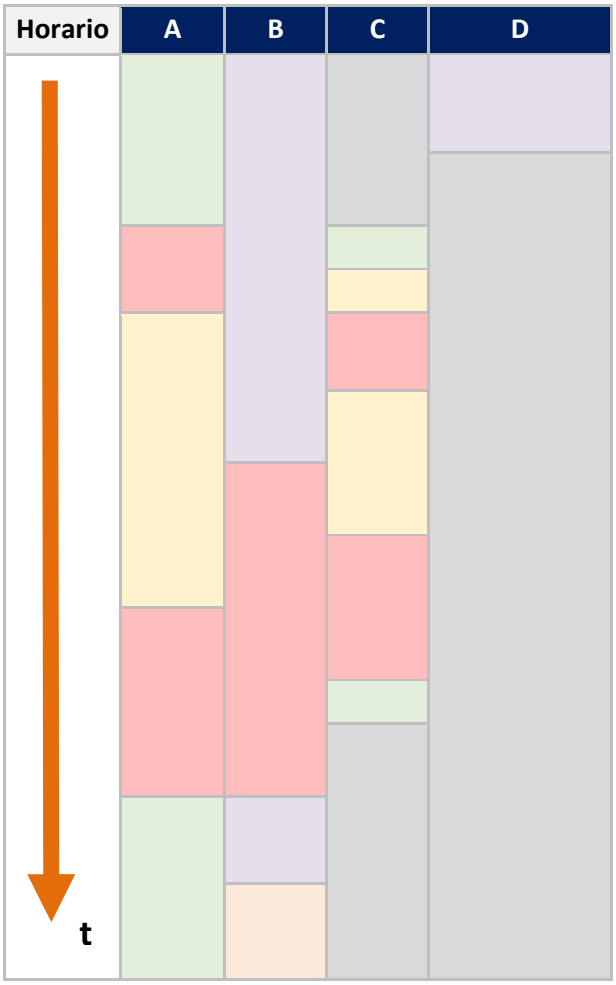
Se observa que el sistema B es el primero que se debe recuperar, lo anterior se debe a que sin él, el sistema C y D no podrían funcionar de forma correcta. El último en recuperarse es el sistema A debido a que su función principal es realizar transferencias de recursos internas y hacia B, por lo que en caso de un incidente en donde se presente indisponibilidad de los cuatro sistemas, se considera que B tiene suficientes recursos para continuar operando mientras que se realiza la recuperación del resto de los servicios.

Adicionalmente, establecimos una clasificación del impacto en tiempo ante incidentes que pudieran causar una afectación en los sistemas que soportan la funcionalidad de los servicios. Los umbrales de impacto en el tiempo se definieron de acuerdo con el horario en el que un posible evento pudiera afectar la operación de los servicios considerando con mayor criticidad los horarios con mayor volumen de operaciones de acuerdo con la siguiente tabla:

Tabla 7. Indicadores de impacto en el tiempo.

Indicador	Impacto (min)		
	Leve	Moderado	Crítico
	0 a 15	16 a 30	> 30
	0 a 30	31 a 60	> 60
	0 a 60	61 a 120	> 120

Tabla 8. Impactos en el tiempo ante la indisponibilidad de los servicios.



Asimismo, se confirmó que de acuerdo con las mejores prácticas y a los impactos en el tiempo definidos para cada servicio el RTO definido para los sistemas A, B, C y D es de dos horas.

Con respecto al punto objetivo de recuperación, dado que se cuenta con una arquitectura que contempla infraestructura de respaldo configurada activo-pasivo y que se cuenta con mecanismos de replicación bidireccional síncrona, determinamos que el punto objetivo de recuperación de los sistemas A, B, C y D es de 0 minutos, es decir que, ante la ocurrencia de un incidente, no existe pérdida de información.

De igual forma, cuantificamos los activos necesarios para la correcta operación de los servicios, así como la prioridad de contar ellos ante la ocurrencia de un incidente.

Tabla 9. Activos necesarios para la correcta operación de los servicios.

