UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Creación de un análisis de riesgos y su mitigación en Continuidad del Negocio para proveedores críticos de un Grupo Financiero.

INFORME DE ACTIVIDADES PROFESIONALES

Que para obtener el título de

Ingeniero Industrial

P R E S E N T A

Judith Molina Guzmán

ASESOR DE INFORME

M.I. Silvina Hernández García.

Ciudad Universitaria, Cd. Mx., 2019

Contenido

Introducción y objetivos

Introducción

El presente documento tiene como objetivo demostrar el trabajo profesional desarrollado en una Institución Financiera, donde los conocimientos adquiridos en la Licenciatura de Ingeniería Industrial han sido de utilidad para diseñar, implementar y evaluar procesos nuevos, así como la mejora de los existentes en lo que respecta a la identificación y análisis de los riesgos sobre los servicios que prestan los proveedores, dando cumplimiento a los cambios regulatorios.

En el año 2014 la Comisión Nacional Bancaria y de Valores (CNBV) encargada de regular a las instituciones financieras, estableció lineamientos a cumplir para dar mayor seguridad en los procesos donde se opera con clientes a través de canales tecnológicos, debido al aumento de los riesgos a los que están expuestos los Bancos y sus clientes. Por lo anterior, se publicó en la Circular Única de Bancos un nuevo requerimiento, donde solicita a las instituciones bancarias realizar una evaluación de riesgos de los proveedores contratados, para medir la disponibilidad de los procesos operativos, servicios de procesamiento, transmisión de datos, custodia y resguardo de información de la Institución, ante eventos que puedan interrumpir su operación normal.

Al no contar con un proceso que dé cumplimiento con lo establecido por la CNBV, se diseñó e implementó un proceso que permitiera evaluar a los proveedores, tomando como referencia lo visto en la asignatura Sistemas de Planeación [1]para la elaboración de un plan, aplicando estrategias de planeación y considerando la toma de decisiones en el corto, mediano y largo plazo, así como, la asignatura de Análisis y Mejora de Procesos para el análisis y diseño de procesos que conforman a la organización.

Tras terminar el diseño del proceso, se formalizaron las actividades, diagramas de flujo, documentos de apoyo y se desarrolló un plan inicial para el análisis de proveedores, del cual se obtuvieron resultados identificando puntos de mejora y dando cumpliendo a la regulación.

[1] Plan de estudios de la Licenciatura en Ingeniería Industrial, Universidad Nacional Autónoma De México, Facultad De Ingeniería

Objetivo general

Diseñar e implementar un procedimiento para la evaluación de riesgos en Continuidad del Negocio a los proveedores críticos de una Institución Financiera, para el cumplimiento de los requerimientos de la Comisión Nacional Bancaria y de Valores (CNBV) establecidos en su Circular Única de Bancos anexo 67 inciso h.

Objetivos específicos

a) Realizar el diseño de un procedimiento, combinando los conocimientos adquiridos en la carrera de Ingeniería Industrial y el conocimiento sobre el tema de Continuidad del Negocio adquirido en la empresa.
b) Proponer mejoras al proceso una vez conocidos los resultados, para mejorar el proceso e incluso hacerlo formal ante la Institución.

Capítulo I: Descripción de la empresa

1.1 Descripción de la empresa

A continuación se presenta la información de la empresa en donde se realizó la actividad profesional.

El trabajo fue desarrollado en la unidad tecnológica de una institución financiera ubicada en Calzada de Tlalpan 2980, Colonia ExHacienda Coapa, Delegación Coyoacán. (figura 1)

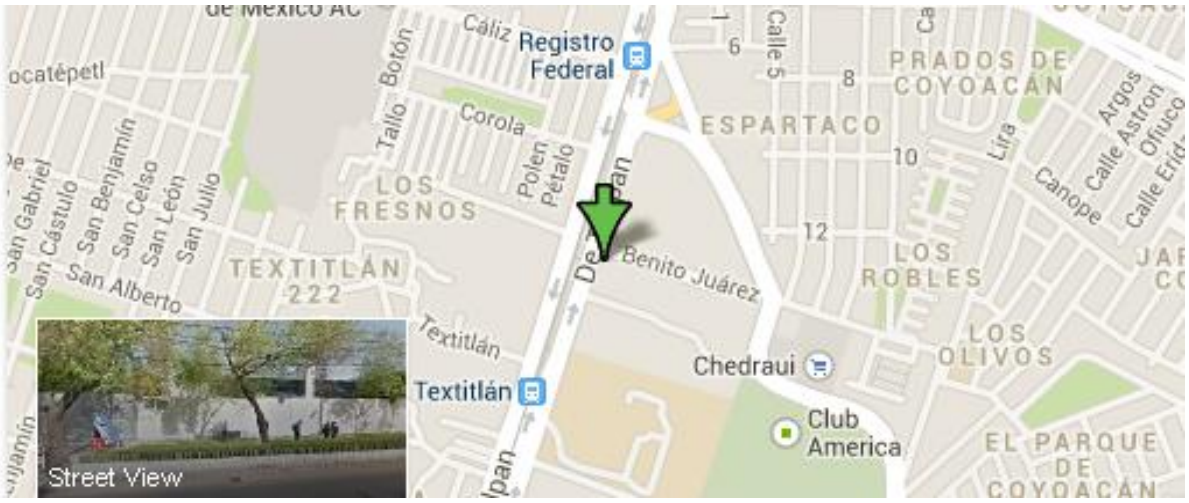


Figura 1 Ubicación geográfica de la Unidad tecnológica

1. 2 Historia de la empresa[2]

En 1986 nace el Banco Mercantil del Norte, S.N.C., nombre que refiere la fusión del Banco Mercantil de Monterrey con el Banco Regional del Norte.

Fundado en 1899 como Banco Mercantil de Monterrey, pues su sede se encuentra en la ciudad con este nombre. En 1947, el mismo grupo fundó el Banco Regional del Norte.

En 1992, en el proceso de privatización de la banca Mexicana, Banorte fue adquirido por el grupo actual de emprendedores accionistas, encabezado por Roberto González Barrera.

Al poco tiempo fue incorporando los servicios de Casa de Bolsa, Factoraje, Almacenadora y Arrendadora, hasta ser un grupo financiero consolidado de fuerte importancia en la banca Mexicana.

En el 2002 compra al grupo financiero Bancrecer para convertirlo definitivamente en Banorte.

En 2006, entra al mercado hispano en Estados Unidos y adquiere el 100% de los activos de Inter National Bank de Texas (INB), un banco instalado en Texas y dos compañías remesadoras en 2007: Uniteller en New Jersey y Motran en California.

En 2010, Banorte anuncia la compra del 100% de sus acciones a Ixe Grupo Financiero, el cuál pagará alrededor de los 1,300 millones de dólares.

Actualmente opera como un grupo financiero denominado Grupo Financiero Banorte (GFNorte), bajo un modelo de banca universal ofreciendo una amplia variedad de productos y servicios a través de su casa de bolsa, las compañías de pensiones y seguros, Afore, sociedades de inversión, así como las empresas de arrendamiento y factoraje y la almacenadora. Al cierre de diciembre del 2015, GFNorte administra US 122 mil millones de dólares en activos.

Banorte, la subsidiaria bancaria de GFNorte, es actualmente la tercera institución bancaria más grande en México medida en tamaño de depósitos y la cuarta en crédito. Es el segundo proveedor más importante en colocación de créditos a gobiernos, el tercer banco más importante en créditos hipotecarios, y el cuarto en cartera comercial y de tarjeta de crédito. Además de aumentar su participación de mercado, Banorte ha consolidado su posición como uno de los bancos más rentables en México, siendo reconocido por sus sólidos fundamentales a través de mostrar buena calidad de activos, así como un fortalecimiento en su nivel de

[2] www.banorte.com "Nuestra historia"

capitalización. Banorte cuenta con más de 12 millones de clientes en el sector bancario, 27 mil empleados atendiendo 1,191 sucursales, 7,425 cajeros automáticos y 6,989 puntos de contacto a través de corresponsales bancarios por todo el país.

Banorte es el único banco comercial, entre las seis instituciones más grandes, que está manejado por un equipo directivo mexicano. Sus decisiones son tomadas localmente sin la influencia de matrices extranjeras, que ha probado ser una ventaja dada la reciente debilidad de muchas instituciones globales.

Su socio estratégico en la Afore es el Instituto Mexicano del Seguro Social (IMSS). En esta línea de negocio, Afore XXI Banorte concretó la adquisición de Afore Bancomer en enero de 2013, convirtiéndose en la operación más significativa del sistema de ahorro para el retiro hasta el momento, creando así la Afore más importante en México.

Las acciones de GFNorte cotizan en la Bolsa Mexicana de Valores (BMV) con el ticker "GFNORTEO" – siendo la cuarta acción más líquida en México y una de las compañías con mayor float, aproximadamente 90% -, en la Bolsa de Valores de Madrid bajo el símbolo "XNOR" y en el mercado estadounidense a través de un ADR listado en el mercado OTCQX con el símbolo de "GBOOY".

1.3 Misión [3]

"Generar confianza y fortaleza financiera para nuestros clientes"

1.4 Visión[4]

"Ser un gran aliado para crecer fuerte con México"

1.5 Valores [5]

Los principios en los cuales la empresa se mueve son las directrices para dar calidad y servicio al cliente a través de sus mecanismos bancarios, los cuales son:

a) Solidaridad: Es una responsabilidad mutua contraída por varias personas, que nos permite comprometernos de manera circunstancial a la causa de otros.
b) Innovación: Es el esfuerzo que hacemos por conseguir algo por nosotros mismos o con la ayuda de los demás; es una fuerza de gran

[3] www.banorte.com "Nuestra identidad"
[4] IDEM
[5] IDEM

poder de transformación, que ha llevado a la humanidad a los más altos niveles de desarrollo y civilización.

c) Lealtad: Es el sentido del compromiso por el bien de los demás, genera un alto sentimiento de apego, fidelidad y respeto, que nos inspiran las personas o grupos en los que interactuamos.
d) Respeto: Es conocer el valor propio y honrar el valor de los demás, es el conocimiento del valor inherente y los derechos humanos de los individuos y de la sociedad
e) Responsabilidad: Es la obligación de responder por los actos que uno ejecuta, sin que sean obligatorios, es la garantía del cumplimiento de compromisos adquiridos, genera confianza, reciprocidad y tranquilidad en las personas.

1.6 Sector

El Grupo Financiero se clasifica en el sector de "servicios"

1.7 Tamaño

a) Personal en nómina: 27,000 trabajadores en nómina interna.
b) Tamaño de la empresa: Grande.

1.8 Procesos principales

En la figura 2 se encuentran los procesos principales del Grupo Financiero, en donde podemos ver que la Captación, la Colocación y los Servicios son los principales procesos de la institución, ya que con ellos se alimenta al banco de dinero y con esto puede realizar todas las demás actividades. El proceso de Continuidad del Negocio en donde se realizó el proyecto, se encuentra inmerso en "Procesos de apoyo – Servicios Corporativos"

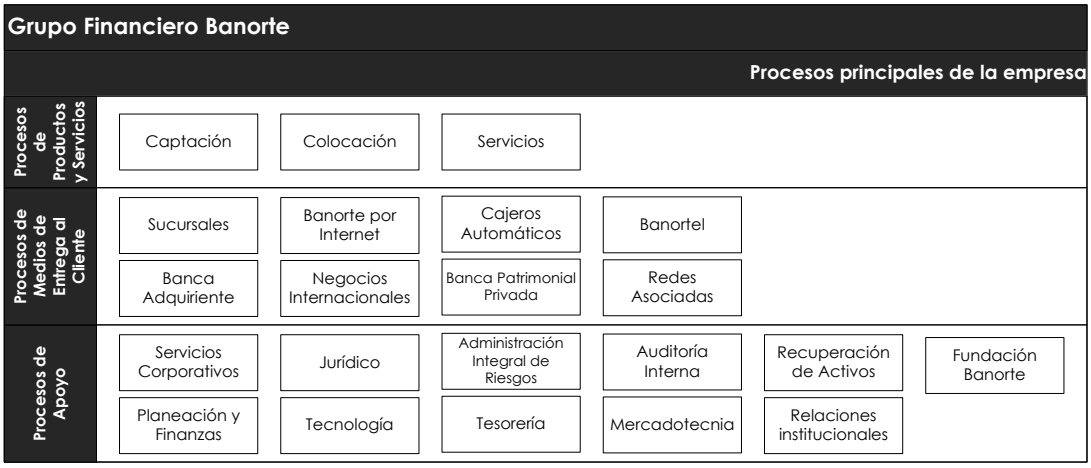


Figura 2 Diagrama de procesos principales del Grupo Financiero

1.9 Organigrama

El Grupo Financiero es una empresa muy grande, la cual está dividida en 15 direcciones generales, que a su vez cuentan con direcciones ejecutivas, en la figura 3 se puede observar a detalle la distribución de la Dirección General de Servicios Corporativos de donde forma parte el área de Continuidad del Negocio y los puestos que ahora la conforman, lo cual nos ayudará a darle claridad a la administración del área, en los siguientes capítulos de este trabajo.

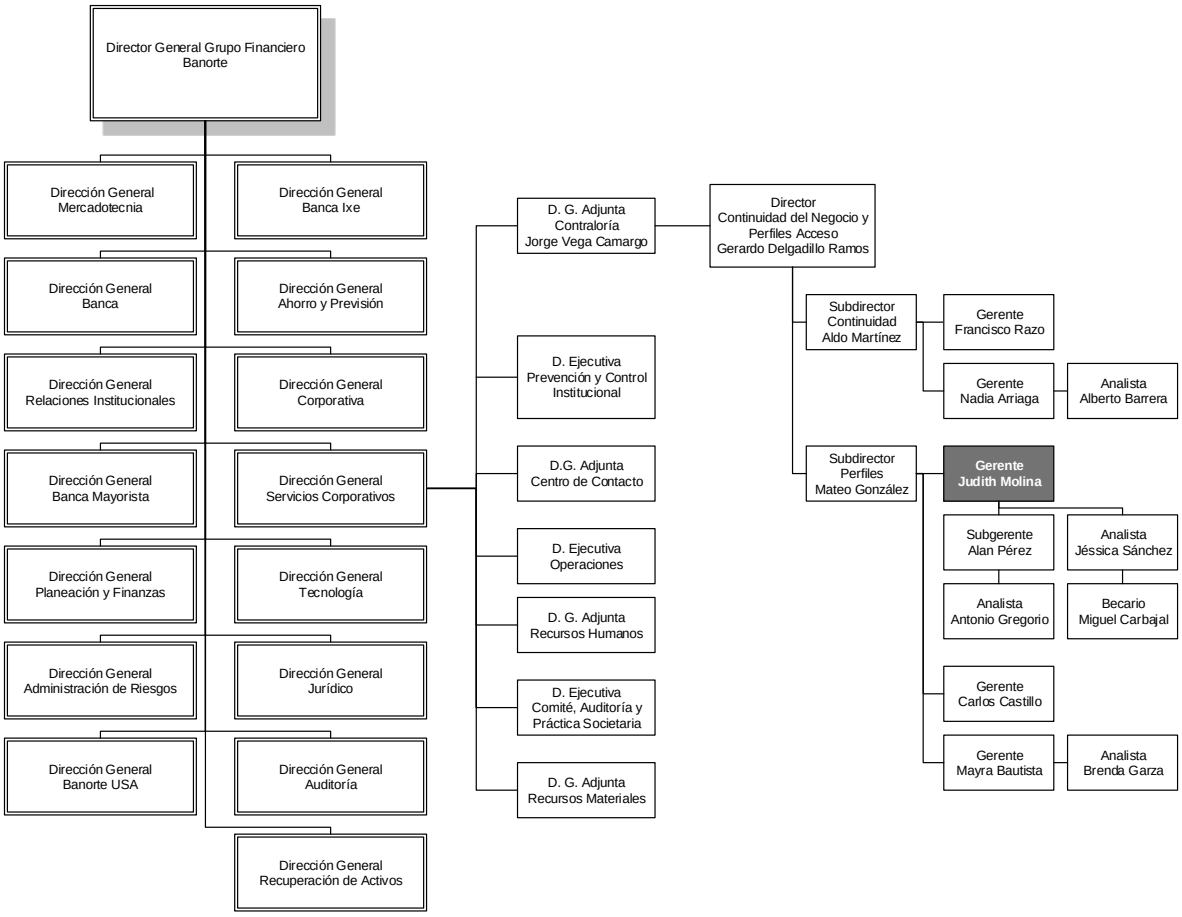


Figura 3 Organigrama general del Grupo Financiero

Capítulo II: Análisis del puesto de trabajo

2.1 Nombre del área

La experiencia profesional se desarrolla dentro del área llamada Continuidad del Negocio.

2.2 Descripción del área

Para conocer la naturaleza y actividades del área en la que se hizo la práctica profesional, se pone a continuación una explicación del tema de Continuidad del Negocio y su metodología de gestión a nivel internacional.

2.3 Continuidad del Negocio y su gestión a nivel internacional

La mayoría de los productos y servicios que son solicitados por la sociedad son proporcionados por empresas. Para estas compañías, es muy importante garantizar a sus clientes un adecuado nivel de seguridad, disponibilidad y confiabilidad de los procesos que son esenciales para el funcionamiento de su empresa, de tal manera que asegure la sobrevivencia de su negocio. Esta disponibilidad se puede ver afectada por factores diversos ya sean naturales, humanos o técnicos. [6]

Derivado de esta necesidad surge el término Continuidad del Negocio la cual se encarga de mitigar los riesgos y recuperar los recursos necesarios de la organización, ya sean humanos, infraestructura, datos vitales, tecnología y equipos de oficina que permitan a continuar con el funcionamiento clave de la organización.

La Continuidad del Negocio es un tema que se reforzó a nivel mundial después del atentado de las Torres Gemelas en el 2001 en Estados Unidos, debido a que varias empresas (e incluso el gobierno) se mostraron vulnerables por la falta de un plan de continuidad del negocio. A partir de ese momento las empresas y gobiernos, se dieron cuenta que debían reforzar e incluso elaborar sus planes para sobrevivir ante las contingencias, creando estrategias e implementando mecanismos para responder a todo tipo de emergencias.

La realización de una buena Gestión de la Continuidad en la organización traerá grandes ventajas como:

- Administrar la continuidad del negocio.
- Resistencia del negocio ante interrupciones.
- Proteger y asegurar la imagen de la empresa.
- Abrir nuevas oportunidades de mercado y ayuda a ganar nuevos negocios.
- Aumentar la disponibilidad del negocio.

[6] "ISO 22301 Seguridad de la Sociedad: Sistemas de Continuidad del Negocio-Requisitos"", British Standards Institute (BSI)

- Estar preparados para afrontar situaciones de interrupción de sus procesos críticos.

2.4 Normas que rigen el proceso de continuidad del negocio

El proceso de Continuidad está regido bajo la metodología BCLS2000 "Administración de Continuidad del Negocio para Profesionales Avanzados" dividida en 10 pasos, emitida por el Instituto Internacional de Recuperación ante Desastres (DRII por sus siglas en inglés) y por la norma ISO 22301 emitido por el Instituto de Estándares Británicos (BSI por sus siglas en inglés) la cual se divide en dos partes (código de prácticas y especificaciones).

2.5 Fases del proceso de continuidad del negocio

Para la implementación del proceso de la Continuidad del Negocio (en adelante BCM) en una organización, se deben tener en cuenta varias fases que son necesarias para el funcionamiento eficaz y ágil de las actividades en una empresa. Estas se encuentran en la metodología propuesta por el Instituto Internacional de Recuperación ante Desastres (DRII por sus siglas en inglés) incluidas en su Programa de Desarrollo Profesional y son[7]:

A. Inicio y gestión del proyecto.
B. Evaluación y control del riesgo.
C. Análisis de impacto del negocio (BIA).
D. Desarrollo de estrategias para la continuidad del negocio.
E. Respuesta ante emergencias.
F. Desarrollo e implementación del BCM.
G. Programa de concientización y capacitación.
H. Mantenimiento y ejercicio del BCM.
I. Comunicación de crisis.
J. Coordinación con Autoridades públicas.

Para la Gestión de la Continuidad del Negocio no es necesario realizar todas las fases antes enlistadas, ya que son realizadas dependiendo de la necesidad y actividades propias del negocio.

A continuación se detallan las fases para un mejor entendimiento del alcance que tiene el equipo de Continuidad del Negocio dentro de una organización:

A. Inicio y gestión del proyecto

El objetivo de esta primera fase, es establecer la necesidad de desarrollar el BCM en la organización, de tal manera que se comunique la importancia de realizar este plan, involucrando a los directivos y el personal de la empresa. Para esto, es importante:

[7] BCLS2000 Administración de Continuidad del Negocio para profesionales avanzados

- Definir un comité responsable del plan.
- Asignar responsabilidades por cada equipo de trabajo.
- Indicar las actividades de cada una de las fases del proyecto.
- Documentar los procesos.
- Presentar los avances.
- Obtener la aprobación por parte de los directivos.

Las responsabilidades del coordinador de esta etapa son:

- Dirigir la definición de objetivos, políticas y actividades críticas.
- Coordinar y organizar directores por cada fase del proyecto.
- Controlar el proceso de BCM a través de métodos de control efectivo y gestión de cambio.
- Presentar el proceso a Directivos y personal.
- Desarrollar el plan y presupuesto para iniciar el proceso.
- Definir y recomendar procesos de estructura y gestión.
- Dirigir el proyecto a desarrollar e implementar el proceso del BCM.

B. Evaluación y control de riesgos

El objetivo de la evaluación de riesgos es identificar las amenazas internas y externas, incluyendo concentraciones de riesgo, que pueden causar la interrupción o pérdida de la Actividades Críticas de una organización, así como la probabilidad (o frecuencia) de que ocurra una amenaza y cómo es vulnerable una organización a varios tipos de amenazas permitiendo su gestión de priorización y control para formar una base en la que se establezca un programa de control y un plan de acción de gestión de riesgo. Para realizar una evaluación y control de riesgos se debe tener en cuenta lo siguiente:

- Identificar riesgos.
- Análisis/Evaluación de riesgos.
- Gestión y Control de riesgos.

Después de realizar la evaluación y el control de riesgos, los resultados obtenidos incluyen la identificación y documentación de:

- La probabilidad de ocurrencia, en la organización, a un tipo específico de amenaza.
- Concentración de riesgos donde el número de Actividades de Misión Crítica es localizado dentro del mismo edificio o en el mismo lugar.
- Una evaluación y análisis de riesgos (combinado con un Análisis de Impacto del Negocio - BIA).
- Una estrategia de gestión de control de riesgo y plan de acción.
- El enfoque de priorización del BCM y control de riesgos.

C. Análisis de impacto del negocio (BIA).

El Análisis de Impacto del Negocio (BIA – Business Impact Analysis) consiste en técnicas y metodologías que pueden ser usadas para identificar, cuantificar y cualificar los impactos de negocio y sus efectos en una organización en caso de pérdida o interrupción de las Actividades de Misión Crítica. Sin embargo, la clave para realizar un Análisis de Impacto del Negocio es analizar el negocio como un todo más no como componentes, procesos o funciones individuales.

El análisis BIA tiene en cuenta el RTO (Recovery Time Objective) y RPO (Recovery Point Objective) que deben ser establecidos por la organización. Están definidos como:

- RTO (Recovery Time Objective): El tiempo entre el punto de interrupción, y el punto en el cuál los sistemas sensibles en el tiempo deben estar funcionando nuevamente, con los datos actualizados.
- RPO (Recovery Point Objective): El punto en el cuál fueron interrumpidas las actividades del sistema debido a la ocurrencia de un determinado evento.

El objetivo de un Análisis de Impacto del Negocio es identificar las actividades de misión crítica de una organización, sus dependencias y sus puntos de fallas así como analizar el impacto y el efecto que se generaría en caso de la perdida e interrupción de las actividades de misión crítica. A su vez, informar y permitir opciones para crear una resistencia en las operaciones de negocio de la organización.

Sin embargo, el BIA posee los siguientes componentes claves:

- Cuestionarios de autovaloración – papel y digitales.
- Listas de comprobación.
- Una Matriz de Análisis de Impacto del Negocio.

Después de realizado el BIA, se obtendrán como resultados, la identificación y documentación de:

- Objetivos y salidas (servicios y productos).
- Actividades de Misión Crítica, sus dependencias y puntos de falla.
- Impactos y efectos (consecuencias) financieros y no financieros como resultado de una interrupción o pérdida de una o más actividades de misión crítica durante varios periodos de tiempo.
- Los objetivos del BCM para cada actividad de misión crítica y sus dependencias.
- Una priorización mínima y aceptable de la recuperación de los recursos.

- Registros/datos vitales.
- Usuarios y Clientes Claves.
- Proveedores (tanto dentro como fuera de la organización).

D. Desarrollo de estrategias para la continuidad del negocio

El propósito del desarrollo de estrategias consiste en identificar las alternativas de recuperación de las operaciones en los marcos de tiempo definidos. El desarrollo de las estrategias del BCM involucra los siguientes aspectos:

- Identificar los requerimientos de continuidad de la organización.
- Evaluar la compatibilidad de las estrategias contra los resultados del BIA.
- Presentar el análisis costo / beneficio de las estrategias de continuidad.
- Seleccionar los sitios alternos y de almacenamiento externo.
- Entender los términos contractuales de los servicios de continuidad del negocio.

Algunas de las alternativas de recuperación comprenden estrategias de almacenamiento externo a la organización (Ej. Hotsite, coldsite, etc.), a su vez procedimientos de recuperación interna documentados, así como acuerdos recíprocos entre empresa-empresa y/o empresa-cliente, o una utilización de combinación de estrategias.

E. Respuesta ante emergencias

El propósito de la fase de respuesta ante emergencias es desarrollar e implementar procedimientos para responder y estabilizar la situación después de un incidente y administrar el centro de operaciones de emergencia a ser utilizado como "centro de mando".

Para cumplir con este propósito es necesario que:

- Identifique componentes de los procedimientos de respuesta a emergencia.
- Especifique los procedimientos de respuesta a emergencia.
- Identifique requerimientos de control y autoridad.
- Procedimientos de control y autoridad.
- Respuesta a emergencia y recuperación de heridos.
- Seguridad y recuperación.

F. Desarrollo e implementación del BCM

Esta fase involucra el diseño, desarrollo e implementación de planes de continuidad del negocio para evitar interrupciones de acuerdo a los marcos establecidos por los RTO'S y RPO'S.

Un buen desarrollo e implementación de un BCM incluye:

- Identificar requerimientos para el desarrollo de los planes.
- Definir requerimientos de control y administración de la continuidad.
- Identificar y definir un formato y la estructura principal de los componentes de los planes.
- Elaborar un borrador de los planes.
- Definir procedimientos de gestión de crisis y continuidad del negocio.
- Definir las estrategias de evaluación de daños y reanudación.
- Desarrollar una introducción general a los planes.
- Desarrollar la documentación de los equipos de operación del negocio.
- Desarrollar la documentación de los equipos de recuperación de tecnología de información.
- Desarrollar el sistema de comunicaciones.
- Desarrollar los planes de los usuarios finales de aplicaciones.
- Implementar los planes.
- Establecer los procedimientos de control y distribución de los planes.

G. Programa de concientización y entrenamiento del BCM

Toda organización que quiera posicionarse en el mercado y estar preparada a cambios en su entorno, requiere de un constante proceso de evolución. Este proceso genera en la mayoría de los casos, cambios al interior de la empresa. Siempre que se presentan estos cambios existe un porcentaje de resistencia al cambio relacionado con el personal que interviene en dicho proceso. Es necesario que la organización prepare a sus empleados ante la presencia de un cambio, logrando minimizar esa resistencia y obteniendo mejor disposición ante situaciones de este tipo creando una cultura de aceptación ante un evento que perturbe su labor.

Son estos algunos motivos por los cuales se presenta en la gestión de continuidad de negocio una fase en la cual se trata la concientización y entrenamiento del BCM y su relación con la implementación mantenimiento, gestión y ejecución del mismo. Este proceso de conciencia es necesario que se realice en toda la organización (no solamente en el área de IT) logrando aumentar la resistencia ante riesgos. Para logran una concientización y entrenamiento necesario:

- Definir objetivos de concientización y entrenamiento.
- Desarrollar e implementar varios tipos de programas de entrenamiento.
- Desarrollar programas de concientización.
- Identificar otras oportunidades de educación.

