Gestión de Riesgo: Resiliencia para la Continuidad del Negocio

¿Por qué la Resiliencia para la Continuidad de Negocio?

El marco de Gestión de Riesgos para la Continuidad de Negocios hace transcender a una organización cuando es resiliente a los desafíos que exigen la ocurrencia de eventos inesperados en su entorno.

Resiliencia Operativa

En las organizaciones se debe desarrollar la capacidad de poder recuperarse de eventos disruptivos sean cuales sean, que aseguren estar preparados a superar los cambios que sufre el entorno para lograr transformar los riesgos en oportunidades…*a esto estamos obligados para transcender*…

Para la Continuidad de Negocio

La Resiliencia Operativa inmersa en el Plan de Continuidad de Negocios, permite identificar los riesgos que se encuentran en el proceso de planificación estratégica, esto facilita identificar las consecuencias de las decisiones y lograr la correcta selección de objetivos que esten integrados en todos los niveles de la organización para estar preparados a cualquier evento disruptivo.

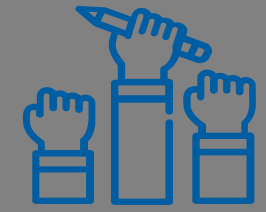

¿Cómo enfrentar
las disrupciones?

A traves de la adaptación operativa de forma ágil y eficiente...

Foco en el desarrollo seguro de productos y servicios digitales basados en la experiencia de uso del Cliente

Metodologías ágiles en los procesos con mayor control de riesgos

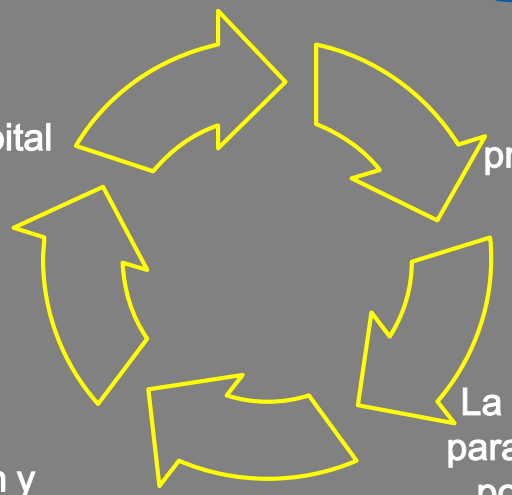
La Gestión de Riesgos Resiliente para la Continuidad del Negocio es posicionada con Operaciones y Negocio



Se refuerza desde la alta gerencia la Cultura de Riesgos para asegurarnos que toda la organización las entiende y comparte

Transformación Digital desarrollada con Gestión y Prevención de Riesgos

Inversión de Capital



...con acciones tácticas dentro del Plan de Continuidad de Negocio

Análisis continuo de los escenarios que podrían presentarse para estar preparados a dar respuesta oportuna a traves de acciones de contingencia definidas.

Información oportuna sobre la ocurrencia continua de eventos internos o externos, para la toma de decisiones inmediatas y efectivas.

Prioridad en proteger a los colaboradores y procesos principales del negocio, contando con planes de recuperación que no comprometan la continuidad.

Evaluación del riesgo de los principales procesos operativos para adecuarlos al tamaño del negocio, apegados al cumplimiento regulatorio y gestionando el riesgo reputacional

