DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

TRABAJO DE TITULACIÓN, PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS E INFORMÁTICA

TEMA: DESARROLLO DE UN PLAN DE CONTINUIDAD DE NEGOCIO BASADO EN ISO22301:2012 PARA LA COOPERATIVA DE AHORRO Y CRÉDITO "29 DE OCTUBRE" LTDA.

AUTORES: HERNÁNDEZ TIPÁN,

OSCAR DAVID

MEDINA MOREJON, BERNARDO

JEROME

DIRECTOR: ING. RON EGAS, MARIO

BERNABÉ

SANGOLQUÍ

2016

CERTIFICADO

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN
CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

CERTIFICACIÓN

Certifico que el trabajo de titulación, "***DESARROLLO DE UN PLAN DE CONTINUIDAD BASADO EN ISO 22301:2012 PARA LA COOPERATIVA DE AHORRO Y CRÉDITO 29 DE OCTUBRE***" realizado por los señores ***HERNANDEZ TIPAN OSCAR DAVID Y MEDINA MOREJON BERNARDO JEROME***, ha sido revisado en su totalidad y analizado por el software anti-plagio, el mismo cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, por lo tanto me permito acreditarlo y autorizar a los señores **HERNANDEZ TIPAN OSCAR DAVID Y MEDINA MOREJON BERNARDO JEROME** para que lo sustenten públicamente.

Quito, 11 de agosto de 2016

Atentamente,

Ing Mario Ron Egas
Director

AUTORÍA DE RESPONSABILIDAD

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN
CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

AUTORÍA DE RESPONSABILIDAD

Yo, **HERNÁNDEZ TIPÁN OSCAR DAVID** con cédula de identidad N° 1718713116 y **MEDINA MOREJÓN BERNARDO JEROME** con cédula de identidad N° 1719287920, declaramos que este trabajo de titulación "**DESARROLLO DE UN PLAN DE CONTINUIDAD BASADO EN ISO 22301:2012 PARA LA COOPERATIVA DE AHORRO Y CRÉDITO 29 DE OCTUBRE**" ha sido desarrollado considerando los métodos de investigación existentes, así como también se ha respetado los derechos intelectuales de terceros considerándose en las citas bibliográficas.

Consecuentemente declaro que este trabajo es de mi autoría, en virtud de ello me declaro responsable del contenido, veracidad y alcance de la investigación mencionada.

Quito, 11 de agosto de 2016

OSCAR DAVID HERNÁNDEZ TIPÁN
C.C 1718713116

BERNARDO JEROME MEDINA MOREJÓN
C.C 1719287920

AUTORIZACIÓN

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN
CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

AUTORIZACIÓN

Yo, **HERNÁNDEZ TIPÁN OSCAR DAVID Y MEDINA MOREJÓN BERNARDO JEROME**, autorizamos a la Universidad de las Fuerzas Armadas ESPE publicar en la biblioteca Virtual de la institución el presente trabajo de titulación "**DESARROLLO DE UN PLAN DE CONTINUIDAD BASADO EN ISO 22301:2012 PARA LA COOPERATIVA DE AHORRO Y CRÉDITO 29 DE OCTUBRE**" cuyo contenido, ideas y criterios son de mi autoría y responsabilidad.

Quito, 11 de agosto de 2016

OSCAR DAVID HERNÁNDEZ TIPÁN
C.C 1718713116

BERNARDO JEROME MEDINA MOREJÓN
C.C 1719287920

DEDICATORIA

Quiero dedicar este trabajo a mi familia, quienes han sido el pilar fundamental para conseguir mis objetivos y metas, han estado de manera incondicional brindándome su apoyo y ánimos para seguir adelante, por todo eso y mucho más este logro es de ellos.

Al Ing. Mario Ron quien ha sido un guía y consejero brindándome sus conocimientos académicos y profesionales para ser buena persona, profesional de bien y contribuir de manera proactiva a la sociedad.

Oscar

Este trabajo está dedicado a mi familia quienes supieron apoyarme en los momentos difíciles con sus sabios consejos y apoyo incondicional sabiendo encaminarme siempre por el camino correcto.

Al Ing. Mario Ron quien con sus conocimientos y guía hizo posible la ejecución de este trabajo aportando su criterio profesional y experiencia como lo haría un amigo.

Bernardo

AGRADECIMIENTO

Quiero agradecer por el presente trabajo a mi familia que con su apoyo desinteresado me han permitido cumplir con este objetivo.

A mi querida ESPE quien fue la cuna de mi crecimiento profesional acogiéndome durante todo el tiempo de mi vida estudiantil, la cual me permitió formarme académicamente con valores y principios para ser un profesional de bien, gracias por todas las alegrías y siempre recordare los momentos vividos en mi querida Institución.

A mis profesores quienes fueron una guía compartiendo sus conocimientos académicos y de vida para aplicarlos a mi profesión.

Oscar

Este trabajo está dedicado a mi familia quienes supieron apoyarme en los momentos difíciles con sus sabios consejos y apoyo incondicional sabiendo encaminarme siempre por el camino correcto.

Al Ing. Mario Ron quien con sus conocimientos y guía hizo posible la ejecución de este trabajo aportando su criterio profesional y experiencia como lo haría un amigo.

Bernardo

ÍNDICE DE CONTENIDO

Contenido

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El presente proyecto propone la elaboración de un Plan de Continuidad de Negocio (BCP) para la Cooperativa de Ahorro y Crédito (COAC) “29 de Octubre”, enfocándose en el cumplimiento de las normas generales vigentes para las instituciones del Sistema Financiero, en las que se estipula que estas deben estar en capacidad de asegurar que su operación sea continua minimizando las pérdidas económicas y de imagen en caso de la materialización de un evento de crisis. Para la elaboración del BCP se tomó como referencia el estándar ISO 22301:2012 así como también las metodologías de análisis de riesgo de la COAC “29 de Octubre” en las que se considera los valores de pérdidas económicas aceptables por la institución, los componentes de hardware y software utilizados para la automatización de los procesos y los servicios críticos identificados en el Análisis de Impacto en el Negocio (BIA), los cuales fueron utilizados para la definición de estrategias para las etapas de antes durante y después de los eventos de crisis. Se obtuvo como resultado procedimientos actualizados, medidas preventivas y correctivas necesarias para establecer un marco de continuidad alineado con los requerimientos de las entidades de control y las necesidades específicas de la COAC “29 de Octubre” y por último un BCP actualizado y alineado a los procesos de negocio ejecutados en la Cooperativa.

PALABRAS CLAVE:

- CONTINUIDAD DE NEGOCIO
- SERVICIOS CRÍTICOS
- BUSINESS IMPACT ANALYSIS
- BCP
- ISO 22301:2012

ABSTRACT

This project proposes the development of a business continuity plan (BCP) for Cooperativa de Ahorro y Crédito (COAC) "29 de Octubre" oriented to the compliance of the general rules applicable to the Financial System institutions which establishes that all the institutions must ensure they are capable to operate continuously and minimize financial and reputational losses in cases of a crisis event materializes. The BCP was done, taking ISO 22301: 2012 standard as reference as well as the COAC “29 de Octubre” methodology of risk analysis which considers the bearable economic loss by the institution, the hardware and software used for the automation of processes and the critical services identified in the BIA, this services was used for the definition of strategies for stages before, during and after the crisis event. It was obtained as a result updated procedures, preventive and corrective measures necessary to establish a framework of continuity aligned with the requirements of the control entities and the specific needs of COAC "29 de Octubre" and finally a BCP updated and aligned to the business processes executed in the Cooperative.

KEY WORDS

- BUSINESS CONTINUITY
- KEY SERVICES
- BUSSINESS IMPACT ANALYSIS
- BCP
- ISO 22301:2012

CAPÍTULO I
ASPECTOS GENERALES

1.1. OBJETIVOS

1.1.1. Objetivo General

Desarrollar un Plan de Continuidad de Negocio basado en ISO 22301:2012 en la Cooperativa de Ahorro y Crédito “29 de octubre” LTDA - Administración Central para mantener la disponibilidad de los servicios críticos provistos por la Dirección de Informática y Comunicaciones.

1.1.2. Objetivos Específicos

i. Evaluar los riesgos Informáticos en la Dirección de Informática y Comunicaciones de la Administración Central de la Cooperativa de Ahorro y Crédito “29 de Octubre” LTDA.

ii. Determinar los servicios críticos en la Informática de Tecnología y Comunicaciones de la Administración Central de la Cooperativa de Ahorro y Crédito “29 de Octubre” LTDA.

iii. Analizar el impacto Operativo que se genera por la no disponibilidad de los servicios críticos de la Dirección de Tecnología y Comunicaciones en la Administración Central de la Cooperativa de Ahorro y Crédito “29 de Octubre” LTDA.

iv. Aplicar las normativas vigentes definidas por las entidades de control para las instituciones financieras frente a la Gestión de Riesgo Operativo y de Continuidad del Negocio de la República del Ecuador.

1.2. INTRODUCCIÓN

La COAC “29 de Octubre” es una institución fundada por personal militar y creada bajo la concepción de estimular y fomentar el ahorro, la prestación oportuna del crédito para sus socios y mejorar la calidad de vida de los mismos.

Actualmente, las actividades y operaciones que realiza la Cooperativa están regidas y amparadas en la ley ecuatoriana; además, está sometida a la aplicación de normas de solvencia, prudencia financiera contable y al control directo de la Superintendencia de Economía Popular y Solidaria de Ecuador.

Durante el paso de los años ha ido creciendo y aumentando la cartera de servicios y productos que ofrece a sus clientes, entre los principales se encuentran:

- 29 Seguro
- Seguro Auto 29
- Habla 29 – Recargas
- Pagos Institucionales
- Pagos de fondos de Reservas
- Venta de Bienes Inmuebles
- Pago de anticipos de sueldos

Adicionalmente posee ciertos productos los cuales se han ido diversificando durante el transcurso de los años:

- Ahorro
    - 29 Card
    - Cuenta Angelitos
    - Cuenta de Ahorros
    - Cuenta mejor Futuro
- Crédito
    - Consumo
    - Microcrédito
    - Mi casa 29
- Inversiones
    - Inversiones a plazo fijo

Con la evolución de los servicios y la diversificación de sus productos la Cooperativa se ha visto en la necesidad de invertir en soluciones e infraestructura tecnológica que soporte la automatización de los procesos que sirven para provisión de dichos servicios.

Dicha automatización ha ayudado a la COAC a llegar a un mayor número de clientes y a mejorar la calidad y disponibilidad de sus servicios, sin embargo asociado a estos beneficios existen riesgos inherentes derivados del uso tanto de los sistemas informáticos como de la infraestructura que lo soporta.

1.2.1. Misión

"Somos una Cooperativa de ahorro y crédito que contribuye al desarrollo del país, con productos y servicios financieros oportunos para nuestros socios y clientes con transparencia, responsabilidad y seguridad." (Cooperativa de Ahorro y Crédito 29 de Octubre, 2016)

1.2.2. Visión 2018

"Ser la Cooperativa de ahorro y crédito con mayor cobertura nacional, consolidados entre las tres más grandes del país, promoviendo productos y servicios financieros de calidad con tecnología de punta y responsabilidad social." (Cooperativa de Ahorro y Crédito 29 de Octubre, 2016)

1.2.3. Estructura Organizacional de la Empresa:

La Cooperativa de Ahorro y Crédito "29 de Octubre" ha establecido su estructura organizacional enfocándose en generar un marco de gobierno corporativo y un esquema de segregación de funciones que aporte al cumplimiento de los objetivos, es así que se han definido áreas estratégicas, operativas y de apoyo las cuales trabajan en conjunto para brindar un servicio de calidad al cliente final.

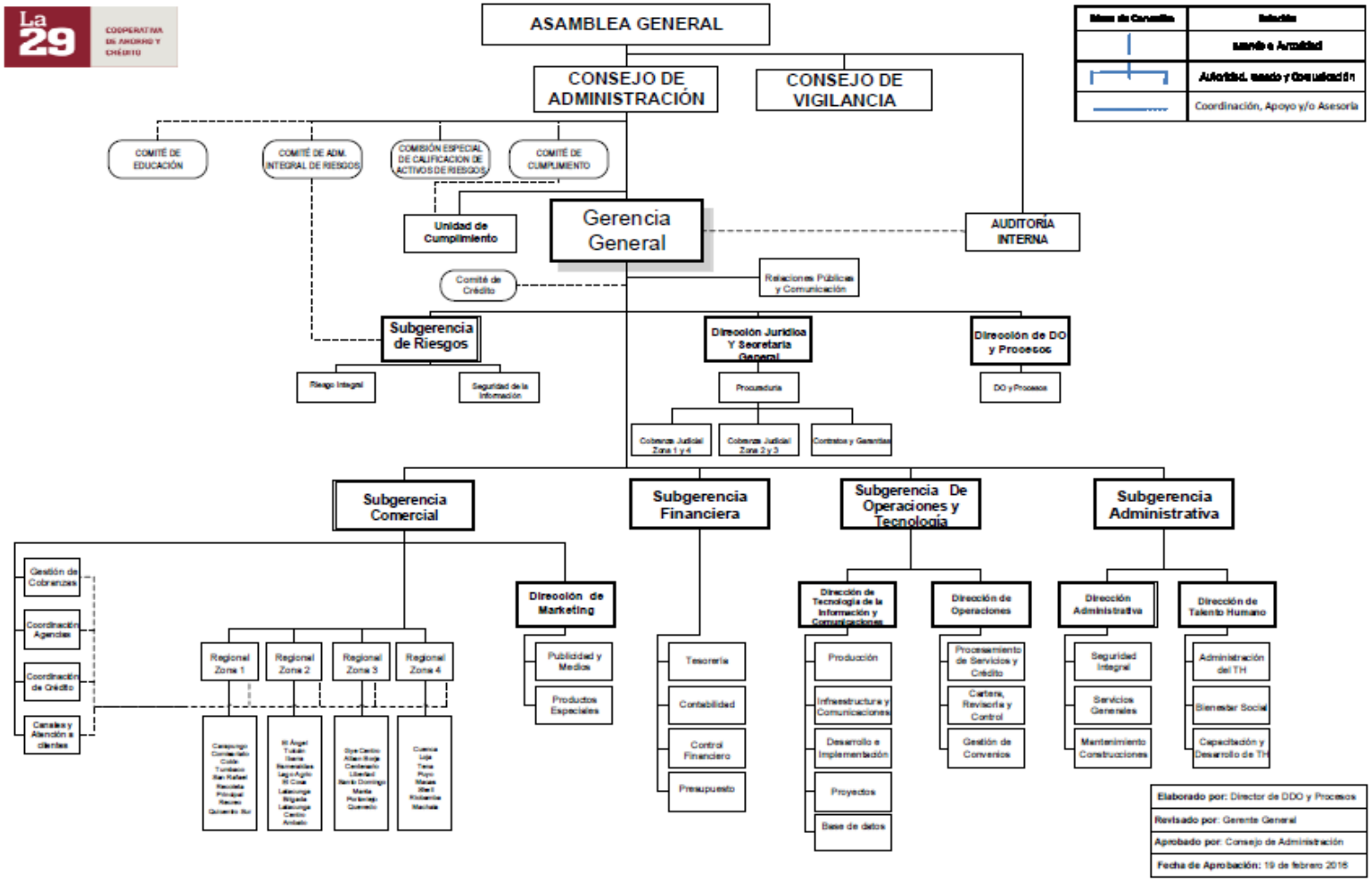


Figura 1 **Organigrama Estructural de la COAC "29 de Octubre"**
Fuente: (Cooperativa de Ahorro y Crédito 29 de Octubre, 2016)

1.2.4. Ubicación del departamento de TI dentro de la Estructura organizacional de la Empresa

El departamento de Tecnología de la Cooperativa 29 de Octubre tiene como principal objetivo el de proveer a las áreas estratégicas y operativas de soluciones informáticas capaces de satisfacer sus necesidades de automatización de una forma eficaz y eficiente.