H. Mantenimiento y ejercicio del BCM

El punto D y F hacen referencia a la realización, desarrollo e implementación de estrategias y/o planes, con el objetivo de su utilización ante una situación de interrupción de un proceso en la organización. Una vez se han declarado y documentado estas estrategias y planes, que contribuyen al proceso de normalización ante una situación de crisis, es necesario realizar pruebas para determinar la eficacia con la que puede continuar el negocio ante la presencia de una posible interrupción. Así mismo se puede evaluar el equipo y personal a cargo de cada actividad crítica, además se realizara una prueba al sistema demostrando competencia y capacidad de continuidad de negocio. Los propósitos de realizar el ejercicio son:

1. Evaluar y permitir el continuo mejoramiento del BCM en la organización logrando una recuperación prioritaria de las actividades críticas de acuerdo con los objetivos de tiempo de recuperación y los objetivos de punto de recuperación asegurando un nivel mínimo de continuidad del negocio.

2. Permite evaluar y mejorar la capacidad de competencia ante la gestión de crisis.

Con la realización del ejercicio se pueden determinar varios aspectos, entre los cuales se listan:

- Identificar el nivel de madures del BCM de la organización.
- Verificación y validación que la continuidad del negocio y los planes de gestión de crisis y estrategias son viables, efectivas, actualizadas y ajustadas al propósito.
- Verificación y validación que la capacidad y competencia de la gestión de crisis de la organización es efectiva, actualizada y ajustada a los propósitos y permiten la gestión, control y coordinación de eventos y estrategias del BCM a nivel táctico y operacional.
- Verificación y validación que los miembros y personal se familiarizan con el entendimiento de roles, responsabilidades y autoridades en la operación de la continuidad del negocio y proceso de administración de crisis.

- La formación de conciencia involucrando individuos usando la continuidad del negocio y los planes de gestión de crisis.
- El ensayo y familiarización de los miembros del equipo y personal con sus roles responsabilidad y autoridad en la operación de la continuidad del negocio y planes de gestión de crisis.
- Pruebas técnicas, logísticas, de administración y otras de sistemas operacionales de continuidad del negocio y planes de gestión de crisis.
- Probar la organización e infraestructura de la gestión de continuidad del negocio incluye centros de comando, áreas de trabajo, recursos de recuperación de tecnología y telecomunicaciones.
- El ensayo de la disponibilidad y traslado del personal.
- Verificación y validación que el plan de continuidad de negocio refleja las actuales prioridades del negocio.
- La disposición de mecanismos para reforzar la continuidad del negocio y auditoria y mantenimiento de la gestión de la crisis.
- Una demostrable continuidad del negocio, capacidad y competencias en la gestión de crisis.
- Documentar resultados.
- Incrementar la cultura de los procedimientos de conciencia.
- Incrementar la conciencia del significado del BCM.
- La oportunidad de identificar defectos y mejorías de la organización del BCM, administración de crisis y planes de continuidad de negocio.
- Documentación y evaluación del ejercicio.

Para lograr estos resultados es necesario seguir un proceso en la elaboración de una prueba.

Principalmente se establecen directores de cada área de organización, se planean los escenarios en los cuales se van a llevar a cabo las pruebas, mismas que deben contar con un grupo de administración encargados de la logística, recursos, listas de verificación y estructura. Posteriormente, se hacen ajustes al programa y se documentan las actividades junto con la información de los participantes, al finalizar, se evalúan y analizan los resultados para considerarlos en las siguientes pruebas.

1) Mantenimiento

El proceso de gestión de continuidad de negocio no finaliza con la realización del documento en el cual se plasman estrategias y se asignan roles o equipos de trabajo a las áreas organizacionales; es quizás el proceso de mantenimiento del plan un punto importante si se quiere hacer uso de este considerando que el negocio continúa y

está en constante cambio. El propósito de este proceso de mantenimiento es asegurar que la gestión de continuidad del negocio incluyendo la gestión de crisis permanezca efectivo, con el objetivo de ser capaz de lograr la recuperación de actividades de misión crítica y sus dependencias dentro de los objetivos de tiempo de recuperación y los objetivos de punto de recuperación asegurando una continuidad de sus servicios y productos.

Con la realización del mantenimiento al BCM podremos obtener:

- Pruebas definidas y documentadas para la gestión y gobierno pro activo del programa de mantenimiento y monitoreo del BCM respecto a actividades de misión crítica y sus dependencias.
- Detalles de todos los cambios de estrategias del BCM y planes de continuidad de negocio documentados con toda la historia de estrategias y detalles de control de versiones.
- Verificación y validación de políticas, estrategias y planes BCM.
- Identificación e inclusión de cambios en los sistemas y proceso de la organización.
- Identificación e inclusión de cambios en legislación y regulación para la industria.
- Verificación y validación de análisis de impacto y de riesgos basados en las estrategias y planes BCM.
- Verificación y validación que las estrategias y planes BCM son actualizados, precisos y completos.
- Verificación y validación que la capacidad del BCM (incluyendo planes y estrategias) son actualizadas.
- Verificación y validación que los planes continuidad de negocio siguen una secuencia lógica, formato, estructura conforme a las directrices y estándares de buenas prácticas.
- Verificación y validación que los cambios de procedimiento y procesos son puestos.
- Verificación y validación que el personal tiene entendido los roles de responsabilidad y le es claro el plan BCM.

Los resultados que se obtendrán con el proceso de mantenimiento son de gran utilidad para la organización, previniendo que los documentos realizados queden obsoletos con el paso de los años. Para realizarlo es necesario tener una clara definición y documentación del programa de mantenimiento y monitoreo, incluyendo políticas, marcos y procesos así como la estrategia de negocio operacional.

La tecnología de información IT es un gran apoyo en los proceso de una organización, es necesario que se realice un análisis de la

tecnología requerida por la organización cuando se tienen interrupciones en el sistema, para este punto el estándar ISO 17999 el cual trata sobre la seguridad de IT será de gran ayuda.

Para la realización de cualquier plan es necesario tener en cuenta la legislación existente, para tener una base y cumplir con la normatividad que se exige. El proceso de mantenimiento requiere de un subconjunto de procesos auditoria ejercicio y aseguramiento que permiten su fortalecimiento, capacidad de continuidad y soporte a la gestión de continuidad de negocio en su aplicación a la organización cuando lo requiera.

2) Auditoria

Luego de haber realizado los procesos de ejercicio y mantenimiento sigue un proceso de auditoría que se hace necesaria en cualquier proceso al interior de la organización. El propósito de la auditoria en la gestión de continuidad de negocio es revisar los estándares del BCM identificando defectos y dificultades, proporcionando recomendaciones de acuerdo a estándares predefinidos. La auditoría revisara varios aspectos en la organización algunos de ellos son:

- Resistencia (aplicación de planes y estrategias en crisis).
- Políticas, estrategias, marcos y planes continúa bajo presión de acuerdo a estrategias, prioridades y objetivos.
- Políticas, estrategias, marcos y planes continúa bajo presión de acuerdo a las directrices de buenas prácticas.
- El BCM es competente de acuerdo al propósito.
- Los planes y soluciones son efectivos y actualizados de acuerdo al propósito.
- Implementa sus programas.
- Documenta el control, procesos y procedimientos operando efectivamente.

En la realización de la auditoria como en cualquier proceso existen componentes. Para el caso el artículo mencionan algunos como son: definición y documentación del programa de auditoria, auditar el plan de auditoria, buscar expertos internos y externos, aplicar los estándares de auditoria, actualizar estrategias del BCM, tener en las normas de requerimientos, legislación directrices de buenas prácticas, estándares (ISO 17999), realizar programas de conciencia y formación, actualizar análisis de impacto, estrategias y planes a ser auditados. Para poder obtener estos resultados el proceso de auditoria debe seguir métodos y/o técnicas que optimicen este

proceso. Algunas técnicas y/o metodologías que se nombran son: Auto evaluación, auditoria forense, cumplimiento de auditoria, diligencia auditoria, viabilidad de auditoria, control de auditoria, mejor valor auditado. Con el seguimiento de estas técnicas y la ayuda de los responsables, el proceso de auditoria podrá cumplir su propósito y así dar un informe para la organización en el cual se presenten los resultados de los procesos auditados.

I. Comunicación de crisis

La comunicación de crisis se propone desarrollar, coordinar, evaluar y ejercitar planes para comunicarlos a directivos, personal, usuarios, proveedores y medios de comunicación, de tal forma que el entorno de la organización se entere de su estado y en caso de crisis poder reaccionar de forma adecuada para minimizar los costos de interrupción de los procesos internos. Para ello, el BCM debe contener un listado de clientes, proveedores y medios de comunicación entre otros, en el cual se muestren los datos básicos de cada contacto.

J. Coordinación con autoridades públicas

La organización debe tener una clara definición y documentación de las políticas a implementar como un documento obligatorio en la organización. Por lo tanto, la organización verá los resultados en la mejoría de los procesos de toda su organización, tomando en cuenta que las políticas están dirigidas a la organización como un todo. En la metodología se describen algunos resultados como los siguientes.

- Un efectivo propósito de competencia y capacidad del BCM.
- Creación de conciencia en toda la organización.
- Una clara definición y documentación de un conjunto de principios del BCM.
- Una clara definición y documentación de un conjunto de guías y estándares mínimos del BCM.
- Una clara definición y documentación de estrategias del BCM.
- Una clara definición y documentación del marco operacional del BCM.
- Asegurar el personal apropiado.
- Una clara definición y documentación de procesos del programa del BCM de gestión de la organización.
- Una clara definición y documentación de garantía de procesos del programa BCM de gestión de la organización.
- Asegurar que los directivos y personal de la organización son conscientes y cumplen con las normas pertinentes y requisitos legislativos.

El documento contiene las políticas de la organización deberá estar compuesto por los siguientes aspectos entre otros.

El alcance

- Declaración del contenido de las políticas.
- Objetivos.
- Roles, responsabilidades.

METODOLOGÍA

Mejores prácticas Disaster Recovery Institute International (DRII)

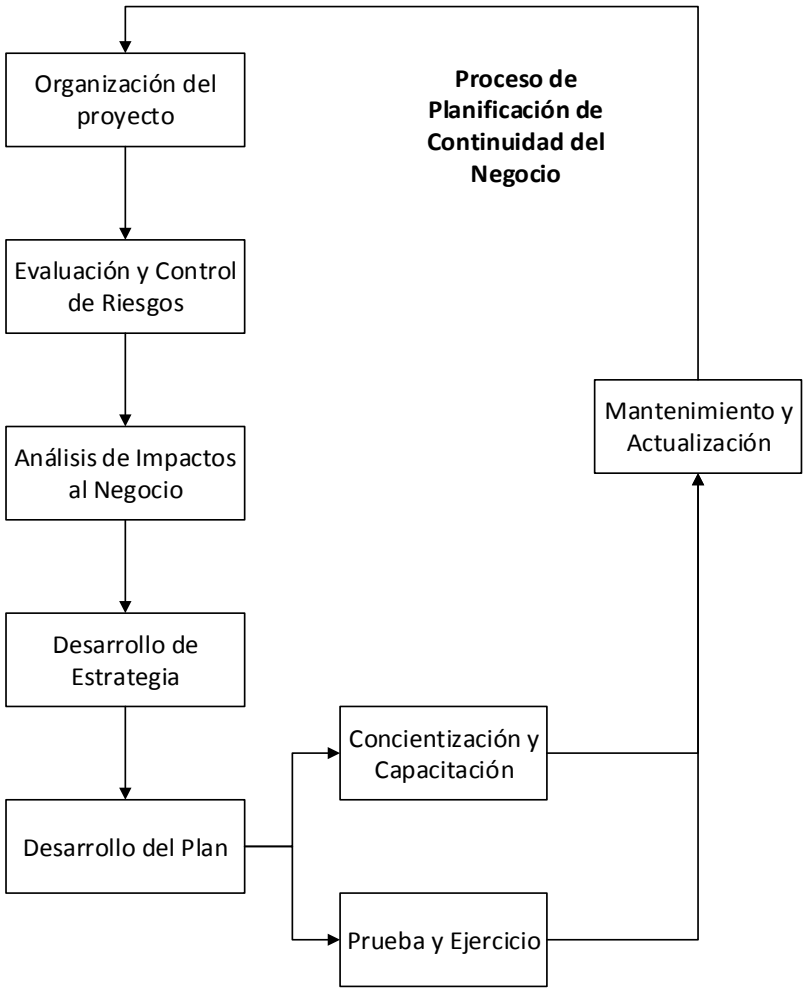


Figura 2.1

2.6 Número de personas en el área

El área de Continuidad del Negocio del Grupo Financiero esta conformado por 14 personas, en la figura 1.3 del capítulo anterior se muestra la distribución del personal y las dependencias entre ellas, así como la relación institucional del área con las otras direcciones generales de la Institución.

2.7 Descripción de las labores desempeñadas

Durante el periodo enero del 2012 a septiembre del 2019, se desempeñaron las siguientes actividades.

Datos de los puestos que se han desempeñado	
Puesto Inicial	Subgerente de Continuidad del Negocio
Puesto intermedio	Gerente de Continuidad del Negocio
Último puesto	Gerente de Perfiles de Acceso

Funciones principales:
Elaboración del plan anual de pruebas de Continuidad del Negocio, con el cual se validan las estrategias de recuperación de los procesos y aplicativos críticos en caso de contingencias.
Actualización de los Centros de Operación Alterno para que en caso de contingencia operativa se tengan los recursos listos para operar.
Actualización del Análisis de Impacto al Negocio de los procesos críticos mejorando la documentación de los procesos.
Administración de la información del área para dar atención oportuna a las auditorías internas y externas.
Elaboración de un tablero con indicadores para informar al inicio del día la apertura de las operaciones de las áreas críticas, canales de atención, edificios corporativos y cambios importantes en los sistemas.
Diseño de un e-learning y del plan de concientización con información básica de las mejores prácticas sobre Continuidad del Negocio para usuarios críticos, personal interno y de nuevo ingreso.
Elaboración de un procedimiento para comparar las bases de datos del personal crítico contra la de Recursos Humanos, para identificar bajas y cambios de área con la finalidad de tener actualizados los planes.
Desarrollo de procedimientos para el Análisis de Criticidad para Proveedores Críticos y Notificación de Contingencias a la Comisión Nacional Bancaria y de Valores.
Elaboración de matrices de cumplimiento para la gestión de Continuidad de acuerdo a lo establecido por la regulación.
Análisis de riesgo de los procesos críticos para identificar controles que mitiguen el impacto de los eventos de contingencia.
Elaboración del proceso de certificación de Perfiles de Acceso, en la que se revisa el acceso de los usuarios dados de alta en las aplicaciones validándolo contra su descripción de puesto, identificando usuarios con accesos innecesarios, solicitando su baja o modificación de atributos reduciendo riesgos potenciales.

Capítulo III: Antecedentes del proyecto

Los Bancos están supervisados por entidades regulatorias del gobierno, que emiten documentos con lineamientos y requisitos a cubrir en procesos claves para poder garantizar la calidad de su operación de acuerdo a estándares internacionales.

Uno de esos reguladores, es la Comisión Nacional Bancaria y de Valores (en adelante CNBV) la cual emitió durante el 2014 cambios en sus "Disposiciones de carácter general aplicables a las instituciones de crédito", en su anexo 67 "Requerimientos mínimos del plan de Continuidad del Negocio" fracción I, inciso h, "Las Instituciones, previo al desarrollo del Plan de Continuidad de Negocio deberán llevar a cabo un análisis de impacto al negocio que: Identifique y evalúe los riesgos relacionados con los procesos operativos y servicios de procesamiento y transmisión de datos contratados con proveedores, así como los relacionados con custodia y resguardo de información de la Institución o de sus clientes." [8]

Por lo que surgió la necesidad de realizar un procedimiento que identifique y evalúe los riesgos de los proveedores críticos, basándose en la metodología de Modelado de Procesos, la cual establece un conjunto de métodos, herramientas y tecnologías para diseñar, representar, analizar y controlar procesos de negocio[9], considerando las siguientes fases.

• Establecimiento de puntos generadores de riesgos: En el capítulo 2 se describe la metodología de Continuidad del Negocio, con la cual se definieron los criterios que evaluarán a los proveedores para identificar riesgos potenciales.

• Identificación de proveedores: Posteriormente, se identificaron los proveedores y se clasificaron de acuerdo a su naturaleza para mantener un inventario actualizado.

• Elaboración del material para la evaluación de proveedores: De acuerdo a los puntos generadores de riesgos identificados, se generó el material para evaluar a los proveedores, el cual consta de un cuestionario que deberá ser llenado por ellos y una plantilla para evaluar sus respuestas.

• Elaboración del procedimiento: Se realizó la documentación y formalización del procedimiento para posteriormente publicarlo en la Normatividad de la Institución.

• Implementación: De acuerdo al plan anual desarrollado, se inició con el procedimiento para los proveedores identificados previamente.

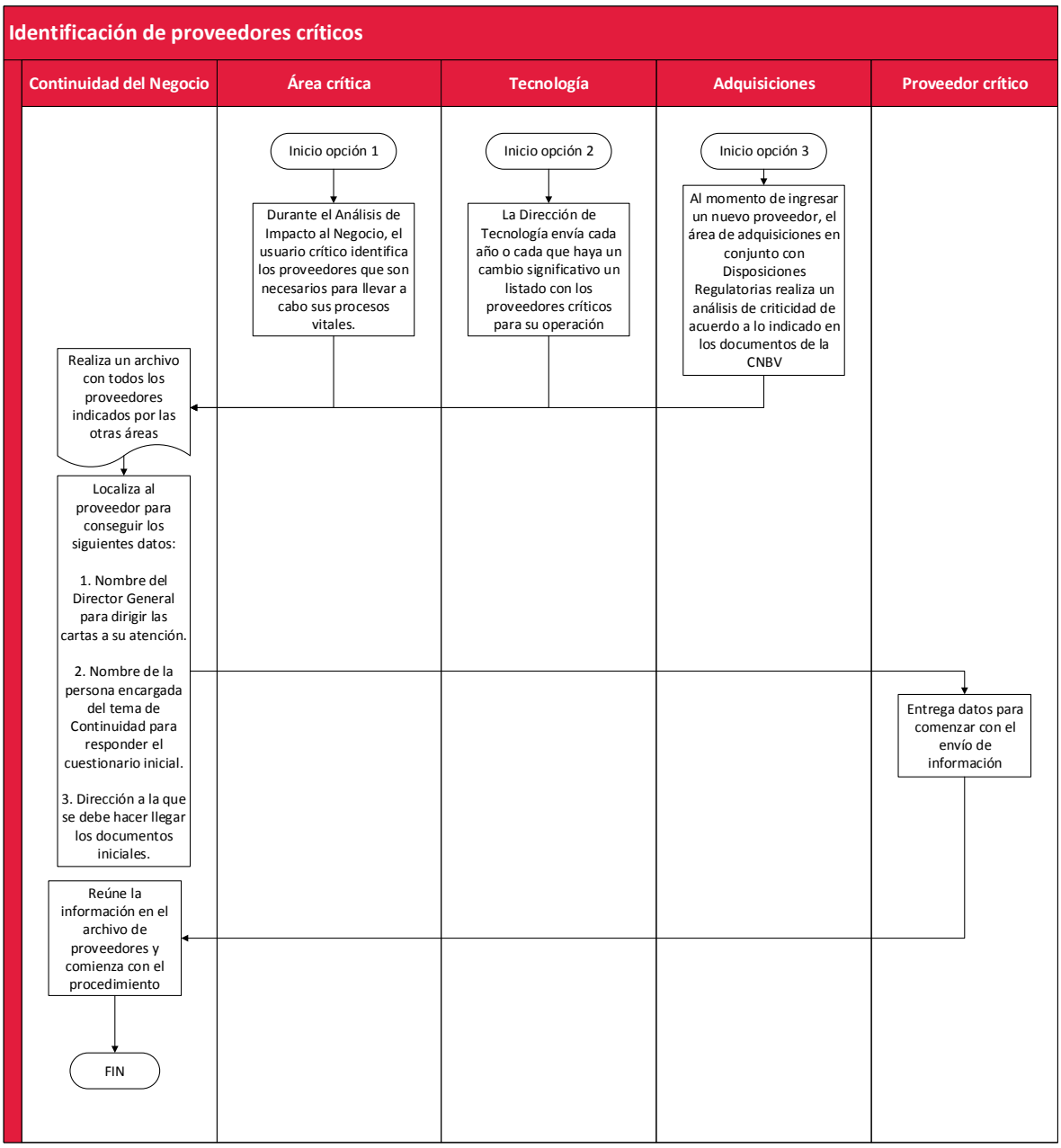
• Generación de resultados: Se analizaron los resultados obtenidos de la implementación de acuerdo al material elaborado, identificando brechas y proponiendo mejoras para el proceso.

[8] Anexo 67 "Requerimientos mínimos del plan de continuidad del negocio", Disposiciones de carácter general aplicables a las instituciones de crédito. Comisión Nacional Bancaria y de Valores.
[9] White, Stephen A., BPMN Guía de referencia y modelado, 2009, p. 20

Capítulo IV: Implementación del proyecto

4.1 Elaboración de una guía para la identificación y clasificación de los proveedores críticos.

Con el siguiente diagrama de bloques se muestra el flujo que se deberá seguir para identificar a los proveedores, siendo esto el insumo del proceso para obtener una relación de proveedores y clasificados como críticos a los que se le deberá enviar el cuestionario para la detección de riesgos.



Al implementar el proceso de identificación, se obtuvieron los resultados indicados en el "Anexo 1: Creación de base de datos con la identificación y clasificación de los proveedores críticos del Grupo Financiero".

En donde se establecen las siguientes clasificaciones de acuerdo al servicio contratado por el proveedor:

- **Operativo relevante (OR)** si no se cuenta con el servicio del proveedor no se puede realizar el proceso crítico del Banco.
- **Procesamiento de datos (PD),** es aquel proveedor que acumula y manipula los datos para producir información significativa para la operativa de un proceso interno de la Institución
- **Transmisión de datos (TD),** proveedor por el cual se realiza transferencia de datos por un canal de comunicación punto a punto o punto a multipunto.
- **Custodia de información (CI),** proveedor por el cual se vigila, cuida y protege información sensible de la operación crítica.
- **Resguardo de información (RI),** proveedor el cual guarda información referente a la operación crítica con el objetivo de futuras aclaraciones.
- **Entidad del Gobierno (EG)**
- **Personal Operativo (PO),** proveedor el cual proporciona personal que da soporte directo o Software o Hardware de la operación crítica.
- **Desarrollo de sistemas (DS)**

4.2 Elaboración del material para la evaluación de proveedores

Después de contar con la lista de los proveedores y datos de contacto, se generó un cuestionario que mide el nivel de madurez de la continuidad del negocio del proveedor crítico, logrando la identificación de riesgos de acuerdo a las mejores prácticas descritas en el punto 2.2.1 Continuidad del Negocio y su gestión a nivel internacional, el cuestionario está desarrollado en el anexo 2 "Cuestionario de evaluación de riesgos para proveedores críticos en materia de Continuidad del Negocio".

Para efectos de realizar un análisis controlado para todos los proveedores, se realizó una plantilla semiautomática que envía el resultado de la evaluación con base a lo que respondieron, tomando en cuenta el impacto que representa para el Grupo Financiero que el proveedor no cuente con elementos adecuados para la administración de la Continuidad del Negocio.

En el anexo 3 "Análisis de proveedores" se puede ver la plantilla desarrollada para esta actividad, la cual considera las siguientes actividades para su diseño:

1. Identificación del proveedor a revisar.
2. Servicios críticos que el proveedor le otorga al Banco.
3. Personal del equipo de Continuidad del Negocio que hace la revisión.
4. Indicación de la severidad en caso de que se materialice un evento: La Severidad de un riesgo es el valor asignado al daño más probable que

produciría si se materializa. Para asignar este valor, la persona que califica deberá imaginar el daño que más frecuentemente podría ocurrir de materializarse el riesgo detectado, y lo habrá comparado con los daños descritos en la siguiente tabla, contando con los siguientes valores a seleccionar.

Severidad		
Seleccionar la severidad del proveedor a revisar		
VALOR CUANTITATIVO	**VALOR CUALITATIVO**	**DESCRIPCIÓN**
2	Insignificante	No afectaría el servicio a los clientes ni a procesos detectados como críticos.
4	Menor	Podría incomodar a los clientes, podría afectar parcialmente los procesos críticos.
12	Moderado	Podría afectar algunos clientes, podría afectar totalmente a un proceso crítico
48	Mayor	Afecta a los clientes y a varios procesos críticos
96	Muy grave	Paraliza la operación de las áreas críticas, no se otorga el servicio a los clientes.
200	Catastrófico	Pérdida potencial de clientes, daño reputacional grave y perdida de la operación de procesos críticos del banco.

5. Indicación de la probabilidad de que se materialice un evento: Número de veces que se ha materializado el riesgo durante un período determinado. Para asignar, el usuario interno al que le presta el servicio el proveedor deberá indicar este valor, contando con los siguientes rubros a seleccionar.

Frecuencia (dato entregado por el negocio)		
Seleccionar la frecuencia del proveedor a revisar		
1	Rara	1 Evento al año o menos
2	Poco Frecuente	de 1 evento al semestre a 2 al trimestre
3	Frecuente	de 1 a 3 eventos por mes
4	Muy Frecuente	de 1 a 4 eventos por semana
5	Casi Cierta	1 evento al día o más

6. Vulnerabilidades: actividades que en caso de no ser cumplidas pudieran ocasionar que al momento de materializarse un riesgo la empresa será susceptible a efectos dañinos para la institución. Para la identificación de dichos valores se deberá revisar el cuestionario previamente llenado por el proveedor y responder cada punto de la siguiente lista.

RIESGOS	VALOR DE NIVEL DE RIESGO Muy alto (4) Alto (3) Medio (2) Bajo (1)
No se cuenta con un análisis de riesgos donde se contemple el edificio desde donde se prestan los servicios.	3
No se encuentran identificados los servicios prestados en sus planes de continuidad	4
No se encuentran identificados los escenarios a los que pudieran estar expuestos los servicios prestados.	3
No se tiene un análisis de impacto al negocio para los servicios contratados	4
No se tiene identificado un tiempo de recuperación objetivo (RTO) para los servicios contratados	4
No se tiene identificado un punto de recuperación objetivo (RPO) para los servicios contratados	4
No se cuenta con una lista de prioridades para levantar los servicios contratados por el Banco	2
No cuenta con planes de recuperación para servicios de tecnología	4
No cuenta con planes que contemplen escenarios de indisponibilidad de edificios	4
No cuenta con planes que contemplen escenarios de indisponibilidad de personal	3
No cuenta con planes que contemplen escenarios de falla por ciberataques	4
No cuenta con un proceso de comunicación en crisis	3
No se hace la notificación detallada de los eventos	2
No se tiene identificado un contacto para notificar un evento	2
No se tiene un tiempo determinado para notificar en caso de un evento	2
No se hacen pruebas de los servicios en un esquema de recuperación ante desastres (Tecnológicos)	4
No se hacen pruebas de conexiones de comunicación	3
No se hacen pruebas de ataque cibernético	4
No se hacen pruebas de estrategias continuidad del negocio de los servicios contratados	4
No se hacen de conocimiento al Banco sobre los resultados de las pruebas realizadas	2
No se hacen las pruebas al menos una vez al año para todos los escenarios	3
No se realizan matrices de pruebas de los servicios	1
No se realizan actas de hechos de las pruebas de los servicios	1

7. Cumplimiento: Al leer las respuestas del proveedor, se va identificando si cada riesgo de la tabla anterior se cumple o no, otorgando un cero en caso de que si se cumpla y un uno en caso de que no se cumpla la actividad.
    - Actividad de riesgo cumplida=0
    - Actividad de riesgo no cumplida=1

8. Resultado final: tomando en cuenta todos los elementos anteriores, el archivo arroja el resultado de la revisión y la calificación final del proveedor.

    - Cálculo= Severidad*Probabilidad*Nivel de riesgo*Cumplimiento

RESULTADO	Rangos de tolerancia
Aceptable	0 al 20%
Parcialmente aceptable	21% al 30%
No aceptable	31% al 100%

4.3 Elaboración del procedimiento

Para que esta propuesta fuera aprobada y formalizada en la institución, se creó y documento un procedimiento de evaluación de proveedores bajo el formato organizacional para su publicación en la Normatividad Institucional, mismo que se detalla en el anexo 4 "Procedimiento institucional: Evaluación de Proveedores Críticos en Materia de BCP".

4.4 Implementación

Para su implementación se elaboró un plan dividido en 3 bloques el cual inicio en enero del 2017.