...y con objetivos operacionales claros

Mantener el nivel de servicio en los límites definidos

Establecer un período de recupera-ción mínimo

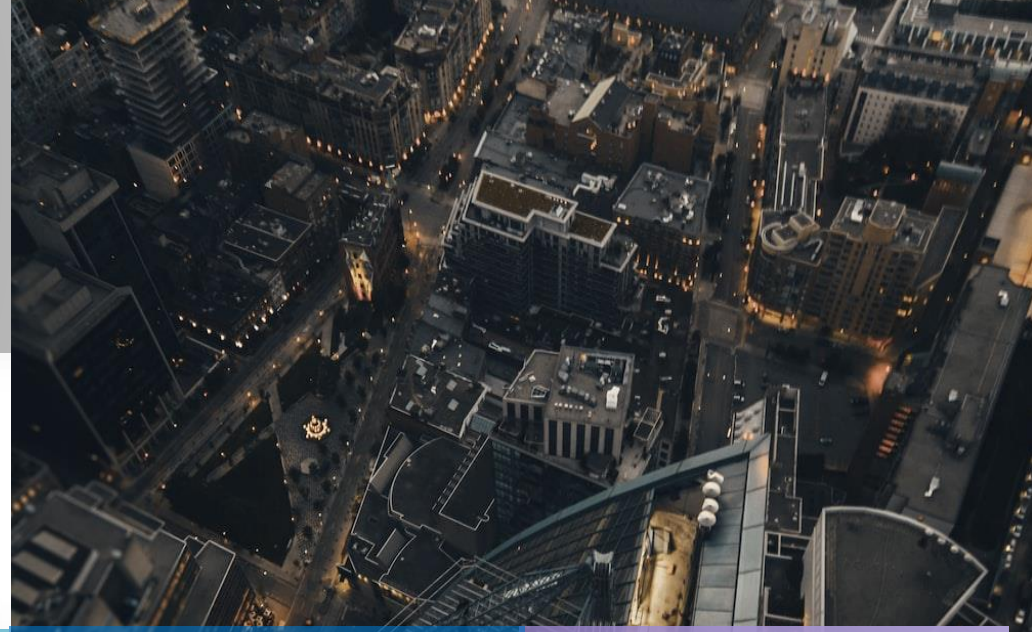
Recuperar la situación inicial antes de cualquier incidente de seguridad

Analizar los resultados y los motivos de los incidentes

Evitar que las actividades de la em-presa se interrumpan

Fuente: INCIBE Instituto Nacional de Ciberseguridad

Factores generadores de Riesgo Operacional



Existen elementos que son detonantes para el proceso de riesgo; los factores que generan Riesgos Operacionales en las Instituciones Financieras se pueden clasificar en:

Ejecución de los procedimientos, Marco de cumplimiento de políticas o leyes.	**Cambios regulatorios, hechos políticos, ciberataques, eventos disruptivos.**	**Interrupciones del negocio, ocurrencia de eventos, daños o afectaciones a la infraestructura.**	**Problemas en los sistemas, en las telecomunicaciones o en los datos.**	**Talento, Valores y Compromiso.**
PROCESOS	EXTERNO	FÍSICO	TECNOLÓGICO	GENTE

Situaciones...

- Reconversión
- Inflación
- Recesión
- Devaluación

- Fuja de Talento
- Disponibilidad de Servicios
- Eficiencia de Procesos

- Salud Laboral
- Pandemia
- Trabajo a distancia

- Retención de Talento
- Cambio en la Forma de Trabajo

- Rentabiliodad y Resultados
- Eficiencia operativa

- Tecnologías emergentes
- Gestión y Prevención de Riesgos

La Gestión de Riesgo es un elemento clave en la Planificación Estratégica del Negocio basada en objetivos que se anticipen, preparen y respondan al entorno para apoyar los resultados financieros esperados

Transformar los riesgos en oportunidades siendo Resilientes

Preparación en el Manejo de Crisis: equipos de análisis y respuesta ejecutiva ante los cambios de entorno y preparación de escenarios. Gestión de los riesgos para reducir el impacto sobre estrategias y resultados. Evaluación del tamaño del negocio para adecuar costos. Foco en rentabilidad. Mecanismos de protección patrimonial.

Rentabilidad del Negocio con Procesos Eficientes: levantamiento y análisis de procesos ajustados al volumen del negocio alineadas a la toma de mejores decisiones. Evaluación continua de procesos para que sean claros y eficientes y los proveedores pasan a ser socios estratégicos. Inversión en Tecnología y Digitalización.

Avanzar en la Transformación Digital: poner el centro en el cliente, proceso continuo y acelerado hacia productos digitales, con foco en experiencia del cliente para entregar calidad y agilidad. Alta capacidad de innovación en productos y servicios ***sostenibles***. Alta capacidad de segmentar clientes para atender necesidades a la medida.

Coherencia entre la Estrategia y la Cultura de Riesgo

01 Cultura y Gestión de Riesgo

La cultura de riesgo abarca los valores y el conocimiento sobre el riesgo que tiene una organización "Cómo se hacen aquí las cosas". Una fuerte Cultura de Riesgos es la que permite la identificación de los riesgos desde la definición de la estrategia logrando alinear los procesos hacia la mitigación de riesgos considerando el entorno competitivo y su evolución.