Esto se ve reflejado tanto en el organigrama institucional como en el organigrama del área de tecnología, los cuales se encuentran publicados en la intranet de la institución y son de conocimiento general de todos los empleados.

Organigrama institucional

El área de Tecnología a través de la Subgerencia de Tecnología de Operaciones y Tecnología ocupada por Marco Antonio Sánchez mantiene una línea directa de reportaje con la Gerencia General lo cual asegura una adecuada comunicación de objetivos, metas, responsabilidades y también sirve como un canal de retroalimentación continuo sobre el desempeño general del área.

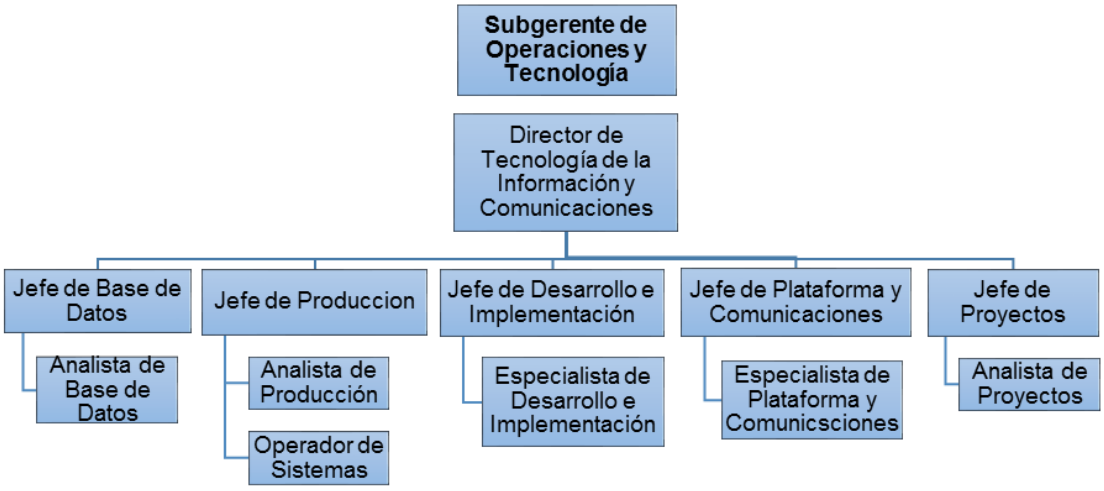


Figura 2: Organigrama del Área de TI

Fuente: (Cooperativa de Ahorro y Crédito 29 de Octubre, 2016)

El organigrama del área de Ti refleja una organización de sub áreas que favorecen a una adecuada segregación de funciones para cada uno de los procesos fundamentales como son gestión de acceso a los recursos informáticos, gestión de cambios y gestión de incidentes.

En caso de existir algún inconveniente o novedad que amerite la intervención de la Dirección de Tecnología se seguirá el flujo establecido siendo el personal operativo quien comunique a las jefaturas respectivas, mismos que a su vez se encargaran de solucionar o escalar hasta la dirección del área.

1.2.5. Inventario de Recursos Administrados por la Dirección de Tecnología y Comunicaciones

El departamento de Tecnología tiene a su cargo la administración, mantenimiento y soporte de equipos computacionales y aplicativos que automatizan los principales procesos de negocio, dicha división ha sido creada tomando en consideración la existencia de una segregación de ambientes fácilmente evidenciable en los equipos que soportan su sistema de Core FITBANK para los cuales se han establecido equipos para entornos de desarrollo pruebas y producción, en el caso del entorno productivo se evidencia tres servidores implementados en un esquema de clúster en donde dos de ellos fungen como servidores de aplicación JBOSS y el tercero corresponde a la herramienta Piranha de Linux, esto a fin de aumentar el nivel de capacidad de los equipos y como consecuencia aportar a la disponibilidad del sistema de Core.

En el caso de la base de datos el sistema FITBANK se ve soportado por una base de datos Oracle 11g montada sobre entornos AIX, la cual adicionalmente mantienen conexión directa con un storage para el almacenamiento de backups y archivelogs los cuales son extraídos a través de crones y comandos RMAN de forma periódica (incrementales) y bajo una calendarización previamente establecida.

1.2.5.1. Inventario de servidores

Tabla 1
Inventario de servidores

Nombre Servidor	Función Servidor	Características	Proveedor (Soporte)	Ubic.
Active Directory	Control De Usuario	Windows Server 2008 / 4gb Ram / 70gb Disco	Coop 29 De Octubre	Data Center
Encriptor	Generador Contraseñas Tarjetas De Debito	N/A	Prosuply	Data Center
Central Ip	Voz Ip	Centos / 8gb Ram / 1tb Disco	Sidevox	Data Center
Central Ip Callcenter	Voz Ip	Centos / 8gb Ram / 1tb Disco	Sidevox	Data Center
Datafast	Switch Para Tarjetas De Debito	Windows Server 2003	Prosuply	Data Center
Balanceador	Balanceador De Aplicativos Web	Centos 6.3 / 4gb Ram / 500gb Disco	Point Technical	Data Center
Core App1	Core Bancario	Centos 6.3 / 64gb Ram / 1tb Disco	Point Technical	Data Center
Core App2	Core Bancario	Centos 6.3 / 64gb Ram / 1tb Disco	Point Technical	Data Center
Blade	Blade Con 18 Máquinas Virtuales	Esxi 5.5 / 32gb Ram / 3tb Disco	Point Technical	Data Center
Blade	Blade Con 13 Máquinas Virtuales	Esxi 5.5 / 32gb Ram / 4tb Disco	Point Technical	Data Center
Blade	Blade Con 17 Máquinas Virtuales	Esxi 5.5 / 16gb Ram / 3tb Disco	Point Technical	Data Center
Blade	Blade Con 13 Máquinas Virtuales	Esxi 5.5 / 40gb Ram / 3tb Disco	Point Technical	Data Center
Blade	Blade Con 1 Máquinas Virtuales	Esxi 5.5 / 16gb Ram / 500 Disco	Point Technical	Data Center

1.2.5.2. Servidores de Base de Datos

El detalle específico de los servidores y sus características es el siguiente

Tabla 2
Base de Datos Principal

ELEMENTO	DESCRIPCIÓN
SERVIDOR IBM	- Equipo de Arquitectura RISC 64 bits - 4 procesadores (cores) POWER7 de 3.0GHz - 32 Gb de memoria RAM, DDR3 1066MHZ. Crece hasta 128Gb. - 2 discos SAS de 3.5“de 146 Gb, de intercambio en caliente, 10K rpm configurados en RAID 1. - 2 interfaces 10/100/1000 Mbps - 2 interfaces FC 4Gbps, en tarjetas PCI independientes - 1 Unidad de cinta DDS-6 DAT 160 de80/160 Gb

Tabla 3
Base de datos de Respaldo

ELEMENTO	DESCRIPCIÓN
SERVIDOR IBM	- Equipo de Arquitectura RISC 64 bits - 4 procesadores (cores) POWER7 de 3.0GHz - 32 Gb de memoria RAM, DDR3 1066 MHZ. Crece hasta 128 Gb. - 2 discos SAS de 3.5“de 146 Gb, de intercambio en caliente, 10K rpm configurados en RAID 1. - 2 interfaces 10/100/1000 Mbps - 2 interfaces FC 4Gbps, en tarjetas PCI independientes - 1 Unidad de cinta DDS-6 DAT 160 de80/160 Gb

1.2.5.3. Infraestructura Virtual

Por otro lado se dispone de infraestructura específica para la implementación de entornos virtuales, en los cuales se ha alojado los aplicativos que automatizan los principales procesos de la compañía, dicha infraestructura se ve soportada por los siguientes equipos:

Tabla 4
Infraestructura Virtual

ELEMENTO	DESCRIPCIÓN
CHASIS C3000	Chasis para Blades con 8 bahias
Blades BL460c	4 Blades con 2 cores de 2.3 Ghz
STORAGE	3PAR 7200 con 10 TB en disco

1.2.5.4. Sistemas de Control Ambiental del Centro de Datos

Estos servidores se encuentran ubicados en el data center de la dirección central de la cooperativa mismo que cuenta con varios controles de protección ambiental mismos que se detallan a continuación:

Tabla 5

Sistemas de Control Ambiental del Centro de Datos

Elemento	Descripción
Sistema de Climatización	Aires acondicionados de precisión redundantes tipo down flow que mantiene condiciones ambientales óptimas para el funcionamiento de servidores y equipos de comunicación.
Sistema de detección y Extinción de incendios	Sistema de detección basado en sensores fotoeléctricos de alto rendimiento. Sistema de extinción por inundación total de agente de extinción hfc 125
Sistema de ups	Sistema redundante distribuido con 2 buses de ups independientes que alimentan cada uno a cada rack
Sistema de monitoreo	Sistema sensores integrados para controlarlos siguientes parámetros: • Temperatura • Humedad • Flujo de aire • Movimiento
Switch kvm	Monitor de 15 pulgadas con teclado y mouse para administrar los diferentes servidores.
Racks de servidores y Comunicaciones	Racks cerrados de 19” de 42u de espacio interior.

1.2.5.5. Equipos de comunicación

LA COAC “29 de Octubre” mantiene un esquema de comunicaciones enfocada en proveer de servicio y conexión a cada una de sus agencias alrededor del país, para esto ha contratado a varios proveedores quienes brindan canales de comunicación redundantes y con velocidades aproximadas de transferencia de 2GB dedicados para las comunicaciones entre las agencias y los servidores centrales en Quito.

Los principales proveedores son Te Uno quienes proveen de un enlace dedicado de 521 Kbps hasta 2048 Kbps correspondiente al enlace principal y la empresa Punto Net quien provee de un enlace dedicado de 128Kbps correspondiente al enlace secundario.

Tabla 6
Administración Central

Equipos de comunicación							
N° equipos	Equipo	Marca	Modelo/ Parte	Puertos	Interfaces		
					Tipo	Total	Libres
1	Switch	Cisco	3560 g catalyst	24	10/100/1000mbps	24	18
1	Switch	Cisco	2960 s catalyst	48	10/100/1000mbps	48	32
1	Switch	D-link	Dgs-1224t	24	10/100/1000mbps	24	5
1	Switch	3com	2024 baseline	24	10/100/1000mbps	24	12
1	Switch	Cisco	2960 s catalyst	48	10/100/1000mbps	48	0
1	Switch	Cisco	2960 s catalyst	48	10/100/1000mbps	48	0
1	Switch	D-link	Dgs-1100	16	10/100/1000mbps	16	8
1	Switch	3com	17471	24	10/100/1000mbps	24	19
1	Switch	Cnet	Csh 1600	16	10/100/1000mbps	16	1
1	Switch	3com	16792	16	10/100/1000mbps	16	0
1	Switch	Trendnet	Trendnet	5	10/100/1000mbps	5	3

Tabla 7
Equipos comunicación WAN

Agencia	Enl. Red	Prov. Principal / Alterno	Kbps Princ	Kbps Alt.	Descripción Equipo	Descrip Equipo Conting
Carapungo	Si	Teuno, Puntonet	2048	768	Switch Gateway Ip Router	Router Cisco 1700

.

1.2.5.6. Inventario de aplicativos gestionados por TI

La infraestructura antes expuesta aloja un sin número de aplicativos desarrollados y adquiridos por la Cooperativa para la automatización de sus procesos, los mismos comprenden aplicativos desde el Core bancario hasta las herramientas de correo electrónico.

Tabla 8
Inventario de aplicativos gestionados por TI

Nombre Servidor	Sistema Versión	Sistema Operativo y Versión	Base de Datos	Función del sistema	Proveedor
Base 24	Detec Sol.	Windows 2008 server	SQL SERVER	Transac. de los productos	IDCE Consult
DGRV	SAP	Windows 2008 server	SQL SERVER	Control y seguimiento del plan estratégico	DGRV
Presupuesto	SPF	Windows 2008 server	SQL SERVER	Sistema de planificación Financiera	B-SOFT
Lavado Prod29	Focus Finan.	Windows 2008 server	SQL SERVER	Análisis financiero	CAEFYC
Riesgo Operat.	Risk Manage	Windows 2008 server	SQL SERVER	Sistemas de Riesgos Integrales	B-SOFT
N/A	Focus Risk	Windows Vista	ACCESS	Análisis de riesgo de crédito	CAEFYC

1.2.6. Diagramas de Red COAC “29 DE OCTUBRE”

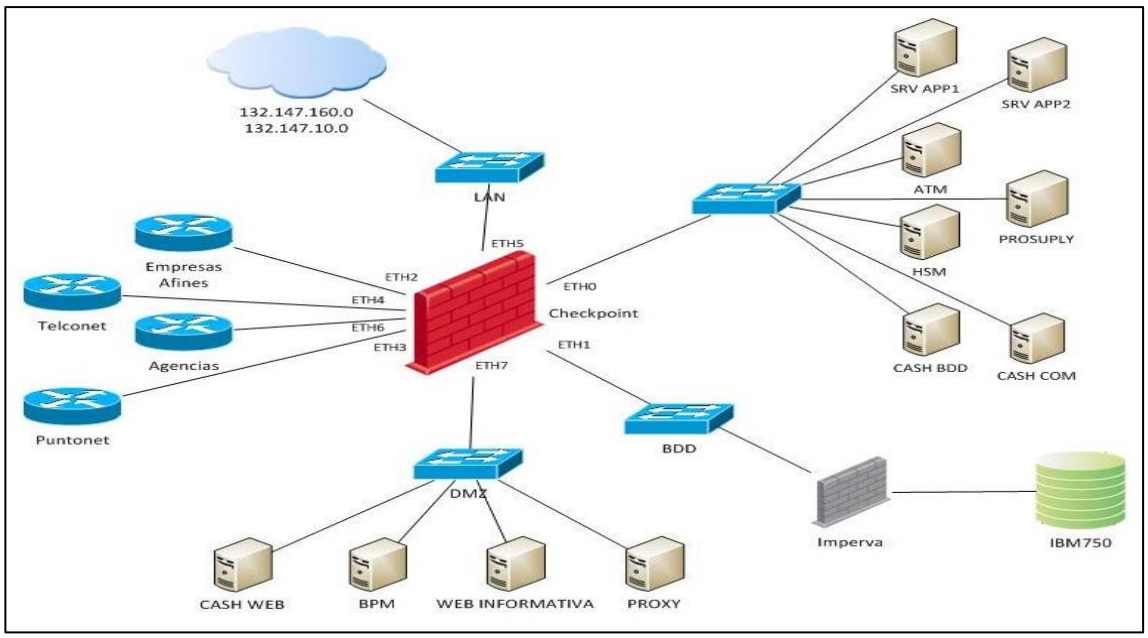


Figura 3 Diagramas de Red COAC “29 DE OCTUBRE”
Fuente: (Cooperativa de Ahorro y Crédito 29 de Octubre, 2016)

1.2.7. Procesos de la Dirección de Informática y Comunicaciones

Considerando la infraestructura necesaria para el soporte de los principales aplicativos y tomando en cuenta la estructura interna y el personal disponible han establecido procesos fundamentales para el área de tecnología misma que se han subdividido en subprocesos y actividades enfocadas en dar un servicio de calidad tanto a sus clientes internos como a sus clientes externos. La agrupación de dichos procesos estaba enfocada en ciertos pilares fundamentales como son: el soporte a usuarios, la administración de infraestructura, la gestión de los servicios de TI, la seguridad en cada una de las capas de los sistemas, el desarrollo de software y la gestión de proyectos obteniendo como resultado los siguientes procesos:

Macro Proceso: GESTIÓN INFORMÁTICA

Procesos:

- Planificación de Gestión de Tecnología dela Información
- Gestión de Plataforma Tecnológica
- Gestión de Producción
- Gestión de Base De Datos
- Gestión de Seguridad y Control dela Información
- Gestión de Desarrollo de Software

Estos procesos en conjunto con la infraestructura tecnológica antes mencionada sirven para proveer de servicios informáticos a las demás áreas de la Cooperativa.