Etapa	Descripción	Tiempo asignado
E	Envío de carta formal para procedimiento	1 semana
C1	Análisis de C1 y envio de C2	2 semanas
C2	Análisis de C2	4 semanas
D	Dictamen	3 semanas
PR	Plan de remediación	2 semanas

PLAN DE IMPLEMENTACIÓN BLOQUE 1

DATOS			ENERO					FEBRERO				MARZO			
No	Proveedor	Tipificación	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11	S12	S13
1	Total Syistem	Negocio	E	C1		C2				D			PR		
2	PROSA	Negocio	E	C1		C2				D			PR		
3	CECOBAN	Negocio	E	C1		C2				D			PR		
4	CMP	Negocio	E	C1		C2				D			PR		

PLAN DE IMPLEMENTACIÓN BLOQUE 2

DATOS			MARZO	ABRIL				MAYO					JUNIO	
No	Proveedor	Tipificación	S13	S14	S15	S16	S17	S18	S19	S20	S21	S22	S23	S24
5	Cometra	Negocio	E	C1		C2				D			PR	
6	Sepsa	Negocio	E	C1		C2				D			PR	
7	Seguritec	Negocio	E	C1		C2				D			PR	
8	Tenoval	Negocio	E	C1		C2				D			PR	
9	Panamericano	Negocio	E	C1		C2				D			PR	
10	Lock	Negocio	E	C1		C2				D			PR	
11	Prosegur	Negocio	E	C1		C2				D			PR	
12	Armstrong	Negocio	E	C1		C2				D			PR	

PLAN DE IMPLEMENTACIÓN BLOQUE 3

DATOS			JULIO	JULIO						AGOSTO				SEPTIEMBRE
No	Proveedor	Tipificación	S25	S26	S27	S28	S29	S30	S31	S32	S33	S34	S35	S36
13	Red Uno	Tecnología	E	C1		C2				D				PR
14	Getronics	Tecnología	E	C1		C2				D				PR
15	SWIFT	Tecnología	E	C1		C2				D				PR
16	KIO	Tecnología	E	C1		C2				D				PR
17	IBM	Tecnología	E	C1		C2				D				PR

4.5 Entrega de resultados

Las actividades se llevaron a cabo de acuerdo a lo planeado obteniendo las siguientes respuestas por parte de los proveedores críticos:

Fase del procedimiento	Proveedores que cumplen con la fase	Porcentaje de participación de los proveedores
Entrega de carta inicial por parte del Banco	21	100%
Entrega de cuestionario respondido por parte del proveedor	15	71%
Análisis y entrega de dictamen por parte del Banco	15	71%
Entrega de plan de remediación por parte del proveedor	14	67%
Envío de carta final por parte del Banco	13	62%

Del total de proveedores, 13 concluyeron el procedimiento lo que representa un 62% de cumplimiento tras la implementación del nuevo procedimiento, encontrando brechas importantes que se describen más adelante.

En el anexo 6 "Análisis de proveedores" se pueden observar los resultados obtenidos, en la siguiente tabla se muestran los resultados de proveedores a los que se les emitió un dictamen:

Proveedor	Resultado	Riesgos no controlados	Riesgos parcialmente controlados	Riesgos controlados
PROSA	Aceptable	3	1	19
CMP	Aceptable	3	2	18
TSYS	No aceptable	18	5	0
SEPSA	Parcialmente aceptable	5	4	14
TECNOVAL	Parcialmente aceptable	5	4	14
PANAMERICANO	Aceptable	5	0	18
COMETRA	Parcialmente aceptable	5	4	14
SEGURITEC	Parcialmente aceptable	5	4	14
GETRONICS	Aceptable	8	1	14
KIO	No aceptable	12	9	2
ASIGNET	No aceptable	5	10	8
CIBERGESTIÓN	No aceptable	10	2	11
IBM	Aceptable			

Conclusiones

Tras el desarrollo de este nuevo procedimiento y tomando los resultados de su implementación, se llegaron a las conclusiones siguientes:

1. La elaboración del procedimiento ayudó al área de Continuidad del Negocio a tener una mayor eficiencia en los tiempos de respuesta con los proveedores, agilizando la solicitud de información a través de un solo documento (llamado aquí cuestionario) el cual considera los criterios necesarios para llevar a cabo un análisis completo de su manejo de la continuidad del negocio, apoyando a cumplir con los objetivos anuales del área. La recomendación de mejora entregada al director del área para este punto, consiste en estructurar todos los procedimientos que conforman el área a través de métricas para poder lograr un mayor entendimiento de los resultados obtenidos y una mejora continua de los procesos. Actualmente, el área de continuidad no tiene normados todos sus procedimientos y los que están normados no son llevados de acuerdo a lo planeado, esta mala práctica debe erradicarse para comenzar a formar procedimientos que ayuden a hacer más eficaz el trabajo, mejorando tiempos y aprovechando los recursos disponibles.
2. Se cumplió con los objetivos propuestos para este trabajo en el diseño e implementación del procedimiento, dando cumplimiento con lo establecido por la Comisión Nacional Bancaria y de Valores a través de su Circular Única de Bancos.
3. Con el paso del tiempo se detectaron brechas que son relevantes para lograr una participación más activa por parte de los proveedores:
    a. Desconocimiento por parte de los proveedores sobre la regulación para prestar sus servicios a una institución financiera. Se propuso emitir junto con las propuestas de licitaciones, un apartado de obligaciones a cumplir que establecen las entidades regulatorias como Banco de México, la Comisión Nacional Bancaria y de Valores, etc para su conocimiento.
    b. Falta de interés por parte de los proveedores activos para cumplir con los lineamientos mínimos del Banco para poder ser clasificados como proveedores críticos. Por lo que se propuso que en caso de no contar con un esquema de Continuidad del Negocio sólido se puede cesar el contrato celebrado anteriormente y en nuevos contratos agregar cláusulas que indiquen que la Institución posee la facultad o derecho de hacerlo.
    c. Se observo que algunos proveedores no tienen conocimiento de las prácticas de Continuidad del Negocio, siendo dictaminados como "No aceptable" presentando muchas áreas de oportunidad en materia de seguridad y prestación de servicios en contingencia.

4. Se presentó un alto porcentaje de proveedores que no cumplieron con todas las etapas del procedimiento, por lo que se entregó una propuesta al director del área para diseñar un nuevo plan para el 2018, en el que se dio un mayor seguimiento con el proveedor para identificar donde se encontró la brecha, durante ese año se logró obtener la información faltante y se revisaron más proveedores, ampliando el alcance y logrando terminar la implementación del procedimiento planteado.

5. Tras concluir mis estudios en la Facultad de Ingeniería adquirí conocimientos para planear, diseñar e implementar nuevos procesos con apoyo de las asignaturas vistas en carrera de Ingeniería Industrial ayudando a cumplir con los objetivos establecidos en la empresa. Estoy segura que en el camino profesional los conocimientos adquiridos en la carrera podrán ser de gran ayuda para impulsar mi trabajo, realizar implementaciones de calidad y sobresalir positivamente.

BIBLIOGRAFÍA

- Plan de estudios de la Licenciatura en Ingeniería Industrial, Universidad Nacional Autónoma De México, Facultad De Ingeniería.

- www.banorte.com “Nuestra historia”

- www.banorte.com “Nuestra identidad”

- “ISO 22301 Seguridad de la Sociedad: Sistemas de Continuidad del Negocio-Requisitos””, British Standards Institute (BSI).

- BCLS2000 Administración de Continuidad del Negocio para profesionales avanzados.

- Anexo 67 “Requerimientos mínimos del plan de continuidad del negocio”, Disposiciones de carácter general aplicables a las instituciones de crédito. Comisión Nacional Bancaria y de Valores.

ANEXO 1: CREACIÓN DE BASE DE DATOS CON LA IDENTIFICACIÓN Y CLASIFICACIÓN DE LOS PROVEEDORES CRÍTICOS DEL GRUPO FINANCIERO.

Nombre	Denominación social	Descripción de la empresa	Servicios críticos para la Institución indicados por el negocio	Naturaleza del proveedor							
				OR	PD	TD	CI	RI	EG	PO	DS
BMV	Bolsa Mexicana de Valores, S.A.B. de C.V.	El Grupo BMV se conforma por empresas que en conjunto ofrecen servicios integrales para facilitar la operación y post-negociación del mercado de valores y derivados en México apoyada por una moderna infraestructura tecnológica y de vanguardia en todas sus empresas.	Realiza los pagos de fondos Inversiones Regulador de Emisiones Proveedor principal del Market data con el que se ejecutan todas y cada una de las órdenes enviadas por los clientes de la Casa de Bolsa. Proveedor del aplicativo SENTRA	x							
Cecoban	Cecoban S.A. de C.V.	Empresa que cuenta con la autorización por parte del Banco de México para proporcionar los servicios de Cámara de Compensación Electrónica Nacional, para las operaciones de Cheques incluyendo el Intercambio de Imágenes, Transferencias de Abonos (TEF), Transferencias de Cargos (Domiciliaciones) y Compensación de Efectivo.	Centraliza el directorio de los Funcionarios de la Banca que atienden los Servicios de Transferencia Electrónica de Fondos (TEF). Si el cliente no se encuentra en el directorio no debe ser atendido. Realiza el intercambio de Cheques, Transferencias Electrónicas, Domiciliaciones con otros bancos. Tiene relación con el servicio de compensación de cheques a nivel nacional (proveedor CMP)		x	x	x				
CMP	Compañía Mexicana de Procesamiento S.A. de C.V.	Ofrece soluciones integrales en el procesamiento masivo de información, almacenamiento y resguardo, así como una amplia gama de servicios de logística y distribución.	Para los procesos relacionados a la compensación de cheques nacionales y reportería de los mismos procesos para el cuadre de compensación neta. Da servicio al banco para la revisión y envío de cheques de otros bancos recibidos en las sucursales,		x	x	x				

			y posteriormente se realiza el envío de la información a Cecoban.								
Prosa	Promoción y Operación S.A. de C.V.	Empresa que permite a las Instituciones que emiten tarjetas de nómina, vales, monederos electrónicos, crédito y débito, acceder a todos los Comercios que cuenten con Terminales Punto de Venta, Cajeros Automáticos, portales de comercio web, entre otros.	Es el proveedor principal para el Switch de operaciones POS entre Bancos del Consorcio y realizar la Compensación y Liquidación de las operaciones para abono a comercios Afiliados. En sistema SAC-PROSA se integran las cifras y reportes de Liquidación POS estos necesarios para el Balanceo contable proceso de Deposito a Comercios. Se tienen todos los reportes de la compensación, se realizan pagos a prosa por medio de SAC. Provee el aplicativo VRM-VISA para monitoreo de operaciones		x	x					
SWIFT	S.W.I.F.T. SCRL	Organización que tiene a cargo una red internacional de comunicaciones financieras entre bancos y otras entidades financieras	Sistema de Mensajerías de liquidaciones de divisas	x		x					
TriOptima	TRIOPTIMA AB	Servicios que ofrecen herramientas críticas de gestión operativa y de riesgo de crédito para la industria: triReduce para la compresión de la cartera; triResolve para la conciliación de cartera, la gestión de garantías y la validación de informes; y triCalculate para analíticas XVA y valoraciones comerciales.	Verifica el cumplimiento de los protocolos internacionales Dodd Frank y EMIR que realiza el Back Office Colaterales, si existe un incumplimiento las contrapartes pueden negarle al Front de Derivados operar con el Banco y poner en riesgo aquellas que ya estaban pactadas anteriormente.	x							

Winston Data	Winston Data SA de CV	Impresión: Procesa altos volúmenes de estados de cuenta mensuales y otros diversos documentos Digitalización: Digitaliza altos volúmenes de documentos en aplicaciones centralizadas así como también en forma descentralizada. Healthcare: otorga soluciones especialmente desarrolladas para el segmento de salud orientado a médicos, farmacias, laboratorios y otros prestadores de servicio. Win Guard: servicio de resguardo y administración de documentos físicos de manera confiable y accesible en ambiente controlado y de alta seguridad.	Intermediario de embosamiento de plásticos TDC						x			
ETV (GSI: Cometra, Seguritec, SEPSA y Tecnoval)	GSI GRUPO DE SEGURIDAD INTEGRAL S.A. DE C.V.	Servicios de guardias especializados Armados y sin armas, traslado y protección a ejecutivos, custodia de mercancías en unidades equipadas con rastreo satelital, seguridad electrónica, servicios de reacción y patrullaje en todo el territorio nacional.	Dotación de efectivo	x								
ETV (PANAMERICANO)	Servicio Pan Americano de Protección, S.A. de C.V.	Traslado de valores, proceso de valores, dotación a cajeros automáticos, importación y exportación de valores	Dotación de efectivo	x								

ETV (ARMSTRONG)	ARMSTRONG ARMORED DE MÉXICO, S.A. DE C.V.	Seguridad en procesos de efectivo y valores. Diseño y fabricación de cajas fuertes y equipos blindados. Instalación, soporte y mantenimiento de equipos blindados. Custodias y transporte de mercancía de alto valor. Cerraduras para cajas fuertes y equipos bancarios.	Dotación de efectivo	x							
GAF	GAF OPERADORA, S.A. DE C.V.	Operadora: Valuación de portafolios de Inversión de Fondos y Siefores Riesgos: Administración y Consultoría en Riesgos Financieros Fondos: Plataforma electrónica de información de Fondos de Inversión	Otorgan el servicio de contabilidad.	x		x					
BOFA	BANK OF AMERICA N.A.		Revisión de seguridad en cheques recibidos a través de la cámara de compensación, SAAC Procesos de cámara tradicional con imagen, atención de imágenes y originales de cheques procesados a través de la cámara , rescates de cheques, atención y solicitud de alertas operativas entre bancos, atención a reembolsos por cheques procesados a través de la cámara, cuadre contable de los procesos de cámara, aplicación de cargos/abonos en línea a cuentas de cheques solicitados por áreas internas administrativas, procesos de recuperación de imágenes para atención a red de sucursales, aplicación de bonificaciones en cuentas de cheques, control de exportación de remesas al extranjero, control de cobranzas				x				

			enviadas y recibidas, proceso de depósito remoto con proveedor GSI y CECOBAN.								
MarkitWire	IHS Markit Ltd	Es una ECC (contraparte central)y autoriza transacciones en instrumentos de efectivo y Derivados en el comercio organizado y extrabursátil (EMIR).	Confirmación y Liquidación de operaciones de productos derivados de posición propia y estructuración con clientes y contrapartes nacionales y extranjeras.	x							
Unisys	Unisys Corporate Compliance	Protección de empresas de servicios financieros – y sus clientes – con sistemas completos de seguridad.	Proporciona un aplicación que se llama Actimize el cual es necesario para PLD Banco y monitorear las alertas operativas en los sistemas				x				
Valmer	Valuación Operativa y Referencias de Mercado, S.A. de C.V.	Valuación Operativa y Referencias de Mercado S.A. de C.V. (VALMER) es una empresa dedicada a proporcionar diariamente, precios actualizados para la valuación de instrumentos financieros, así como, servicios integrales de cálculo, información, análisis y riesgos, relacionados con dichos precios.	Captación Institucional y Trading (Compra-Venta Directo), generación de información de pérdidas y ganancias de los portafolios de mercados y aseguramiento que las operaciones concertadas se encuentren registradas correctamente en los sistemas transaccionales. Lleva a cabo la gestión, revisión y validación de cuentas y registros contables de mercados financieros que opera la institución. Realiza el alta y administración de los valores (mercado de dinero, capitales, sociedades de inversión, etc.) y derechos corporativos y patrimoniales a los que son sujetos dichos valores. Administración de pasivos bursátiles del banco y el movimiento de cartera de clientes mediante traspaso								

			de valores así como la liberación y/o bloqueo de garantías bursátiles. Alta para de contratos para derivados, mercado de dinero, operadora de fondos, capitales y alta de cuentas de cheques. Proporciona la información correspondiente a Riesgo Mercado, Contraparte y Liquidez de manera diaria y regulatoria a diversas áreas. Las responsabilidades y actividades en materia de servicios de inversión.								
BIVA	BOLSA INSTITUCIONAL DE VALORES S.A. DE C.V	Bolsa de mercado de valores	Bolsa de mercado de valores								
AMIB	Asociación Mexicana de Intermediarios Bursátiles	Intermediario bursátil con la participación de 25 Casas de Bolsa y actualmente agrupa a 35 Casas de Bolsa autorizadas por la Secretaría de Hacienda y Crédito Público y por la Comisión Nacional Bancaria y de Valores; adicionalmente tiene afiliadas a 29 Operadoras de Fondos de Inversión y 3 empresas de corretaje de mercado de dinero.	Es la entidad regulatoria a quien se debe enviar la información contable						x		
EUROCLEAR	EUROCLREAR GROUP	Liquidación de transacciones de valores, así como en la custodia y la administración de activos de estos valores.	Liquidación de operaciones internacionales	x							

FIDEM	Consulting IT services Fidem, S. C.	Servicios orientados a solucionar y orientar a nuestros clientes sobre la valuación de instrumentos de deuda y derivados considerando metodologías estándar de mercado que permitan conciliar los criterios y diferencias entras las áreas funcionales de la organización.	Sistema de individualización en caso de no contar con el podríamos incumplir las instrucciones de los clientes o entregar información incorrecta que pueda generar quebrantos a la Institución.	x							
Indeval	S.D. Indeval Institución para el Depósito de Valores, S.A. de C.V.	Custodia y Administración de Valores. Transferencia electrónica de valores. Transferencia electrónica de efectivo. Compensación de operaciones y liquidación DVP. Liquidación de operaciones (diversos plazos) para el Mercado de Dinero (directo y reporto) y Mercado de Capitales (operaciones pactadas en la Bolsa). Administración de Colaterales.	Liquidación de operaciones de mercado de Dinero y Mercado de capitales con custodia externa. Proporciona aplicativo Indeval. Sociedad depositante a cargo de la custodia de las posiciones y administración de derechos corporativos	x							
FITCH	Fitch Inc	Servicios de información financiera con operaciones en más de 30 países. Fitch Group está compuesto por: Fitch Ratings, líder mundial en calificación crediticia e investigación; Fitch Solutions, un proveedor líder de datos de mercado crediticio, herramientas analíticas y servicios de riesgo; y Fitch Learning, una destacada firma de	Envío mensual de carta de calificación de los fondos. Se usa para cierre de mes y no se pondría la calificación actualizada, no se puede operar si no se cuenta con la calificación								

		capacitación y desarrollo profesional									
Buzón-e	Buzón E, S.A. de C.V.	Empresa dedicada a automatizar y optimizar procesos de negocio y procesos de intercambios de documentos electrónicos fiscales y no fiscales.	Proceso de enlace entre el sistema (SIAB) y el cliente para expedir las facturas de los servicios.	x							
Caarem	Confederación de Asociaciones de Agentes Aduanales de la República Mexicana, A.C.	Representa los intereses gremiales de los Agentes Aduanales y trabaja de manera conjunta con las autoridades en el incremento de la competitividad del comercio exterior a través de las aduanas	Confederación de Asociaciones de Agentes Aduanales de la República Mexicana. emisión de cartas de cupo (permisos para la entrada a deposito fiscal) se necesita la validación de esta entidad que es el enlace entre los Agentes Aduanales y el almacén.						x		
Proveedor de Rucam	Secretaria de Economía	El Registro Único de Certificados, Almacenes y Mercancías (RUCAM) es un registro público a cargo de la Secretaría de Economía (SE) en el cual se inscriben los certificados de depósito y bonos de prenda, así como las bodegas propias o habilitadas de los Almacenes Generales de Depósito. A través del RUCAM, el usuario podrá consultar y solicitar la certificación de la información registrada, facilitando el mercado de financiamiento con certificados de depósito y bonos de	Se expiden los bonos de prenda o certificación de depósitos						x		

		prenda y mejorando el acceso al crédito.									
SAP	SAP SE	SAP ERP es un software de planificación de recursos empresariales	Es el sistema donde se registran todas las operaciones contables de Almacenadora.	x							
Proveedor de NAFIN	Nacional Financiera, S.N.C., I.B.D. (NAFINSA)	Nacional Financiera contribuye al desarrollo económico de México, facilitando el acceso de las mi pymes, emprendedores y proyectos de inversión prioritarios al financiamiento y otros servicios de desarrollo empresarial, así como contribuir a la formación de mercados financieros y fungir como fiduciario y agente financiero del Gobierno Federal, que permita impulsar la innovación, mejorar la productividad, la competitividad, la generación de empleos y el crecimiento regional.	Provee el aplicativo en donde el analista de operaciones descarga los documentos cedidos a AyF para poder realizar el factoraje cadenas productivas.						x		
ACCENTURE	Accenture PLC	Empresa multinacional dedicada a la prestación de servicios de consultoría, servicios tecnológicos y de outsourcing	Proveedor de personal operativo							x	

ACI	ACI Worldwide, Inc.	Empresa especializada en pagos rápidos, simples y seguros en todo el mundo al conectar más formas de pago con más capacidades de pago que cualquier otro proveedor. Ofrecen el rendimiento, la seguridad y la escalabilidad que necesita para tener éxito hoy y mañana. Con UP, sus posibilidades de pago son ilimitadas.	Proporciona el sistema de B24, dueño del código fuente								x
Aluxit	GRUPO ALUX TECHNOLOGIES SA DE CV	Ofrece servicios para la seguridad de la información, análisis forense, análisis de riesgos y vulnerabilidades	Proveedor que ejecuta los escaneos de Pruebas de Intrusión.							x	
AVAYA	AVAYA INC.	Proveedor de teléfonos inteligentes y dispositivos multimedia que mejoran la colaboración y productividad dentro de las empresas	Provee el servicio de telefonía	x							
Black Core	Sistemas Blackcore de México S.A. de C.V.	Empresa especializada en Software y diseño	Dicho proveedor tiene el código fuente de aplicativos como SAX, ARM, SISE								x
BMC	BMC Software, Inc.	Servicios que ofrecen velocidad, agilidad y eficiencia para enfrentar los desafíos empresariales en las áreas de gestión del servicio, automatización, operaciones y servidor central.	Proveedor indispensable para aplicativo de operativa de la mesa de ayuda de ATM´s	x							
Capgemini	CAPGEMINI MEXICO S DE RL DE CV	Líder mundial en consultoría, servicios de tecnología y transformación digital.	Proporciona personal que presta servicios al Banco para mantenimiento e incidencias.							x	

Deloitte	Deloitte Touche Tohmatsu Limited	es la marca en la que decenas de miles de dedicados profesionales, en firmas independientes alrededor del mundo, colaboran para proveer servicios de auditoría, consultoría, asesoría financiera, asesoría de riesgo, impuestos y servicios relacionados.	Proveedor que ejecuta los escaneos de Pruebas de Intrusión.							X	
Diebold (Wincor)	Diebold de México, S.A. de C.V.	Proporciona hardware, software, y servicios para comercios y banca minorista.	Empresa que brinda soporte y mantenimiento a cajeros automáticos (ATMs) del Banco							X	
ESQ	ESQ Business Services	Soluciones de gestión de transacciones empresariales de clase empresarial que permiten a los bancos, minoristas y proveedores de servicios gestionados monitorear y administrar de manera proactiva las infraestructuras críticas de cajeros automáticos y pagos.	Servicio terciarizado, son los encargados de la operación, Soporte de Hardware y Software para Tandem							X	
HITSS	Hitss Solutions, S.A. de C.V.	Empresa de Soluciones Digitales y Servicios de TI	Provee personal de soporte para gestión de mantenimiento e incidencias.							X	
HP	HP Inc.	Servidores, equipos de almacenamiento y redes, programas de cómputo y servicios para terceras empresas.	Servicio terciarizado, son los encargados de la operación, Soporte de Hardware y Software para Tandem							X	
IBM	International Business Machines Corporation	Empresa multinacional estadounidense de tecnología y consultoría	Servicio terciarizado, son los encargados de la tecnología							X	
INDRA	Indra Sistemas, S.A.	Empresa global de consultoría y tecnología.	Provee personal de soporte para gestión de mantenimiento e incidencias.							X	

KEY	KEY SOFTWARE SOLUTIONS INC	Empresa consultora de desarrollo de software y tecnología de la información, dedicada al desarrollo de aplicaciones tradicionales y basadas en Internet	Servicio terciarizado, son los encargados de la operación, Soporte de Hardware y Software para Tandem							X	
LGEC	LGEC, S.A. de C.V.	Empresa dedicada al diseño y desarrollo de sistemas	Dicho proveedor tiene el código fuente de aplicativo SPEI								X
IRS	IRS, S.L.	Compañía dedicada a la consultoría e integración de telecomunicaciones y tecnologías de la información	Provee personal de soporte para gestión de mantenimiento e incidencias.							X	
NRC	NCR Corporation	Empresa de innovación y desarrollo de tecnología la empresa brinda soluciones que ayudan a mejoran el flujo de ingresos, reducir los costos de operación y mejorar la captación de nuevos clientes.	Provee personal de soporte para gestión de mantenimiento e incidencias. Atienden Ingeniería del proveedor directamente los ATM´S físicamente. Se conectan los sistemas referente a seguimiento de incidentes del proveedor y la Institución.							X	
PWC	PricewaterhouseCoopers LLP	Apoya a diversos sectores con retos en materia de gestión de talento, transformación digital, riesgos, crecimiento de estrategia y regulaciones, entre otros.	Proveedor que ejecuta los escaneos de Pruebas de Intrusión.							X	
QUITZE	Quitze soluciones	soluciones de software a la medida; desarrollando nuevas funcionalidades o reglas de negocio post implementación, basados en la administración y automatización de procesos.	Proveedor indispensable para aplicativo de operativa de la mesa de ayuda de ATM´s	X							
SASA			Proveedor indispensable para aplicativo de operativa de la mesa de ayuda de ATM´s	X							

SIMP			Son los encargados de la operación, Soporte de Hardware y Software							x	
SOFTTEK	Valores Corporativos Softtek, S.A. de C.V.	Desarrollo de software y otros servicios relacionados con las tecnologías de la información y la comunicación	Provee personal de soporte para gestión de mantenimiento e incidencias.							x	
Telesoft	Telesoft Technologies Ltd	Productos y servicios de Ciberseguridad, telecomunicaciones móviles e infraestructura gubernamental	Dueños del código del sistema que emplea Centro de Contacto								x
TELMEX (REDUNO)	Teléfonos de México, S.A.B. de .C.V. Consorcio Red Uno, S.A. de C.V.	Soluciones integrales, innovadoras y de clase mundial, a través de tecnologías de punta.	Servicio administrado de los enlaces contratados con así como los enlaces de sucursales, edificios administrativos y enlaces de cajeros	x							
Wincor	Diebold de México, S.A. de C.V.	Proporciona hardware, software, y servicios para comercios y banca minorista.	Personal que presta servicios al Banco para mantenimiento e incidencias							x	
BMC	BMC Software, Inc.	Otorga servicios de TI diversos (certificaciones, Servicios de consultoría, Soporte técnico)	Empresa que brinda servicios como Gestión de servicios de Tecnologías de la Información a las diferentes áreas o ramas del Grupo Financiero	x							
Coltomex	Coltomex S.A. de C.V.	Impresión fija y variable, insertado de hasta 4 piezas proporcionadas por el cliente, ensobrado manual y automático de estados de cuenta, personalización, clasificación y entrega a mensajerías; Desarrollo de Software.	Ensobrado y enviado de estados de cuenta y personalización de tarjetas a clientes			x	x				
ECODEX	Desarrollo Corporativo de Negocios en Tecnología de la Información, S.A. de C.V.	Timbrado Estados de Cuenta, generación cadenas de Certificado Física Digital por Internet				x	x				
F5	F5 Networks Mexico S. De R. L. De C. V.	Administración de servicios F5 Networks									

HITACHI DATA SYSTEMS	Hitachi Data Systems S.A. de C.V	Empresa dedicada al soporte sobre plataformas de Storage; se dedica a administrar los diferentes componentes de almacenamiento y respaldos (Hardware & Software)									
IKUSI MICRONET	IKUSI REDES DE TELECOMUNICACIONES, S.L.	Desarrolla actividades en el campo de la ingeniería tecnológica y el desarrollo para la transformación de negocios digitales	Soporte y administración de la Tecnología e Infraestructura para telecomunicaciones							x	
KIO NETWORKS	METRO NET S.A.P.I. DE C.V. Internet Networks, S.A. de C.V	Ofrece un portafolio de infraestructuras y servicios de tecnologías de información de misión crítica.	KIO Data Center Services. Localidad donde se encuentra ubicado el Centro Computo Alterno (CCA)	x							
Metro Red	MEXICO RED DE TELECOMUNICACIONES, S. DE R.L. DE C.V.	Operadores de servicios de telecomunicaciones alámbricas	Proveedor de Fibras Ópticas	x							
Oracle	Oracle Corporation	compañía especializada en el desarrollo de soluciones de nube y locales.	Reporte y escalamiento de eventos presentados en equipos o sistemas.							x	
VERITRAN	On Time Mobile Technologies S.A. de C.V.	Incorpora nuevas tecnologías e impulsa tu transformación digital para optimizar experiencias de uso, eficiencia operacional y agilidad, brindando innovación en tus productos y servicios.	Proveedor externo que brinda una tecnología de seguridad para autenticar a dos factores.								
Cibergestión	Cibergestión Hipotecaria, S.L	Servición de formalización hipotecaria, crédito al consumo online, Back Office (BPO) , automatización y transformación digital, vinculación con el cliente	Formalización de Créditos Hipotecarios		x	x	x	x			

MasterCard	Mastercard International Incorporated	Ofrece soluciones de pago digital en todo el mundo y ofrece beneficios para consumidores, empresas, comerciantes, emisores y gobiernos.	Administración del programa de lealtad (MasterCard Rewards System MRS)		x	x					
Microsoft	Microsoft México, S. de R.L. de C.V.	Es una compañía tecnológica multinacional. Desarrolla, manufactura, licencia y provee soporte de software para computadores personales, servidores, dispositivos electrónicos y servicios.	Proveedor de correo y paquetería (word, excel,PP) en la nube, yammer y one drive	x				x			

ANEXO 2: CUESTIONARIO DE CONTINUIDAD DEL NEGOCIO PARA PROVEEDORES CRÍTICOS

Antecedente

Para el Grupo Financiero contar con una buena Gestión de la Continuidad del Negocio demuestra un gran compromiso y sensibilización con nuestros clientes y con nuestros colaboradores. Es por esto que contar con un proveedor que tiene la posibilidad de proporcionar continuidad ante algún evento perturbador es un tema importante para la Institución al momento de considerar la adquisición de cualquier servicio.