02 Perfil de Riesgo en la Organización

Es el reflejo de la situación de la gestión de riesgos de la Institución en un momento determinado.

03 Gobierno Corporativo y Riesgo Reputacional

Es el conjunto de percepciones que se tienen sobre la empresa y los diversos grupos de interés internos y externos con los cuales se relaciona la misma.

49.3%

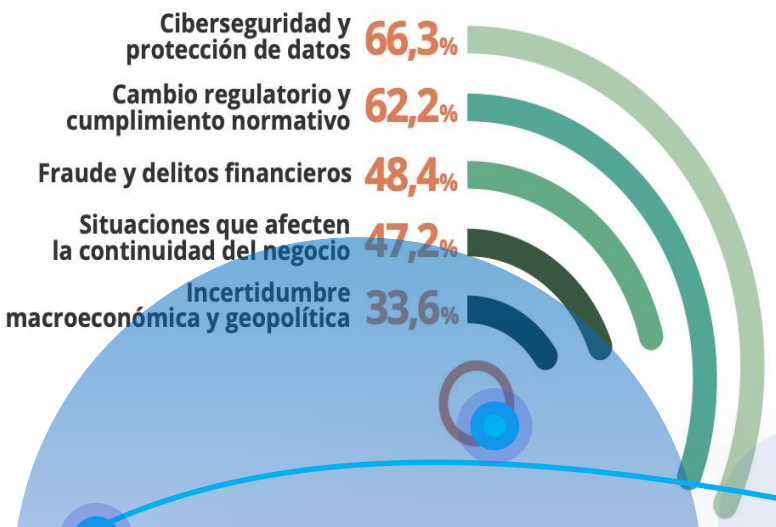
"La gestión de riesgos es muy importante en sus organizaciones, la consideran como un área estratégica para el logro de los objetivos organizacionales y la continuidad de sus negocios"

"El 41,4% de los participantes del estudio considera que la gestión de riesgos es importante, sin embargo, en sus organizaciones hace falta mayor compromiso por parte de todos los colaboradores. Adicionalmente, el 8,9% dice que la gestión de riesgos en sus organizaciones es un área de poca importancia y que la mayoría de empleados no le ven valor..."

Fuente: Pirani. Estudio de Gestión de Riesgos en Latinoamérica 2022 realizado por 485 encuesta virtual CEO, directores y gerentes de riesgos, analistas y gestores de riesgos, oficiales de cumplimiento, auditores internos, analistas de seguridad de la información, entre otros, de países como Colombia, México, Perú, Ecuador, Venezuela, Guatemala, República Dominicana, Chile, Bolivia y Costa Rica.

Principales resultados del Estudio 2023

5 Riesgos más importantes para las organizaciones



3 Dificultades que enfrenta el área de gestión de riesgos

3 Retos en gestión de riesgos para 2023

Es el conjunto de percepciones que se tienen sobre la empresa y los diversos grupos de interés internos y externos con los cuales se relaciona la misma.

La Banca es un negocio basado en la Confianza

La Gestión de Riesgo debe ser el habilitador para establecer el Apetito y Tolerancia al Riesgo en la organización

Es el reflejo de la situación de la gestión de riesgos de la Organización en un momento determinado.

Apetito de Riesgo

Límites de **aceptación de riesgo según la capacidad** y las políticas establecidas derminados a partir del proceso de identificación y análisis de los riesgos. El apetito de riesgo es una decisión, es por ello que requiere una **apropiada cultura de riesgo y buenas prácticas de gobierno corporativo** impulsada desde la directiva y adoptadas en todos los niveles de la institución.

Tolerancia al Riesgo

Es el **nivel de riesgo que puede soportar una institución sin afectar la continuidad del negocio**. Puede estar definido por variación en los resultados, cumplimiento regulatorio, capacidad de endeudamiento, o cualquier exposición que afecte la reputación institucional. **La tolerancia al riesgo debe estar alineada con el apetito de riesgo en el marco de la Cultura de Riesgo de la Institución y presente en la planificación estratégica.**

Gestión de riesgo

Es el proceso ejecutado desde la alta gerencia que involucra a todo el personal de una organización, aplicado en la definición de la estrategia y diseñado para identificar eventos potenciales que pudieran afectar el negocio.