1.3. PLANTEAMIENTO DEL PROBLEMA

Toda empresa u organización sin importar su tamaño o el coste de las medidas de seguridad implantadas, necesita un Plan de continuidad de negocio que contemple las tareas para que la organización continúe con su actividad a pesar de eventos o incidencias que afecten sus operaciones y que tenga como objetivo proteger los servicios críticos y operativos del negocio contra desastres naturales o fallas mayores que provoquen la interrupción de las operaciones de la empresa, disminuyendo el impacto en las pérdidas de tipo financiero, de información crítica del negocio, credibilidad y productividad, debido a que los recursos de la organización no estén disponibles.

La Cooperativa de Ahorro y Crédito 29 de Octubre LTDA. Al ser una entidad financiera está controlada por la Superintendencia de Economía Popular y Solidaria (SEPS) y se rige bajo normativas vigentes de la Superintendencia de Bancos y Seguros (SBS), en las cuales se detallan normativas que se deben cumplir, La Cooperativa no cuenta con un Plan de Continuidad de Negocio

actualizado en el que se detalle el plan y las estrategias previstas para restablecer las funciones críticas de la organización ante situaciones de riesgo que puedan afectar de manera grave los servicios que ofrece la Institución como se detalla en el LIBRO I.- NORMAS GENERALES PARA LAS INSTITUCIONES DEL SISTEMA FINANCIERO, TITULO X.- DE LA GESTION Y ADMINISTRACIÓN DE RIESGOS, CAPITULO V.- DE LA GESTIÓN DE RIESGO OPERATIVO SECCIÓN IV.- CONTINUIDAD DEL NEGOCIO, Articulo 15. Por lo que es necesario el Desarrollo de un plan de Continuidad que contemple mencionada normativa.

Actualmente la Cooperativa de Ahorro y Crédito 29 de Octubre LTDA. Se encuentra en la finalización del proceso de cambio de CORE Bancario por lo que el Plan de Continuidad del Negocio que se encuentra implementado en la Cooperativa esta desactualizado y por lo tanto obsoleto. En tal sentido es necesaria la implementación de un nuevo Plan de continuidad de negocio acorde al nuevo CORE Bancario y a las especificaciones de las entidades de control ya que tarde o temprano la institución se encontrará con una incidencia de seguridad o desastre que afecte los servicios que ofrece.

1.4. JUSTIFICACIÓN

Las empresas u organizaciones están continuamente experimentando situaciones de emergencia o catástrofes que ponen en peligro las operaciones o servicios que brinda la empresa, por lo que un Plan de Continuidad del Negocio (BCP) describe como reiniciar las operaciones críticas de la organización después de una interrupción.

El Plan de Continuidad de negocio se enfoca en recuperar los sistemas, operaciones y servicios críticos después de una interrupción estrepitosa en la organización, por lo que es fundamental que cada Organización o Institución sea Privada como Pública cuente con un Plan actualizado donde se detallen las

estrategias de reanudación del negocio y permita proteger los procesos críticos y operativos del negocio por la interrupción abrupta, disminuyendo el impacto en pérdidas de tipo financiero, de información crítica del negocio, credibilidad y productividad.

La Cooperativa de Ahorro y Crédito 29 de Octubre LTDA. Al ser una institución financiera está controlada por la Superintendencia de Economía Popular y Solidaria(SEPS) además tiene vigentes normativas de la Superintendencia de Bancos y Seguros (SBS) en las que se especifica que las instituciones controladas deben administrar la Continuidad del negocio, manteniendo procedimientos actualizados, a fin de garantizar su capacidad para operar de manera continua y minimizar las perdidas en caso de una interrupción del negocio, para el efecto las instituciones del sistema Financiero deben establecer un proceso de administración de la Continuidad del negocio, tomando como referencia el estándar ISO 22301.

Actualmente la Cooperativa de Ahorro y Crédito 29 de Octubre LTDA. Cuenta con un Plan de Continuidad del Negocio desactualizado que se encuentra caduco y obsoleto, el cual no cumple con las Normativas de las entidades de control vigentes, por lo que surge la necesidad del Desarrollo de un Plan de Continuidad del Negocio que cumpla con las normativas vigentes para instituciones del sistema financiero que se encuentre alineado a ISO 22301.

1.5. ALCANCE

El Plan de Continuidad del Negocio (BCP) será desarrollado en base a la referencia del estándar ISO 22301 y cumpliendo con las normativas vigentes de las diferentes entidades de control para instituciones financieras considerando lo siguiente:

- La definición de objetivos, estrategias, procedimientos, metodología y planes para la administración de la continuidad de negocio en la Dirección de Tecnología y Comunicaciones de la Cooperativa de Ahorro y Crédito “29 de Octubre” LTDA.
- Procedimientos operativos, tecnológicos, de emergencias y comunicaciones para cada servicio crítico de la Dirección de Tecnología y Comunicaciones de la Administración Central de la Cooperativa de Ahorro y Crédito “29 de Octubre” LTDA.
- Análisis de impacto que tendría una interrupción de los procesos que soportan los principales productos y servicios que ofrece la Dirección de Tecnología y Comunicaciones de la Administración Central de la Cooperativa de Ahorro y Crédito “29 de Octubre” LTDA., determinando el impacto en términos de magnitud de daños, el período de recuperación y tiempos máximos de interrupción que puedan ocasionar los siniestros.
- Análisis que identifique los principales escenarios de riesgos para la Dirección de Tecnología y Comunicaciones de la Administración Central de la Cooperativa de Ahorro y Crédito “29 de Octubre” LTDA., incluyendo las fallas en la tecnología de la información, tomando en cuenta el impacto y la probabilidad de que sucedan.
- Estructuración de planes y definición de estrategias para los servicios críticos que permitan mantener la continuidad de los procesos que soportan los principales productos y servicios que ofrece la Dirección de Tecnología y Comunicaciones de la Administración Central de la Cooperativa de Ahorro y Crédito “29 de Octubre” LTDA., dentro del tiempo objetivo de recuperación definido para cada servicio, mismos que deben tomar en cuenta, al menos lo siguiente: la seguridad de personal, habilidades y conocimientos asociados al servicio, instalaciones alternas de trabajo, infraestructura alterna de procesamiento e información que soporte el proceso, seguridad de la información y equipamiento necesario para el proceso.

CAPÍTULO II
MARCO TEÓRICO

2.1. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

El concepto de recuperación de desastres surgió en la década de los 70 como una respuesta al incremento en la automatización de las empresas y a la conciencia que se generó en los administradores de tecnología al entender la dependencia que tenían las organizaciones sobre los sistemas que ellos administraban, es así que se colaron ciertas ideas en torno a cómo incrementar la disponibilidad de esos sistemas surgiendo alternativas como enlaces redundantes, sistemas de control ambiental de centros de datos, generación de sites alternos y otros que ayudarían a los administradores a mantener sus sistemas en línea.

En un inicio los sistemas estaban basados en el procesamiento por lotes en grandes mainframes por lo que la empresa no sufría pérdidas significativas en caso de que los sistemas se paren por uno o dos días, sin embargo una vez que los sistemas empezaron ejecutar procesamientos, interacciones con bases de datos y comunicaciones con otros usuarios en tiempo real el problema se magnifico siendo cada vez más necesario el disponer de un hotspot donde se puedan levantar servidores alternos que soporten la transaccionalidad de los sistemas de Core de la empresa, esta oportunidad fue aprovechada por algunas empresas las cuales se dedicaban a proveer de servicios de alojamiento de servidores y arrendamiento de equipos que estuvieran a la par de los servidores de la organización.

Esta alternativa represento un gran avance en términos de continuidad para los administradores ya que a un costo razonable podían reducir las pérdidas económicas y de información cuando un incidente se presente.

1.1.1. Continuidad del Negocio

La continuidad del negocio se ve traducida en la capacidad que tenga la empresa de mantener su negocio en operación y continuar ofreciendo sus servicios ante una situación adversa o un incidente imprevisto. Por lo tanto podríamos definirla de la siguiente manera.

"La continuidad del servicio involucra capacidades tácticas y estratégicas pre aprobadas por la dirección de una entidad para responder a incidentes e interrupciones del servicio con el fin de poder continuar con sus operaciones a un nivel aceptable previamente definido." (Ferrer, 2015)

Un adecuado sistema de gestión de la continuidad del negocio debe poseer ciertos productos o elementos para asegurar el cumplimiento de su objetivo, estos son:

- Business Impact Analysis (Análisis de Impacto del Negocio).
- Risk Assesment (Evaluación o Valoración de Riesgos).
- Estrategias de Continuidad.
- Estructura Organizacional para la Continuidad (Roles, responsabilidades y procedimientos).
- Procesos de Continuidad.
- Plan de Pruebas del Plan de Continuidad.

2.2. PLAN DE CONTINUIDAD DEL NEGOCIO

2.2.1. Definición de plan de continuidad del NEGOCIO

El plan de continuidad de negocios es un conjunto de procedimientos documentados e información que ha sido desarrollada, recopilada y mantenida a

disposición para su uso durante un incidente, para permitir a la organización continuar con la entrega de sus servicios más importantes y urgentes a un nivel aceptable previamente acordado. El plan de continuidad de negocios se actualiza y mantiene a través del proceso de Gestión de Continuidad de Negocio que se definió anteriormente. Este reducirá el número y la magnitud de las decisiones que se toman durante un período en que los errores pueden resultar mayores. El Plan establecerá, organizará y documentará los riesgos, responsabilidades, políticas y procedimientos, acuerdos con entidades internas y externas.

Un claro ejemplo de la ausencia de un plan de continuidad de negocios es cuando se malogra el disco duro de una computadora, en realidad no cuesta nada repararlo, pero el daño y el impacto que puede causar es inmensurable si es que no hay ningún plan de mitigación ante su pérdida

Como menciona Hotchkiss (2010) *"Un Evento de pequeño impacto también puede causar daño en términos de tiempo de reparación"*, como en el ejemplo antes mencionado, una pequeña deficiencia puede causar un impacto bastante limitado en negocio, pero puede llegar a costar una gran cantidad de dinero el repararlo debido a la falta de planificación. Esto significa que se debe tener en cuenta el impacto y el daño, así como el costo de recuperación y así poder obtener una idea razonable del costo de no tener un plan de continuidad.

2.2.2. OBJETIVOS GENERAL Y ESPECÍFICOS DEL BCP

2.2.2.1. Objetivo General

Definir las acciones, procedimientos y recurso humano para garantizar la rápida y oportuna recuperación y puesta en funcionamiento de los sistemas y servicios informáticos que apoyan el cumplimiento de los procesos críticos del negocio, ante eventos que podrían alterar el normal funcionamiento de la Tecnología de la Información y Comunicaciones.

2.2.2.2. Objetivos Específicos

- Identificar y analizar posibles riesgos que pueden afectar a continuidad de las operaciones de los procesos informáticos de la institución.
- Contar con documentación detallada y clara, de procesos y procedimientos para atender cualquier evento que afecte la disponibilidad de los sistemas informáticos y de comunicaciones que apoyan a los procesos críticos del negocio.
- Asignar responsabilidades al personal en cada uno de los procedimientos necesarios para ejecutar el plan de continuidad, garantizando la restauración de las operaciones de los servicios Informáticos en el tiempo requerido.

2.3. ESTANDAR ISO 22301:2012

El nombre completo de esta norma es ISO 22301:2012 Seguridad de la sociedad – Sistemas de gestión de la continuidad del negocio – Requisitos. Esta norma ha sido creada por especialistas en el tema y funge como marco de referencia para gestionar la continuidad del negocio en una organización.

Por lo tanto se enfoca en la especificación de los requisitos para elaborar un sistema de gestión que se encargue de proteger a la organización y su negocio de incidentes que provoquen la interrupción o cese de sus actividades, poniendo énfasis en reducir la probabilidad de ocurrencia de dichos incidentes y asegurar una rápida y oportuna recuperación en caso de que sucedan.