Activo	Descripción	Prioridad
Personal	Operadores de los sistemas	Alta
	Soporte de primer nivel	Alta
	Soporte de segundo nivel	Alta
	Equipo de continuidad operativa	Media
	Equipo de desarrollo de los sistemas	Baja
	Equipo de pruebas de los sistemas	Baja
Instalaciones	Sitio operativo principal	Alta
	Sitio operativo alterno	Alta
	Centro de datos principal	Alta
	Centro de datos alterno	Alta
Mobiliario, equipamiento y consumibles	Servidores	Alta
	Equipos de telecomunicaciones (ruteadores, switches, firewalls, entre otros)	Alta
	Equipo de cómputo personal	Alta
	Mobiliario para estación de trabajo	Alta
	Equipo de cómputo personal (laptop)	Alta
	Impresora	Baja
Sistema de información y comunicaciones	Red de comunicación entre centros de datos	Alta
	Red de comunicación con los usuarios de los sistemas	Alta
	Teléfonos	Media
	Servicio de correo electrónico	Media

d. Plan de atención a incidentes

Si bien el área X ya contaba con un plan de atención a incidentes, actualizamos dicho plan para considerar la evaluación del impacto del incidente en cada una de sus fases a fin de determinar si era necesario activar alguna de las estrategias de continuidad implementadas.

Los incidentes en el área X se clasifican conforme a dos prioridades:

- Alta: El tiempo de solución previsto para este tipo de incidentes es de 20 minutos.
- Normal: El tiempo de solución previsto para incidentes con clasificación normal es de 60 minutos.

Un incidente puede derivar en una crisis, la cual es una situación en la que un proceso crítico resulta afectado derivado de la ocurrencia de un incidente que puede causar un impacto generalizado en los sistemas administrados por X, un incumplimiento contractual, regulatorio o incluso un daño reputacional al área.

Una crisis es declarada por el Comité de Respuesta a Emergencias con base en la siguiente información:

- El servicio afectado, su estado y cuánto tiempo lleva presentándose el incidente.
- Los procesos críticos próximos a ejecutarse.
- El tiempo objetivo de recuperación establecido para los servicios.
- Las afectaciones probables del incidente a otro sistema.

El Comité de Respuesta a Emergencias se integra por los directores del área X responsables de la operación, así como de la infraestructura tecnológica que soporta los sistemas. Sus principales obligaciones son:

- Declarar una crisis.
- Instruir la activación de las estrategias de continuidad implementadas.
- En caso de la ejecución de un procedimiento de continuidad, establecer la estrategia para el regreso a la operación normal, una vez solucionado el incidente.
- Evaluar los pasos a seguir, en caso de que la ejecución de un procedimiento de continuidad no dé resultados satisfactorios.
- Instruir el envío de notificaciones a los usuarios de los sistemas.

El flujo de comunicación que el personal del área X debe seguir está dividido en las siguientes fases:

- **Detección y reporte:** En esta fase se identifica el incidente y se reporta por los medios establecidos al soporte de primer nivel.

- **Diagnóstico:** En esta fase se realiza el diagnóstico inicial del incidente y se determina si es necesario convocar al Comité de Respuesta a Emergencias.

- **Atención:** En esta fase las áreas competentes (soporte de primer y segundo nivel) inician la atención del incidente. De igual forma el área encargada de la continuidad de negocio da seguimiento a las acciones realizadas para solucionar el incidente y verifica si algún proceso crítico está siendo afectado con el objeto de notificar al Comité de Respuesta a Emergencias.

- **Seguimiento:** En esta fase el equipo de continuidad operativa evalúa el impacto del incidente y da seguimiento a las acciones realizadas para solucionarlo.

- **Recuperación:** En esta fase el Comité de Respuesta a Emergencias evalúa el incidente y determina si es necesaria la activación de alguna de las estrategias de continuidad.

- **Restauración:** En esta fase se llevan a cabo las acciones necesarias para regresar al flujo de operación normal, una vez que el proceso crítico afectado fue recuperado y el incidente solucionado.