01
IDENTIFICACIÓN

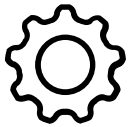
Implica reconocer posibles fallos o deficiencias en procesos, personas, factores externos o sistemas dentro de una organización

02
MEDICIÓN

Se miden los riesgos en términos de probabilidad de ocurrencia-frecuencia e impacto-severidad

03
MITIGACIÓN

Una vez identificado los riesgos se evalúa su tratamiento y mitigación para minimizar su impacto y probabilidad de ocurrencia



04
MONITOREO Y CONTROL

Seguimiento que permite garantizar que las medidas de mitigación reduzcan la posibilidad de que un evento se materialice

05
INFORMACIÓN

Informar al Gobierno Corporativo de los riesgos gestionados, sus controles y mitigantes.

Metodológicamente la gestión integral de riesgo se encarga de identificar, medir, monitorear y controlar para mitigar e informar a las unidades funcionales sobre los distintos riesgos a los que se encuentra expuesta la organización.

Tipos de Riesgo

Los riesgos financieros:

Hacen referencia a todo evento que pueda comprometer los objetivos relacionados con la gestión financiera de una organización, originando un impacto económico que afecta a los resultados (lo que ganamos o perdemos).

Los riesgos NO financieros :

Son aquellos que están asociados con los riesgos de empresa en marcha, afectan a la continuidad del negocio en el marco del contexto interno y externo, como actúa sobre la organización exponiéndola a eventos que tengan un impacto financiero.

Pasar de la Continuidad a la Sostenibilidad del Negocio

DESDE 1950

Gestión de desastres naturales, como terremotos, incendios e inundaciones

- El enfoque se centraba principalmente en la protección de registros físicos

DESDE 1980

Las organizaciones empezaron a reconocer la importancia de la planificación y preparación para interrupciones operativas

- Se desarrollaron métodos rudimentarios de backup y recuperación de datos, con un enfoque en proteger registros y documentos físicos clave.

DESDE EL AÑO 2000

Planes de Recuperación involucrando a toda la empresa

BCGM experimentó una transformación radical impulsada por la rápida evolución de la tecnología y la creciente complejidad de los riesgos.

Estándares y Normas

Definiciones mundiales de estándares y directrices

- Basilea II: se fomenta que las entidades financieras establezcan estrategias de mitigación de riesgos operativos
- ISO 22301: establece un marco para la gestión de la continuidad del negocio

HISTORIA RECIENTE

BIA y Evaluación de Riesgos:

Se dio un enfoque más estructurado, permitiendo a las organizaciones comprender sus operaciones críticas, evaluar vulnerabilidades y diseñar planes de contingencia efectivos.

Reconocimiento de los Riesgos Sistémicos

La globalización y la interconexión de las organizaciones llevaron a una mayor conciencia sobre los riesgos sistémicos y la necesidad de una preparación más avanzada

PRESENTE Y FUTURO

Transformación y Resiliencia Digital:

La virtualización, la nube y la movilidad cambiaron la forma en que se aborda la continuidad y la recuperación. Estas tecnologías permitieron una **mayor flexibilidad y agilidad en la recuperación, así como la resiliencia en el entorno digital.**

Ciberseguridad y Prevención de Riesgos de Ciberfraude

Con el auge de los ciberataques, la BCGM se adaptó para **abordar la ciberseguridad como un componente crucial de la continuidad del negocio**, protegiendo así la integridad y seguridad de los datos en un mundo cada vez más digital.

Modelo de Continuidad del Negocio

Proceso que contemplan la participación de las unidades involucradas, los cuales continuamente son revisados y actualizados con las oportunidades de mejora identificadas.