Esta norma obedece a un proceso de optimización y regularización de los estándares y buenas prácticas en torno al aseguramiento de la continuidad del negocio, tratando de alinearse con las demás normas que aportan tanto a la

seguridad de los sistemas como al gobierno y gestión de las mismas, esta evolución obedece al siguiente esquema:

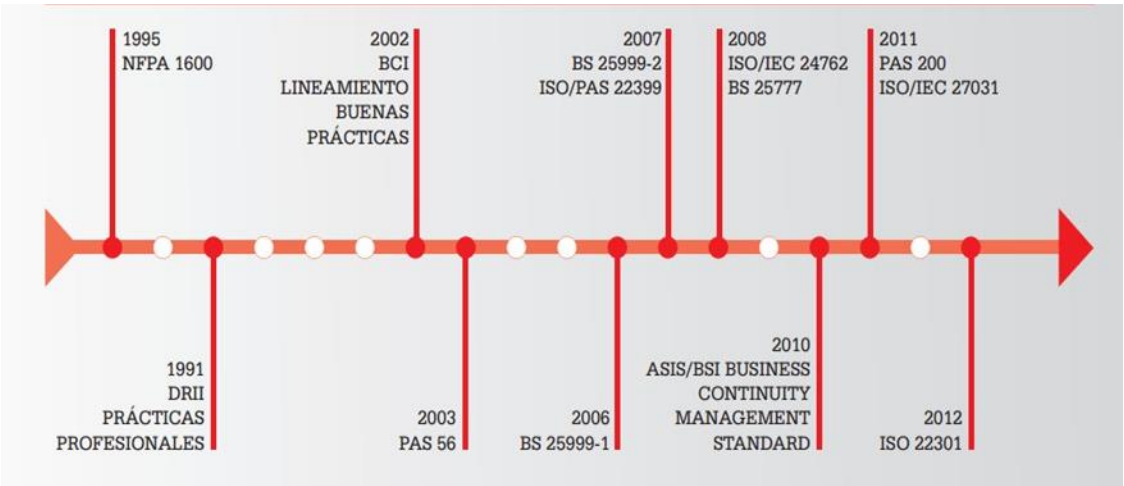


Figura 4 Evolución de los Estándares en Continuidad del Negocio

Fuente: (Alexander, 2013)

El estándar ISO 22301:2012 “Seguridad de la Sociedad: Sistemas de Continuidad del Negocio-Requisitos” aplica el ciclo PDCA - Plan-Do-Check-Act para la planificación, establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y la mejora continua de su efectividad.

El modelo ha sido creado con consistencia con otros estándares de gestión, tales como: ISO 9001:2008, ISO 27001:2005, ISO 20000-1:2011, ISO 14001:2004 y con el ISO 28000:2007.

Esta norma ha sido creada de tal forma que establece que el sistema de Gestión de la Continuidad del Negocio tome insumos de las partes interesadas y los requerimientos para la gestión de la continuidad para transformarlos a través de procesos y actividades en resultados de continuidad capaces de cumplir con los parámetros establecidos por el negocio.

El proceso es claramente descrito en la siguiente figura.

Figura 5 Ciclo PDCA aplicado al Proceso de Continuidad del Negocio

Fuente: (Alexander, 2013)

Como producto de este proceso la norma establece la entrega de una serie de documentos obligatorios los cuales deben estar formalizados y deben ser de conocimiento de las partes interesadas.

Documentación requerida por la ISO 22301:2012 (International Standard organization, 2012):

- Lista de requisitos legales, normativos y de otra índole.
- Alcance del SGCN.
- Política de la continuidad del negocio.
- Objetivos de la continuidad del negocio.
- Evidencia de competencias del personal.
- Registros de comunicación con las partes interesadas.
- Análisis del impacto en el negocio.
- Evaluación de riesgos, incluido un perfil del riesgo.
- Estructura de respuesta a incidentes.
- Planes de continuidad del negocio.

- Procedimientos de recuperación.
- Resultados de acciones preventivas.
- Resultados de supervisión y medición.
- Resultados de la auditoría interna.
- Resultados de la revisión por parte de la dirección.
- Resultados de acciones correctivas.

Para el presente trabajo se generaran aquellos documentos que se enmarquen dentro del alcance del proyecto.

2.4. METODOLOGÍAS

Para los propósitos de este proyecto y en pro de cumplir con los estándares propuestos por la institución se utilizó la metodología de evaluación de riesgo operativo de la COAC 29 de Octubre misma que esta basa en el método de MOSLER el cual tiene como núcleo la identificación, análisis y evaluación de los factores de riesgo asociados a los procesos de la compañía, para el caso específico de este trabajo se realizara en base a procesos dela Dirección de Informática y Comunicaciones de la Administración Central de la COAC “29 de Octubre”

2.4.1. Metodología de Evaluación de Riesgo Operativo COAC “29 de Octubre”

La metodología de evaluación de riesgos de la COAC “29 de Octubre” se divide en dos sub metodologías basadas en el tipo de evaluación de riesgo que se quiera realizar ya sea esta cuantitativa o cualitativa, para el caso específico de este proyecto se tomara como referencia la metodología cualitativa de administración de riesgo.

2.4.1.1. Metodología Cualitativa de Administración de Riesgo Operativo

Esta metodología cumple con un proceso ordenado de fases, mismas que se generan en secuencia y cada fase previa sirve de insumo para la fase subsecuente. El flujo es el siguiente:

Figura 6 Metodología Cualitativa de Administración de Riesgo Operativo

Fuente: (Cooperativa de Ahorro y Crédito 29 de Octubre, 2015)

Fase 1: Identificación de Riesgos

La identificación de riesgos es realizada por los analistas de la Dirección de Riesgos en coordinación con los dueños y/o responsables de cada proceso.

La asignación de los “Dueños del Proceso” es realizada en base a su nivel jerárquico dentro de la estructura del área y así como de su conocimiento del proceso como tal, n tal sentido el dueño del proceso será el responsable por la administración del proceso completo así como también de la identificación de subprocesos y la asignación del personal adecuado para su correcta ejecución e identificación de riesgos asociados.

Esta actividad consiste en reconocer e identificar las fallas o insuficiencias que puedan generar pérdidas monetarias, de información, reputacional /

imagen, por mala calidad/oportunidad o tiempo; o en su defecto afectar los objetivos estratégicos y la continuidad del negocio.

La identificación de riesgos se puede realizar utilizando las siguientes herramientas.

- Talleres de trabajo y entrevistas in situ.- Actividades que se realiza con los dueños y/o responsables de cada proceso, la prioridad es para los procesos críticos.
- Organigramas funcionales.- Que permiten entender la naturaleza y el campo de acción de las operaciones de la cooperativa y a su vez evitar que una misma persona, unidad o área realice funciones que no respetan la adecuada segregación de labores evitando el conflicto de intereses que puedan generar eventos de riesgo operativo.
- Diagramas de flujo.- Que permiten identificar y familiarizarnos con los diferentes subprocesos que se realiza en el giro del negocio para una acertada identificación de los eventos en base a las actividades que se realiza en la institución.
- Base de datos.- Base de datos sobre eventos individuales con pérdidas en el pasado para identificar las tendencias y causas principales.
- Árbol de decisión.- Herramienta utilizada para facilitar la identificación de los eventos de riesgo y su tipo a los responsables de cada proceso.
- Informes: Informes de organismos de control interno y externo (Auditoria Interna, Auditoria Externa), entre otros.
- Reclamos de Clientes**:** Información de clientes que han presentado reclamos a la Cooperativa.

Una vez levantada la información con las herramientas antes descritas se deben registrar los eventos de riesgo por cada subproceso y clasificarlos de acuerdo a su línea de negocio, factor y tipo de evento.

En la identificación de eventos de riesgo se debe establecer dos tipos: reales y potenciales.

- *Evento Real***:** Su identificación permite a la cooperativa establecer el perfil de riesgo, así como realizar el respectivo tratamiento de acuerdo al nivel de riesgo del evento y finalmente conformar una base de datos de calidad para el desarrollo de los modelos cuantitativos.
- *Evento Potencial***:** El objetivo de la identificación es enfocarse a prevenir la materialización de los eventos.

Fase II: Medición

La valoración de cada uno de los eventos de riesgo, se realiza considerando los pesos definidos en la escala de probabilidad de ocurrencia y de impacto, esta valoración es de carácter subjetivo, para el presente caso las escalas referenciales serán:

MAPA DE CALOR

Es una herramienta gerencial que brinda criterios de decisión a la alta dirección frente a los cambios que deben ser realizados en la institución para controlar los riesgos existentes.

El resultado de la valoración de los eventos de riesgos nos da una probabilidad e impacto que se visualiza gráficamente en este mapa por colores indicando la severidad de cada uno de los eventos de riesgos.

Mapa de Calor de acuerdo a los límites de exposición en USD, está en función del margen operativo promedio de la cooperativa con un porcentaje de perdida que está dispuesto a asumir la Cooperativa, estos valores podrán ser ajustados de acuerdo la necesidad institucional.

				CATEGORIAS DE PROBABILIDAD DE OCURRENCIA				
				Muy Bajo	Bajo	Medio	Alto	Muy Alto
			Frecuencia	0,2	0,5	1	2	12
			Probabilidad en dias	0,0005	0,0014	0,0027	0,0055	0,0329
				1	2	3	4	5
CATEGORIAS DE IMPACTO	Muy Alto	$ 6.600	5	$ 1.320	$ 3.300	$ 6.600	$ 13.200	$ 79.200
	Alto	$ 5.280	4	$ 1.056	$ 2.640	$ 5.280	$ 10.560	$ 63.360
	Medio	$ 3.960	3	$ 792	$ 1.980	$ 3.960	$ 7.920	$ 47.520
	Bajo	$ 2.640	2	$ 528	$ 1.320	$ 2.640	$ 5.280	$ 31.680
	Muy Bajo	$ 1.320	1	$ 264	$ 660	$ 1.320	$ 2.640	$ 15.840

Figura 7 Mapa de Calor
Fuente: (Cooperativa de Ahorro y Crédito 29 de Octubre, 2015)

Severidad del Riesgo

CATEGORIA	VALOR	DESCRIPCIÓN
Muy Alto	5	Riesgo cuya probabilidad de ocurrencia es muy alta, es decir, se tiene un alto grado de seguridad de que este se presente. Una vez al mes (12 veces)
Alto	4	Riesgo cuya probabilidad de ocurrencia es alta, es decir, al menos una vez cada 6 meses (2 veces)
Medio	3	Riesgo cuya probabilidad de ocurrencia es media, es decir, al menos una vez al año (1 vez)
Bajo	2	Riesgo cuya probabilidad de ocurrencia es baja, es decir, al menos una vez cada 2 años (0.5 veces)
Muy Bajo	1	Riesgo cuya probabilidad de ocurrencia es muy baja, es decir, al menos una vez cada 5 años (0.20 veces)

Figura 8 Categorías de Probabilidad de Ocurrencia
Fuente: (Cooperativa de Ahorro y Crédito 29 de Octubre, 2015)

CATEGORIA	VAL.	DESCRIPCIÓN
Muy Alto	5	Riesgo cuya materialización influye gravemente en el desarrollo del proceso y el cumplimiento de sus objetivos, impidiendo finalmente que éste se desarrolle
Alto	4	Riesgo cuya materialización dañaría significativamente el desarrollo del proceso y el cumplimiento de sus objetivos, impidiendo finalmente que éste se desarrolle de forma normal
Medio	3	Riesgo cuya materialización causaría un deterioro en el desarrollo del proceso, dificultando o retrasando el cumplimiento de sus objetivos, impidiendo que este se desarrolle de forma adecuada
Bajo	2	Riesgo que causa un daño menor en el desarrollo del proceso y que no afecta mayormente el cumplimiento de sus objetivos estratégicos
Muy Bajo	1	Riesgo que puede tener un pequeño o nulo efecto en el desarrollo del proceso y que no afecta al cumplimiento de sus objetivos estratégicos

Figura 9 Categorías de Impacto
Fuente: (Cooperativa de Ahorro y Crédito 29 de Octubre, 2015)

NIVEL DE SEVERIDAD DEL RIESGO	
Muy bajo	ACEPTABLE
Bajo	
Medio	
Alto	INACEPTABLE
Muy alto	

Figura 10 Nivel de Riesgo Aceptable
Fuente: (Cooperativa de Ahorro y Crédito 29 de Octubre, 2015)

NIVEL DE PROBABILIDAD	(P)	IMPACTO	(I)	SEVERIDAD DEL RIESGO	(P x I)
Muy Alto	5	Muy Alto	5	Muy Alto	25
Muy Alto	5	Alto	4	Muy Alto	20
Muy Alto	5	Medio	3	Muy Alto	15
Muy Alto	5	Bajo	2	ALTO	10
Muy Alto	5	Muy bajo	1	ALTO	5
Alto	4	Muy Alto	5	Muy Alto	20
Alto	4	Alto	4	Muy Alto	16
Alto	4	Medio	3	ALTO	12
Alto	4	Bajo	2	ALTO	8
Alto	4	Muy bajo	1	Medio	4
Medio	3	Muy Alto	5	Muy Alto	15
Medio	3	Alto	4	Muy Alto	12
Medio	3	Medio	3	ALTO	9
Medio	3	Bajo	2	Medio	6
Medio	3	Muy bajo	1	BAJO	3
Bajo	2	Muy Alto	5	Muy Alto	10
Bajo	2	Alto	4	ALTO	8
Bajo	2	Medio	3	Medio	6
Bajo	2	Bajo	2	Bajo	4
Bajo	2	Muy bajo	1	Bajo	2
Muy Bajo	1	Muy Alto	5	ALTO	5
Muy Bajo	1	Alto	4	ALTO	4
Muy Bajo	1	Medio	3	Medio	3
Muy Bajo	1	Bajo	2	Bajo	2
Muy Bajo	1	Muy bajo	1	Muy bajo	1

Figura 11 Nivel de Severidad del Riesgo
Fuente: (Cooperativa de Ahorro y Crédito 29 de Octubre, 2015)

Fase III: CALCULO DE CONTROLES

Realizada la identificación de los riesgos operativos en el proceso, deben identificarse los controles existentes, cuyo propósito es minimizar la materialización de esos riesgos en el proceso. También es posible que producto de este análisis se determine inexistencia de controles asociados a los riesgos.