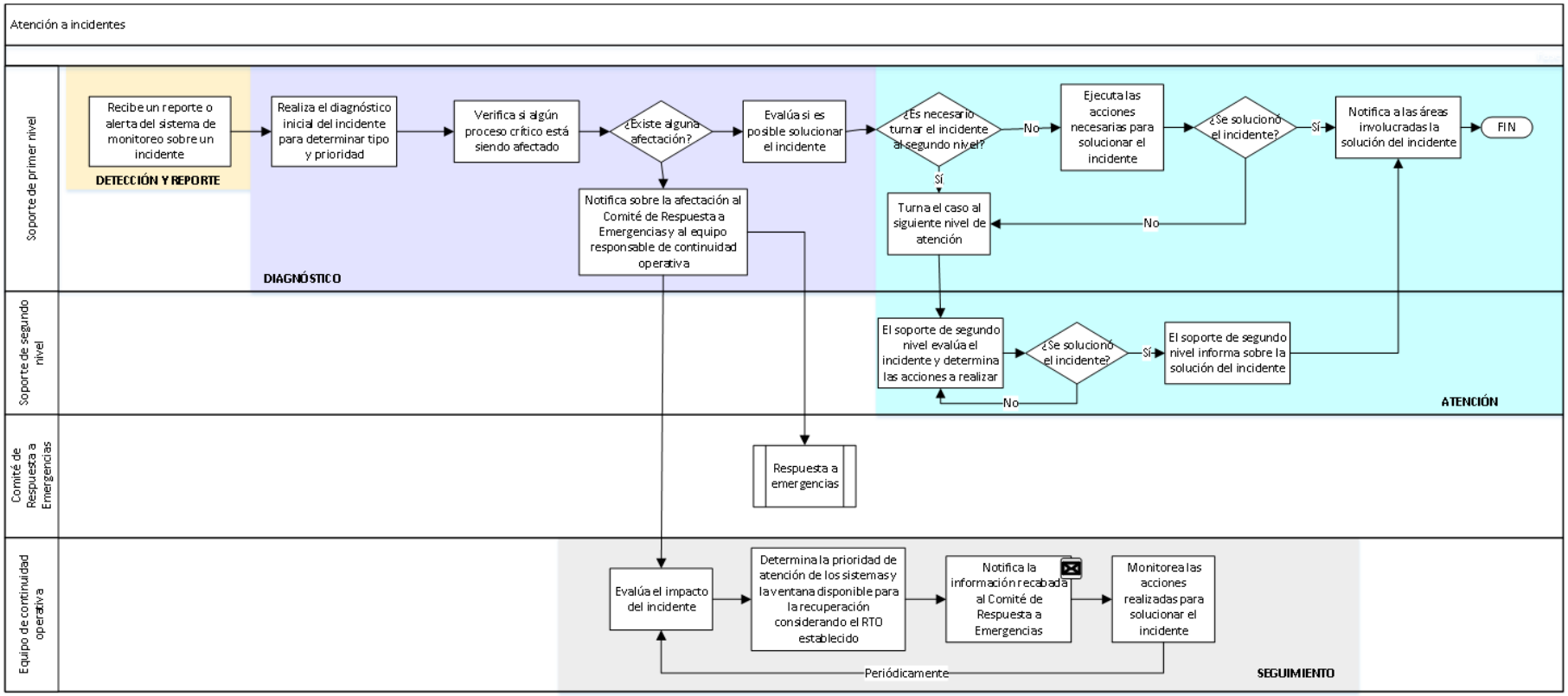


Diagrama 3. Flujo de comunicación para la atención de incidentes.