Adicional a lo anterior y por lo señalado en el inciso h, fracción I del Anexo 67 de las Disposiciones de carácter general aplicables a las Instituciones de Crédito (Circular Única de Bancos) que establecen los "Requerimientos mínimos del plan de continuidad de negocio", se informa que la Institución llevará a cabo la presente evaluación de riesgos para continuidad del negocio sobre procesos operativos y servicios de procesamiento contratados con proveedores que soportan procesos vitales para el banco.

En resumen, con el objeto de verificar que nuestros proveedores críticos utilicen un esquema de continuidad de negocio que brinde un nivel de confiablidad operativa aceptable, de acuerdo con lo establecido en la Circular Única de Bancos, se solicita a su institución que el responsable del Plan de Continuidad del Negocio responda en conjunto con personal de Infraestructura, de Comunicaciones y quien considere necesario, el presente documento el cual se divide en secciones para un mejor manejo de la información.

SECCIÓN A

Identificación de servicios prestados y alcances en la Continuidad del Negocio

#	Pregunta	Respuesta / Evidencia requerida
1	Nombre del proveedor	*[Nombre completo de su empresa]*
2	Tipo de empresa	*[Tipo de servicio que presta: Negocio, Soporte, Comunicaciones, etc]*
3	Nombre de quien responde el presente cuestionario	*[Tarjeta de presentación del que responde el cuestionario, si son varios colocar en orden de contacto con nosotros, especificar: nombre, puesto organizacional y números de contacto]*
4	Servicios contratados por el Banco	*[Listado de servicios prestados a nuestra Institución, de preferencia colocarlos por prioridad ya sea por volumen, criticidad identificada, etc]*
5	Descripción de los servicios	*[Evidencia: flujo de servicios considerando la comunicación con la*

#	Pregunta	Respuesta / Evidencia requerida
	contratados	*gente de la Institución, en caso de contar con un PIM previamente entregado a la empresa favor de adjuntarlo como evidencia]*
6	Territorio nacional al que le presta servicio a la Institución.	*[Cobertura del servicio tomando en cuenta todo el territorio nacional, p.e. empresas de valores que solo atienden el norte del país, indicar los estados donde dota los cajeros automáticos, empresas de data center indicar que está centralizados en la CDMX pero el soporte es para todo el país, etc.]*
7	Descripción de la Gestión de Continuidad del Negocio en su empresa	*[Descripción de cómo se lleva a cabo la Continuidad del Negocio p.e. hay un área específica que se encarga del BCM o sólo hay una persona encargada sin embargo hay una persona por área que cuenta con el BCM en su perfil organizacional ante recursos humanos, o no se cuenta actualmente con una gestión de continuidad pero se está implementando un plan para contar con un equipo, etc]*
8	Lista de los servicios que tiene contratado con la Institución que están contemplados en su Gestión de Continuidad del Negocio	*[Tomando en cuenta el listado del punto A.4 indicar los que están dentro del alcance de su gestión de continuidad del Negocio, en caso de no ser el 100% de los servicios indicar la causa de los faltantes]*
9	Indique el grado de madurez de Continuidad del Negocio actual para su empresa.	*[Ayudándose de la siguiente tabla en caso de no tenerlo identificado:* *1. Operativo: Se llevan a cabo algunas acciones preventivas, con objeto de poder tomar medidas en caso de contingencia. No existen planes de actuación específicos definidos en caso de contingencias.* *2. Táctico: Existen planes de continuidad ante algunos escenarios definidos* *3. Gestionado: Existe un sistema de gestión relacionado con la continuidad del negocio* *4. Eficiente: Se llevan a cabo mediciones de la efectividad y de la eficiencia del sistema de gestión y de los controles y medidas en materia de continuidad* *5. Perfeccionado: Se encuentran implementadas las mejores prácticas de la industria. Existe un sistema que se mejora anualmente y se retroalimenta con el SGCN, así como el feedback de las partes interesadas y con los cambios de situación de entorno que puedan afectar a la organización.]*
10	Sobre qué metodología está fundamentada el área de Continuidad del Negocio	*[Indicar el nombre de la metodología, ISO, BSI, DRI, etc.]*
11	Regulaciones externas que revisan su plan de Continuidad del Negocio de manera continua	*[Indicar el nombre de la regulación así como la frecuencia con la que hace las revisiones a su BCM]*

SECCIÓN B

Análisis y tratamiento de riesgos

#	Pregunta	Respuesta / Evidencia requerida
12	¿Quién es responsable de evaluar, identificar y rastrear los riesgos a los que está sujeta su organización?	*[Nombre del departamento y puesto, así como la descripción de las funciones principales]*

#	Pregunta	Respuesta / Evidencia requerida
13	¿Cómo identifica y evalúa los riesgos la organización?	
14	¿Cuál es el proceso de establecer criterios para la evaluación de riesgo?	
15	¿Cómo determinan el valor del riesgo? (financiera, seguridad, reputación, legal)	
16	¿Cómo cuantifican la pérdida de datos por la materialización de cada riesgo identificado?	
17	¿Qué medios se emplean para cuantificar el impacto de las interrupciones potenciales para los procesos, aplicaciones, tecnologías o recursos?	
18	¿Su organización cuenta con un modelo de evaluación de riesgos institucional?	*[Evidencia: modelo de evaluación de riesgos institucional publicado]*
19	¿Cómo evalúa el riesgo calificado? (Por ejemplo, confidencialidad, integridad, disponibilidad)	
20	¿Cómo le dan seguimiento al tratamiento de los riesgos identificados?	
21	¿Este departamento centraliza y canaliza los riesgos a todos los interesados? P.e. los riesgos de edificio son enviados al área de protección civil y continuidad del negocio para alimentar sus procesos.	*[Evidencia: catálogo o clasificación de riesgos que alimenta al BCM]*
22	En caso de no contar con un departamento que alimente los procesos de Continuidad del Negocio, indicar cómo adquiere ésta área los riesgos de la empresa y que tipo de riesgos requiere para comenzar su análisis	*[Evidencia: documento que avale los riesgos identificados por el equipo BCM]*
23	¿Los riesgos encontrados por el BCM son transmitidos a los responsables para su tratamiento?	
24	¿Cómo se lleva a cabo el análisis de riesgos por instalación?	
25	Nombre de los edificios donde se lleva a cabo los servicios contratados	*[Evidencia: listado de sucursales, edificios corporativos donde se realizan los servicios]*
26	¿Están contemplados los edificios desde donde se	*[Evidencia: extracto de documento de análisis de riesgos donde se encuentre en el alcance los edificios mencionados en el punto B.14]*

#	Pregunta	Respuesta / Evidencia requerida
	presta el servicio a la Institución en su análisis de riesgos?	
27	¿Se lleva a cabo un análisis de riesgos del servicio prestado a cada cliente?	
28	¿Estos riesgos son notificados al cliente?	
29	¿Cuál es su proceso de notificación al cliente?	

SECCIÓN C

Análisis de Impacto al Negocio

#	Pregunta	Respuesta / Evidencia requerida
30	Cuenta con un proceso establecido para la realización del análisis de Impacto al Negocio.	*[Evidencia: política donde establezca de manera oficial el procedimiento del BIA]*
31	Establece una metodología para basarse en la solicitud de requerimientos para la realización del BIA (obtención de datos) ¿Por medio de qué método o herramienta se realiza este proceso? Por ejemplo: entrevistas con dueños de procesos, mesas de trabajo, entrega de cuestionarios, etc.	*[Evidencia: política donde establezcan los datos a recabar los datos del BIA]*
32	¿De acuerdo a los datos obtenidos cuentan con un procedimiento para cuantificar y evaluar los impactos potenciales? ¿Se toman en cuenta impactos financieros y no financieros?	*[Evidencia: descripción breve sobre la cuantificación de impactos]*
33	Se cuenta con una escala determinada de criticidad	*[Evidencia: escala de criticidad oficial]*
34	¿Se identifican los recursos externos en su BIA, son identificados los clientes? ¿Se encuentra nuestra Institución en esa lista de identificación?	*[Evidencia: lista de identificación de clientes]*
35	¿Se da una prioridad de recuperación a cada cliente? ¿Cómo se determina esa prioridad? ¿Cuál es la prioridad del Banco dentro de su BIA?	*[Evidencia: lista de prioridad de clientes]*
36	Cuenta con un listado de procesos críticos en donde se enlisten los servicios prestados al Banco	*[Evidencia: listado de procesos críticos señalando los que son para el Banco]*
37	Cada proceso o servicio crítico identificado cuenta con un RTO	*[Evidencia: RTO de cada proceso o servicio prestado]*
38	Cada proceso o servicio crítico identificado cuenta con un RPO	*[Evidencia: RPO de cada proceso o servicio prestado]*
39	¿En su BIA se encuentra identificado las interdependencias entre los procesos?	*[Evidencia: mostrar lista de interdependencias]*

SECCIÓN D

Estrategias

#	Pregunta	Respuesta / Evidencia requerida
41	¿Cuenta con alternativas de Continuidad del Negocio que no requieren de COAs o CCA? ¿Cómo fueron establecidos? P.E. trabajo activo activo entre edificios, subcontratar, incremento de capacidad, procedimientos manuales, acuerdos recíprocos, etc.	
42	¿Cuenta con un Centro de Operación Alterna? En caso afirmativo ¿Para qué tipo de eventos de contingencia lo usan?	
43	¿Cuentan con un Centro de Cómputo Alterno?	
44	En caso de contar con un CCA ¿Cuáles son las premisas que tiene su empresa para dirigir su operación a este centro?	*[Evidencia: proporcionar un esquema de conexión entre ambiente productivo y alterno]*
45	¿Qué estrategias tiene su organización para el escenario de indisponibilidad eléctrica?	
46	¿Qué estrategias tiene su organización para el escenario de indisponibilidad de personal?	
47	¿Qué estrategias tiene su organización para el escenario de ataque cibernético?	
48	¿Qué estrategias tiene su organización para el escenario de pandemias o epidemias?	
49	¿Alguna de sus estrategias es administrada por un tercero o proveedor externo? En caso afirmativo indique cual	
50	Para todas sus estrategias ¿es posible trabajar en un periodo prolongado? (4 semanas mínimo de trabajo)	
51	¿Todas las estrategias cubren los RTO indicados para el Banco en la sección anterior?	

SECCIÓN E

Planes de Continuidad

#	Pregunta	Respuesta / Evidencia requerida
52	Su institución cuenta con un Plan de respuesta en Emergencias	*[Evidencia: copia controlada de su plan de emergencias en donde se detalle lo siguiente.* *1. Etapas de su plan de respuesta* *2. Lineas de tiempo del plan* *3. Responsables por etapa]*
53	Cuenta con un Centro de Operaciones en Emergencias (EOC)	*[Definición de quienes conforman el EOC, que funciones principales tiene, plano de distribución del EOC]*
54	Cuenta con un plan de comunicación ante contingencias	*[Evidencia: copia controlada de su plan de comunicación en contingencias]*
55	¿El plan de comunicación hace referencia a sus clientes? ¿Cuál es el procedimiento de notificación hacia el Banco?	
56	¿Hay una persona responsable de comunicar al Banco las contingencias?	*[Información de contacto]*
57	A qué contacto del Banco se le notifica	*[Información de contacto]*
58	En qué tiempo se le notifica a la Institución sobre su evento de contingencia	*[Evidencia: copia controlada de su plan de comunicación en contingencias donde indique el tiempo a comunicar a la Institución o clientes]*
59	Cuenta con un Plan de Manejo de Crisis	*[Evidencia: copia controlada de su plan de manejo de crisis en donde se detalle lo siguiente.* *1. Etapas de su plan de manejo de crisis (desde la activación hasta la restauración)* *2. Líneas de tiempo del plan* *3. Responsables por etapa]*
60	¿Con qué frecuencia son actualizados sus planes de continuidad?	

SECCIÓN F

Concientización y entrenamiento

#	Pregunta	Respuesta / Evidencia requerida
61	¿Cuenta con un plan de concientización sobre temas de Continuidad en su empresa?	*[Evidencia: copia controlada de su plan de concientización o en su caso pauta de campaña diseñada por el equipo de comunicación interna]*
62	¿Cómo es comunicado el plan de continuidad a las partes interesadas?	*[Evidencia: política donde se hable de la difusión del plan]*
63	Su empresa cuenta con ejercicios para el plan ante indisponibilidad de personal (considerando eventos naturales, pandemias y epidemias, intoxicaciones, etc). En qué frecuencia se realizan	*Describa brevemente su tipo de pruebas realizadas para este escenario* *[Evidencia: acta de pruebas realizadas]*
64	Su empresa cuenta con ejercicios para el plan ante indisponibilidad técnica (considerando falla en CCP, falla en enlaces de comunicaciones, etc). En qué frecuencia se realizan	*Describa brevemente su tipo de pruebas realizadas para este escenario* *[Evidencia: acta de pruebas realizadas]*
65	Su empresa cuenta con ejercicios para el plan ante indisponibilidad de edificios principales (considerando eventos naturales, sociales como marchas, bloqueos, etc). En qué frecuencia se realizan	*Describa brevemente su tipo de pruebas realizadas para este escenario* *[Evidencia: acta de pruebas realizadas]*
66	Su empresa cuenta con ejercicios para el plan ante vulnerabilidades a la seguridad informática (considerando ataques cibernéticos, Pishing, ataque de fuerza bruta, etc). En qué frecuencia se realizan	*Describa brevemente su tipo de pruebas realizadas para este escenario* *[Evidencia: acta de pruebas realizadas]*
67	Para los ejercicios antes descritos ¿se hacen pruebas en conjunto con el Banco? En caso afirmativo, ¿Se realizan matrices de prueba y actas de hechos?	*[Evidencia: matriz y acta de pruebas realizadas]*
68	¿Son notificados sus resultados? ¿A quién se le notifica?	*[Evidencia: notificación a contacto interno sobre pruebas realizadas]*

GLOSARIO DE TÉRMINOS RELACIONADOS A LA CONTINUIDAD DEL NEGOCIO

A

ABM	Asociación de Bancos de México se ha desempeñado como el organismo cúpula de las instituciones de crédito del país con el fin de facilitar la comunicación entre ellas para construir consensos en temas que requieren el establecimiento de estándares que eleven la eficiencia del sector así como representarlas y defender los intereses generales en cualquier gestión común ante la administración pública y ante organizaciones privadas.
Activación	La implementación de procedimientos, actividades y planes de continuidad del negocio en respuesta a un incidente, emergencia, evento o crisis.
Acuerdo de nivel de servicio (SLA por sus siglas en inglés)	Convenio formal entre un proveedor de servicios y su cliente (sean estos internos o externos), que abarca la naturaleza, calidad, disponibilidad, alcance y respuesta del proveedor de servicios. El SLA debe cubrir las situaciones del día a día, así como situaciones de desastre, según vaya cambiando la necesidad del servicio.
Administrador del plan de continuidad del negocio	Persona responsable de la documentación, mantenimiento y distribución del plan.
Alcance	Límite que aplica a un proceso, procedimiento, certificación, contrato, etc. y que detalla las especificaciones y responsabilidades de todas las partes para la elaboración de un producto, la entrega de un servicio, un proyecto o cualquier otra actividad en la que debamos realizar una inversión o gasto.
Alerta	Notificación de una situación que podría derivar en una interrupción. Generalmente incluye lineamientos para que el personal se prepare ante una posible activación de los planes.
Alta disponibilidad	Protocolo de diseño de un sistema y su implementación asociada que asegura un cierto grado absoluto de continuidad operacional durante un período de medición dado.
Amenaza	Situación o condición natural u ocasionada por el hombre que puede causar una interrupción de las operaciones o servicios de una organización.
Análisis costo-beneficio	Proceso (después del BIA y la evaluación de riesgos) que facilita, a nivel financiero, las diferentes opciones estratégicas para la gestión de la continuidad y que compara el costo de cada opción con la suma ahorrada.
Análisis de brechas	Proceso comparativo que identifica la diferencia entre el resultado real y el deseado.
Análisis de brechas de seguridad / Monitoreo de amenazas	Proceso de recopilación de información sobre seguridad con el objetivo de identificar posibles violaciones de seguridad de las instalaciones, la operación o los sistemas.
Análisis de causa raíz (RCA por sus siglas en inglés)	Proceso que identifica la causa raíz de un incidente o problema. Generalmente se refiere a fallas de infraestructura de TI.
Análisis de impacto al negocio (BIA por sus siglas en inglés)	Proceso de evaluación de las operaciones y del efecto que una interrupción tendría en ellas. Incluye no sólo el análisis de impacto al negocio, que es la identificación de los activos, funciones, procesos y recursos críticos, sino también la evaluación de los posibles daños o pérdidas que pudieran afectar a la organización como resultado de una interrupción o un cambio en el negocio. Este análisis identifica: a) cómo se va a manifestar la pérdida o daño b) cómo aumenta el grado de daño o pérdida en función del tiempo transcurrido después del incidente c) los servicios y recursos mínimos (humanos, físicos y financieros) necesarios para restablecer los procesos de negocio y seguir operando en un nivel mínimo aceptable d) el tiempo y el

	nivel en el cual las actividades, funciones y servicios de la organización deben ser recuperados
Análisis de riesgos	Proceso de cuantificación de las amenazas a una organización y la probabilidad de que se materialicen.
Aplicación	Software que realiza una función específica y que se puede ejecutar sin que el usuario cuente con privilegios de administrador del sistema.
Árbol de llamadas	Documento que describe gráficamente las responsabilidades y el orden en que deben producirse las llamadas a los diferentes niveles de la organización, así como a los clientes y proveedores y otros contactos clave en caso que se produzca una emergencia, catástrofe o situación de indisponibilidad grave. En la actualidad, los árboles de llamadas pueden generarse y activarse a través de un software especializado.
Área alterna de trabajo	Ambiente preparado para la recuperación, con los elementos críticos requeridos por una estación de trabajo (por ejemplo, escritorio, teléfono, hardware, software, comunicaciones, entre otros). (DRJ)
Arquitectura	Estructura de un sistema o un servicio de TI que incluye las relaciones de sus componentes y el ambiente en el que se encuentran. También incluye los estándares y los lineamientos que rigen el diseño y la evolución del sistema.
Ataque cibernético	Intromisión al entorno informático de una organización a través del espacio cibernético con el fin de interrumpir, desactivar, destruir o controlar malintencionadamente un entorno informático o de infraestructura, destruir la integridad de los datos o robar información.
Auditor	Persona con competencias para llevar a cabo una auditoría.
Auditoría	Revisión sistemática para determinar si las actividades y sus resultados cumplen con los planes existentes y si estos se aplican eficazmente y son adecuados para cumplir con la política y los objetivos de la organización. Una auditoría puede ser: a.- Interna: llevada a cabo por el personal de la propia organización b.- Externa: llevada a cabo por un tercero especializado. En continuidad del negocio, se puede realizar con el objetivo de validar que el plan cumple con las mejores prácticas o para obtener una certificación
Autenticación	Proceso de verificación de la identidad u otros atributos asumidos por una entidad (usuario, proceso o dispositivo) o bien la verificación del origen y la integridad de los datos. A menudo es un prerrequisito para permitir el acceso a los recursos en un sistema de información.
Autoridades financieras	Conjunto de Instituciones Públicas que tienen por objeto la supervisión y regulación de las entidades que forman parte del sistema financiero, propiciar su sano desarrollo, así como la protección de los usuarios de servicios financieros. Cada organismo se ocupa de atender las funciones específicas que por Ley le son encomendadas
Autoridades no financieras	Dependencias o entidades del sector público responsables de efectuar acciones destinadas a la protección de la sociedad contra peligros que pudieran surgir, las cuales tienen autoridad local, estatal o federal en caso de presentarse algún contingencia
Autorización	Privilegio otorgado a un usuario para acceder a un programa o realizar un proceso.

C

Cadena de suministros	Serie de procesos vinculados desde la adquisición de materia prima hasta la entrega de productos o servicios al usuario final a través de los medios de transporte. Incluye proveedores, vendedores, plantas de producción,

	proveedores de logística, centros internos de distribución, distribuidores, mayoristas y otras entidades orientadas al usuario final.
Capacidad	Propiedad de un individuo, organización o comunidad relacionada con las fortalezas, atributos y recursos disponibles para desempeñar una determinada tarea o cometido. La evaluación de la capacidad es un término que designa el proceso por el cual se compara la capacidad de un grupo contra los objetivos deseados, identificando así brechas que requieren una acción futura.
Capacitación/Entrenamiento	Proceso por el cual se enseñan habilidades y conocimientos orientados a la realización de una actividad específica de manera competente o calificada. Mientras que la concientización está generalmente dirigida a todo el personal, la capacitación está dirigida al personal con funciones y responsabilidades específicas.
Cartera de aplicaciones	Base de datos o documento estructurado que se usa para gestionar las aplicaciones en su ciclo de vida. Contiene atributos clave para todas las aplicaciones. Algunas veces se implementa como parte de la cartera de servicios o del sistema de gestión de la configuración.
Categorías de riesgo	Tipos de riesgo similares son agrupados bajo un título clave, también conocido como "categorías de riesgo". Estas categorías incluyen reputación, estrategia, financieros, inversiones, infraestructura operativa, negocio, cumplimiento regulatorio, subcontratación, personas, tecnología y conocimientos.
Causa raíz	Causa original de un incidente o problema.
Centro de comando de incidentes	Ubicación cercana al lugar en el que se produjo el evento desde la cual se monitorean y controlan las actividades de respuesta a la emergencia.
Centro de operaciones de emergencia o COE (EOC por sus siglas en inglés)	Ubicación física o virtual desde la cual se gestiona la crisis y se toman decisiones estratégicas orientadas a la continuidad y recuperación de operaciones. El centro de comando de incidentes le reporta al COE.
Checklist	a. Herramienta para recordar o validar que las tareas se han completado y los recursos están disponibles y para informar sobre el estatus de la recuperación. b. Lista de elementos (nombres, tareas, etc.) que deben ser verificados.
Ciclo de vida de la gestión de la continuidad del negocio	Conjunto de actividades que cubren todos los aspectos y fases del programa de gestión de continuidad del negocio.
Cold Site	Ubicación alterna que cuenta con la infraestructura necesaria para la operación de un centro de cómputo, pero no dispone de ningún hardware de computadora, equipos de telecomunicaciones, líneas de comunicación, etc. preinstalados. Estos deben ser adquiridos o instalados en el momento de producirse el desastre. También puede ser utilizado como sitio alterno para recuperar las funciones del negocio.
Comité directivo de continuidad del negocio	Grupo directivo responsable de dar dirección, asesoría y guía y aprobar los recursos financieros y materiales necesarios del programa de continuidad. En tiempos de crisis, se convierte en el comité de manejo de crisis.
Concientización en continuidad del negocio	Proceso orientado a que las personas se familiaricen con las responsabilidades y los conceptos relacionados con la continuidad del negocio a través de la observación o de la práctica, propiciando de esta manera cambios de conducta.
Confidencialidad	Propiedad por la cual se permite el acceso a la información únicamente a personas previamente autorizadas.

Contingencia	Cualquier evento accidental, malicioso o natural que amenace o rompa con el flujo normal de las operaciones o servicios críticos del negocio, por suficiente tiempo como para afectar la recuperación de las operaciones definidas como críticas (Vitales) para el negocio.
Contingencia operativa	Cualquier evento fortuito que dificulte o inhabilite a una Organización a prestar sus servicios o realizar sus procesos, cuya actualización derive en daño o pérdida para sus clientes, para el público en general, para sus contrapartes o para la Organización misma.
Continuidad	Capacidad estratégica y táctica de una organización, previamente aprobada por la administración, para planificar y responder a las condiciones, situaciones y eventos con el fin de continuar las operaciones a un nivel aceptable predefinido. ASIS Nota del Editor: La continuidad, tal como se utiliza en la presente Norma, es el término más general para la continuidad operativa y comercial para garantizar la capacidad de una organización y seguir operando fuera de las condiciones normales de funcionamiento. Se aplica no sólo a las empresas de lucro sino a organizaciones de cualquier naturaleza tales como organizaciones no gubernamentales, de interés público y organizaciones gubernamentales. (ASIS)
Continuidad del negocio	Capacidad de una organización para continuar con la entrega de sus productos o servicios después de una interrupción a un nivel predefinido aceptable.
Control	Medios de gestión de riesgos, como políticas, procedimientos, directrices, prácticas o estructuras organizacionales, que pueden ser de carácter administrativo, técnico, de gestión o legal. (ISACA)
Controles de seguridad	Procedimientos de gestión, operativos y técnicos, implementados para un sistema de información con el fin de proteger la confidencialidad, integridad y disponibilidad del sistema y su información. En español, el término se puede utilizar además en relación con la seguridad física y la protección de las personas.
Coordinador de continuidad del negocio	Persona responsable de planificar, desarrollar, implementar, difundir y gestionar el programa de continuidad del negocio.
Coordinador departamental de continuidad	Miembro que actúa como enlace y que es responsable del plan de continuidad de su departamento.
Crisis	Evento crítico que, si no se maneja de manera adecuada, podría afectar drásticamente la rentabilidad, reputación o capacidad operativa de una organización, o bien, un suceso o percepción de amenaza a las operaciones, al personal, los accionistas, las partes interesadas, la marca, la reputación y la confianza o los objetivos estratégicos o de negocio de una organización.
Criterios de riesgo	Términos de referencia contra los cuales se evalúa la importancia de un riesgo.
Cronograma de recuperación del negocio	Secuencia o representación gráfica en función del tiempo, de un conjunto de actividades a implementar tras una interrupción. Puede variar de minutos a semanas, dependiendo de los requisitos de recuperación y de la metodología.

D

Declaración	Anuncio formal por parte del personal previamente autorizado de que se prevé o se ha producido un desastre o una interrupción grave con el consecuente despliegue de acciones de mitigación predeterminadas (por ejemplo, desplazamiento a una ubicación alterna).

Degradación de servicio	Estrategia de recuperación que consiste en que los servicios TI se proporcionen con un menor nivel de servicio o tiempo de respuesta.
Delegación de autoridad	Cesión de funciones de mando a otras personas de niveles subordinados.
Denegación de servicio (DoS por sus siglas en inglés)	Ataque a un sistema de computadoras o a una red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.
Departamento/Área/Función del negocio	Conjunto de actividades que se desarrolla para cumplir con los requisitos específicos de una organización. Algunos ejemplos son: Contabilidad, Finanzas, Recursos Humanos, TI, etc.
Dependencia	Relación o interacción de una actividad o proceso con respecto a otro.
Desastre	Acontecimiento catastrófico repentino (previsto o imprevisto) que causa daños o pérdidas inaceptables.
Detonante	Suceso que causa la activación de una respuesta.
Disponibilidad	Característica que permite que los datos estén accesibles de acuerdo a los niveles de servicio acordados.
Distribución automática de llamadas (ACD por sus siglas en inglés)	Redireccionamiento de llamadas telefónicas entrantes a la persona adecuada en el menor tiempo posible con el apoyo de la tecnología. También se conoce como distribución automatizada de llamadas.
Documento	Información y su medio de soporte (papel, dispositivos magnéticos, ópticos o electrónicos o de imagen).
Downtime/Tiempo de inactividad	Período en el que un servicio o sistema no está operando como resultado de una interrupción.
Downtime aceptable	Tiempo máximo sin operaciones que una organización está dispuesta a tolerar, desde el momento de la interrupción hasta la restauración.