Tabla 9
Oportunidad de la acción del control

CLASIF.	SIGLA	DESCRIPCIÓN
Preventivo	PV	Controles de alto nivel orientados a prevenir la causa del riesgo en una etapa muy temprana.
Correctivo	CV	Controles claves que actúan durante el proceso y que permiten corregir las deficiencias
Detectivo	DT	Controles claves que sólo actúan una vez que el proceso ha terminado

Fuente: Cooperativa de Ahorro y Crédito 29 de Octubre, 2015

Tabla 10
Periodicidad en la acción del control

CLASIF.	SIGLA	DESCRIPCIÓN
Permanente	PE	Controles claves aplicados durante todo el proceso, es decir en cada operación
Periódico	PD	Controles claves aplicados en forma constante solo cuando ha transcurrido un período específico de tiempo
Ocasional	OC	Controles claves que se aplican solo en forma ocasional en un proceso

Fuente: Cooperativa de Ahorro y Crédito 29 de Octubre, 2015

Tabla 11
Automatización en la aplicación del control

CLASIF.	SIGLA	DESCRIPCIÓN
100% Automatizada	AT	Controles claves incorporados en el proceso, cuya aplicación es completamente informatizada. Están incorporados en los sistemas informatizados.
Semi-Automatizada	SA	Controles claves incorporados en el proceso, cuya aplicación es parcialmente desarrollada mediante sistemas informatizados
Manual	MA	Controles claves incorporados en el proceso, cuya aplicación no considera uso de sistemas informatizados

Fuente: Cooperativa de Ahorro y Crédito 29 de Octubre, 2015

La valoración de la efectividad del control esta dictada en base al conjunto de características antes expuestas y obedece al siguiente cuadro:

Tabla 12
Escala de Eficiencia de Controles

Eficiencia de control			Efectividad de Control	Valor Diseño del Control
Periodicidad	Oportunidad	Automatización		
Permanente	Preventivo	Automatizado	Optimo	5
Permanente	Preventivo	Semi Automatizado		
Permanente	Preventivo	Manual		
Permanente	Correctivo	Automatizado		
Permanente	Correctivo	Semi Automatizado		
Permanente	Correctivo	Manual		
Permanente	Detectivo	Automatizado	Bueno	4
Permanente	Detectivo	Semi Automatizado		
Permanente	Detectivo	Manual		
Periódico	Preventivo	Automatizado		
Periódico	Preventivo	Semi Automatizado		
Periódico	Preventivo	Manual		
Periódico	Correctivo	Automatizado	Más que regular	3
Periódico	Correctivo	Semi Automatizado		
Periódico	Correctivo	Manual		
Periódico	Detectivo	Automatizado		

Continua

Periódico	Detectivo	Semi Automatizado		
Periódico	Detectivo	Manual		
Ocasional	Preventivo	Automatizado	Regular	2
Ocasional	Preventivo	Semi Automatizado		
Ocasional	Preventivo	Manual		
Ocasional	Correctivo	Automatizado		
Ocasional	Correctivo	Semi Automatizado		
Ocasional	Correctivo	Manual		
Ocasional	Detectivo	Automatizado	Deficiente	1
Ocasional	Detectivo	Semi Automatizado		
Ocasional	Detectivo	Manual		
No determinado	No determinado	No determinado		

Fuente: Cooperativa de Ahorro y Crédito 29 de Octubre, 2015

2.4.2. Metodología para cálculo de Riesgo Residual COAC "29 OCTUBRE"

La presente metodología permite calcular el riesgo residual una vez que se implemente los controles respetivos y/o mediante el avance de los planes acción para mitigar el riesgo.

Mitigando el riesgo con controles

Un riesgo se puede mitigar a través de controles, que debe traducirse en una disminución de la posibilidad de ocurrencia y/o del impacto del riesgo; por es importante asegurar que los controles sean comprensivos de todos los riesgos y que los mismos estén funcionando en forma oportuna, efectiva y eficiente. (Cooperativa de Ahorro y Crédito 29 de Octubre, 2015)

Los controles se clasifican de la siguiente forma:

- Preventivo
- Detectivo
- Correctivo

La combinación de los controles, según su clasificación, tipo de automatización y frecuencia permite determinar el **nivel de eficacia** (*Matriz de eficacia basado en controles*).

Tabla 13
Matriz de eficacia basada en controles

EFICACIA	
CONTROLES APLICADOS	NIVEL EFICACIA
Preventivos, Detectivos, Correctivos	Muy Alta (5)
Preventivos y Detectivos	Alta (4)
Preventivos y Correctivos	Media (3)
Detectivos y Correctivos	Baja (2)
Un solo tipo de control	Muy Baja (1)

Fuente: Cooperativa de Ahorro y Crédito 29 de Octubre, 2015

Otro elemento que considera la metodología es el **nivel de eficiencia**, basado el costo de implementar los controles y los beneficios que se obtiene (*Matriz de eficiencia basado en controles*).

Tabla 14
Escala de mitigación de Controles

EFICIENCIA				
	Costo			
Beneficio		Alto	Medio	Bajo
	Alto	3	4	5
	Medio	2	3	4
	Bajo	1	2	3

Fuente: Cooperativa de Ahorro y Crédito 29 de Octubre, 2015

Matriz de porcentaje de mitigación

La siguiente matriz expone los cortes de porcentaje de mitigación para calcular el residual, considerando el valor de la efectividad y el valor inherente (probabilidad de ocurrencia o impacto).

Efectividad	Inherente	% mitigación		Residual
5	5	100	80	1
		70	60	2
		50	40	3
		30	20	4
	4	100	60	1
		50	40	2
		30	20	3
	3	100	40	1
		30	20	2
		10	10	3
	2	100	20	1
4	5	100	80	1
		70	60	2
		50	40	3
		30	20	4
	4	100	70	1
		60	40	2
		30	20	3
	3	100	40	1
		30	20	2
	2	100	20	1

Efectividad	Inherente	% mitigación		Residual
3	5	100	90	2
		80	60	3
		50	20	4
	4	100	90	1
		80	60	2
		50	20	3
	3	100	60	1
		50	20	2
	2	100	20	1
2	5	100	80	3
		70	30	4
	4	100	80	2
		70	30	3
	3	100	80	1
		70	30	2
	2	100	30	1
1	5	100	60	4
	4	100	60	3
	3	100	60	2
	2	100	60	1

Figura 12 Matriz de porcentaje de mitigación
Fuente: Cooperativa de Ahorro y Crédito 29 de Octubre, 2015

2.4.3. Metodología Análisis de Impacto del Servicio – BIA COAC "29 OCTUBRE"

El análisis de impacto al negocio (Business Impact Analysis o BIA) es un elemento utilizado para estimar la afectación que podría padecer una organización como resultado de la ocurrencia de algún incidente o un desastre.

A diferencia de una evaluación de riesgos, que se enfoca en cómo podría verse afectada una organización a través de la identificación, análisis y valoración de amenazas de seguridad con base en su impacto sobre los activos críticos y la probabilidad de ocurrencia, el BIA es un proceso más especializado en la identificación de los tipos de impacto, orientado en conocer qué podría verse afectado y las consecuencias sobre los procesos de negocio.

También, el BIA puede ser considerado como una fase a ejecutar durante el desarrollo de un Plan de Recuperación ante Desastres (DRP), y por lo tanto de un Plan de Continuidad del Negocio (BCP), debido a que permite a las

organizaciones estimar la magnitud del impacto operacional y financiero asociado a una interrupción.

Características del análisis de impacto

El Business Impact Analysis tiene dos objetivos principales; el primero de ellos consiste en proveer una base para identificar los procesos críticos para la operación de una organización. Una vez generado ese punto de partida, el segundo se refiere a la priorización de ese conjunto de procesos, siguiendo el criterio de cuanto mayor sea el impacto, mayor será la prioridad.

El BIA está directamente relacionado con aquellos procesos que poseen un tiempo crítico para su operación, porque si bien todos los procesos sujetos a un tiempo crítico son de misión crítica, no todos los procesos de misión crítica están relacionados con un tiempo crítico para su ejecución.

Para ello se define el Tiempo Objetivo de Recuperación (RTO por sus siglas en inglés), que es el período permitido para la recuperación de una función, y el Punto Objetivo de Recuperación (RPO) que describe la antigüedad máxima de los datos para su restauración, es decir, la tolerancia que el negocio puede permitir para operar con datos de respaldo, por lo que el RPO estará en función de las actividades primordiales de una organización.

Leyenda:

Valor hasta:	7	Inferior	
Valor hasta:	9	Baja	
Valor hasta:	11	Alta	
Valor hasta:	15	Extrema	

Tabla 15
BIA - Evaluación de Servicios

Tolerancia	Tolerancia	Impacto	Impacto	Criticidad	Valor
Hasta 3 horas	5	Superior	10	Extrema	15
Hasta 3 horas	5	Mayor	8	Extrema	13
Hasta 3 horas	5	Importante	6	Alta	11
Hasta 3 horas	5	Menor	4	Baja	9
Hasta 3 horas	5	Inferior	2	Inferior	7
Hasta 6 horas	4	Superior	10	Extrema	14
Hasta 6 horas	4	Mayor	8	Extrema	12
Hasta 6 horas	4	Importante	6	Alta	10
Hasta 6 horas	4	Menor	4	Baja	8
Hasta 6 horas	4	Inferior	2	Inferior	6
Hasta 12 horas	3	Superior	10	Extrema	13
Hasta 12 horas	3	Mayor	8	Alta	11
Hasta 12 horas	3	Importante	6	Baja	9
Hasta 12 horas	3	Menor	4	Inferior	7
Hasta 12 horas	3	Inferior	2	Inferior	5
Hasta 24 horas	1	Superior	10	Alta	11
Hasta 24 horas	1	Mayor	8	Baja	9
Hasta 24 horas	1	Importante	6	Inferior	7
Hasta 24 horas	1	Menor	4	Inferior	5
Hasta 24 horas	1	Inferior	2	Inferior	3
Más de 24 horas	0	Superior	10	Alta	10
Más de 24 horas	0	Mayor	8	Baja	8
Más de 24 horas	0	Importante	6	Inferior	6
Más de 24 horas	0	Menor	4	Inferior	4
Más de 24 horas	0	Inferior	2	Inferior	2

Tabla 16
Grado de afectación del servicio por criticidad

Afectación total	Valor	Clasificación
Del 0%	4	INFERIOR
Desde 1% hasta el 25%	6	BAJO
Desde 26% hasta el 50%	7	MEDIO
Desde 51% hasta el 75%	8	ALTO
Más de 75%	10	ALTO

CAPÍTULO III
ANÁLISIS Y EVALUACIÓN

3.1. INICIO DE GESTIÓN DE CONTINUIDAD DEL NEGOCIO

Para el inicio del Plan de Continuidad del Negocio basada en los aspectos de la norma internacional ISO/IEC 22301:2012 y para su aplicación en COAC “29 DE OCTUBRE” en este ítem se presentan todos los servicios tecnológicos que provee la Dirección de Informática y Comunicaciones los cuales permiten soportar las actividades de cada área de negocio enfatizando los niveles de disponibilidad tolerables por ellos.

3.1.1. Síntesis

Para la implementación de un Plan de Continuidad de Negocio para COAC “29 DE OCTUBRE” se debe contar con estrategias que permitan actuar de manera eficaz en caso de recuperación ante desastres, crisis y cualquier emergencia que afecte al negocio para lo cual es fundamental el respaldo y compromiso de la Alta Gerencia para la creación, implementación y difusión de las políticas de BCP definidas para los procesos críticos de la Institución.

Las políticas de Continuidad de Negocio permiten establecer el alcance de implementación de BCP y el desarrollo de un plan determinado de trabajo proporcionando una serie de normas impuestas por la Alta Gerencia de COAC “29 DE OCTUBRE” para soportar todos los procesos críticos de negocio.

3.1.2. Requisitos Normativos – Entes Reguladores.

LIBRO I.- NORMAS GENERALES PARA LAS INSTITUCIONES DEL SISTEMA FINANCIERO, TITULO X.- DE LA GESTIÓN Y ADMINISTRACIÓN DE RIESGOS CAPITULOV.- DE LA GESTIÓN DE RIESGO OPERATIVO SECCIÓN IV.- CONTINUIDAD DEL NEGOCIO. (Superintendencia de Bancos, 2015)

ARTÍCULO 15.- Las instituciones controladas deben administrar la continuidad del negocio, manteniendo procedimientos actualizados, a fin de garantizar su capacidad para operar en forma continua y minimizar las pérdidas en caso de una interrupción del negocio. (Artículo sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

Para el efecto, las instituciones del sistema financiero deben establecer un proceso de administración de la continuidad del negocio, tomando como referencia el estándar ISO 22301 o el que lo sustituya, y considerar al menos lo siguiente:

15.1 La definición de objetivos, políticas, estrategias, procedimientos, metodología, planes y presupuesto para la administración de la continuidad.

15.2 Un comité de continuidad del negocio que esté conformado como mínimo por los siguientes miembros: el funcionario responsable de la unidad de riesgos, quien lo preside, el funcionario responsable de la administración de la continuidad, quien hará las veces de secretario, el funcionario responsable del área de tecnología de la información, el funcionario responsable del área de talento humano, el auditor interno, solo con voz, y el máximo representante de cada una de las áreas involucradas en el proceso de administración de la continuidad.

El comité de continuidad del negocio debe sesionar mínimo con la mitad más uno de sus integrantes, al menos una vez cada trimestre, y sus decisiones serán tomadas por mayoría absoluta de votos. El presidente del comité tendrá voto dirimente. El comité de continuidad del negocio debe dejar evidencia de las decisiones adoptadas, las cuales deben ser conocidas y aprobadas por el comité de administración integral de riesgos.

El comité de continuidad del negocio debe tener al menos las siguientes responsabilidades:

15.2.1. Monitorear la implementación del plan y asegurar el alineamiento de éste con la metodología; y, velar por una administración de la continuidad del negocio competente;

15.2.2. Proponer cambios, actualizaciones y mejoras al plan;

15.2.3. Revisar el presupuesto del plan y ponerlo en conocimiento del comité de administración integral de riesgos;

15.2.4. Dar seguimiento a las potenciales amenazas que pudieran derivar en una interrupción de la continuidad de las operaciones y coordinar las acciones preventivas; y,

15.2.5. Realizar un seguimiento a las medidas adoptadas en caso de presentarse una interrupción de la continuidad de las operaciones;

15.3 Análisis de impacto que tendría una interrupción de los procesos que soportan los principales productos y servicios. Para ello, deben determinar el impacto en términos de magnitud de daños, el período de recuperación y tiempos máximos de interrupción que puedan ocasionar los siniestros.

El análisis de impacto debe ser revisado periódicamente y actualizado cuando existan cambios en la organización o en su entorno, que puedan afectar sus resultados;

15.4 Análisis que identifique los principales escenarios de riesgos, incluyendo las fallas en la tecnología de la información, tomando en cuenta el impacto y la probabilidad de que sucedan. Para ello, debe seguirse una metodología consistente con aquella utilizada para la evaluación de los demás riesgos;

15.5 Evaluación y selección de estrategias de continuidad por proceso que permitan mantener la continuidad de los procesos que soportan los principales productos y servicios, dentro del tiempo objetivo de recuperación definido para cada proceso, mismas que deben tomar en cuenta, al menos lo siguiente: la seguridad del personal, habilidades y conocimientos asociados al proceso, instalaciones alternas de trabajo, infraestructura alterna de procesamiento e información que soporte el proceso, seguridad de la información y equipamiento necesario para el proceso;

15.6 Realización de pruebas del plan de continuidad del negocio que permitan comprobar su efectividad y realizar los ajustes necesarios, cuando existan cambios que afecten la aplicabilidad del plan o al menos una (1) vez al año;

15.7 Procedimientos de difusión, comunicación, entrenamiento y concienciación del plan y su cumplimiento; e,

15.8 Incorporación del proceso de administración de la continuidad del negocio al proceso de administración integral de riesgos, que

garantice la actualización y mejora continúa del plan de continuidad del negocio.