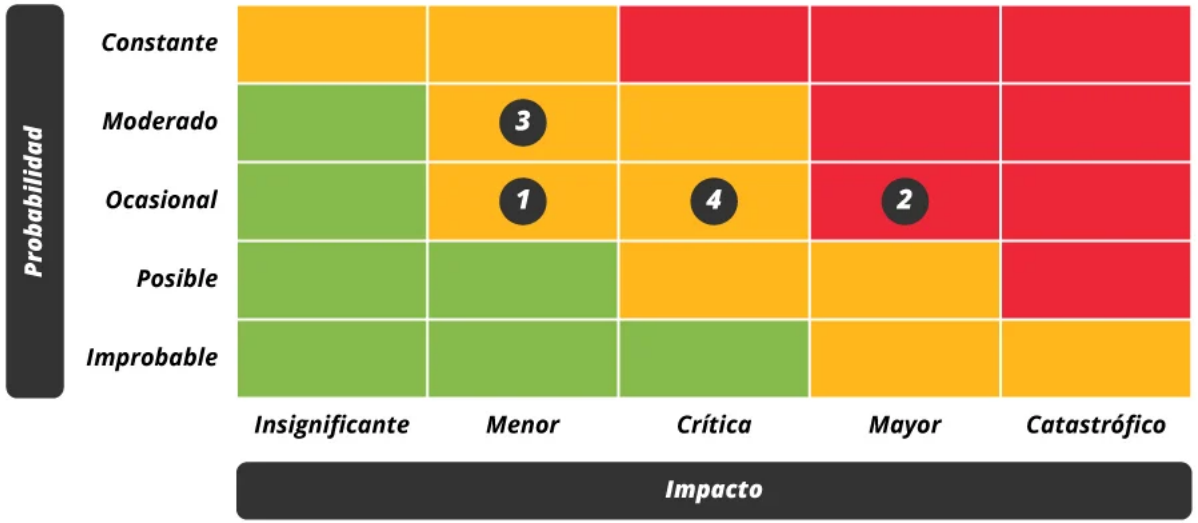
Pasos del Modelo de Continuidad de Negocios como Habilitadores

Identificación y Evaluación de Riesgos

Como resultado del análisis se consideran las amenazas que deben ser atendidas con prioridad, con el propósito de:

1. Implementar mitigantes para evitar o reducir su impacto y
2. Desarrollar estrategias que permitan mantener operativos los procesos críticos en caso de que alguna se materialice

Mapa de Riesgo Resultante



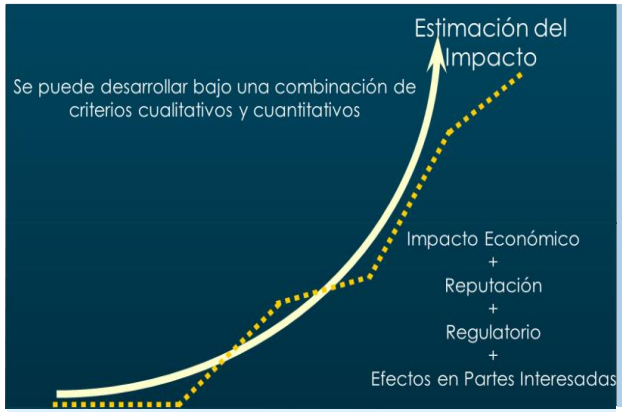
Amenazas	
	EVENTOS NATURALES
1	Deslaves o Deslizamiento de Tierras
2	Inestabilidad del terreno
3	Sismicidad
4	Lluvias Severas, Inundaciones
5	Vientos (Vientos de Alta Velocidad, Huracanes, Tornados)
6	Descargas Eléctricas
7	Epidemia - Pandemia
	EVENTOS TECNICOS
8	Falla Eléctrica
9	Falla Central Telefónica
10	Falla en equipos críticos Telecomunicaciones
11	Falla de Software
12	Falla en equipos críticos de TI
	ACTIVIDADES MALINTENCIONADAS
13	Actos de Terrorismo
14	Quebrantamiento de la Seguridad Física
15	Quebrantamiento de la Seguridad de la Información
16	Ataques de Seguridad de Red
17	Inseguridad Ciudadana
18	Manifestaciones
	PROVEEDORES DE SERVICIO
19	Falla del Servicio de Electricidad
20	Falla proveedor de Comunicaciones (Data y Telefonía)
22	Falla del Servicio de Gas
23	Escasez de combustible
24	Falla del Servicio de Saneamiento Urbano
25	Falla del Servicio de Agua
	FUEGO
26	Fallas del Sistema de detección y extinción de Incendios

Metodología para Análisis de Impacto del Negocio

Business Impact Analysis (BIA)