E

Ejercicio	En su definición original en inglés, los ejercicios están orientados a las personas y las pruebas a los componentes físicos (sistemas, equipos, etc.). En América Latina se usa indistintamente la palabra "prueba" para ambos conceptos.
Emergencia	1. Situación inesperada que puede derivar en lesiones o muerte, daño a la propiedad o interrupción de la operación normal de una organización. 2. Suceso imprevisto y repentino que requiere de una acción inmediata.
Emergencia nacional	Situación que supone una amenaza a gran escala al bienestar de la población civil o a la protección de una o varias comunidades y de la cual se tiene que hacer cargo el sector público.
Equipo de continuidad del negocio	Grupo de personas responsables del desarrollo, implementación, pruebas, mantenimiento y ejecución de los planes de continuidad de la organización.
Equipo de gestión de incidentes (IMT por sus siglas en inglés)	Grupo de personas capacitadas responsables del desarrollo y la implementación, a través de la toma de decisiones, del plan de respuesta a incidentes.
Equipo de manejo de crisis (CMT por sus siglas en inglés)	Grupo directivo responsable de la toma de decisiones estratégicas relacionadas con la continuidad y la recuperación tras una interrupción y de la gestión de la comunicación interna y externa, teniendo siempre en cuenta la imagen de la organización. Es el único equipo autorizado para activar los planes y todos los equipos que son activados en un incidente deben reportarle. En operación normal se denomina Comité directivo de continuidad del negocio y en operación de contingencia se denomina Equipo de manejo de crisis.

Equipo de recuperación del negocio	Grupo de personas del área de TI responsables del desarrollo, implementación, pruebas, mantenimiento y ejecución del plan de recuperación de desastres.
Equipo de respuesta a emergencias (ERT por sus siglas en inglés) / Brigada de emergencia	Grupo de personas que generalmente integran la brigada de emergencia y han sido entrenadas para proporcionar asistencia inmediata en una emergencia.
Escalación	Proceso por el cual la información relacionada con un evento es comunicada al nivel superior a través de la cadena de mando de una organización con la finalidad de involucrar a los niveles de decisión adecuados.
Escenario	Diseño de una serie de condiciones ficticias, pero probables, con base en un análisis de riesgos previo, que podrían generar una interrupción, alteración o pérdida relacionada con algún aspecto de las operaciones de una organización y que se utiliza en el desarrollo de una prueba de continuidad o recuperación. Generalmente, el diseño del escenario es responsabilidad del coordinador de continuidad del negocio.
Estrategia de continuidad del negocio	Curso de acción definido previamente (y aprobado por el comité directivo) con el fin de proteger la viabilidad de la empresa y reanudar sus actividades críticas en los plazos establecidos. Las estrategias seleccionadas deben cubrir los RTOs identificados en el BIA.
Estrategias de recuperación	Curso de acción definido previamente (y aprobado por el comité directivo) con el fin de asegurar la reanudación de los servicios y los sistemas críticos de TI (con base en los RTOs identificados en el BIA).
Evacuación	Proceso de desalojo de personas para alejarlas de áreas peligrosas en una ubicación, de forma organizada, supervisada y por fases, generalmente coordinado por brigadistas.
Evaluación	Inspección y análisis para verificar el cumplimiento de un estándar o un conjunto de lineamientos, por ejemplo, la validez de los registros o el cumplimiento de las metas de eficiencia y efectividad. (ITIL)
Evaluación de daños	Proceso de estimación o determinación de los efectos de un incidente sobre las personas, el medio ambiente, los activos y la operación de una organización.
Evaluación de vulnerabilidades	Revisión sistemática de un sistema de información o producto para determinar la suficiencia de las medidas de seguridad, identificar deficiencias de seguridad, proporcionar datos para predecir la eficacia de las medidas de seguridad propuestas y confirmar que tales medidas son idóneas después de la implementación. (CNSSI-4009)
Evaluación y control de riesgos	Proceso para identificar los riesgos de una organización, evaluar las funciones esenciales necesarias para continuar las operaciones del negocio, definir los controles necesarios para reducir la exposición de la organización y evaluar el costo de dichos controles. Con frecuencia implica una evaluación de la probabilidad de ocurrencia de un evento en particular.
Evento/Incidente	Suceso que origina una interrupción o que posee el potencial para generar una interrupción.
Evidencia	Serie de documentos, archivos u otros elementos de información que se examinan durante una auditoría y que muestran cómo se maneja la operación de una organización.

F

Failover	Capacidad de cambiar automáticamente (generalmente sin intervención humana o advertencia) a un sistema de información redundante debido al fallo o terminación anormal del sistema activo.
Falla	Pérdida de la habilidad para operar de acuerdo a las especificaciones establecidas o para entregar el resultado esperado. El término "falla" puede ser utilizado cuando nos referimos a servicios de TI, procesos, actividades, elementos de configuración, etc. Una falla a menudo causa un incidente.
Funciones críticas	Actividades esenciales ejecutadas por las organizaciones, especialmente después de una interrupción de sus actividades normales.

G

Gerente de tecnologías de información (CIO por sus siglas en inglés)	Persona responsable de: a. Proporcionar asesoramiento y otro tipo de asistencia para el gerente de la organización y para otros miembros de la alta dirección de la organización, con el objetivo de asegurar que los sistemas de información son adquiridos y los recursos de información son gestionados de modo consistente con las leyes, órdenes ejecutivas, directivas, políticas, reglamentos y las prioridades establecidas por el gerente; b. Desarrollar, mantener y facilitar la implementación de una arquitectura de sistemas de información integrada y sólida para la organización; y c. Promover el efectivo y eficaz diseño y operación de los principales procesos de gestión de recursos de información de la organización, incluyendo las mejoras en los procesos de trabajo de la misma. (CNSSI-4009)
Gestión de activos	Función responsable de dar seguimiento e informar del valor de los activos financieros en todo su ciclo de vida. Forma parte de los servicios de activos y del proceso de gestión de la configuración. (ITIL)
Gestión de continuidad del negocio (BCM por sus siglas en inglés)	Proceso holístico que tiene como función identificar las posibles amenazas a la organización y los impactos resultantes si estas amenazas se materializaran, y que proporciona un marco para incrementar la resiliencia organizacional y, como consecuencia, la capacidad de una respuesta efectiva que proteja los intereses de las partes interesadas clave, la reputación, la marca y las actividades que generan valor.
Gestión de desastres/emergencias	1. Un proceso continuo de prevención, mitigación, estar preparado, de respuesta. 2. Mantener la continuidad durante la emergencia y recuperación de un incidente que amenaza la vida, la propiedad, las operaciones, o el medio ambiente. (NFPA 1600) 3. Programa que implementa la misión, la visión, los objetivos estratégicos, los objetivos y el marco de gestión del programa y de la organización. (BCI)
Gestión de emergencias	Gestión de emergencias es responsabilidad de los gobiernos y de las autoridades del sector público cumpliendo con las regulaciones y leyes relacionadas con la respuesta a emergencias. [BCI]
Gestión de incidentes	Proceso mediante el cual una organización responde y controla un incidente utilizando procedimientos o planes de respuesta de emergencia. (DRJ)
Gestión de recursos	Proceso para identificar los recursos disponibles y tener acceso oportuno a aquellos necesarios para prevenir, mitigar, preparar, responder y mantener la continuidad durante un incidente o en el proceso de recuperación.

Gestión de riesgos	Desarrollo estructurado y aplicación de la cultura de gestión, a través de políticas, procedimientos y prácticas por medio de la definición de actividades para la identificación, análisis, evaluación y control de los riesgos.
Gestión de riesgos empresariales (ERM por sus siglas en inglés)	Proceso llevado a cabo por el comité directivo y otros ejecutivos, orientado a la definición de la estrategia y que aplica a toda la organización, diseñado tanto para identificar eventos que puedan afectar a la organización como para gestionar los riesgos que forman parte de su apetito al riesgo, y que tiene como objetivo proporcionar una garantía razonable relacionada con el logro de los objetivos de la organización. Generalmente se evalúan en términos de probabilidad y magnitud del impacto, para poder así determinar una respuesta estratégica y monitorear su progreso.
Gestión del cambio	Enfoque sistemático para hacer frente a los cambios, tanto desde una perspectiva organizacional como individual.
Gobierno	Función a través de la cual una organización se asegura de que las políticas y la estrategia se están implementando y de que los procesos requeridos se siguen correctamente. Incluye la definición de funciones y responsabilidades, mediciones y estructura de reporte, y la toma de decisiones para resolver los problemas identificados.
Gobierno corporativo	Sistema o proceso por el cual se requiere que los directores de una organización lleven a cabo y cumplan sus responsabilidades y obligaciones legales, morales y regulatorias.
Gobierno, riesgo y cumplimiento (GRC por sus siglas en inglés)	GRC es el término general que abarca el enfoque de una organización sobre el riesgo y éstas tres áreas. Interpretado de manera diferente en distintas organizaciones, GRC típicamente incluye actividades como gobierno corporativo, gestión de riesgo empresarial (ERM por sus siglas en inglés) y cumplimiento corporativo con las leyes y reglamentos aplicables. (BCI)

H

Herramienta de continuidad	Herramienta tecnológica donde se encuentran documentados las diversas etapas de la metodología de Continuidad del Negocio (BC y DR) Análisis de Riesgos, Análisis de Impacto al Negocio, Estrategias, Planes, Pruebas.
Hot site	Ubicación alterna que ya cuenta con el equipo de cómputo, los servidores, las telecomunicaciones y la infraestructura ambiental necesarios para recuperar las funciones del negocio o los sistemas de información críticos.

I

Impacto	Efecto, aceptable o no, que un evento tiene en una organización. Los tipos de impactos al negocio son normalmente descritos como financieros y no financieros, y posteriormente se dividen en tipos específicos, dependiendo del sector.
Incidente	Suceso que tiene el potencial para generar una interrupción, alteración, pérdida, emergencia, crisis, desastre o catástrofe.
Infraestructura crítica	Componentes físicos o servicios de apoyo que sirven de base para la operación y que si dejaran de funcionar o fueran destruidos, provocarían un impacto que afectaría gravemente a una organización, comunidad, nación, etc.

Instalación	Planta, maquinaria, equipos, inmuebles, edificios, vehículos, sistemas de información, facilidades de transporte y otros artículos de la infraestructura o de la planta y los sistemas relacionados que tienen una función o servicio distinto y cuantificable.(BCI) Edificio permanente, disponible para su uso cuando es necesario para el Plan de Continuidad del Servicio de TI. [ITIL]
Instalación de respaldo	Una instalación "fallback" es otro sitio o edificio que puede ser utilizado cuando el sitio original no se puede utilizar o no está disponible. Término utilizado también para indicar un plan alternativo, plan B o plan de respaldo y como último recurso alternativo
Instalaciones primarias	Ubicación en donde se desarrollan las operaciones cotidianas en tiempos de operación normal.
Integridad de datos	Propiedad que garantiza que los datos no se han modificado, destruido o perdido debido a acciones no autorizadas o accidentales.
Interdependencias	Relación por la cual dos o más procesos o aplicaciones están vinculados entre sí para su funcionamiento, es decir, uno de ellos es proveedor del otro.
Interrupción	Evento que detiene las funciones, operaciones o procedimientos habituales de la organización, sea éste previsto (por ejemplo, huracanes, disturbios políticos) o imprevisto (por ejemplo, un apagón, un ataque terrorista o una falla de la tecnología).

J

Just-in-time (JIT)	Sistema que permite obtener los materiales, los recursos o la información de los que dependen los procesos críticos del negocio exactamente en el momento en que son requeridos, sin necesidad de mantener un inventario intermedio

M

Manejo de crisis	Proceso por el cual una organización dirige una serie de actividades ante una interrupción que amenaza a la organización, a las partes interesadas y al público en general, con el objetivo de evitar o reducir al mínimo el daño a la rentabilidad, la imagen y la capacidad operativa de la organización.
Mantenimiento del plan	Proceso de gestión por el cual se asegura la actualización, vigencia y pertinencia de la información relacionada con la continuidad.
Medidas preventivas	Controles para impedir eventos no deseables o mitigar sus efectos.
Mejora continua	Proceso recurrente de optimización del programa de gestión con el fin de lograr mejoras en el rendimiento general de manera consistente con la política, las metas y objetivos de la entidad.
Mejores prácticas	Conjunto de actividades o procesos que han sido aplicados con éxito en un determinado contexto y que se espera que, en contextos similares, rindan resultados similares.
Métrica	Medición de un proceso, servicio o actividad de TI y reporte de los resultados para apoyar su gestión. (ITIL)
Misión	Descripción completa, pero breve, del propósito y las intenciones globales de la organización. Se establece lo que debe ser alcanzado, pero no cómo debe hacerse.
Mitigación de riesgos	Priorización, evaluación e implementación de controles o medidas de reducción de riesgos apropiadas recomendadas en el proceso de gestión de riesgos.

Mitigación del riesgo	Decisión informada para no involucrarse o retirarse de una situación de riesgo. (BCI)
Modelo de madurez de la continuidad del negocio (BCMM por sus siglas en inglés)	Metodología que permite evaluar el nivel de preparación de una organización en función de su plan de continuidad del negocio.
Monitoreo activo	Proceso por el cual se revisa continuamente y de manera automatizada el comportamiento de un elemento de configuración o de un servicio de TI.
Movilización	Desplazamiento del personal involucrado en las actividades de recuperación a las diversas ubicaciones alternas una vez que se ha activado el plan.

N

Nivel de preparación	Grado de conocimiento y capacidad de actuación ante un evento inesperado que pudiera derivar en una interrupción de las operaciones. Aplica tanto a nivel organización como individual.
Norma/Estándar	1. Descripción detallada, elaborada con el fin de obtener un nivel de ordenamiento óptimo en un contexto dado. Para efectos de una certificación, la norma se vuelve obligatoria. 2. Un requisito obligatorio. Algunos ejemplos: ISOIIEC 20000 (norma internacional), estándar de seguridad interna para la configuración de Unix, o un estándar del gobierno que establece cómo deben mantenerse los registros financieros. El término "norma" también se utiliza para referirse a un código de práctica o especificación publicado por una organización de estándares, como ISO o BSI.

O

Objetivo de punto de recuperación (RPO por sus siglas en inglés)	Punto de referencia anterior al que debe ser restaurada la información usada por un proceso de negocio después de una interrupción, para lograr su reanudación. Cada organización deberá definir su "pérdida máxima de información".
Objetivo de tiempo de recuperación (RTO por sus siglas en inglés)	Periodo inmediatamente posterior a la ocurrencia de un incidente dentro del cual deben reanudarse o recuperarse: — la entrega de productos o servicios — las actividades críticas — los recursos NOTA: El RTO debe ser menor al tiempo en el que los impactos financieros y operacionales identificados en el BIA sean inaceptables.
Objetivo del negocio	Meta de un proceso de negocio o de la organización en general.

P

Pandemia	Enfermedad epidémica o infecciosa que puede tener un impacto a nivel mundial.
Partes interesadas	Individuo o grupo que tiene un interés en el desempeño o éxito de una organización, por ejemplo, clientes, socios, empleados, accionistas, propietarios, la comunidad local, organizaciones del primer nivel de respuesta, gobierno o instituciones regulatorias.

Peligro	Fenómeno, sustancia, actividad humana o condición peligrosa que puede causar la pérdida de vidas, lesiones u otros impactos a la salud, así como daños a la propiedad, pérdida de servicios, trastornos sociales y económicos o daños ambientales. Nota del Editor del UNDR: Los peligros de interés para la reducción del riesgo de desastres como indicados en la nota 3 del marco de referencia de Hyogo son "... peligros de origen natural y los peligros ambientales y tecnológicos relacionados." Tales riesgos se derivan de una variedad de características geológicas, meteorológicas, hidrológicas, fuentes oceánicas, biológicas y tecnológicas, actuando a veces en combinación. En ajustes técnicos, los riesgos se describen cuantitativamente por la frecuencia probable de ocurrencia de diferentes intensidades para diferentes áreas, como se determina a partir de datos históricos o análisis científico. (UNDR)
Peligro biológico	Propiedad que tiene alguna actividad, servicio o substancia, de producir efectos nocivos o perjudiciales en la salud humana. (Protección Civil - México)
Peligro natural	Proceso o fenómeno natural que tiene lugar en la biosfera que puede resultar en un evento perjudicial y causar la muerte o lesiones, daños materiales, interrupción de la actividad social y económica o degradación ambiental. CENAPRED (Centro Nacional de Prevención de Desastres - México)
Peligro tecnológico	Amenaza originada por accidentes tecnológicos o industriales, procedimientos peligrosos, fallos de infraestructura o de ciertas actividades humanas, que pueden causar muerte o lesiones, daños materiales, interrupción de la actividad social y económica o degradación ambiental. Algunos ejemplos son: contaminación industrial, radiación nuclear, desechos tóxicos, rupturas de presas, accidentes de transporte, explosiones de fábricas, incendios y derrames químicos. También pueden generarse directamente como resultado de la materialización de un riesgo de origen natural.
Pérdidas	Recursos irrecuperables como consecuencia de una interrupción. Puede referirse a vidas, ingresos, participación en el mercado, imagen pública, instalaciones o capacidad operativa.
Personal crítico	Son aquellos usuarios indispensables para la generación de procesos que conllevan la rentabilidad del negocio.
Plan de contingencias	Documento que contiene un conjunto de acciones y procedimientos definidos previamente, que serán utilizados en incidentes menores que afecten únicamente la operación (no a las personas) cuya duración sea menor al RTO.
Plan de continuidad de operaciones (COOP por sus siglas en inglés)	Plan de continuidad del sector público en Estados Unidos.
Plan de continuidad del negocio (BCP por sus siglas en inglés)	Documento que contiene un conjunto de acciones y procedimientos definidos previamente, con responsabilidades claramente establecidas, para ser ejecutados después de una interrupción de las operaciones, con el objetivo de cumplir con la entrega de los productos y servicios críticos a un nivel aceptable y dentro de los marcos de tiempo predefinidos.
Plan de manejo de crisis	Documento que contiene un conjunto de acciones y procedimientos definidos previamente, con responsabilidades claramente establecidas, para enfrentar un incidente mayor o crisis. Ver definición de "crisis". El responsable de su desarrollo e implementación es el comité directivo.
Plan de recuperación ante desastres (DRP por sus siglas	Documento que contiene un conjunto de acciones y procedimientos definidos previamente, con responsabilidades claramente establecidas, para

en inglés)	la recuperación del componente tecnológico, sistemas y servicios de telecomunicaciones.
Plan de respuesta a emergencias	Documento que contiene un conjunto de acciones y procedimientos definidos previamente, con responsabilidades claramente establecidas, para estabilizar un incidente que ponga en riesgo las vidas y la propiedad.
Plan de sucesión de gestión ejecutiva	Documento que permite asegurar la continuidad de la autoridad, la toma de decisiones y la comunicación en caso de que, repentinamente, algún miembro clave de la dirección no pueda ejercer sus funciones.
Plan del ejercicio	Ver Planificación de la prueba
Planificación de contingencias	Proceso de elaboración de acuerdos y procedimientos avanzados que permiten a una organización responder a un evento no deseado que repercute negativamente en la organización. (DRJ)
Planificación de continuidad del negocio	Proceso de desarrollar procedimientos y lineamientos que permitan a las organizaciones responder a una interrupción, de tal manera que las funciones críticas del negocio puedan continuar dentro de los niveles acordados. El resultado final del proceso de planificación es el plan de continuidad del negocio. (BCI)
Planificación de la prueba	Programación de las diversas actividades que serán llevadas a cabo antes, durante y después de la prueba con el objetivo de evaluar los componentes del plan, por ejemplo, las tareas, equipos y procedimientos.
Planificación de recuperación ante desastres	Actividades asociadas con la planificación para la disponibilidad continua y restauración de la infraestructura de TI. (BCI)
Política de continuidad del negocio	Marco de referencia que establece los objetivos, los principios y el enfoque de la gestión de continuidad de una organización, los productos y servicios de la misma y cómo serán entregados, y las funciones y responsabilidades principales de la gestión de continuidad y cómo se reportará el estatus a la dirección ejecutiva.
Póliza todo riesgo	Seguro en el que, respecto al objeto asegurado, se garantizan conjunta y simultáneamente todos los riesgos que puedan afectarle, excepto los riesgos explícitamente excluidos de la póliza. Ver Todos los peligros
Preparación	Actividades implementadas antes de un incidente que pueden ser utilizadas para apoyar y mejorar la mitigación de interrupciones, así como la respuesta y recuperación ante las mismas. (BCI)
Preparación ante emergencias	Situación en la que se encuentra una organización o comunidad en relación con su capacidad de respuesta a una emergencia de forma coordinada, oportuna y efectiva, con el fin de minimizar el daño a las personas y a la propiedad.
Prevención	Medidas que permiten a una organización evitar, impedir o reducir el impacto de un incidente.
Primer nivel de respuesta	Personas o instituciones de algún servicio de emergencia del sector público que llegan primero a la escena de una emergencia. Generalmente es la policía, los bomberos o los servicios médicos de emergencia.
Prioridad	Categoría utilizada para identificar la importancia relativa de un incidente, problema o cambio. Está basada en el impacto y la urgencia, y se utiliza para identificar los tiempos requeridos en las acciones a seguir. Por ejemplo, un acuerdo de nivel de servicio (SLA por sus siglas en inglés) puede especificar los incidentes prioritarios que deben resolverse en un plazo máximo de 12 horas.
Probabilidad	Posibilidad verosímil y fundada de que algo suceda, haya sido esto definido, medido o estimado objetiva o subjetivamente. Se pueden utilizar términos descriptivos generales (tales como "improbable", "poco probable", "probable", "casi seguro"), frecuencias o probabilidades matemáticas. Puede

	ser expresado cualitativa o cuantitativamente.
Procedimientos de recuperación	Acciones documentadas necesarias para restaurar los datos de un sistema de información y la capacidad de cómputo después de una falla del sistema.
Procedimientos manuales	Método alternativo de trabajo en el que no se utilizan los sistemas o el software que regularmente está disponible. Las medidas y métodos de trabajo provisionales ayudan a mitigar el impacto de un evento durante un periodo corto.
Procesos críticos	Son las actividades del negocio (productos o servicios) que por su importancia no pueden ser interrumpidos su operación ya que afecta de forma directa a la satisfacción del cliente, a la eficiencia económica e imagen y/o reputación de la organización.
Proceso de negocio	Secuencia de procedimientos interdependientes y vinculados que contribuyen a la entrega de un producto o servicio. Algunos ejemplos son pago de nómina, reclutamiento y selección de personal, cuentas por cobrar, etc.
Programa	Grupo de iniciativas relacionadas que se gestionan en forma coordinada, con el fin de obtener un nivel de control y los beneficios que no serían posibles a partir de la gestión individual de las iniciativas. Los programas pueden incluir elementos de trabajos relacionados fuera del alcance de las iniciativas distintas del programa. (FCD-1)
Programa de continuidad del negocio	Proceso de gestión y gobierno en curso, que es apoyado por la alta dirección, con los recursos adecuados para implementar y mantener la gestión de continuidad del negocio. (ISO 22301)
Programa de gestión de continuidad del negocio	Proceso de gestión y gobierno continuo que cuenta con el apoyo de la alta dirección y con los recursos apropiados para asegurar que se toman las medidas necesarias para identificar el impacto de pérdidas potenciales, mantener planes y estrategias viables de recuperación y asegurar la continuidad de productos y servicios a través de la capacitación, las pruebas y ejercicios y la actualización. En general, en América Latina los términos "programa de gestión de la continuidad del negocio" y "sistema de gestión de la continuidad del negocio" se usan indistintamente.
Prueba	Simulación de una interrupción de las operaciones para evaluar los componentes de un plan (por ejemplo, tareas, equipos y procedimientos) con el objetivo de comprobar su viabilidad.
Prueba a gran escala/Prueba integral	Ejecución de todos los planes y procedimientos de recuperación de la organización completa. Evaluación de las capacidades alternas de operación en un ambiente altamente estresado. Eventualmente, se podría involucrar al sector público.
Prueba de escritorio	Método de ensayo para ejercitar los planes, en el que los participantes revisan y discuten los planes de acción y procedimientos sin ejecutarlos, en un ambiente seguro y libre de estrés. Puede llevarse a cabo con uno o varios equipos o departamentos. Por lo general, requiere la guía de un facilitador.
Prueba de recuperación ante desastres	Método de ensayo o ejecución (dependiendo del objetivo y el alcance definido para el ejercicio) de los planes de acción y procedimientos de recuperación de los servicios de TI y telecomunicaciones.
Prueba del árbol de llamadas	Proceso manual o automatizado para validar la información contenida en el árbol de llamadas.
Prueba funcional	Ejecución de los planes y procedimientos de recuperación de un área o línea del negocio.

Prueba paso a paso	Método similar a la prueba de escritorio en el que se siguen todos los pasos del plan y sólo se ejecutan algunas acciones seleccionadas en la planificación de la prueba.
Punto único de falla (SPOF por sus siglas en inglés)	Componente único que forma parte de un sistema o proceso, y que en caso de falla, detendría completamente dicho sistema o proceso. Deberían ser identificados en cualquier sistema o proceso con un objetivo de alta disponibilidad.

R

Reanudación	Conjunto de actividades orientadas a retomar o continuar las funciones y operaciones predefinidas del negocio después de una interrupción.
Recuperación	Actividades y programas diseñados para regresar las condiciones a un nivel que sea aceptable para la entidad. (NFPA 1600)
Recuperación ante desastres (DR por sus siglas en inglés)	Capacidad de una organización para recuperar y restablecer el componente TI (infraestructura, telecomunicaciones, sistemas, aplicaciones y datos) después de una interrupción. Aspecto tecnológico de la continuidad del negocio.
Recuperación de datos	Restauración de los archivos de la computadora desde dispositivos de copia de seguridad, con el objetivo de restaurar programas y datos de producción al estado que tenían en el momento de la última copia de seguridad segura, almacenada en el exterior.
Red alterna de comunicaciones	Respaldo de la red de comunicaciones primaria en caso de su indisponibilidad.
Reducción de riesgos	Aplicación selectiva de técnicas y principios de gestión adecuados para reducir la probabilidad de la ocurrencia de una interrupción o mitigar su impacto, o ambos.
Reducción del riesgo de desastre	Concepto y práctica de reducir el riesgo de desastres mediante esfuerzos sistemáticos dirigidos al análisis y a la gestión de los factores causales de los desastres, lo que incluye la reducción del grado de exposición a las amenazas, la disminución de la vulnerabilidad de la población y la propiedad, una gestión sensata de los suelos y del medio ambiente, y el mejoramiento de la preparación ante los eventos adversos. (UNISDR)
Redundancia	Estrategia para duplicar recursos, ya sean tecnológicos, físicos o humanos, cuando el recurso original es único y crítico. Este concepto está relacionado con el punto único de falla.
Registros vitales	Información, en formato electrónico o físico, que es esencial para preservar, continuar o recuperar las operaciones de la organización y para proteger los derechos de la organización y a sus empleados, clientes y partes interesadas.
Remediación	Acción enfocada a la solución de un problema determinado ante un evento. Ejemplo: identificar un nuevo sitio para reubicar un equipo que fue dañado por causa de una inundación.
Resiliencia	Capacidad de una organización para mantener sus funciones y su estructura críticas ante cualquier cambio interno o externo y regresar a un nivel aceptable de rendimiento en un periodo mínimo después de una interrupción.
Respaldo	En TI, es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.
Respuesta a emergencias	Reacción inmediata y acciones posteriores ante una situación inesperada, con el objetivo de proteger vidas y reducir la severidad del impacto. Dependiendo del evento, las autoridades del sector público tienen la

	responsabilidad de cumplir con las regulaciones y leyes relacionadas con esta respuesta.
Respuesta a incidentes	Conjunto de acciones realizadas por una organización ante un desastre u otro evento importante que pueda afectar significativamente a la organización, a su gente o su capacidad de operación normal. Puede incluir: evacuación, activación de un DRP, evaluación de daños o cualquier otra medida necesaria para llevar a la organización a un estatus más estable.
Restauración	Proceso para la reparación de los daños ocasionados por el incidente, por ejemplo, instalaciones físicas, hardware, activos y estaciones de trabajo entre otros, con el fin de regresar al sitio primario y, en consecuencia, a las operaciones normales.
Retorno de la inversión (ROI por sus siglas en inglés)	Medición de los beneficios esperados de una inversión. En el sentido más simple, es el beneficio neto de una inversión dividida por el valor neto de los activos invertidos.
Riesgo	Probabilidad de que se presente un evento que pudiera causar daños o pérdidas o afectar la capacidad para alcanzar los objetivos del negocio, asociado a la vulnerabilidad de la organización ante esa amenaza. En el contexto de gestión del riesgo corporativo, riesgo se refiere al potencial de que el resultado de una acción o actividad (incluyendo la no acción) resulte en un resultado diferente.
Riesgo aceptable	Nivel de pérdida que una sociedad o comunidad considera aceptable, con base en sus condiciones sociales, económicas, políticas, culturales, técnicas y ambientales existentes.
Riesgo de desastre	Posibles pérdidas que ocasionaría un desastre en términos de vidas, las condiciones de salud, los medios de sustento, los bienes y servicios, y que podrían ocurrir en una comunidad o sociedad particular en un período específico de tiempo en el futuro. (UNISDR)
Riesgo del negocio	Exposición a factores tanto internos como externos que pueden afectar la capacidad de la organización para proporcionar un servicio o producto, o que pueden generar una caída en la demanda de los mismos, situaciones que pueden representar un impacto financiero inesperado. Ejemplo: las tabacaleras tienen como riesgo del negocio el enfrentar demandas de salud, campañas para que la gente deje de fumar, etc.
Riesgo operacional	Riesgo de pérdida resultante de controles y procedimientos inadecuados o fallidos. Incluye la pérdida por eventos relacionados con tecnología e infraestructura, fallas, interrupciones de negocios, problemas relacionados con el personal y eventos externos, tales como los cambios regulatorios. Se basa en el riesgo de la operación, independientemente del riesgo del negocio en particular.
Riesgo residual	Nivel de riesgo remanente después de que se han implementado todas las acciones costo-efectivas para reducir el impacto, la probabilidad y las consecuencias de un riesgo o grupo de riesgos específicos, sujeto al apetito al riesgo de una organización.