ARTÍCULO 16.- El plan de continuidad del negocio debe contener al menos los procedimientos operativos, tecnológicos, de emergencias y comunicaciones para cada proceso crítico y para cada escenario cubierto, los cuales deben considerar, según corresponda, como mínimo lo siguiente. (Artículo sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

16.1 Escenarios de riesgos y procesos críticos cubiertos y alertas de los escenarios y procesos críticos no cubiertos por el plan;

16.2 Roles y responsabilidades de las personas encargadas de ejecutar cada actividad;

16.3 Criterios de invocación y activación del plan;

16.4 Responsable de su actualización;

16.5 Acciones y procedimientos a ejecutar antes, durante y después de ocurrido el incidente que ponga en peligro la operatividad de la institución, priorizando la seguridad del personal;

16.6 Tiempos máximos de interrupción y de recuperación de cada proceso;

16.7 Acciones y procedimientos a realizar para trasladar las actividades de la institución a ubicaciones transitorias alternativas o para el restablecimiento de los procesos críticos de manera urgente;

16.8 Información vital y cómo acceder a ella (incluye información de clientes, contratos, pólizas de seguro, manuales técnicos y de operación, entre otros);

16.9 Comunicaciones con el personal involucrado, sus familiares y contactos de emergencia, para lo cual debe contar con la información para contactarlos oportunamente (direcciones, teléfonos, correos electrónicos, entre otros);

16.10 Interacción con los medios de comunicación;

16.11 Comunicación con los grupos de interés;

16.12 Establecimiento de un centro de comando (considerar al menos un sitio principal, y uno alterno); y,

16.13 Ante eventos de desastre en el centro principal de procesamiento, los procedimientos de restauración en una ubicación remota de los servicios de tecnología de la información deben estar dentro de los parámetros establecidos en el plan, permitiendo una posterior recuperación de las condiciones previas a su ocurrencia. La ubicación remota no debe estar expuesta a los mismos riesgos del sitio principal.

3.1.3. ISO/IEC 22301/2012: Objetivos y Políticas

La ISO/IEC 22301:2012 provee aspectos y requisitos necesarios para el establecimiento de un BCP que debe cumplir con los siguientes puntos:

3.1.3.1. Definir objetivos de la continuidad del negocio

La definición de los objetivos para la continuidad del negocio debe considerar las estrategias de negocio a fin de alinearse a las necesidades específicas de las áreas de la empresa así como también a los procesos claves que soportan dichos servicios críticos.

Objetivos de Continuidad del Negocio

- Asegurar el restablecimiento de las operaciones, (sus procesos e infraestructura), considerados como críticos y que son esenciales para enfrentar la provisión del servicio que brinda la Cooperativa, según los tiempos definidos en los procedimientos.
- Desarrollar los procedimientos a ser ejecutados por personal de la Cooperativa, en caso de que ocurran eventos de riesgos que afecten la disponibilidad de los servicios críticos.
- Probar, comunicar, capacitar y mantener actualizado el Plan de Negocio, sus procedimientos e inventarios detallados en el Plan.

3.1.3.2. Definir Políticas de Continuidad de Negocio

La definición de políticas es fundamental para lograr los objetivos planteados, de tal forma que el Plan de Continuidad de Negocio se encuentre respaldado por normativas que apoyen la obtención de los resultados esperados para COAC “29 DE OCTUBRE”.

La Alta Dirección de COAC “29 DE OCTUBRE” considera al Plan de Continuidad de Negocio y su aplicación como de alta prioridad e importancia; definiendo como estratégico su desarrollo, implementación, difusión y aplicación. Además establece, valida y aprueba la política de Continuidad del Negocio haciendo referencia a los objetivos y al alcance (incluyendo limitaciones) del BCP.

Todo el personal de COAC “29 DE OCTUBRE” debe acoger las políticas, procedimientos, medidas preventivas y correctivas, de tal forma que permita responder satisfactoriamente ante situaciones que afecten los servicios definidos como críticos para la Cooperativa, considerando la afectación de los procesos e infraestructura física, informática y en general, su estabilidad y buena reputación.

Políticas de Continuidad de Negocio Generales COAC “29 de Octubre”

- El plan de continuidad de Negocio se ejecutara conforme a las políticas y metodología definida en el Manual Integral de Riesgos Capítulo: Administración del Plan de Continuidad del Negocio vigente en la Cooperativa.
- El Comité de Continuidad de Negocio es el responsable de la gestión para la elaboración, control, mantenimiento, ejecución, aplicación y difusión del Plan de Continuidad de Negocio, conforme se describe en el antes mencionado manual.
- La Cooperativa contará con un plan actualizado, que garantice el restablecimiento de las operaciones en caso de una interrupción del negocio.
- La Subgerencia de Riesgos será responsable de coordinar y efectuar la capacitación a los empleados involucrados, para que conozcan las actividades que deben ejecutar de forma efectiva y eficiente en el caso de activarse el Plan de Continuidad de Negocio según sea el evento.
- Es responsabilidad de los dueños de procesos relacionados con los servicios críticos, desarrollar y actualizar los procedimientos de los planes de Continuidad de Negocio bajo los lineamientos determinados por la Subgerencia de Riesgos.

- El Gerente General, tiene la potestad de activar el plan de Continuidad de Negocio en caso de considerarlo necesario, en su ausencia delegará al Secretario de Comité de Continuidad de Negocio.
- Los responsables de las áreas según corresponda deben aplicar las medidas preventivas que permitan mitigar los eventos, descritos en el Plan de Continuidad de Negocio.
- El Comité de Continuidad de Negocio validará que las diferentes áreas ejecuten las medidas preventivas y cuando sea necesario solicitará la documentación que respalde la ejecución de las mismas.

Políticas de Continuidad de Negocio Específicas COAC "29 de Octubre"

Política de análisis de impacto del negocio:

"Todo servicio debe contar con su respectivo análisis de impacto al negocio (Business Impact Analysis B.I.A.), metodología utilizada para identificar la criticidad en base a la tolerancia e impacto, según los criterios de calificación aprobados por la Alta Gerencia que se complementan con la metodología de Administración Riesgos implementada para la Cooperativa".

Política de infraestructura de Continuidad de Negocio

"La infraestructura implementada para la ejecución de los procedimientos de Continuidad de Negocio no podrá ser utilizada, bajo ningún concepto, para otros fines que no sea la de garantizar la recuperación de las operaciones y servicios."

Política de pruebas

"Las pruebas controladas de Continuidad de Negocio, se realizarán de forma planificada y se registrarán los resultados en formularios establecidos para el efecto, sean estos satisfactorios o insatisfactorios. Las pruebas se realizarán según la frecuencia y los procedimientos definidos en el Plan de Continuidad de Negocio."

Políticas de capacitación y difusión

"Todos los responsables de la ejecución de la Continuidad de Negocio y sus procedimientos, deberán participar en el Plan de Capacitación y ser evaluados periódicamente incluyendo al personal back up o alterno."
"Los Procedimientos de Continuidad de Negocio deberán ser difundidos al interior de la Cooperativa, precautelando el acceso según la confidencialidad de la información y facilitando su acceso al personal designado para la ejecución en todo momento."

Política de activación de la Continuidad de Negocio

"La activación del Plan de Continuidad de Negocio solo podrá realizarse con la respectiva autorización, según lo definido dentro de este documento y siguiendo las directrices institucionales de comunicación interna y externa."

Política de Manejo de medios

"En momentos de crisis, cualquier comunicado, declaración a los medios, organismos de control, clientes y público en general deberá realizarse bajo los lineamientos definidos y autorización de la Alta Dirección de la Cooperativa."

Política de Mantenimiento

"El Plan de Continuidad de Negocio, deberán revisarse al menos 1 vez al año."

"Las políticas, objetivos y procedimientos se deberán actualizar cada vez que exista alguna modificación en los procesos, infraestructura o nuevo componente tecnológico relacionado con los servicios críticos en el análisis del impacto al negocio y que pueda afectar la efectividad del Plan o sus procedimientos."

Política de registro de eventos de Continuidad de Negocio

"Toda incidencia que requiera la activación parcial o total del Plan deberá obtener la respectiva autorización y en los formatos establecidos, también deberá ser coordinada con el Comité de Continuidad de Negocio, según lo detallado en este documento."

Política de Aprovisionamiento de recursos Plan de Continuidad de Negocio

La Alta Dirección de COAC "29 DE OCTUBRE" debe establecer como punto de partida la asignación de roles y responsabilidades del personal denominado crítico según el conocimiento y competencia para el BCP. Además de proporcionar los recursos necesarios para determinar, implementar, operar, monitorear, revisar y mejorar el Plan de Continuidad de Negocio.

Para la implementación del Plan de Continuidad de Negocio es necesario la elaboración de un presupuesto en base a los recursos requeridos por un BCP y las estrategias definidas para asegurar el éxito del proyecto.

Los presupuestos de gasto e inversión para la implementación del Plan de Continuidad de Negocio se elaboraran anualmente y corresponden al Comité de Continuidad de Negocio para su respectiva aprobación y desarrollo.

El presupuesto deberá considerar los siguientes puntos:

- Infraestructura física y tecnológica a ser implementada.
- Recursos para implementación de procedimientos propios de BCP.
- Presupuesto para pruebas, capacitaciones y simulacros.
- Valores para movilización y ejecución de procedimientos en caso de ser necesaria la aplicación del Plan.

Cada rubro presentado en el presupuesto deberá ser sustentado con el respectivo análisis B.I.A, cronograma de implementación de la infraestructura, plan de pruebas, capacitaciones y simulacros.

En las revisiones del Plan de Continuidad de Negocio o en las pruebas y simulacros se podrá identificar la necesidad de realizar ajustes al presupuesto anual, siendo requerido el cumplimiento de los lineamientos y justificativos descritos en este capítulo.

Política de Concientización, Conocimiento y Preparación de Plan de Continuidad de Negocio

Para la puesta en marcha del Plan de Continuidad de Negocio es necesario que se asignen responsabilidades al personal critico competente y capacitado para cumplir con los roles definidos en el BCP para otorgar las respectivas autorizaciones, empoderamiento y liderazgo según el nivel de la afectación y de indisponibilidad del servicio crítico. Además de informar al personal interno y proveedores involucrados o relacionados en los procedimientos a ejecutar y

previa autorización del Comité de Continuidad de Negocio informar a los clientes afectados.

El Comité de Continuidad de Negocio debe analizar si es necesario una previa preparación y entrenamiento al personal critico seleccionado para las diferentes tareas asignadas referentes al BCP. De ser necesario el Comité de Continuidad de Negocio debe proporcionar entrenamiento, preparación o capacitación impartida, que permita proveer habilidades, grados de calificación o experiencias ganadas analizando la efectividad del entrenamiento realizado.