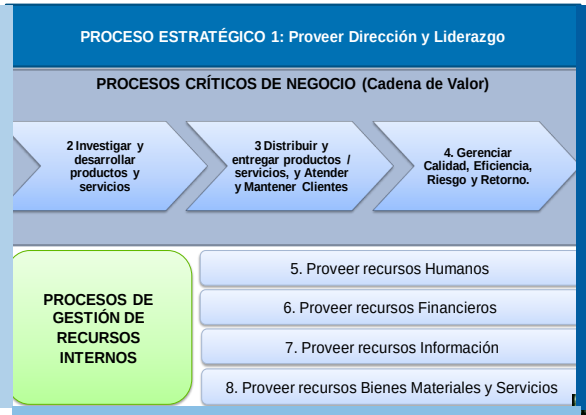
Priorizar las Procesos Críticos según la metodología basada en:

1. El impacto financiero ocasionado por una interrupción
2. La prioridad determinada por juicio del experto que define orden de recuperación y
3. El análisis transaccional, legal y reputacional.



Análisis Financiero

Se evalúa cual es el impacto financiero ocasionado por una posible interrupción de los procesos de negocio

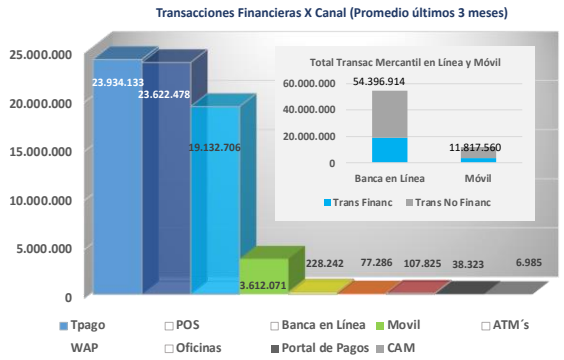


Análisis Cualitativo

Se toma en cuenta la opinión de los expertos en la prioridad de recuperación de procesos

Análisis Transaccional

Cual proceso tiene mayor número de operaciones que impacte al cliente de manera significativa



CIBERSEGURIDAD

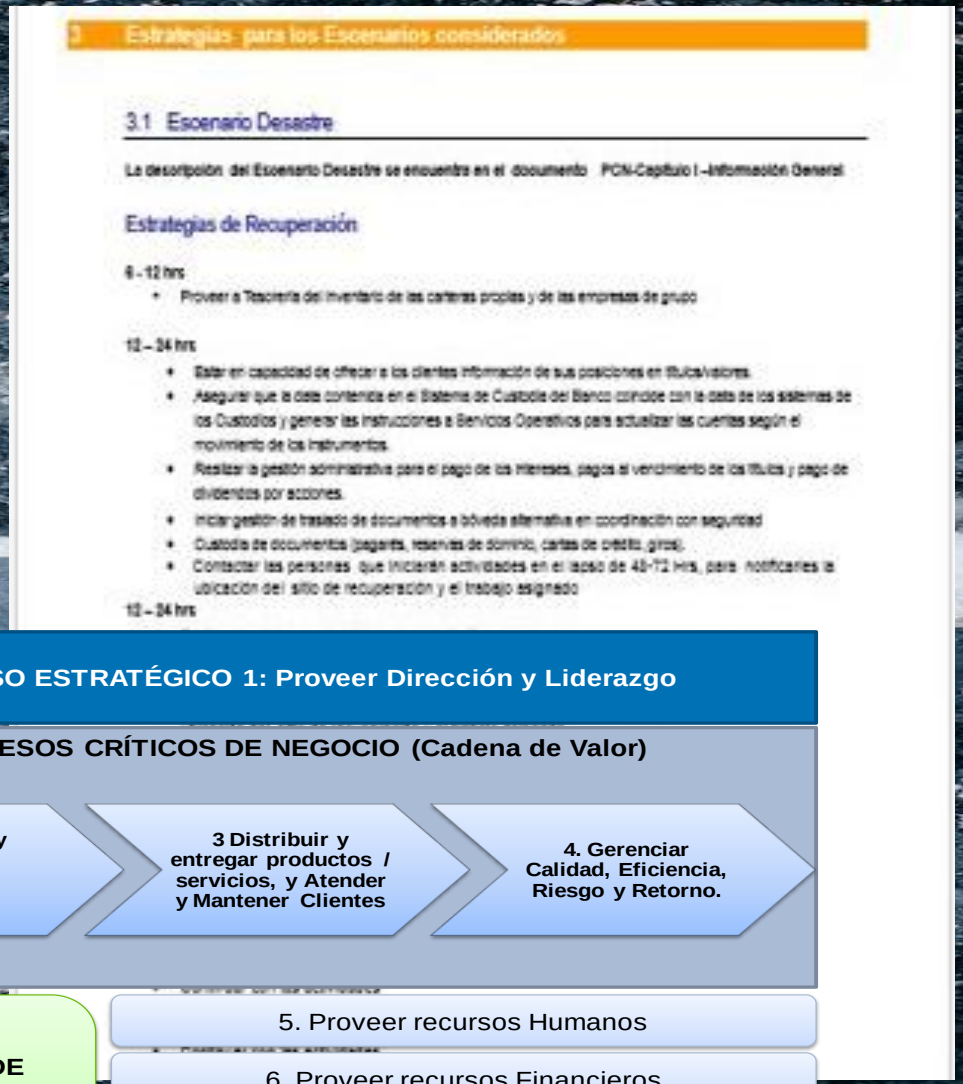
Se identifican los procesos mas susceptibles a ser objetivos de ataques de la ciberdelincuencia