S

Salvar/Rescatar	Recuperar efectos personales, documentación, oficinas y equipo de cómputo después de un incidente.

Seguridad	Este término se puede utilizar tanto para la información como para las instalaciones físicas. En información, es la práctica de proteger información ante el uso indebido (acceso no autorizado, divulgación, alteración o destrucción). Con respecto a las instalaciones físicas, es la práctica que resulta del establecimiento y el mantenimiento de medidas de protección de las instalaciones y las personas. Estas medidas pueden incluir una combinación de disuasión, prevención, detección, recuperación y corrección, y debe formar parte del enfoque de gestión de riesgos de la empresa.
Seguro	Contrato para financiar el costo del riesgo. Ante la ocurrencia de un evento denominado riesgo (pérdida), el seguro pagará al asegurado el monto contratado. (BCI). Medio para la cobertura de los riesgos al transferirlos a una aseguradora que se va a encargar de garantizar o indemnizar todo o parte del perjuicio producido por la aparición de determinadas situaciones accidentales.
Seguro de pérdidas consecuenciales (BI por sus siglas en inglés)	Cobertura contratada para casos de interrupción de las operaciones. Es un término usado ampliamente en la industria de los seguros para referirse a un seguro que cubre pérdidas (generalmente se cuantifica en ingresos perdidos) debido a la interrupción temporal de las operaciones. Impacto causado a la organización por causa de diferentes tipos de interrupciones. Normalmente se cuantifica en ingresos perdidos.
Servicios en la nube	Modelo de prestación de servicios de negocio y tecnología que permite al usuario acceder a un catálogo de servicios estandarizados y responder con ellos a las necesidades de su negocio, de forma flexible y adaptativa.
Servicios esenciales	Servicios de infraestructura sin los cuales un edificio o área estarían inutilizados e impedidos para proporcionar sus servicios normales de operación; típicamente incluye: servicios (agua, gas, electricidad, telecomunicaciones) y también pueden incluir sistemas de respaldo de electricidad y de control ambiental. (BCI)
Servicios subcontratados o tercerizados	Una perspectiva de servicios, comúnmente usada en TI, que hace hincapié en el hecho de que son gestionados de manera externa.
Simulacro	Ejercicio relacionado normalmente con el plan de respuesta a emergencias y que tiene como objetivo que los participantes pongan en práctica los procedimientos de evacuación, refugio en el lugar u otros procedimientos relacionados con la seguridad de las personas, dirigidos normalmente por los brigadistas.
Sistema de comando de incidentes (ICS por sus siglas en inglés)	Estructura organizacional usada por el sector público en Estados Unidos para manejar información, logística y comunicaciones durante un evento de emergencia o desastre.
Sistema de gestión	Conjunto de elementos interrelacionados o interacción de una organización para establecer políticas y objetivos y los procesos para alcanzar esos objetivos. 1) Un sistema de gestión puede abordar una sola disciplina o varias disciplinas 2) Los elementos del sistema incluyen la estructura de la organización, las funciones y responsabilidades, la planificación, la operación, etc. 3) El alcance de un sistema de gestión puede incluir la totalidad de la organización o una o varias funciones o secciones específicas dentro de un grupo de organizaciones.
Sistema de gestión de continuidad del negocio (BCMS por sus siglas en inglés)	Ver "Programa de gestión de continuidad del negocio".

Sitio alterno	Ubicación alterna usada por el negocio cuando la principal no está disponible. Se recomienda que esté a una distancia considerable de las instalaciones primarias. a.- Localidad física donde puede ubicarse un centro de cómputo alterno designado para la recuperación b.- Localidad física preparada para la recuperación de las unidades de negocio con los elementos críticos requeridos, por ejemplo, escritorios, teléfonos, hardware, software, comunicaciones, entre otros.
Sitio secundario	Ver sitio alterno
Subcontratación	Transferencia de las funciones del negocio a un proveedor externo independiente. También denominado Servicios tercerizados.
Suplidor/Proveedor	Tercera parte responsable del suministro de bienes o servicios. (ITIL)
Suplidor/Proveedor de servicios	Organización externa o área interna de la propia organización que proporciona productos o servicios.
Suspensión temporal	Período de tiempo después de una interrupción en el que se espera que un servicio, sistema, proceso o función de negocio esté inutilizable o inaccesible.

T

Táctico	Segundo nivel de los tres niveles de planificación y entrega (estratégico, táctico, operativo). Las actividades tácticas incluyen los planes a medio plazo necesarios para alcanzar objetivos específicos, por lo general en un periodo de semanas a meses.
Tarjeta de bolsillo	Información de contacto de emergencia en formato portátil reducido.
Tecnologías de información - TI (IT por sus siglas en inglés)	Utilización de la tecnología para almacenar, comunicar o procesar información. La tecnología generalmente incluye computadoras, telecomunicaciones, aplicaciones, servidores, bases de datos y cualquier otro programa o sistema. La información puede incluir datos del negocio, imágenes, video, voz, etc. Las tecnologías de información se utilizan con frecuencia para apoyar los procesos del negocio a través de los servicios de TI.
Tiempo de respuesta	Una medida del tiempo entre la solicitud del servicio y su obtención. El término aplica en tecnología, respuesta a emergencias, etc.
Tiempo máximo tolerable de inactividad (MTD por sus siglas en inglés)	Tiempo máximo que un proceso puede ser interrumpido sin causar un daño significativo a la misión de la organización.
Todos los peligros	Plan o enfoque de continuidad o emergencias que cubre o es aplicable a todos los riesgos posibles. FEMA Ver Póliza todo riesgo
Tolerancia al riesgo	Estado de preparación de una organización para soportar el riesgo después de los tratamientos de riesgo, con el fin de lograr sus objetivos. La tolerancia al riesgo puede estar limitada por requisitos legales o regulatorios.
Transferencia del riesgo	Técnica común utilizada por los gerentes de riesgos para hacer frente o mitigar los posibles riesgos de la organización. Una serie de técnicas que describen los distintos medios para hacer frente a los riesgos a través de seguros y productos similares. (DRJ)
Tratamiento del riesgo	Proceso de modificación de los riesgos que consiste en la selección e implementación de una o más opciones, como por ejemplo: eliminar el riesgo (hacer que el origen del riesgo desaparezca), mitigar el riesgo, modificar la probabilidad, compartir el riesgo, retener el riesgo o incluso incrementarlo buscando una oportunidad o beneficio. Una vez

	implementado el tratamiento, éste se convierte en un control (o también puede llegar a modificar controles existentes).

U

Unidad de negocio/ Departamento/Área	Cada una de las divisiones de una organización que realiza una serie de funciones específicas. Ejemplos de unidades de negocio incluyen los puntos de venta y el departamento de Recursos Humanos.

V

Vulnerabilidad	Grado de exposición de una persona, activo, proceso, información, infraestructura y otros recursos a las acciones o efectos de un riesgo, suceso u otro acontecimiento.

W

Warm site	Ubicación alterna de procesamiento que está equipada con algún hardware e interfases de comunicaciones, acondicionamiento eléctrico y ambiental, que sólo estará en capacidad operacional una vez que sean suministrados los componentes faltantes y se desarrolle una labor de configuración.

Fuentes

ASIS	ASIS Internacional es una comunidad global con más de 38,000 profesionales de la seguridad que desarrollan funciones relacionadas con la protección de los activos (personas, propiedad e información).
AS/NZ 5050	AS/NZS 5050 explica cómo aplicar AS/NZS ISO 31000 a riesgos relacionados con alguna interrupción e incluye una guía detallada de las características de estos riesgos y el marco de gestión de riesgos a través del cual se administran.
ASIS/BSI BCM.01-2010	Este estándar, que reunió a expertos mundiales en gestión de la continuidad y planificación para contingencias, representa un consenso de las mejores prácticas en la gestión de la continuidad del negocio. Es una herramienta útil para cualquier tamaño o tipo de organización que desee mejorar su preparación, desempeño y resultados. Especifica los requisitos para planificar, establecer, implementar, operar, monitorear, revisar, probar, actualizar y mejorar un sistema de gestión de continuidad del negocio.
Business Continuity Institute (BCI)	El BCI se ha establecido como una organización líder de afiliación y certificación de los profesionales de la continuidad de todo el mundo y ofrece una amplia gama de recursos para los profesionales que quieren elevar los niveles de resiliencia dentro de su organización o que quieren dedicarse a la continuidad del negocio.

British Standards Institute (BSI)	El British Standards Institute ayuda a las organizaciones de todo el mundo a hacer de la excelencia un hábito. Durante más de un siglo han estado desafiando la mediocridad y la complacencia para ayudar a desarrollar la excelencia en la gente y los productos y servicios. Esto significa que enseña a las empresas a mejorar su desempeño, a reducir los riesgos y a lograr un crecimiento sustentable. Es el organismo nacional de estándares del Reino Unido y el primer organismo nacional de normalización.
Norma Británica BS 25999	Fue la primera norma dedicada a la gestión de la continuidad del negocio a nivel mundial, y fue desarrollada por un grupo de expertos de clase mundial que representan una sección transversal de los sectores de la industria y el gobierno para establecer el proceso, los principios y la terminología de la gestión de la continuidad del negocio, para minimizar el impacto de cualquier interrupción de las operaciones que pudiera afectar a una organización.
Committee on National Security Systems (CNSS)	El CNSS proporciona un foro para la discusión de asuntos políticos y es responsable de establecer las políticas, lineamientos, instrucciones, procedimientos operativos, orientación y asesorías de seguridad de la información a nivel nacional para los departamentos del gobierno de los EE.UU. y los organismos del Sistema Nacional de Seguridad (NSS por sus siglas en inglés) a través de su sistema de emisión.
DRI Internacional (DRII)	El DRI Internacional, originalmente Disaster Recovery Institute, fundado en 1988, es una organización sin fines de lucro con la misión de hacer que el mundo esté preparado. Como organismo global de educación y certificación en continuidad del negocio y planificación de recuperación ante desastres, establece el estándar de profesionalismo. Después de más de 25 años de servicio, sigue siendo la organización más antigua, más grande y la más extendida de su tipo.
Disaster Recovery Journal (DRJ)	Proporciona conocimiento profundo por parte de expertos en la planificación de continuidad del negocio. Es una publicación ampliamente leída en el sector y ofrece conferencias que tienden a ser los eventos con mayor asistencia en la industria de la continuidad. Tiene abundancia de recursos y materiales disponibles para su uso y consulta.
European Central Bank (ECB)	El ECB y los bancos centrales nacionales constituyen el eurosistema, es decir, el sistema central bancario del área europea. Su objetivo principal es mantener la estabilidad de precios, salvaguardando el valor del euro.
FCD 1 Federal Continuity Directive	Es un documento desarrollado y promulgado por el Department of Homeland Security (DHS) de EE.UU., en coordinación con el CAG y en consulta con el CPCC, que dirige los departamentos ejecutivos y las agencias para la elaboración de los requisitos de planificación de continuidad identificados y los criterios de evaluación. Las directrices federales de continuidad proveen dirección al poder ejecutivo federal para el desarrollo de planes y programas de continuidad.
Federal Final Institutions Examination Council (FFIEC)	Responsable de desarrollar sistemas de notificación uniformes para las instituciones financieras supervisadas por el gobierno federal y sus sociedades, así como para las filiales de ambas. Dirige a las escuelas para los examinadores empleados por las cinco agencias federales miembros representadas en el Consejo y pone a disposición aquellas escuelas de empleados de agencias estatales que supervisan instituciones financieras.
Health Insurance Portability and Accountability Act of 1996 (HIPPA)	Acrónimo de Health Insurance Portability and Accountability Act. El objetivo principal de este estatuto federal de los EE.UU. es ayudar a los asegurados a mantener su cobertura de seguro. Las regulaciones de HIPAA se aplican a los planes de salud, centros de atención de salud (entidades que facilitan las

	transacciones electrónicas de datos a través de la "traducción" de los mismos entre los planes de salud y proveedores cuando se utilizan sistemas de información no compatibles).
Health Information Technology for Economic and Clinical Health Act (HITECH)	HITECH fue promulgada como parte de la ley estadounidense de Recuperación y Reinversión de 2009; se convirtió en ley el 17 de febrero de 2009 y promueve la adopción y uso significativo de la tecnología de la información. La sección D de esta ley aborda los problemas de privacidad y seguridad asociados con la transmisión electrónica de información sobre la salud, en parte, a través de varias disposiciones que refuerzan la imposición civil y criminal de las reglas de HIPAA.
International Organization for Standardization (ISO)	ISO es el desarrollador más grande del mundo de normas internacionales voluntarias. Las normas internacionales dan especificaciones de vanguardia para productos, servicios y buenas prácticas, ayudando a que la industria sea más eficiente y eficaz. Desarrolladas a través de un consenso global, ayudan a romper las barreras del comercio internacional. ISO es una red de organismos nacionales de estandarización.
Norma ISO 31000	Esta norma, llamada "Gestión de riesgos, principios y directrices", proporciona los principios, el marco de referencia y el proceso de gestión de riesgos. Puede ser utilizada por cualquier organización sin importar su tamaño, actividad o sector. Implementar ISO 31000 aumenta la probabilidad de las organizaciones para lograr sus objetivos, mejorar el proceso de identificación de oportunidades y amenazas y asignar y utilizar de manera efectiva los recursos para el tratamiento de riesgos.
Information Technology Infrastructure Library (ITIL)	ITIL es un marco ampliamente adoptado para la gestión de servicios de TI. Proporciona un enfoque práctico, sin complicaciones, para la identificación, planificación, entrega y soporte de servicios de TI a las organizaciones.
Monetary Authority of Singapore (MAS)	Banco central de Singapur que promueve el crecimiento económico sostenido y no inflacionista a través de la formulación de una política monetaria adecuada y la vigilancia de las tendencias emergentes y las potenciales vulnerabilidades macroeconómicas. Gestiona el tipo de cambio de Singapur, así como las reservas de divisas y liquidez en el sector bancario. MAS también es una superintendencia integrada que supervisa todas las instituciones financieras de Singapur: bancos, aseguradoras, intermediarios del mercado de capitales, asesores financieros y la bolsa de valores.
National Fire Protection Association (NFPA)	Organización internacional sin fines de lucro con la misión de reducir la carga mundial de incendios y otros peligros sobre la calidad de vida proveyendo y abogando por códigos y normativas consensuadas, así como por la investigación, la formación y la educación. Es el recurso principal para el estudio, la investigación y el análisis de datos sobre incendios.
Norma NFPA 1600	La Norma NFPA de Preparación Nacional está siendo ampliamente utilizada tanto por entidades públicas y privadas, como por instituciones sin fines de lucro y no gubernamentales en el ámbito local, regional, nacional e internacional. Ha sido adoptada por el Departamento de Seguridad Nacional de Estados Unidos bajo consenso voluntario como estándar para la preparación en casos de emergencia.
National Institute of Standards and Technology (NIST)	El NIST es responsable de desarrollar estándares y directrices, incluyendo los requisitos mínimos, para proporcionar la seguridad de la información adecuada para todas las operaciones de una organización y sus activos, pero tales normas y directrices no se aplican a los sistemas de seguridad nacional. Es uno de los laboratorios de física más antiguos de la nación. Es una agencia federal no regulatoria dentro del Departamento de Comercio de Estados

	Unidos.
NIST SP 800-34	Guía de planificación de contingencia para los sistemas de información federal. Proporciona instrucciones, recomendaciones y consideraciones para la planificación ante contingencias que afecten al sistema de información federal. Esta publicación ayuda a las organizaciones a comprender el objetivo, el proceso y el formato de desarrollo de la planificación de contingencias relacionadas con los sistemas de información mediante directrices prácticas basadas en sucesos reales.
National Emergency Crisis and Disaster Management Authority (NCEMA)	La NCEMA trabaja bajo la supervisión del Consejo Nacional Superior de Seguridad. Es el cuerpo nacional principal que establece el estándar de los Emiratos Árabes Unidos responsable de regular y coordinar todos los esfuerzos de emergencia y manejo de crisis así como el desarrollo de un plan nacional para responder a emergencias. La misión del NCEMA es coordinar todos los esfuerzos nacionales para salvar vidas, conservar propiedades y activos nacionales dificultando el efecto de emergencias y crisis.
Singapore SS-540	Estándar que establece el marco para el análisis y la implementación de estrategias, procesos y procedimientos. La norma se centra en la resiliencia y la protección de los activos críticos (humanos, del medio ambiente, intangibles y físicos) y en la gestión de la continuidad y la recuperación de las funciones críticas de una organización de cualquier tamaño.
United Nations International Strategy for Disaster Reduction (UNISDR)	La UNISDR se creó como un departamento de la Secretaría de las Naciones Unidas con el objetivo de asegurar la ejecución de la estrategia internacional para la reducción de desastres. El objetivo de UNISDR es servir como punto focal en el sistema de las Naciones Unidas en los esfuerzos de coordinación de la reducción del desastre y asegurar sinergias entre actividades de reducción del desastre. La reducción del riesgo de desastres (DRR por sus siglas en inglés) pretende reducir el daño causado por riesgos naturales como terremotos, inundaciones, sequías y ciclones, a través de una ética de la prevención. La estrategia internacional para la reducción de desastres refleja un cambio del enfoque tradicional en la atención de desastres a la reducción de desastres, y en efecto procura promover una "cultura de la prevención

ANEXO 3: EVALUACIÓN DE PROVEEDORES

Revisión de riesgos en Continuidad del Negocio de proveedores críticos

Proveedor a revisar:	
Procesos del proveedor:	
Persona BCP que hace la revisión:	

1. Severidad: La Severidad de un riesgo es el valor asignado al daño más probable que produciría si se materializa.

Seleccione el valor de la severidad para el proveedor a revisar

No afectaría el servicio a los clientes ni a procesos detectados como críticos.

Podría incomodar a los clientes, podría afectar parcialmente los procesos críticos.

Podría afectar algunos clientes, podría afectar totalmente a un proceso crítico

Afecta a los clientes y a varios procesos críticos

Paraliza la operación de las áreas críticas, no se otorga el servicio a los clientes.

Pérdida potencial de clientes, daño reputacional grave y perdida de la operación de procesos críticos del banco.

2. Probabilidad o frecuencia: Número de veces que se ha materializado el riesgo durante un período determinado.

Seleccione el valor de la frecuencia indicada por el usuario interno para el proveedor a revisar

1 Evento al año o menos

de 1 evento al semestre a 2 al trimestre

de 1 a 3 eventos por mes

de 1 a 4 eventos por semana

1 evento al día o más

1 Evento al año o menos

3. Vulnerabilidades: actividades que en caso de no ser cumplidas pudieran ocasionar que al momento de materializarse un riesgo la empresa será susceptible a efectos dañinos para el Banco. Para la identificación de dichos valores se deberá revisar el cuestionario previamente llenado por el proveedor y responder cada punto de la siguiente tabla.

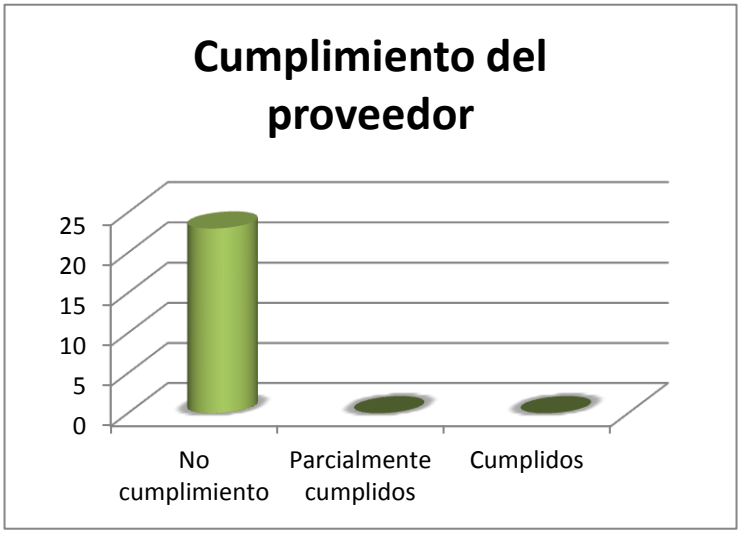
De acuerdo al siguiente catálogo de riesgos asigne el valor que crea responda mejor a la situación de la empresa a revisar

Etapa	Riesgo	Cumplimiento	Observaciones
Análisis de Riesgos	No se cuenta con un análisis de riesgos donde se contemple el edificio desde donde se prestan los servicios a Banorte		
Análisis de Impacto al Negocio	No se encuentran identificados los servicios prestados a Banorte en sus planes de continuidad		
Análisis de Impacto al Negocio	No se encuentran identificados los escenarios a los que pudieran estar expuestos los servicios prestados a Banorte		
Análisis de Impacto al Negocio	No se tiene un análisis de impacto al negocio para los servicios prestados a Banorte		
Análisis de Impacto al Negocio	No se tiene identificado un RTO para los servicios prestados a Banorte		
Análisis de Impacto al Negocio	No se tiene identificado un RPO para los servicios prestados a Banorte		
Análisis de Impacto al Negocio	No se cuenta con una lista de prioridades para levantar los servicios prestados a Banorte		
Planes de Continuidad	No cuenta con planes de recuperación para servicios de tecnología que presta a Banorte		
Planes de Continuidad	No cuenta con planes que contemplen escenarios de indisponibilidad de edificios donde se prestan los servicios a Banorte		
Planes de Continuidad	No cuenta con planes que contemplen escenarios de indisponibilidad de personal		
Planes de Continuidad	No cuenta con planes que contemplen escenarios de falla por ciberataques		
Comunicación en crisis	No cuenta con un proceso de comunicación en crisis hacia Banorte		
Comunicación en crisis	No se hace la notificación detallada de los eventos hacia Banorte		
Comunicación en crisis	No se tiene identificado un contacto para notificar a Banorte un evento		
Comunicación en	No se tiene un tiempo determinado para		

crisis	notificar a Banorte en caso de un evento		
Comunicación en crisis	No se hacen pruebas de los servicios prestados a Banorte en un esquema de contingencia DRP		
Mantenimiento y pruebas	No se hacen pruebas de conexiones de comunicación con Banorte		
Mantenimiento y pruebas	No se hacen pruebas de ataque cibernético con Banorte		
Mantenimiento y pruebas	No se hacen pruebas de estrategias BCP de los servicios prestados a Banorte		
Mantenimiento y pruebas	No se hacen de conocimiento a Banorte sobre los resultados de las pruebas realizadas		
Mantenimiento y pruebas	No se hacen las pruebas al menos una vez al año para todos los escenarios		
Mantenimiento y pruebas	No se realizan matrices de pruebas de los servicios prestados a Banorte		
Mantenimiento y pruebas	No se realizan actas de hechos de las pruebas de los servicios prestados a Banorte		

4. Resultado final: a continuación se muestra el resultado de la revisión y la calificación final del proveedor revisado

Resultado del proveedor:	RESULTADO
No cumplimiento	0
Parcialmente cumplidos	0
Cumplidos	0



ANEXO 4: PROCEDIMIENTO INSTITUCIONAL

PROCEDIMIENTO

1. Nombre

9. Evaluación de Continuidad del Negocio para proveedores críticos

2. Objetivo

Dar cumplimiento a la regulación externa contenida en los siguientes artículos

Sec.	GERENTE DE CONTINUIDAD DEL NEGOCIO	DIRECTOR DE INFRAESTRUCTURA TRANSFORMACIÓN Y ARQUITECTURA TÉCNICA	DIRECTOR DE CONTROL DE DISPOSICIONES REGULATORIAS	SUBGERENTE DE CONTINUIDAD DEL NEGOCIO	PUNTO ÚNICO DE CONTACTO DEL PROVEEDOR CRÍTICO	DIRECTOR/SUBDIRECTOR DE CONTINUIDAD Y PERFILES	DIRECTOR GENERAL ADJUNTO DE CONTRALORÍA	SUBDIRECTOR DE AUDITORÍA TI
1.		Cada inicio de año manda por medio de correo electrónico el listado de sus proveedores críticos que ayudar a soportar la estrategia de DRP y su punto de contacto						
2.			Cada que se incorpora un proveedor, realiza un análisis de criticidad de acuerdo a lo establecido en la Circular Única de Bancos emitida por la CNBV, en caso de que sea un proveedor catalogado como crítico comparte la información de contacto del proveedor para realizar su evaluación en continuidad del negocio					
3.				Cada inicio de año manda por medio de correo electrónico un listado de las altas, bajas o cambios de proveedores críticos que soportan algún proceso crítico en el Análisis de Impacto al Negocio (BIA) ver glosario proporcionando los datos de contacto del proveedor.				
4.	Recibe notificación de nuevos proveedores críticos y realiza un plan anual de revisión. Envía correo con plan al subdirector de continuidad y perfiles							
5.						Recibe plan de revisión de proveedores anual e indica cambios por correo electrónico en caso de tenerlos.		
6.	Recibe visto bueno o realiza modificaciones en caso de que aplique							
7.	Envía correo a los contactos de proveedores para solicitar información (nombre del director de la empresa, dirección física para el envío de correspondencia, contacto de continuidad del negocio en la institución)							
8.					Responde correo con la información solicitada.			
9.	Recibe la información del proveedor y realiza carta de inicio donde solicita que el proveedor llene un cuestionario para conocer aspectos importantes sobre la continuidad del negocio. Adicional solicita evidencias sobre los puntos indicados en el cuestionario. Manda el oficio a firmas por correo electrónico a la							

	Dirección General Adjunta de Contraloría.							
10.							Recibe carta y firma. Envía original por valija institucional.	
11.	Recibe carta firmada y envía al proveedor el oficio junto con un disco donde está el cuestionario y las evidencias solicitadas. Se especifica un plazo no mayor a 15 días hábiles para remitir su información.							
12.					Recibe oficio y disco. Contesta el cuestionario y adjunta evidencias en el tiempo estipulado. Envía la información de acuerdo a lo establecido en la carta.			
13.	Recibe la información y la analiza, Detecta riesgos potenciales en materia de continuidad del negocio y comparte las observaciones por medio de un dictamen en donde se detalla lo encontrado y se da un plazo no mayor a 15 días hábiles para entregar un plan de remediación o evidencia que solvente los puntos encontrados. Redacta el oficio y se lo envía al Director General Adjunto de Contraloría para su firma.							
14.						Recibe correo electrónico con el dictamen y lo firma. Envía original por valija institucional.		
15.	Envía la carta dictamen al proveedor.							
16.					Recibe el dictamen y entrega plan de remediación en el tiempo establecido.			
17.	Recibe plan de remediación o evidencia que solvente las observaciones por parte del proveedor. Se envía una carta de cierre recordando que se debe de dar seguimiento al plan entregado							
18.					Recibe carta de cierre y dan seguimiento al plan junto con el Gerente de Continuidad del Negocio			
19.	Envía resultados de dictamen al Subdirector de Auditoría TI encargado.							
20.								Recibe el dictamen del proveedor y plan de remediación, en caso de que no se cumplan las fechas establecerá mecanismos que ayuden al cumplimiento por parte del proveedor.
21.	Envía dictamen y contactos al personal interno del área de continuidad para las gestiones de pruebas y matriz de escalamiento del proveedor.							