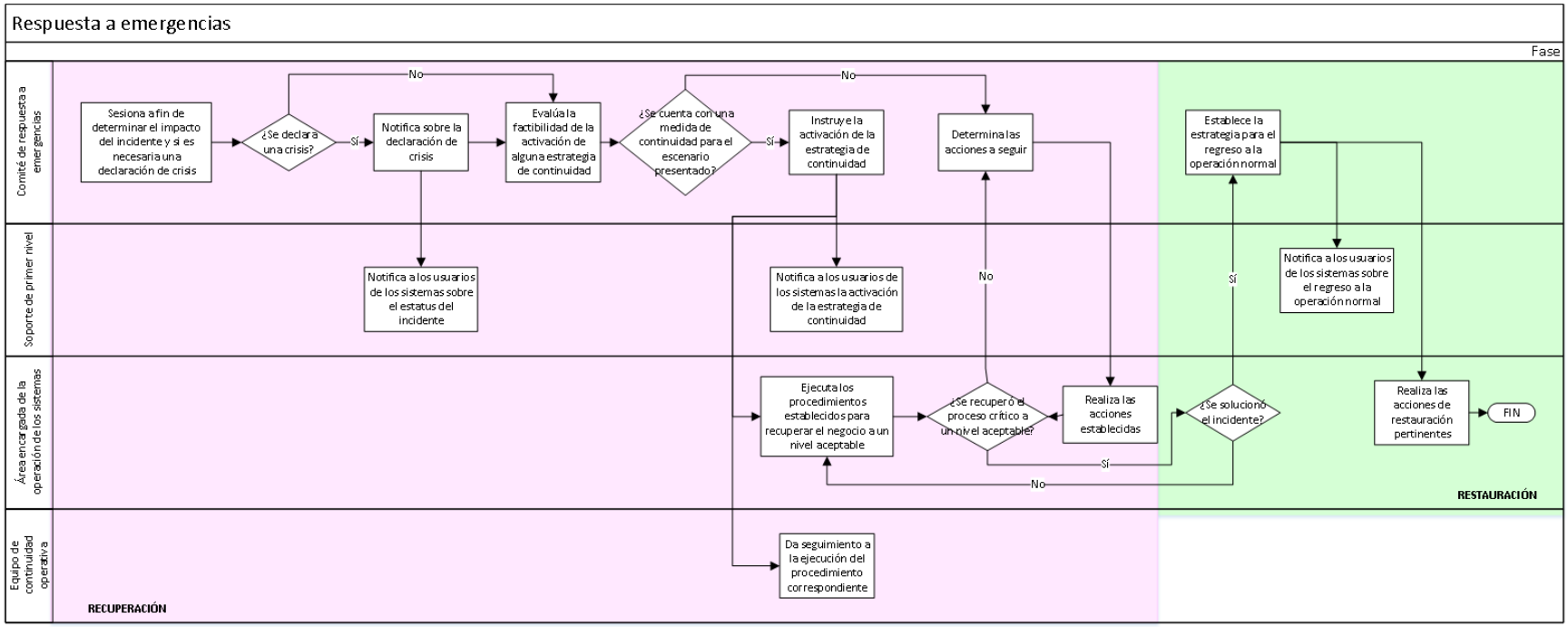


Diagrama 4. Flujo de comunicación para la respuesta a emergencias.

6. Conclusiones

Si bien el área X ya contaba con un marco de continuidad de negocio implementado, las mejoras realizadas contribuyeron a contar con objetivos claros conocidos por todo el personal involucrado en la operación y soporte de los sistemas, así como con la definición de responsables de cada fase de respuesta ante la ocurrencia de un incidente. Adicionalmente, la actualización al análisis de riesgos y de impactos al negocio permitió confirmar que, de conformidad con su tolerancia de riesgo, el área cuenta con controles implementados a fin de mitigar los principales riesgos a los que está expuesta, así como con procesos críticos bien identificados y priorizados.

En resumen, las principales acciones en las que participé consistieron en:

1. Evaluación del marco de continuidad de negocio del área X con respecto a la norma ISO 22301 a fin de verificar su alineación a este e identificar áreas de oportunidad.
2. Atención de las áreas de oportunidad identificadas, entre las que se encuentran: la documentación del alcance, política y roles y responsabilidades del SGCN; la documentación del proceso de gestión de riesgos; la actualización del análisis de riesgos y de impactos al negocio; así como la actualización del plan de atención de incidentes.