3.1.4. DIAGRAMA DE PROCESOS BPMN 2.0

MACROPROCESO: Gestión Informática

PROCESO: Gestión de Plataforma Tecnológica

SUBPROCESO: Control y Soporte de Hardware y Software

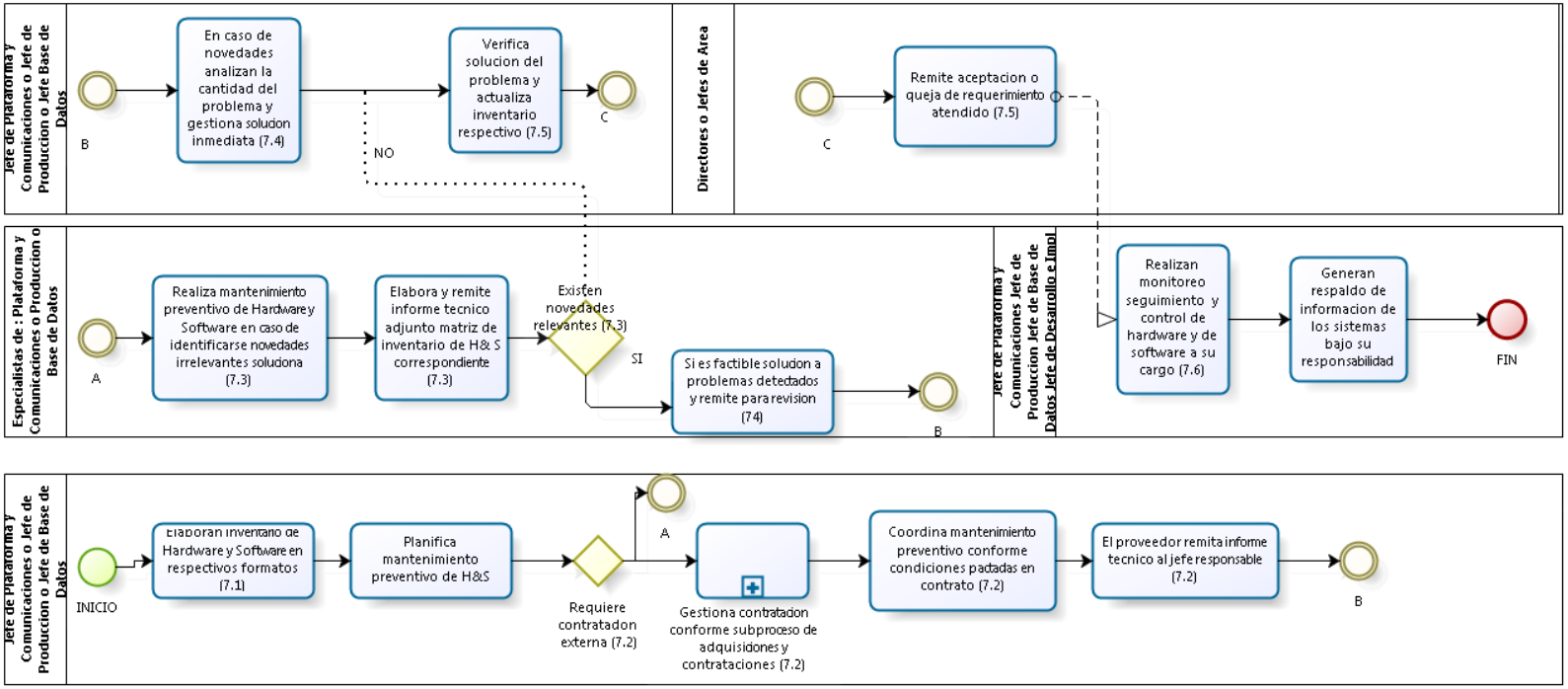


Figura 13 Gestión de Plataforma Tecnológica

PROCESO: Gestión de Base de Datos

SUBPROCESO: Administración de Base de Datos

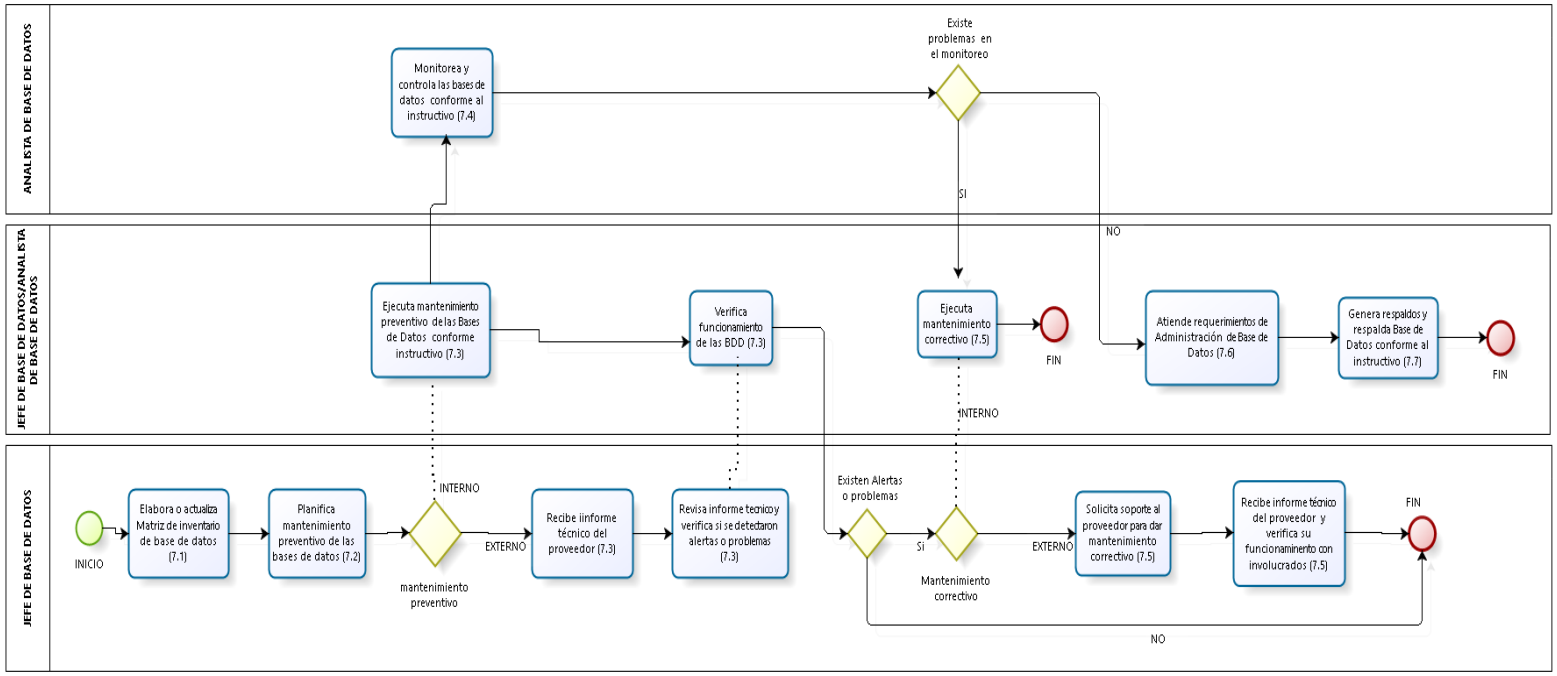


Figura 14 Gestión de Base de Datos

PROCESO: Gestión de Seguridad y Control dela Información

SUBPROCESO: Seguridad y Control dela Información

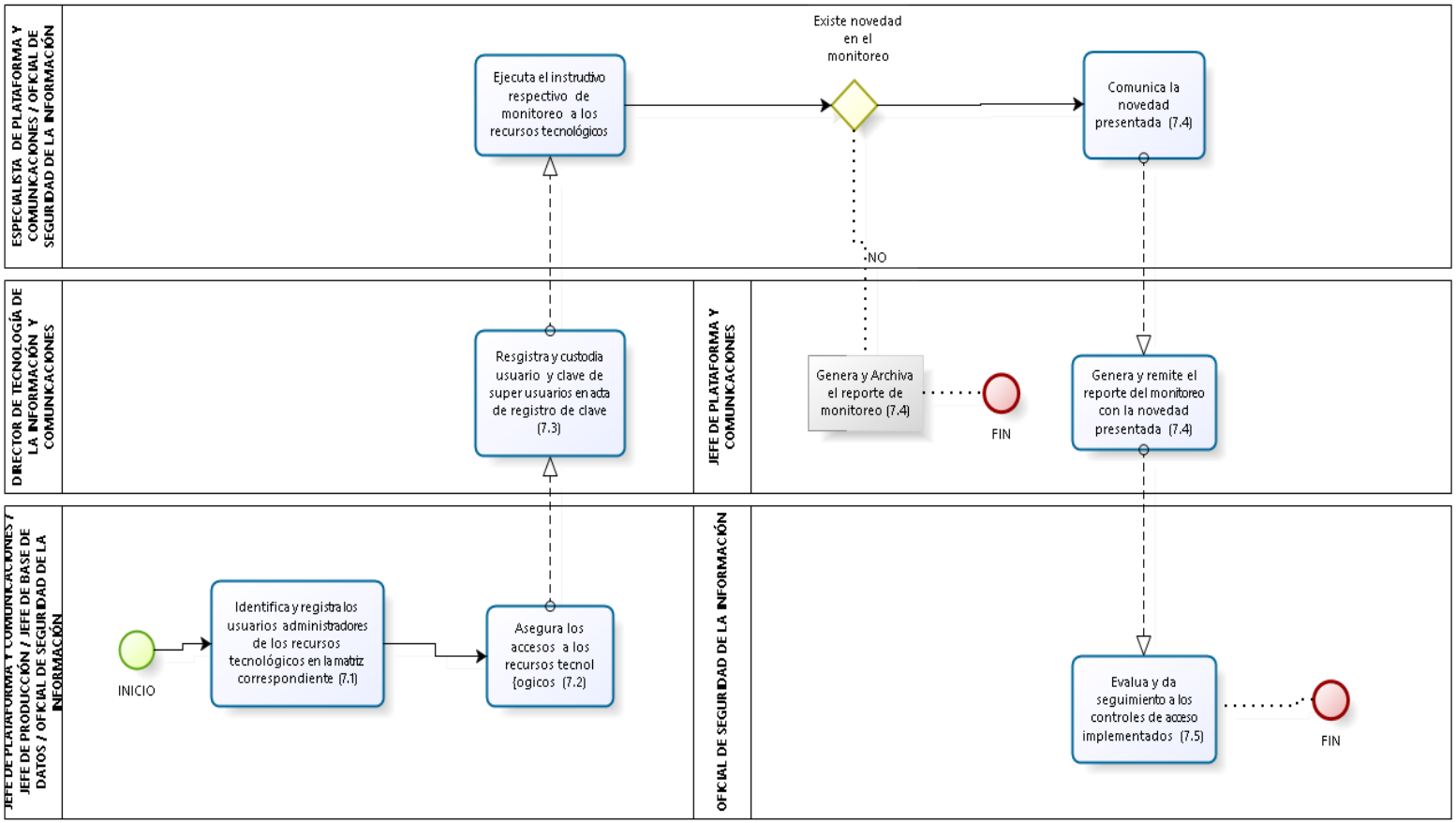


Figura 15 Gestión de Seguridad y Control dela Información

PROCESO: Gestión de Producción

SUBPROCESO: Administración de Servicios de Tecnología de Información

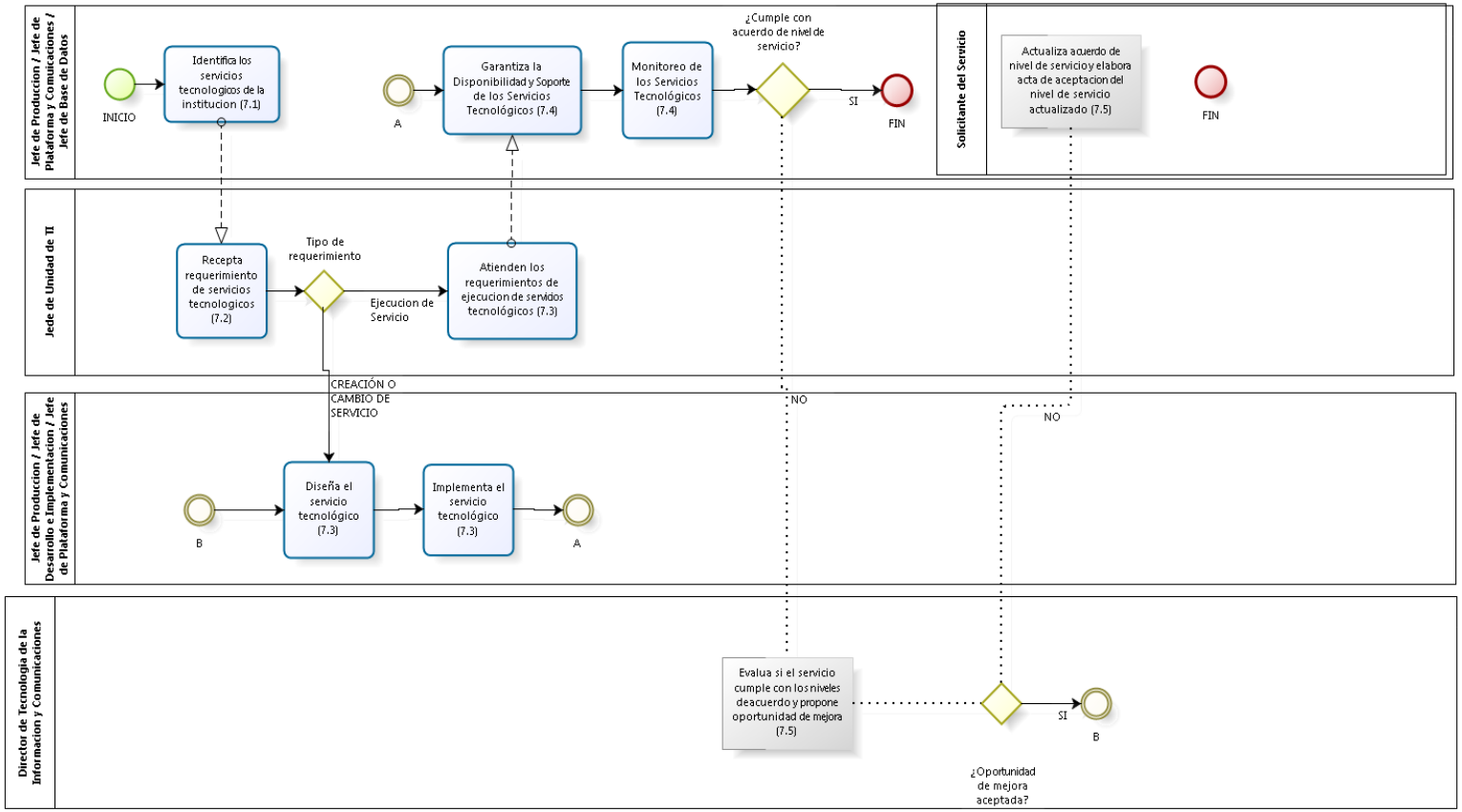


Figura 16 Gestión de Producción

3.1.5. Comité de continuidad de Negocio

El Comité de Continuidad de Negocio es el responsable de supervisar y coordinar las acciones definidas para viabilizar la implementación del Plan de Continuidad y Contingencia, alineado con la estrategia del negocio.

El Comité de Continuidad de Negocio asegurará la implementación y eficiencia de los procedimientos; así como la dotación de la infraestructura y recursos operativos y tecnológicos que viabilicen el cumplimiento de los objetivos y de las necesidades de negocio de la Cooperativa 29 de Octubre Ltda. Corresponde a los líderes definidos en el marco de referencia del Plan y los diferentes anexos, el cumplimiento de las políticas, estrategias, procedimientos y actualización de los documentos que conforman el Plan de Continuidad de Negocio.

3.1.5.1. Responsabilidades del comité de continuidad de negocio

- Disponer el desarrollo e implantación del Plan de Continuidad de Negocio, sus anexos y procedimientos, garantizando integralmente la correcta ejecución, difusión, pruebas y simulacros al interior de la cooperativa 29 de Octubre Ltda.
- Informar al Consejo de Administración de la cooperativa 29 de Octubre Ltda. de los avances en el desarrollo, aplicación, capacitación, difusión y resultados de las pruebas y simulacros, sean estos satisfactorios o insatisfactorios.
- Solicitar al Consejo de Administración de la cooperativa 29 de Octubre Ltda. la aprobación del marco de referencia de este Plan, incluyendo objetivos, estrategias, políticas, entre otros.

- Definir los líderes principales y alternos que asumirán las actividades previstas en el Plan de Continuidad de Negocio.
- Revisar y actualizar el Plan de Continuidad de Negocio y cualquiera de sus modificaciones. Disponer la realización de pruebas.

- Disponer la difusión, capacitación y entrenamiento al personal principal y alternos en el Plan de Continuidad de Negocio, sus objetivos, políticas, procedimientos a cargo de ese personal y medidas preventivas en el caso de eventos que deriven en una activación del Plan.
- Disponer la elaboración de los presupuestos, analizar y solicitar la respectiva aprobación de presupuestos anuales o emergentes necesarios para la aplicación de los planes de Continuidad de Negocio.
- Todos los que se definan en el Plan de Continuidad de Negocio.

3.1.5.2. Conformación del Comité de Continuidad de Negocio

El Comité estará integrado por:

- Gerencia General, quien lo preside y tendrá voto dirimente.
- Sub Gerencia de Riesgos Integrales, secretaria del comité
- Director de Marketing.
- Directora de Desarrollo Organizacional y Procesos.
- Director de Talento Humano
- Subgerencia Comercial
- Subgerencia de Operaciones y Tecnología
- Subgerencia Financiera
- Subgerencia Administrativa

- Jefe de Seguridad Integral
- Auditor Interno, solo con voz.

El Comité podrá invitar a sus sesiones a diferentes áreas de la cooperativa 29 de Octubre Ltda., proveedores y miembros del Consejo de Administración para discutir, evaluar y proponer mejoras al Plan de Continuidad de Negocio y/o sus anexos.

Los invitados solo podrán emitir informes, opiniones y participar en las discusiones del Comité, sin tener voto, ni responsabilidad dentro de las decisiones del Comité.

El presente Comité lo presidirá la Gerencia General y la Jefatura de Riesgos actuará como secretario, llevando las actas y el seguimiento de las definiciones tomadas.

La ejecución y seguimiento a las actividades para el desarrollo, implantación, capacitación, comunicación, pruebas y simulacros estará a cargo del secretario del Comité.

3.1.5.3. Responsabilidades de los miembros del comité

Presidente del Comité

- Presidir las sesiones ordinarias, extraordinarias y emergentes del Comité.
- Convocar, por intermedio del secretario, las sesiones extraordinarias del Comité.

- Participar con voz y voto en el análisis y discusión de los asuntos a tratar en las sesiones.
- Someter a conocimiento y aprobación al Consejo de Administración de la cooperativa 29 de Octubre Ltda. los documentos e información de responsabilidad del Comité.
- Firmar las actas de las sesiones.
- El Presidente del Comité tendrá voto dirimente, en los casos que se presenten empates en las votaciones.