4. Narrativa

Sec.	Responsable	Actividad	Relaciones
1	**DIRECTOR DE INFRAESTRUCTURA TRANSFORMACIÓN Y**	Cada inicio de año manda por medio de correo electrónico el listado de sus proveedores críticos que ayudar a soportar la estrategia de DRP y su punto de contacto	

	ARQUITECTURA TÉCNICA		
2	**DIRECTOR DE CONTROL DE DISPOSICIONES REGULATORIAS**	Cada que se incorpora un proveedor, realiza un análisis de criticidad de acuerdo a lo establecido en la Circular Única de Bancos emitida por la CNBV, en caso de que sea un proveedor catalogado como crítico comparte la información de contacto del proveedor para realizar su evaluación en continuidad del negocio	
3	**SUBGERENTE DE CONTINUIDAD DEL NEGOCIO**	Cada inicio de año manda por medio de correo electrónico un listado de las altas, bajas o cambios de proveedores críticos que soportan algún proceso crítico en el Análisis de Impacto al Negocio (BIA) ver glosario proporcionando los datos de contacto del proveedor.	
4	**GERENTE DE CONTINUIDAD DEL NEGOCIO**	Recibe notificación de nuevos proveedores críticos y realiza un plan anual de revisión. Envía correo con plan al subdirector de continuidad y perfiles	
5	**DIRECTOR/SUBDIRECTOR DE CONTINUIDAD Y PERFILES**	Recibe plan de revisión de proveedores anual e indica cambios por correo electrónico en caso de tenerlos.	
6	**GERENTE DE CONTINUIDAD DEL NEGOCIO**	Recibe visto bueno o realiza modificaciones en caso de que aplique	
7	**GERENTE DE CONTINUIDAD DEL NEGOCIO**	Envía correo a los contactos de proveedores para solicitar información (nombre del director de la empresa, dirección física para el envío de correspondencia, contacto de continuidad del negocio en la institución)	
8	**PUNTO ÚNICO DE CONTACTO DEL PROVEEDOR CRÍTICO**	Responde correo con la información solicitada.	
9	**GERENTE DE CONTINUIDAD DEL NEGOCIO**	Recibe la información del proveedor y realiza carta de inicio donde solicita que el proveedor llene un cuestionario para conocer aspectos importantes sobre la continuidad del negocio. Adicional solicita evidencias sobre los puntos indicados en el cuestionario. Manda el oficio a firmas por correo electrónico a la Dirección General Adjunta de Contraloría	
10	**DIRECTOR GENERAL ADJUNTO DE CONTRALORÍA**	Recibe carta y firma. Envía original por valija institucional.	
11	**GERENTE DE CONTINUIDAD DEL NEGOCIO**	Recibe carta firmada y envía al proveedor el oficio junto con un disco donde está el cuestionario y las evidencias solicitadas. Se especifica un plazo no mayor a 15 días hábiles para remitir su información.	
12	**PUNTO ÚNICO DE CONTACTO DEL PROVEEDOR CRÍTICO**	Recibe oficio y disco. Contesta el cuestionario y adjunta evidencias en el tiempo estipulado. Envía la información de acuerdo a lo establecido en la carta.	
13	**GERENTE DE CONTINUIDAD DEL NEGOCIO**	Recibe la información y la analiza, Detecta riesgos potenciales en materia de continuidad del negocio y comparte las observaciones por medio de un dictamen en donde se detalla lo encontrado y se da un plazo no mayor a 15 días hábiles	

		para entregar un plan de remediación o evidencia que solvente los puntos encontrados. Redacta el oficio y se lo envía al Director General Adjunto de Contraloría para su firma.	
14	**DIRECTOR GENERAL ADJUNTO DE CONTRALORÍA**	Recibe correo electrónico con el dictamen y lo firma. Envía original por valija institucional.	
15	**GERENTE DE CONTINUIDAD DEL NEGOCIO**	Envía la carta dictamen al proveedor.	
16	**PUNTO ÚNICO DE CONTACTO DEL PROVEEDOR CRÍTICO**	Recibe el dictamen y entrega plan de remediación en el tiempo establecido.	
17	**GERENTE DE CONTINUIDAD DEL NEGOCIO**	Recibe plan de remediación o evidencia que solvente las observaciones por parte del proveedor. Se envía una carta de cierre recordando que se debe de dar seguimiento al plan entregado	
18	**PUNTO ÚNICO DE CONTACTO DEL PROVEEDOR CRÍTICO**	Recibe carta de cierre y dan seguimiento al plan junto con el Gerente de Continuidad del Negocio	
19	**GERENTE DE CONTINUIDAD DEL NEGOCIO**	Envía resultados de dictamen al Subdirector de Auditoría TI encargado.	
20	**SUBDIRECTOR DE AUDITORÍA TI**	Recibe el dictamen del proveedor y plan de remediación, en caso de que no se cumplan las fechas establecerá mecanismos que ayuden al cumplimiento por parte del proveedor.	
21	**GERENTE DE CONTINUIDAD DEL NEGOCIO**	Envía dictamen y contactos al personal interno del área de continuidad para las gestiones de pruebas y matriz de escalamiento del proveedor.	
FIN DEL PROCEDIMIENTO			

ANEXO 5: PLANTILLAS DE CARTAS CON LOS PROVEEDORES

Ciudad de México, FECHA DE ELABORACIÓN

NOMBRE LEGAL DE LA EMPRESA

DIRECCIÓN DE LA EMPRESA

Asunto: Dictamen de "Evaluación de riesgos para continuidad del negocio".

At´n.: NOMBRE DEL DIRECTOR DE LA EMPRESA
PUESTO LEGAL
NOMBRE DEL ENCARGADO DE CONTINUIDAD EN LA EMPRESA
PUESTO LEGAL

En relación al escrito emitido por Banco Mercantil del Norte, S.A., Institución de Banca Múltiple, Grupo Financiero Banorte (en adelante Banorte) el FECHA DE ENTREGA DEL ESCRITO A LA EMPRESA y, recibido por NOMBRE LEGAL DE LA EMPRESA (en adelante NOMBRE CORTO DE LA EMPRESA) el mismo día, mediante el cual se solicitó la información descrita en el Cuestionario de Continuidad del Negocio a fin de realizar la "evaluación de riesgos para continuidad del negocio" sobre procesos operativos y servicios de procesamiento contratados con proveedores que soportan procesos vitales para Banorte.

Mediante el presente manifestamos que una vez analizada dicha información se determinó que NOMBRE DEL PROVEEDOR **CUMPLIMIENTO OTORGADO POR EL ANÁLISIS DEL ANEXO 2** con la "Evaluación de riesgos para continuidad del negocio" realizada en cumplimiento al inciso h, fracción I del Anexo 67 de las Disposiciones de carácter general aplicables a las Instituciones de Crédito (Circular Única de Bancos) que establecen los "Requerimientos mínimos del plan de continuidad de negocio", observando los siguientes elementos de riesgo:

1. LISTA DE ELEMENTOS DE RIESGOS DETECTADOS

Para pronta referencia se adjunta como **ANEXO 1: Revisión de riesgos en Continuidad del Negocio de proveedores críticos** el Dictamen que contiene el detalle de las observaciones antes mencionadas.

Por lo anterior, se requiere atentamente a NOMBRE DE LA EMPRESA remitir a más tardar en un plazo que no exceda los 15 días hábiles siguientes al día de la recepción del presente dictamen, evidencia que permita verificar la atención de las observaciones antes

descritas, o en su caso, un plan de remediación que contenga las acciones, plazos y responsables que consideren para atender dichas observaciones. Dicha información deberá remitirse en formato PDF a la atención de la Sub-Dirección de Continuidad del Negocio de Banorte (Gerardo Delgadillo Ramos), con domicilio en Tlalpan 2980, Colonia Ejidos de Santa Úrsula, Delegación Coyoacán, C.P. 4850 y, a la dirección de correo electrónico continuidad.del.negocio@banorte.com

Es importante señalar que de no recibir la información en tiempo y forma, la Sub-Dirección de Continuidad del Negocio de Banorte procederá a informar los riesgos identificados al Comité correspondiente.

Atentamente,

Lic. Jorge Eduardo Vega Camargo
Director General Adjunto de Contraloría.

ANEXO 6: ANÁLISIS DE PROVEEDORES

Proveedor a revisar:	Promoción y Operación S.A. de C.V.
Procesos del proveedor:	Switch de transacciones electrónicas, compensación intercambio y liquidación de transacciones, POS Adquirente, PROCOM, PROINFO, Autorización
Persona BCP que hace la revisión:	Judith Molina Guzmán

1. Severidad: La Severidad de un riesgo es el valor asignado al daño más probable que produciría si se materia.

Seleccione el valor de la severidad para el proveedor a revisar

Pérdida potencial de clientes, daño reputacional grave y perdida de la operación de procesos críticos del banco.

2. Probabilidad o frecuencia: Número de veces que se ha materializado el riesgo durante un período determinados.

Seleccione el valor de la frecuencia indicada por el usuario interno para el proveedor a revisar

1 Evento al año o menos

3. Vulnerabilidades: actividades que en caso de no ser cumplidas pudieran ocasionar que al momento de materializarse un riesgo la empresa será susceptible a efectos dañinos para Banorte. Para la identificación de dichos valores se deberá revisar el cuestionario previamente llenado por el proveedor y responder cada punto de la siguiente tabla.

De acuerdo al siguiente catálogo de riesgos asigne el valor que crea responda mejor a la situación de la empresa a revisar

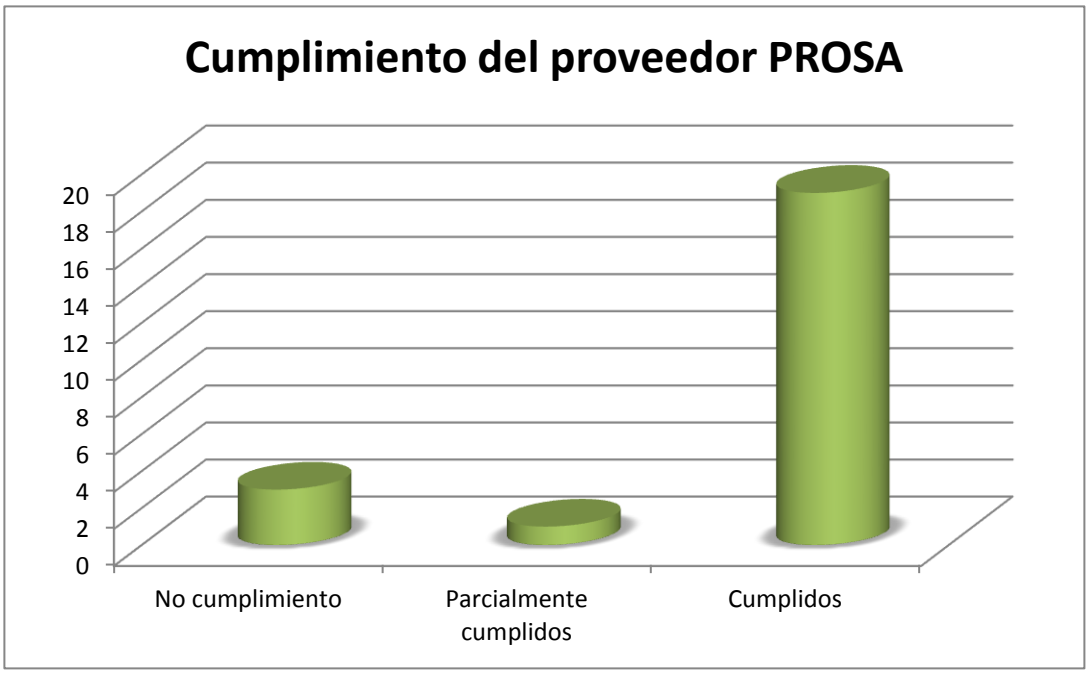
Etapa	Riesgo	Cumplimiento	Comentario
Análisis de Riesgos	No se cuenta con un análisis de riesgos donde se contemple el edificio desde donde se prestan los servicios a Banorte	Si	
Análisis de Impacto al Negocio	No se encuentran identificados los servicios prestados a Banorte en sus planes de continuidad	Si	
Análisis de Impacto al Negocio	No se encuentran identificados los escenarios a los que pudieran estar expuestos los servicios prestados a Banorte	Si	
Análisis de Impacto al Negocio	No se tiene un análisis de impacto al negocio para los servicios prestados a Banorte	Si	

Análisis de Impacto al Negocio	No se tiene identificado un RTO para los servicios prestados a Banorte	Si	
Análisis de Impacto al Negocio	No se tiene identificado un RPO para los servicios prestados a Banorte	Si	
Análisis de Impacto al Negocio	No se cuenta con una lista de prioridades para levantar los servicios prestados a Banorte	Si	
Planes de Continuidad	No cuenta con planes de recuperación para servicios de tecnología que presta a Banorte	Si	
Planes de Continuidad	No cuenta con planes que contemplen escenarios de indisponibilidad de edificios donde se prestan los servicios a Banorte	Si	
Planes de Continuidad	No cuenta con planes que contemplen escenarios de indisponibilidad de personal	Si	
Planes de Continuidad	No cuenta con planes que contemplen escenarios de falla por ciberataques	Parcial	En el cuestionario indican que no cuentan con un plan que cubra las amenazas tecnológicas de ataque cibernético (Phising, DDOS, Malware,Cyberfraude) y en las evidencias enviadas se hace mención de un plan, sin embargo no es robusto y no cuenta con medidas claras sobre el procedimiento ante ciertas amenazas.
Comunicación en crisis	No cuenta con un proceso de comunicación en crisis hacia Banorte	Si	
Comunicación en crisis	No se hace la notificación detallada de los eventos hacia Banorte	Si	
Comunicación en crisis	No se tiene identificado un contacto para notificar a Banorte un evento	Si	
Comunicación en crisis	No se tiene un tiempo determinado para notificar a Banorte en caso de un evento	Si	
Comunicación en crisis	No se hacen pruebas de los servicios prestados a Banorte en un esquema de contingencia DRP	Si	
Mantenimiento y pruebas	No se hacen pruebas de conexiones de comunicación con Banorte	Si	
Mantenimiento y pruebas	No se hacen pruebas de ataque cibernético con Banorte	No	No se cuenta con evidencia de que realizan pruebas para los escenarios de ataque cibernético, pudiendo verse comprometida la información de nuestros clientes.

Mantenimiento y pruebas	No se hacen pruebas de estrategias BCP de los servicios prestados a Banorte	No	No se cuenta con evidencia de que realizan pruebas para los escenarios de indisponibilidad de edificio principal e indisponibilidad del personal, pudiendo afectar los tiempos comprometidos con Banorte para la realización de los procesos.
Mantenimiento y pruebas	No se hacen de conocimiento a Banorte sobre los resultados de las pruebas realizadas	No	No se hace la notificación con el resultado de las pruebas a Banorte y no llega a las partes interesadas (Continuidad del Negocio, Recuperación Ante Desastres, Auditoría)
Mantenimiento y pruebas	No se hacen las pruebas al menos una vez al año para todos los escenarios	Si	
Mantenimiento y pruebas	No se realizan matrices de pruebas de los servicios prestados a Banorte	Si	
Mantenimiento y pruebas	No se realizan actas de hechos de las pruebas de los servicios prestados a Banorte	Si	

4. Resultado final: a continuación se muestra el resultado de la revisión y la calificación final del proveedor revisado

Resultado del proveedor:	Aceptable
No cumplimiento	3
Parcialmente cumplidos	1
Cumplidos	19



Proveedor a revisar:	Compañía Mexicana de Procesamiento S.A. de C.V.
Procesos del proveedor:	Cámara de Compensación Electrónica, Cámara de Intercambio de Imágenes, Banco de Imágenes y Aclaraciones
Persona BCP que hace la revisión:	Judith Molina Guzmán

1. Severidad: La Severidad de un riesgo es el valor asignado al daño más probable que produciría si se materia.

Seleccione el valor de la severidad para el proveedor a revisar

Podría afectar algunos clientes, podría afectar totalmente a un proceso crítico

2. Probabilidad o frecuencia: Número de veces que se ha materializado el riesgo durante un período determinados.

Seleccione el valor de la frecuencia indicada por el usuario interno para el proveedor a revisar

1 Evento al año o menos

3. Vulnerabilidades: actividades que en caso de no ser cumplidas pudieran ocasionar que al momento de materializarse un riesgo la empresa será susceptible a efectos dañinos para Banorte. Para la identificación de dichos valores se deberá revisar el cuestionario previamente llenado por el proveedor y responder cada punto de la siguiente tabla.

De acuerdo al siguiente catálogo de riesgos asigne el valor que crea responda mejor a la situación de la empresa a revisar

Etapa	Riesgo	Cumplimiento	Observaciones
Análisis de Riesgos	No se cuenta con un análisis de riesgos donde se contemple el edificio desde donde se prestan los servicios a Banorte	Si	
Análisis de Impacto al Negocio	No se encuentran identificados los servicios prestados a Banorte en sus planes de continuidad	Si	
Análisis de Impacto al Negocio	No se encuentran identificados los escenarios a los que pudieran estar expuestos los servicios prestados a Banorte	Si	
Análisis de Impacto al Negocio	No se tiene un análisis de impacto al negocio para los servicios prestados a Banorte	Si	
Análisis de Impacto al Negocio	No se tiene identificado un RTO para los servicios prestados a Banorte	Si	

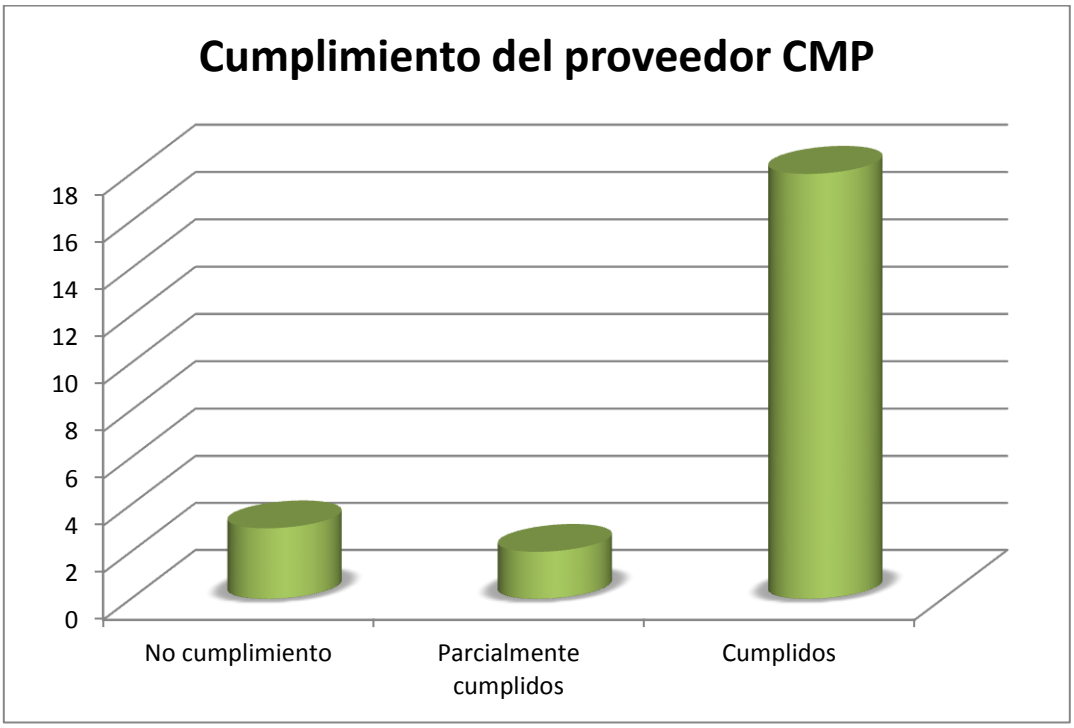
Análisis de Impacto al Negocio	No se tiene identificado un RPO para los servicios prestados a Banorte	Parcial	Está identificado de 1 hr sin embargo no se alinea al RPO del banco de cero pérdida de datos.
Análisis de Impacto al Negocio	No se cuenta con una lista de prioridades para levantar los servicios prestados a Banorte	Si	
Planes de Continuidad	No cuenta con planes de recuperación para servicios de tecnología que presta a Banorte	Si	
Planes de Continuidad	No cuenta con planes que contemplen escenarios de indisponibilidad de edificios donde se prestan los servicios a Banorte	Si	
Planes de Continuidad	No cuenta con planes que contemplen escenarios de indisponibilidad de personal	Si	
Planes de Continuidad	No cuenta con planes que contemplen escenarios de falla por ciberataques	Si	
Comunicación en crisis	No cuenta con un proceso de comunicación en crisis hacia Banorte	Si	
Comunicación en crisis	No se hace la notificación detallada de los eventos hacia Banorte	Si	
Comunicación en crisis	No se tiene identificado un contacto para notificar a Banorte un evento	Si	
Comunicación en crisis	No se tiene un tiempo determinado para notificar a Banorte en caso de un evento	Si	
Comunicación en crisis	No se hacen pruebas de los servicios prestados a Banorte en un esquema de contingencia DRP	Si	
Mantenimiento y pruebas	No se hacen pruebas de conexiones de comunicación con Banorte	Si	
Mantenimiento y pruebas	No se hacen pruebas de ataque cibernético con Banorte	No	No se cuenta con evidencia de que realizan pruebas para la amenaza de ataque cibernético que pudiera comprometer la información de nuestros clientes.

Mantenimiento y pruebas	No se hacen pruebas de estrategias BCP de los servicios prestados a Banorte	No	No se cuenta con evidencia de que realizan pruebas para los escenarios de indisponibilidad de edificio principal e indisponibilidad del personal, pudiendo afectar los tiempos comprometidos con Banorte para la realización de los procesos.
Mantenimiento y pruebas	No se hacen de conocimiento a Banorte sobre los resultados de las pruebas realizadas	Parcial	Se hace la notificación con el resultado de las pruebas al contacto interno del Banco, sin embargo esa información no llega a las partes interesadas (Continuidad del Negocio, Recuperación Ante Desastres, Auditoría)
Mantenimiento y pruebas	No se hacen las pruebas al menos una vez al año para todos los escenarios	No	No se realizan las pruebas de ataque cibernético ni de las estrategias BCP con una frecuencia adecuada.
Mantenimiento y pruebas	No se realizan matrices de pruebas de los servicios prestados a Banorte	Si	
Mantenimie	No se realizan actas de hechos de las pruebas de los	Si	

nto y pruebas	servicios prestados a Banorte		

4. Resultado final: a continuación se muestra el resultado de la revisión y la calificación final del proveedor revisado

Resultado del proveedor:	Aceptable
No cumplimiento	3
Parcialmente cumplidos	2
Cumplidos	18



Proveedor a revisar:	Total System Services de México, S.A. de C.V.
Procesos del proveedor:	•SIAM; sistema integral de administración de mensajerías. •Personalización de Tarjetas Priority Pass. •Personalización: TDC Banorte e IXE y TDD IXE. •Ventas cruzadas

Persona BCP que hace la revisión:	**Judith Molina Guzmán**

1. Severidad: La Severidad de un riesgo es el valor asignado al daño más probable que produciría si se materia.

Seleccione el valor de la severidad para el proveedor a revisar

Podría incomodar a los clientes, podría afectar parcialmente los procesos críticos.

2. Probabilidad o frecuencia: Número de veces que se ha materializado el riesgo durante un período determinados.

Seleccione el valor de la frecuencia indicada por el usuario interno para el proveedor a revisar

1 Evento al año o menos

3. Vulnerabilidades: actividades que en caso de no ser cumplidas pudieran ocasionar que al momento de materializarse un riesgo la empresa será susceptible a efectos dañinos para Banorte. Para la identificación de dichos valores se deberá revisar el cuestionario previamente llenado por el proveedor y responder cada punto de la siguiente tabla.

De acuerdo al siguiente catálogo de riesgos asigne el valor que crea responda mejor a la situación de la empresa a revisar

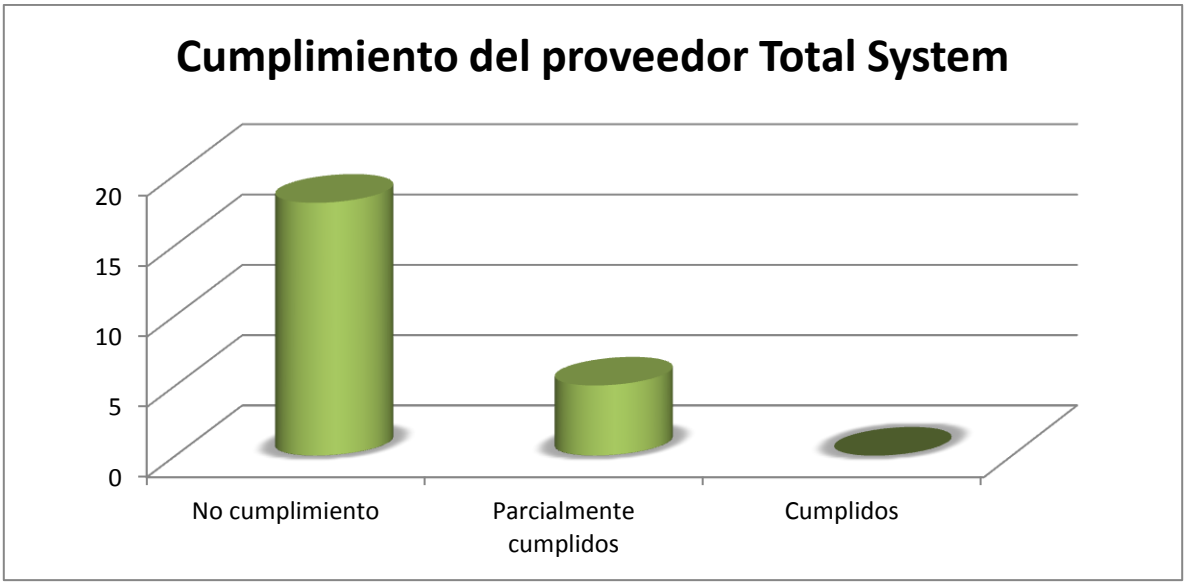
Etapa	Riesgo	Cumplimiento	Comentario
Análisis de Riesgos	No se cuenta con un análisis de riesgos donde se contemple el edificio desde donde se prestan los servicios a Banorte	No	El proveedor indica que está en proceso de implentación
Análisis de Impacto al Negocio	No se encuentran identificados los servicios prestados a Banorte en sus planes de continuidad	No	El proveedor indica que está en proceso de implentación
Análisis de Impacto al Negocio	No se encuentran identificados los escenarios a los que pudieran estar expuestos los servicios prestados a Banorte	No	El proveedor indica que está en proceso de implentación
Análisis de Impacto al Negocio	No se tiene un análisis de impacto al negocio para los servicios prestados a Banorte	No	El proveedor indica que está en proceso de implentación
Análisis de Impacto al Negocio	No se tiene identificado un RTO para los servicios prestados a Banorte	Parcial	En el cuestionario indica que es de 72 horas sin embargo no hay un documento que verifique la

			información.
Análisis de Impacto al Negocio	No se tiene identificado un RPO para los servicios prestados a Banorte	Parcial	En el cuestionario indica que es de 48 horas sin embargo no hay un documento que verifique la información.
Análisis de Impacto al Negocio	No se cuenta con una lista de prioridades para levantar los servicios prestados a Banorte	No	El proveedor indica que está en proceso de implentación
Planes de Continuidad	No cuenta con planes de recuperación para servicios de tecnología que presta a Banorte	No	El proveedor indica que está en proceso de implentación
Planes de Continuidad	No cuenta con planes que contemplen escenarios de indisponibilidad de edificios donde se prestan los servicios a Banorte	No	El proveedor indica que está en proceso de implentación
Planes de Continuidad	No cuenta con planes que contemplen escenarios de indisponibilidad de personal	No	El proveedor indica que está en proceso de implentación
Planes de Continuidad	No cuenta con planes que contemplen escenarios de falla por ciberataques	No	El proveedor indica que está en proceso de implentación
Comunicación en crisis	No cuenta con un proceso de comunicación en crisis hacia Banorte	Parcial	El proveedor indica su procedimiento de comunicación en crisis hacia Banorte sin embargo no cuenta con un documento de evidencia que lo valide.
Comunicación en crisis	No se hace la notificación detallada de los eventos hacia Banorte	Parcial	El proveedor indica su procedimiento de comunicación en crisis hacia Banorte sin embargo no cuenta con un documento de evidencia que lo valide.