Posterior a la conclusión de la implementación de las mejoras descritas en el presente documento se realizó una prueba de la estrategia de continuidad de traslado a los servidores de respaldo, cuyos principales objetivos eran verificar si se cumplían los tiempos y puntos objetivos de recuperación y prioridad de recuperación de los sistemas, los cuales se definieron en el análisis de impactos al negocio. En dicha prueba mi participación consistió en coordinar las actividades e interacciones entre áreas, revisar los guiones técnicos y operativos para asegurar que las actividades consideradas cumplieran con las fases establecidas, monitorear la prueba durante su ejecución y posteriormente, realizar el análisis de los resultados obtenidos a fin de verificar si los objetivos de la prueba se habían alcanzado, elaborar el informe de resultados y presentarlo a los directivos del área X.

Como resultado de la prueba, no se tuvo pérdida de información en los sistemas A, B, C y D durante el traslado a la infraestructura de respaldo y su operación pudo ser recuperada en un tiempo menor a dos horas. De igual forma, se probó el flujo de comunicación del plan de atención a incidentes, en donde se tuvo la participación del rol del Comité de Respuesta a Emergencias, así como del equipo de continuidad.

Durante el periodo de tiempo que he laborado en el área X se ha continuado con la realización de pruebas periódicas de las estrategias de continuidad establecidas. Asimismo, se realiza una evaluación y actualización anual de la vigencia de la documentación que soporta el marco de continuidad de negocio implementado.

De esta forma, es posible concluir que el área X cuenta con un mejor marco de administración de riesgos y de atención a incidentes que hacen más eficiente y segura la operación de los sistemas críticos que administra. No obstante, lo anterior, se requiere continuar con las revisiones y actualizaciones periódicas a fin de mantener este marco vigente, incorporar nuevos riesgos y fortalecer las estrategias de continuidad a través del uso de las nuevas tecnologías.

7. Bibliografía

[1] Bank for Intenational Settlements and International Organization of Securities Commissions (2012). *Principles for financial market infrastructures.* CPMI-IOSCO. ISBN 92-9131-108-1.

[2] Bauer, Erick; Adams, Randee; Eustace, Daniel (2012). *Beyond Redundancy.* John Wiley & Sons, Inc. New Jersey, USA. ISBN: 978-1-118-10491-0

[3] CS IL BCM 5000 (2015). *Auditoría de programas de GCN*. The International Consortium for Organizational Resilience (ICOR), Lombard Illinois, USA.

[4] DRI International (2014). *BCLS 2000 Administración de Continuidad de Negocio para Profesionales Avanzados*. DRI International.

[5] Elinwood, Justin (2017). *An Introduction to Metrics, Monitoring, and Alerting*. https://www.digitalocean.com/community/tutorials/an-introduction-to-metrics-monitoring-and-alerting

[6] Gómez, Diego (2014). *Sistemas críticos. https://es.slideshare.net/difago/sistemas-crticos.*

[7] Gravic Inc. (2018). *Choosing a Business Continuity Solution to Match Your Business Availability Requirements.* Gravic Shadowbase. Pennsylvania.

[8] Heidi, Erika (2016). *What is High Availability?*. https://www.digitalocean.com/community/tutorials/what-is-high-availability

[9] Information Technology Infrastructure Library (2009). *ITIL V3 Foundation Handbook*. London, TSO.

[10] International Organization for Standardization (2012). *Societal security – Business continuity management systems – Requirements* (ISO standard no. ISO 22301:2012).

[11] Oracle9i Real Application Clusters Concepts (2001). *High Availability Concepts and Best Practices.* Release 1 (9.0.1), Part Number A89867-02. Oracle.

[12] Rodriguez Dapena, Patricia (2009). Asegurar que el software se construye fiable y seguro*. Revista Española de Innovación, Calidad e Ingeniería de Software*. Vol. 5, No. 2.

[13] Summerville, Ian (2005). *Ingeniería del Software.* Pearson Educación. Madrid. ISBN 84-7829-074-5