Plan de Continuidad de Negocios

Documentación de la Prioridad de Recuperación de los Procesos según el BIA

1. En el Plan de Continuidad de Negocios se describen los escenarios identificados en la evaluación de riesgo y se documentan, por cada unidad responsable de los procesos críticos, los procedimientos detallados de recuperación siguiendo la prioridad establecida y aprobada en el Análisis de Impacto del Negocio (BIA).

2. Se alinea con la estrategia de recuperación definida y sus procesos hacen uso, a través de los colaboradores críticos identificados, de la plataforma tecnológica disponible



3 Estrategias para los Escenarios considerados

3.1 Escenario Desastre

La descripción del Escenario Desastre se encuentra en el documento PCN-Capítulo I –Información General

Estrategias de Recuperación

6 - 12 hrs

- Proveer a Tesorería del inventario de las carteras propias y de las empresas de grupo

12 – 24 hrs

- Estar en capacidad de ofrecer a los clientes información de sus posiciones en títulos/valores.
- Asegurar que la data contenida en el Sistema de Custodia del Banco coincide con la data de los sistemas de los Custodios y generar las instrucciones a Servicios Operativos para actualizar las cuentas según el movimiento de los instrumentos.
- Realizar la gestión administrativa para el pago de los intereses, pagos al vencimiento de los títulos y pago de dividendos por acciones.
- Iniciar gestión de traslado de documentos a bóveda alternativa en coordinación con seguridad
- Custodia de documentos (pagarés, reservas de dominio, cartas de crédito, giros).
- Contactar las personas que iniciarán actividades en el lapso de 48-72 hrs, para notificarles la ubicación del sitio de recuperación y el trabajo asignado

12 – 24 hrs

Pruebas de Contingencia y Desastre

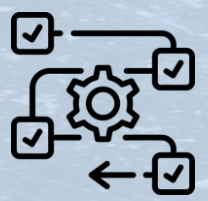
¿Qué nos ha ayudado a mejorar nuestros resultados? Los simulacros de materialización de escenarios

Planificación

Planificar con tiempo e involucrar a todos los que participan en las pruebas: técnicos, usuarios, auditores y continuidad

Comunicación entre equipos de tecnología, de continuidad y usuarios

Mantener una comunicación efectiva presencial y a través de medios digitales, aclarando los objetivos y el diseño de las pruebas**. El compromiso de los participantes es fundamental**



Scripts de pruebas de usuarios y procedimientos técnicos actualizados

Los procesos son renovados o surgen nuevos continuamente por lo cual los scripts tanto de usuarios como técnicos deben ser actualizados

Actualización del CPDA segun el BIA

Los nuevos procesos incorporados en el BIA deben tener en el CPDA la plataforma tecnológica que los soporta. Asimismo, la plataforma existente debe ser actualizada

Actualización de la plataforma de seguridad de la información y ciberseguridad

Monitoreo de intrusos, protección de la replica de datos y backups

Identificación de las oportunidades de mejora

Determinar en cuales aspectos podemos mejorar, validar la autonomía de los centros alternos y la conectividad de clientes, técnicos y usuarios

“El cambiante entorno corporativo exige resiliencia para ser sostenible…”

VGS