Comunicación en crisis	No se tiene identificado un contacto para notificar a Banorte un evento	Parcial	El proveedor indica el personal a quien notificarán sobre la crisis hacia Banorte sin embargo no cuenta con un documento de evidencia que lo valide.
Comunicación en crisis	No se tiene un tiempo determinado para notificar a Banorte en caso de un evento	No	El proveedor indica que está en proceso de implentación
Comunicación en crisis	No se hacen pruebas de los servicios prestados a Banorte en un esquema de contingencia DRP	No	El proveedor indica que está en proceso de implentación
Mantenimiento y pruebas	No se hacen pruebas de conexiones de comunicación con Banorte	No	El proveedor indica que está en proceso de implentación
Mantenimiento y pruebas	No se hacen pruebas de ataque cibernético con Banorte	No	El proveedor indica que está en proceso de implentación
Mantenimiento y pruebas	No se hacen pruebas de estrategias BCP de los servicios prestados a Banorte	No	El proveedor indica que está en proceso de implentación
Mantenimiento y pruebas	No se hacen de conocimiento a Banorte sobre los resultados de las pruebas realizadas	No	El proveedor indica que está en proceso de implentación
Mantenimiento y pruebas	No se hacen las pruebas al menos una vez al año para todos los escenarios	No	El proveedor indica que está en proceso de implentación
Mantenimiento y pruebas	No se realizan matrices de pruebas de los servicios prestados a Banorte	No	El proveedor indica que está en proceso de implentación
Mantenimiento y pruebas	No se realizan actas de hechos de las pruebas de los servicios prestados a Banorte	No	El proveedor indica que está en proceso de implentación

4. Resultado final: a continuación se muestra el resultado de la revisión y la calificación final del proveedor revisado

Resultado del proveedor:	No aceptable
No cumplimiento	18
Parcialmente cumplidos	5
Cumplidos	0



Proveedor a revisar:	**Grupo GSI (Cometra, SEPSA, Seguritec, Tecnoval)**
Procesos del proveedor:	**Traslado de valores, verificación de concentraciones, preparación de dotaciones, cajeros automáticos**
Persona BCP que hace la revisión:	**Judith Molina Guzmán**
Tipo de proveedor:	**Operativo**

1. Severidad: La Severidad de un riesgo es el valor asignado al daño más probable que produciría si se materia.

Seleccione el valor de la severidad para el proveedor a revisar

Pérdida potencial de clientes, daño reputacional grave y perdida de la operación de procesos críticos del banco.

2. Probabilidad o frecuencia: Número de veces que se ha materializado el riesgo durante un período determinados.

Seleccione el valor de la frecuencia indicada por el usuario interno para el proveedor a revisar

1 Evento al año o menos

3. Vulnerabilidades: actividades que en caso de no ser cumplidas pudieran ocasionar que al momento de materializarse un riesgo la empresa será susceptible a efectos dañinos para Banorte. Para la identificación de dichos valores se deberá revisar el cuestionario previamente llenado por el proveedor y responder cada punto de la siguiente tabla.

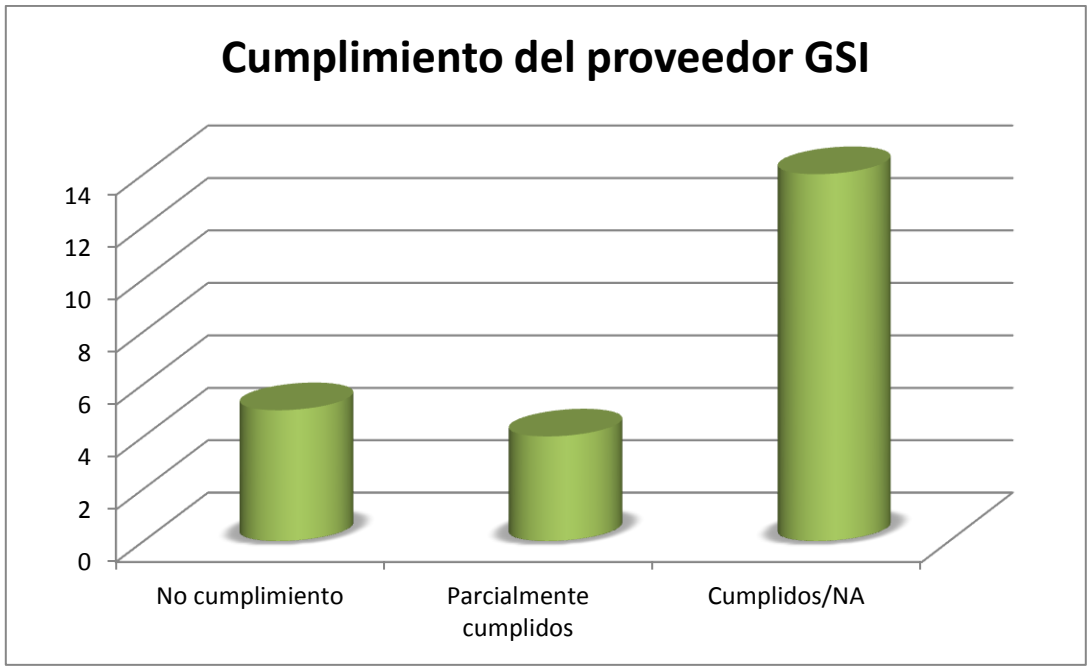
De acuerdo al siguiente catálogo de riesgos asigne el valor que crea responda mejor a la situación de la empresa a revisar

Etapa	Riesgo	Cumplimiento	Comentario
Análisis de Riesgos	No se cuenta con un análisis de riesgos donde se contemple el edificio desde donde se prestan los servicios a Banorte	Parcial	Entregar documento que se indica "PLAN COB ACTUALIZACIÓN 10, ENERO 2017"
Análisis de Impacto al Negocio	No se encuentran identificados los servicios prestados a Banorte en sus planes de continuidad	Parcial	Entregar documento que se indica "PLAN COB ACTUALIZACIÓN 10, ENERO 2017"
Análisis de Impacto al Negocio	No se encuentran identificados los escenarios a los que pudieran estar expuestos los servicios prestados a Banorte	Si	
Análisis de Impacto al Negocio	No se tiene un análisis de impacto al negocio para los servicios prestados a Banorte	Parcial	Entregar documento que se indica "PLAN COB ACTUALIZACIÓN 10, ENERO 2017"
Análisis de Impacto al Negocio	No se tiene identificado un RTO para los servicios prestados a Banorte	Si	
Análisis de Impacto al Negocio	No se tiene identificado un RPO para los servicios prestados a Banorte	No	No lo indican en el documento
Análisis de Impacto al Negocio	No se cuenta con una lista de prioridades para levantar los servicios prestados a Banorte	Si	No cuenta con un listado puesto que son pactados con Banorte al momento de una contingencia
Planes de Continuidad	No cuenta con planes de recuperación para servicios de tecnología que presta a Banorte	NA	
Planes de Continuidad	No cuenta con planes que contemplen escenarios de indisponibilidad de edificios donde se prestan los servicios a Banorte	Si	
Planes de Continuidad	No cuenta con planes que contemplen escenarios de indisponibilidad de personal	Si	
Planes de Continuidad	No cuenta con planes que contemplen escenarios de falla por ciberataques	NA	
Comunicación en crisis	No cuenta con un proceso de comunicación en crisis hacia Banorte	Parcial	Si bien comentan cómo es el flujo de su comunicación, no entregaron una matriz de escalamiento donde indique su proceso de comunicación
Comunicación en crisis	No se hace la notificación detallada de los eventos hacia Banorte	Si	

Comunicación en crisis	No se tiene identificado un contacto para notificar a Banorte un evento	NA	
Comunicación en crisis	No se tiene un tiempo determinado para notificar a Banorte en caso de un evento	No	No entregaron una matriz de escalamiento donde indique su proceso de comunicación y tiempos
Comunicación en crisis	No se hacen pruebas de los servicios prestados a Banorte en un esquema de contingencia DRP	NA	
Mantenimiento y pruebas	No se hacen pruebas de conexiones de comunicación con Banorte	No	No realizan pruebas de comunicación con Banorte en caso de una contingencia
Mantenimiento y pruebas	No se hacen pruebas de ataque cibernético con Banorte	NA	
Mantenimiento y pruebas	No se hacen pruebas de estrategias BCP de los servicios prestados a Banorte	No	
Mantenimiento y pruebas	No se hacen de conocimiento a Banorte sobre los resultados de las pruebas realizadas	No	
Mantenimiento y pruebas	No se hacen las pruebas al menos una vez al año para todos los escenarios	No	
Mantenimiento y pruebas	No se realizan matrices de pruebas de los servicios prestados a Banorte	No	
Mantenimiento y pruebas	No se realizan actas de hechos de las pruebas de los servicios prestados a Banorte	No	

4. Resultado final: a continuación se muestra el resultado de la revisión y la calificación final del proveedor revisado

Resultado del proveedor:	Parcialmente aceptable
No cumplimiento	5
Parcialmente cumplidos	4
Cumplidos/NA	14



Proveedor a revisar:	**Servicio Pan Americano de Protección S.A. de C.V.**
Procesos del proveedor:	**Empresa de traslado de valores**
Persona BCP que hace la revisión:	**Judith Molina Guzmán**
Tipo de proveedor:	**Operativo**

1. Severidad: La Severidad de un riesgo es el valor asignado al daño más probable que produciría si se materia.

Seleccione el valor de la severidad para el proveedor a revisar

Pérdida potencial de clientes, daño reputacional grave y perdida de la operación de procesos críticos del banco.

2. Probabilidad o frecuencia: Número de veces que se ha materializado el riesgo durante un período determinados.

Seleccione el valor de la frecuencia indicada por el usuario interno para el proveedor a revisar

1 Evento al año o menos

3. Vulnerabilidades: actividades que en caso de no ser cumplidas pudieran ocasionar que al momento de materializarse un riesgo la empresa será susceptible a efectos dañinos para Banorte. Para la identificación de dichos valores se deberá revisar el cuestionario previamente llenado por el proveedor y responder cada punto de la siguiente tabla.

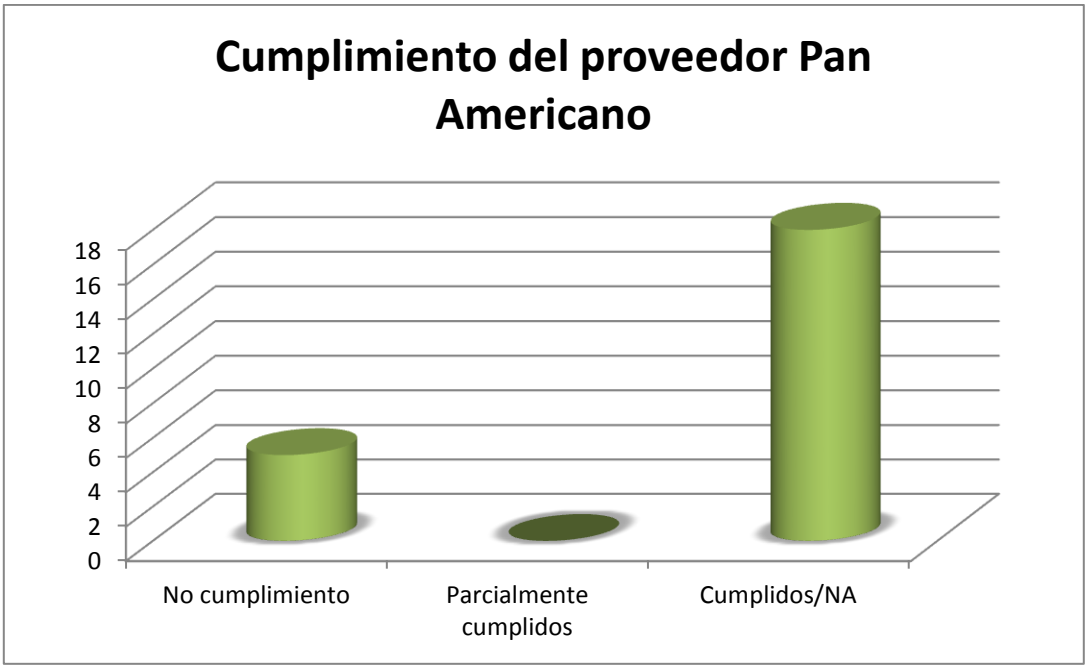
De acuerdo al siguiente catálogo de riesgos asigne el valor que crea responda mejor a la situación de la empresa a revisar

Etapa	Riesgo	Cumplimiento	Comentario
Análisis de Riesgos	No se cuenta con un análisis de riesgos donde se contemple el edificio desde donde se prestan los servicios a Banorte	Si	
Análisis de Impacto al Negocio	No se encuentran identificados los servicios prestados a Banorte en sus planes de continuidad	Si	
Análisis de Impacto al Negocio	No se encuentran identificados los escenarios a los que pudieran estar expuestos los servicios prestados a Banorte	Si	
Análisis de Impacto al Negocio	No se tiene un análisis de impacto al negocio para los servicios prestados a Banorte	Si	
Análisis de Impacto al Negocio	No se tiene identificado un RTO para los servicios prestados a Banorte	Si	
Análisis de Impacto al Negocio	No se tiene identificado un RPO para los servicios prestados a Banorte	Si	
Análisis de Impacto al Negocio	No se cuenta con una lista de prioridades para levantar los servicios prestados a Banorte	Si	No cuenta con un listado puesto que son pactados con Banorte al momento de una contingencia
Planes de Continuidad	No cuenta con planes de recuperación para servicios de tecnología que presta a Banorte	NA	
Planes de Continuidad	No cuenta con planes que contemplen escenarios de indisponibilidad de edificios donde se prestan los servicios a Banorte	Si	
Planes de Continuidad	No cuenta con planes que contemplen escenarios de indisponibilidad de personal	Si	
Planes de Continuidad	No cuenta con planes que contemplen escenarios de falla por ciberataques	NA	
Comunicación en crisis	No cuenta con un proceso de comunicación en crisis hacia Banorte	Si	
Comunicación en crisis	No se hace la notificación detallada de los eventos hacia Banorte	Si	
Comunicación en crisis	No se tiene identificado un contacto para notificar a Banorte un evento	Si	
Comunicación en crisis	No se tiene un tiempo determinado para notificar a Banorte en caso de un evento	Si	
Comunicación en crisis	No se hacen pruebas de los servicios prestados a Banorte en un esquema de	NA	

	contingencia DRP		
Mantenimiento y pruebas	No se hacen pruebas de conexiones de comunicación con Banorte	No	
Mantenimiento y pruebas	No se hacen pruebas de ataque cibernético con Banorte	NA	
Mantenimiento y pruebas	No se hacen pruebas de estrategias BCP de los servicios prestados a Banorte	No	
Mantenimiento y pruebas	No se hacen de conocimiento a Banorte sobre los resultados de las pruebas realizadas	No	
Mantenimiento y pruebas	No se hacen las pruebas al menos una vez al año para todos los escenarios	No	
Mantenimiento y pruebas	No se realizan matrices de pruebas de los servicios prestados a Banorte	No	
Mantenimiento y pruebas	No se realizan actas de hechos de las pruebas de los servicios prestados a Banorte	No	

4. Resultado final: a continuación se muestra el resultado de la revisión y la calificación final del proveedor revisado

Resultado del proveedor:	Aceptable
No cumplimiento	5
Parcialmente cumplidos	0
Cumplidos/NA	18



Proveedor a revisar:	Getronics (México), S. de R.L. de C.V.
Procesos del proveedor:	Proveedores de la red LAN (Servicio de mantenimiento preventivo, proactivo, reactivo y correctivo)
Persona BCP que hace la revisión:	Judith Molina Guzmán

1. Severidad: La Severidad de un riesgo es el valor asignado al daño más probable que produciría si se materia.

Seleccione el valor de la severidad para el proveedor a revisar

Paraliza la operación de las áreas críticas, no se otorga el servicio a los clientes.

2. Probabilidad o frecuencia: Número de veces que se ha materializado el riesgo durante un período determinados.

Seleccione el valor de la frecuencia indicada por el usuario interno para el proveedor a revisar

1 Evento al año o menos

3. Vulnerabilidades: actividades que en caso de no ser cumplidas pudieran ocasionar que al momento de materializarse un riesgo la empresa será susceptible a efectos dañinos para Banorte. Para la identificación de dichos valores se deberá revisar el cuestionario previamente llenado por el proveedor y responder cada punto de la siguiente tabla.

De acuerdo al siguiente catálogo de riesgos asigne el valor que crea responda mejor a la situación de la empresa a revisar

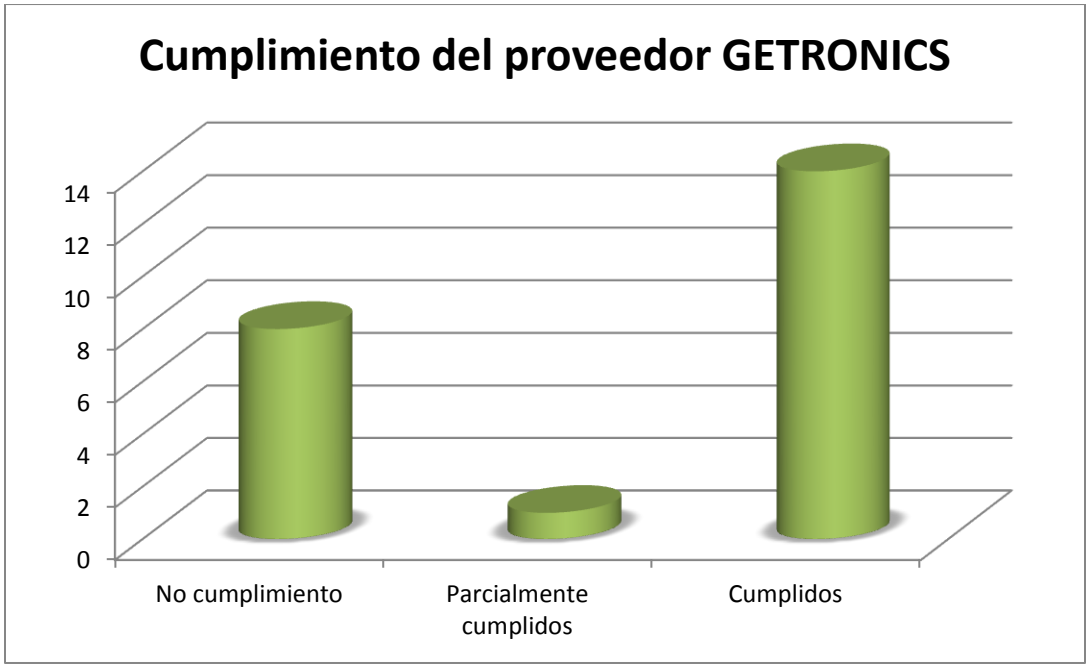
Etapa	Riesgo	Cumplimiento	Comentario
Análisis de Riesgos	No se cuenta con un análisis de riesgos donde se contemple el edificio desde donde se prestan los servicios a Banorte	Si	
Análisis de Impacto al Negocio	No se encuentran identificados los servicios prestados a Banorte en sus planes de continuidad	Si	
Análisis de Impacto al Negocio	No se encuentran identificados los escenarios a los que pudieran estar expuestos los servicios prestados a Banorte	Si	
Análisis de Impacto al Negocio	No se tiene un análisis de impacto al negocio para los servicios prestados a Banorte	Si	
Análisis de Impacto al Negocio	No se tiene identificado un RTO para los servicios prestados a Banorte	Si	

Análisis de Impacto al Negocio	No se tiene identificado un RPO para los servicios prestados a Banorte	No	No se encuentra el RPO en el documento "Disaster Recovery Plan & Business Continuity Plan" y tampoco se comenta el RPO en el "Cuestionario para proveedores del Grupo Financiero Banorte"
Análisis de Impacto al Negocio	No se cuenta con una lista de prioridades para levantar los servicios prestados a Banorte	Si	
Planes de Continuidad	No cuenta con planes de recuperación para servicios de tecnología que presta a Banorte	Si	
Planes de Continuidad	No cuenta con planes que contemplen escenarios de indisponibilidad de edificios donde se prestan los servicios a Banorte	Si	
Planes de Continuidad	No cuenta con planes que contemplen escenarios de indisponibilidad de personal	Si	
Planes de Continuidad	No cuenta con planes que contemplen escenarios de falla por ciberataques	No	No se encuentra en el documento "Disaster Recovery Plan & Business Continuity Plan" referencia de ataques cibernéticos, en el "Cuestionario para proveedores del Grupo Financiero Banorte" se indica que no tienen desarrollados esos planes.
Comunicación en crisis	No cuenta con un proceso de comunicación en crisis hacia Banorte	Si	
Comunicación en crisis	No se hace la notificación detallada de los eventos hacia Banorte	Si	
Comunicación en crisis	No se tiene identificado un contacto para notificar a Banorte un evento	Si	
Comunicación en crisis	No se tiene un tiempo determinado para notificar a Banorte en caso de un evento	Si	
Comunicación en crisis	No se hacen pruebas de los servicios prestados a Banorte en un esquema de contingencia DRP	Parcial	Se hacen referencia en el "Cuestionario para proveedores del Grupo Financiero Banorte" sin ebmargo no se encuentra evidencia de pruebas DRP en el documento "Disaster Recovery Plan & Business Continuity Plan"
Mantenimiento y pruebas	No se hacen pruebas de conexiones de comunicación con Banorte	No	
Mantenimiento y pruebas	No se hacen pruebas de ataque cibernético con Banorte	No	

Mantenimiento y pruebas	No se hacen pruebas de estrategias BCP de los servicios prestados a Banorte	Si	
Mantenimiento y pruebas	No se hacen de conocimiento a Banorte sobre los resultados de las pruebas realizadas	No	No se hace la notificación con el resultado de las pruebas a Banorte y no llega a las partes interesadas (Continuidad del Negocio, Recuperación Ante Desastres, Auditoría)
Mantenimiento y pruebas	No se hacen las pruebas al menos una vez al año para todos los escenarios	No	
Mantenimiento y pruebas	No se realizan matrices de pruebas de los servicios prestados a Banorte	No	
Mantenimiento y pruebas	No se realizan actas de hechos de las pruebas de los servicios prestados a Banorte	No	

4. Resultado final: a continuación se muestra el resultado de la revisión y la calificación final del proveedor revisado

Resultado del proveedor:	No aceptable
No cumplimiento	8
Parcialmente cumplidos	1
Cumplidos	14



Proveedor a revisar:	KIO Networks
Procesos del proveedor:	Servicios de colocación, de conectividad, posiciones de BCP, Salida a internet en el centro de datos
Persona BCP que hace la revisión:	Judith Molina Guzmán

1. Severidad: La Severidad de un riesgo es el valor asignado al daño más probable que produciría si se materia.

Seleccione el valor de la severidad para el proveedor a revisar

Podría incomodar a los clientes, podría afectar parcialmente los procesos críticos.

2. Probabilidad o frecuencia: Número de veces que se ha materializado el riesgo durante un período determinados.

Seleccione el valor de la frecuencia indicada por el usuario interno para el proveedor a revisar

1 Evento al año o menos

3. Vulnerabilidades: actividades que en caso de no ser cumplidas pudieran ocasionar que al momento de materializarse un riesgo la empresa será susceptible a efectos dañinos para Banorte. Para la identificación de dichos valores se deberá revisar el cuestionario previamente llenado por el proveedor y responder cada punto de la siguiente tabla.

De acuerdo al siguiente catálogo de riesgos asigne el valor que crea responda mejor a la situación de la empresa a revisar

Etapa	Riesgo	Cumplimiento	Comentario
Análisis de Riesgos	No se cuenta con un análisis de riesgos donde se contemple el edificio desde donde se prestan los servicios a Banorte	Parcial	En el cuestionario hacen referencia al documento "Evaluación de riesgo" como evidencia de que se cuenta con el análisis, sin embargo no se compartió dicho documento para

			corroborar a detalle
Análisis de Impacto al Negocio	No se encuentran identificados los servicios prestados a Banorte en sus planes de continuidad	Parcial	En el cuestionario hacen referencia al documento "Plan de continuidad del negocio" como evidencia de que se cuenta con la identificación de procesos, sin embargo no se compartió dicho documento para corroborar a detalle
Análisis de Impacto al Negocio	No se tiene un análisis de impacto al negocio para los servicios prestados a Banorte	Parcial	En el cuestionario hacen referencia al documento "Consolidado BIA" como evidencia de que se cuenta con el análisis, sin embargo no se compartió dicho documento para corroborar a detalle
Análisis de Impacto al Negocio	No se tiene identificado un RTO para los servicios prestados a Banorte	Parcial	En el cuestionario hacen referencia al documento "Consolidado BIA" como evidencia de

			que se cuenta con el RTO mencionado (servicio de colocación 10 segundos y salida a internet 10 minutos), sin embargo no se compartió dicho documento para corroborar a detalle
Análisis de Impacto al Negocio	No se cuenta con una lista de prioridades para levantar los servicios prestados a Banorte	Parcial	En el cuestionario hacen referencia al documento "Resumen ejecutivo BIA" como evidencia de que se cuenta con una lista de prioridades de recuperación, sin embargo no se compartió dicho documento para corroborar a detalle
Planes de Continuidad	No cuenta con planes de recuperación para servicios de tecnología que presta a Banorte	Parcial	En el cuestionario hacen referencia a los documentos "DRP infraestructura" y "DRP Circuito de internet" como

			evidencia de que se cuenta con planes de recuperación TI, sin embargo no se compartió dicho documento para corroborar a detalle
Planes de Continuidad	No cuenta con planes que contemplen escenarios de indisponibilidad de edificios donde se prestan los servicios a Banorte	No	No se comenta en los planes con los que cuenta KIO planes para este escenario.
Planes de Continuidad	No cuenta con planes que contemplen escenarios de indisponibilidad de personal	No	No se comenta en los planes con los que cuenta KIO planes para este escenario.
Planes de Continuidad	No cuenta con planes que contemplen escenarios de falla por ciberataques	No	Si bien comentan que su plan si contempla este escenario no viene ningún documento que indique dónde encontrarlo
Comunicación en crisis	No cuenta con un proceso de comunicación en crisis hacia Banorte	No	No cuenta con un proceso de comunicación hacia Banorte
Comunicación en crisis	No se hace la notificación detallada de los eventos hacia	No	No se indica los aspectos a comunicar a Banorte

	Banorte		
Comunicación en crisis	No se tiene identificado un contacto para notificar a Banorte un evento	No	
Comunicación en crisis	No se tiene un tiempo determinado para notificar a Banorte en caso de un evento	No	No cuentan con tiempos detallados para el escalamiento y comunicación de los eventos hacia Banorte
Comunicación en crisis	No se hacen pruebas de los servicios prestados a Banorte en un esquema de contingencia DRP	Parcial	En el cuestionario hacen referencia al documento "Reporte de prueba" como evidencia de que se realizan pruebas, sin embargo no se compartió dicho documento para corroborar a detalle
Mantenimiento y pruebas	No se hacen pruebas de conexiones de comunicación con Banorte	No	
Mantenimiento y pruebas	No se hacen pruebas de ataque cibernético con Banorte	No	
Mantenimiento y pruebas	No se hacen pruebas de estrategias BCP de los servicios prestados a	No	

	Banorte		
Mantenimiento y pruebas	No se hacen de conocimiento a Banorte sobre los resultados de las pruebas realizadas	No	
Mantenimiento y pruebas	No se hacen las pruebas al menos una vez al año para todos los escenarios	No	
Mantenimiento y pruebas	No se realizan matrices de pruebas de los servicios prestados a Banorte	No	
Mantenimiento y pruebas	No se realizan actas de hechos de las pruebas de los servicios prestados a Banorte	No	

4. Resultado final: a continuación se muestra el resultado de la revisión y la calificación final del proveedor revisado

Resultado del proveedor:	No aceptable
No cumplimiento	14
Parcialmente cumplidos	7
Cumplidos	2