Vocales

- Asistir a las sesiones del Comité.
- Participar con voz y voto en el análisis y discusión de los asuntos a tratar en las sesiones.
- Proponer asuntos a tratar en el Comité, en materia de Continuidad de Negocio y medidas preventivas.
- Ejecutar e informar de las acciones tomadas que le fueran asignadas.
- Suscribir las actas de las sesiones del Comité.
- Las demás que determine el Comité.

Secretario

- Recopilar con anticipación los asuntos a tratar en las sesiones del Comité.
- Preparar y proponer la agenda de trabajo de las sesiones del Comité y comunicarla a sus integrantes.
- Asistir a las sesiones del Comité con derecho a voz y voto.
- Realizar las actas de sesiones del Comité y ponerla en consideración para su aprobación.
- Dar seguimiento a los acuerdos y tareas asignadas en el Comité e informar los resultados en la siguiente reunión.

- Las demás que se deriven de la naturaleza de su cargo y aquellas que sean señaladas por el Comité.
- Administración del Plan de Continuidad de Negocio, asegurando el cumplimiento y ejecución de las actividades para el desarrollo, implementación, capacitación, comunicación, pruebas y simulacros y actualización del Plan.

3.1.5.4. Sesiones del Comité

El Comité se reunirá en sesiones ordinarias, sesiones extraordinarias y emergentes, cuando las convoque su Presidente o a solicitud de por lo menos la mitad más uno de sus miembros. Las sesiones emergentes se podrán realizar con al menos el 30% de los integrantes del Comité.

Las convocatorias y agenda de trabajo de las sesiones ordinarias se comunicarán con cinco días hábiles de anticipación y las extraordinarias con al menos un día de antelación o la situación la requiera.

En caso de presentarse eventos que requieran la aplicación del Plan de Continuidad de Negocio, cualquiera de los miembros del Comité deberá informar a la Presidencia y Secretaría del Comité para realizar convocatorias emergentes que se realizarán de forma inmediata.

Para que las sesiones ordinarias se consideren instaladas, debe estar por lo menos la mitad más uno de sus integrantes.

Por cada Comité celebrado se levantará la respectiva acta que se someterá a consideración y aprobación en la siguiente sesión, en la que se realiza el seguimiento de las acciones a ejecutar. Cada acta será firmada por todos los miembros que hubieren asistido y contendrá los datos siguientes:

- Lugar fecha y número ascendente de sesión;
- Lista de asistencia;
- Asuntos tratados;
- Acuerdos tomados, asignación de tareas y quiénes los ejecutarán
- Hora de inicio y término de la sesión.

3.1.5.5. Suplencias

En ausencia del Presidente del Comité, presidirá el Secretario del Comité.

3.2. IDENTIFICACIÓN, GESTIÓN Y CONTROL DE RIESGOS

En este ítem se presentan los principales riesgos existentes asociados a los procesos críticos de Gestión Informática de COAC “29 DE OCTUBRE”. Se describen a continuación los aspectos de la norma internacional ISO/IEC 22301:2012 en la evaluación y gestión de los riesgos existentes y las acciones necesarias para su aplicación e implementación en COAC “29 DE OCTUBRE”.

3.2.1. Síntesis

Para la determinación de eventos internos y externos que pueden afectar de manera negativa la Continuidad de Negocio en COAC ”29 DE OCTUBRE” se debe describir los controles necesarios para prevenir o mitigar los efectos potenciales de riesgos de manera continua e interactiva basado en la planificación que se realiza para la obtención de resultados, estableciendo los eventos reales y potenciales que pueden ocasionar riesgos a la continuidad del Negocio y pérdidas financieras para la institución.

En análisis de riesgos, la correcta identificación permite continuar con una adecuada implementación de controles y políticas que permitan minimizar los

eventos de riesgo en los procesos críticos. La Alta Dirección de COAC”29 DE OCTUBRE” deciden cuáles acciones a tomar frente a los riesgos identificados, esta acción se conoce como el tratamiento del riesgo, misma que se debe analizar utilizando criterios técnicos; de tal forma que la información en la que se base la definición de decisión final tenga confiabilidad y precisión para asegurar la continuidad del negocio.

Las opciones disponibles de tratamiento para minimizar la probabilidad de que los riesgos identificados se materialicen se definen a continuación:

Asumir.- Se acepta la exposición aunque eso signifique que el nivel de riesgo aumente.

Mitigar.- No se acepta el nivel de riesgo inherente y se toman acciones para reducirlo (disminuirlo).

Controlar.- Se acepta la exposición pero se toman medidas para que no aumente el nivel de riesgo (mantener el nivel de riesgo).

Transferir.- No se acepta en nivel de riesgo inherente y se toman acciones para trasladar el riesgo a un tercero.

3.2.2. Identificación, Evaluación, Gestión y Control de Riesgos

Es necesario que la organización adopte una metodología para la identificación, evaluación, gestión y control de los riesgos existentes en los procesos críticos del negocio, para que a través de la valoración previa de las amenazas y vulnerabilidades de incidentes en los mismos, se logre determinar las causas y probabilidades y poder dimensionar el impacto de un determinado incidente en el negocio.

La organización debe:

- Identificar Amenazas
- Identificar Vulnerabilidades
- Estimar el impacto en la organización de cada amenaza identificada.
- Determinar los riesgos a partir de las amenazas y vulnerabilidades identificadas.
- Registrar los riesgos y documentar toda la información identificada.
- Identificar los riesgos de procesos críticos y tratarlos de acuerdo al nivel de aceptación del riesgo que ha sido determinado previamente por la Alta Gerencia.
- Realizar el mantenimiento de los riesgos y controles de cambios relevantes en los procesos críticos de la organización cada cierto tiempo.

En tal sentido como parte de la implementación de esta norma en la COAC “29 de Octubre” se realizaron las siguientes actividades:

- Conocimiento y comprensión de los potenciales de pérdidas:

  - Identificar las amenazas internas y externas conocidas que pueden causar interrupción de las actividades más urgentes de la organización. Tales como: Desastres Naturales, ocasionados por el hombre de manera intencional o accidental, amenazas externas, tecnológicas, con identificación previa y sin ella y controlables o que escapan del nivel del control de la organización.
  - De acuerdo al enfoque de la Alta Dirección, determinar un sistema de puntuación en la evaluación del riesgo para los impactos y las probabilidades.
  - Estimar el impacto en la organización de cada amenaza utilizando el sistema de puntuación de acuerdo.

- Determinar la probabilidad de ocurrencia de cada amenaza y el peso utilizando el sistema de puntuación.
- Calcular el riesgo de cada amenaza mediante la combinación de las puntuaciones de impacto y la probabilidad, de acuerdo con una fórmula acordada.
- Dar prioridad a las amenazas según el nivel de impacto en las actividades más urgentes.
- Determinar temas legales o regulatorios relacionados.
- Establecer un continuo soporte al proceso de evaluación.

- Determinar controles para prevenir y/o mitigar el efecto de los potenciales de incidentes que causan daños y pérdidas

- Identificar, evaluar y escoger metodologías adecuadas para facilitar el análisis y gestión de riesgos, para ello es necesario previamente realizar un análisis costo beneficio, ventajas-desventajas de la metodología a usar.

- Revisar la efectividad de los controles a implementar
  - Realizar una planificación previa de los controles a implementar.
  - Validar el costo/ beneficio y prioridades de dichos controles.
  - Establecer comunicaciones efectivas y acuerdos de nivel de servicios referente a continuidad de negocios con proveedores, entidades estrechamente ligadas y ciudadanos, así como los integrantes propios de la organización.
  - Seleccionar las respuestas efectivas y oportunas ante los riesgos: aceptar, evitar, controlar, monitorear, compartir o transmitir.

- Evaluar y Controlar los Riesgos
  - Determinar escenarios de desastres de acuerdo a los riesgos expuestos de la organización

- Clasificarlos riesgos considerando: riesgos bajo el control de la organización, riesgos más allá del control, amenazas con aviso previo (lluvias) y sin aviso previo (terremoto).
- Evaluar el impacto de los riesgos en activos tangibles e intangibles de la organización como: personal, tecnologías de información e infraestructura.
- Evaluar controles alineados a los impactos debido a riesgos de incidentes o desastres, como por ejemplo: controles preventivos (detectores de humo en caso incendio), detectivos (uso de antivirus) y correctivos (Planes de Continuidad).

3.2.2.1. Identificación de amenazas

Tabla 17
Lista Amenazas COAC "29 DE OCTUBRE"

Tipo de la Amenaza	Factor de la Amenaza	Descripción
1.1 Fuego	1. Desastres Naturales	Incendios: posibilidad de que el fuego acabe con la información
1.2 Daños Por Agua	1. Desastres Naturales	Inundaciones: posibilidad de que el agua acabe con la información
1.3 Desastres Naturales	1. Desastres Naturales	Incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, erupción volcánica
2.1 Fuego	2. De origen Industrial	Incendio: posibilidad de que el fuego acabe con la información
2.2 Daños por Agua	2. De origen Industrial	Escapes, Fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema
2.3 Desastre Industriales	2. De origen Industrial	Desastres Debidos a la actividad humana: explosiones, derrumbes, sobrecarga eléctrica.
2.4 Contaminación	2. De origen Industrial	Polvo, Suciedad
2.5 Avería de origen físico o lógico	2. De origen Industrial	Fallos en los equipos y/o fallos en los programas. Puede ser debida a un efecto de origen o sobrevenida durante el funcionamiento del sistema
2.6 Corte de Suministro Eléctrico	2. De origen Industrial	Cese de la alimentación de potencia
2.7 Condiciones Inadecuadas de temperatura y/o humedad	2. De origen Industrial	Deficiencia en la aclimatación de las instalaciones, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frio. Exceso de humedad

Continua 

2.8 Fallos de servicio de Comunicación	2. De origen Industrial	Cese de la capacidad de trasmitir datos de un sitio a otro
2.9 Interrupción de otro Servicios y Suministros Esenciales	2. De origen Industrial	Otros servicios o recursos de los que depende la operación de los equipos
2.10 Degradación de los soportes de almacenamiento de la información	2. De origen Industrial	Como consecuencia del paso del tiempo
3.1 Errores de los Usuarios	3. Errores o Fallos no Intencionados	Equivocaciones de las personas cuando usan los servicios, datos, etc.
3.2 Errores del Administrador	3. Errores o Fallos no Intencionados	Equivocaciones de personas con responsabilidades de Instalación y operación
3.3 Errores de monitorización	3. Errores o Fallos no Intencionados	Inadecuado registro de actividades: falta de registros, registro incompletos
3.4 Errores de Configuración	3. Errores o Fallos no Intencionados	Introducción erróneos
3.5 Deficiencias de la Organización	3. Errores o Fallos no Intencionados	Cuando no está claro quien tiene que hacer exactamente qué y cuando
3.6 Difusión de software dañino	3. Errores o Fallos no Intencionados	Propagación inocente de virus, espías (spyware) gusanos, troyanos, bombas Lógicas
3.7 Errores de re-encaminamiento	3. Errores o Fallos no Intencionados	Envió de Información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información a donde o por donde no es debido

Continua

3.8 Errores de secuencia	3. Errores o Fallos no Intencionados	Alteración accidental del orden
3.9 Escapes de Información	3. Errores o Fallos no Intencionados	La información llega accidentalmente al conocimiento de personas que no deberían tener conocimiento de ella, sin que la información en si misma se alterada
3.10 Alteración de la Información	3. Errores o Fallos no Intencionados	Alteración accidental de la información
3.11 Introducción de Información Incorrecta	3. Errores o Fallos no Intencionados	Inserción accidental de la información incorrecta
3.12 Degradación de la Información	3. Errores o Fallos no Intencionados	Esta amenaza solo se identifica sobre datos en general, pues cuando la información está en algún soporte informático hay amenazas especificas
3.13 Destrucción de la Información	3. Errores o Fallos no Intencionados	Perdida accidental de la Información
3.14 Divulgación de la Información	3. Errores o Fallos no Intencionados	Revelación por indiscreción Incontinencia Verbal, medios electrónico , soporte papel
3.15 Vulnerabilidades de los programas (software)	3. Errores o Fallos no Intencionados	Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario
3.16 Errores de mantenimiento / actualización de programas (software)	3. Errores o Fallos no Intencionados	Defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.
3.17 Errores de mantenimiento /actualización de equipos (hardware)	3. Errores o Fallos no Intencionados	Defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal del uso.

Continua 

3.18 Caída del sistema por agotamiento de recursos	3. Errores o Fallos no Intencionados	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada
3.19 Indisponibilidad del personal	3. Errores o Fallos no Intencionados	Ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público
4.1 Manipulación de la configuración	4. Ataques Intencionales	Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento
4.2 Suplantación de la identidad del usuario	4. Ataques Intencionales	Cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios
4.3 Abuso de privilegios de acceso	4. Ataques Intencionales	Cada usuario disfruta de un nivel de privilegios para un determinado propósito: cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia hay problemas.
4.4 Uso no previsto	4. Ataques Intencionales	Utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet. Bases de datos personales, programas personales, almacenamiento de datos personales, etc.
4.5 Difusión de software dañino	4. Ataques Intencionales	Propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.
4.6 Encaminamiento de mensajes	4. Ataques Intencionales	Envío de información a un destino incorrecto a través de un sistema o una red que llevan la información a donde o por donde no es debido: puede tratarse de mensajes entre personas, entre procesos o entre unos y otros
4.7 Alteración de secuencia	4. Ataques Intencionales	Alteración del orden de los mensajes transmitidos con ánimo de que el nuevo orden altere el significado del conjunto de mensajes, perjudicando a la integridad de los datos afectados

Continua

4.8 Acceso no autorizado	4. Ataques Intencionales	El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización
4.9 Análisis de tráfico	4. Ataques Intencionales	El atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios.
4.10 Repudio	4. Ataques Intencionales	Negación a posteriori de actuaciones o compromisos adquiridos en el pasado
4.11 Intercepción de Información (escucha)	4. Ataques Intencionales	El atacante llega a tener acceso a información que no le corresponde, sin que la información en sí misma se vea alterada
4.12 Modificación de la información	4. Ataques Intencionales	Alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio
4.13 Introducción de falsa información	4. Ataques Intencionales	Inserción interesada de información falsa, con ánimo de obtener un beneficio o causar un perjuicio
4.14 Corrupción de la Información	4. Ataques Intencionales	Degradación intencional de la información falsa, con ánimo de obtener un beneficio o causar in perjuicio
4.15 Destrucción de la Información	4. Ataques Intencionales	Eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio
4.16 Divulgación de información	4. Ataques Intencionales	Revelación de información
4.17 Manipulación de programas	4. Ataques Intencionales	Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza
4.18 Denegación de servicio	4. Ataques Intencionales	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada
4.19 Robo	4. Ataques Intencionales	La sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad

Continua 

4.20 Ataque destructivo	4. Ataques Intencionales	Vandalismo, terrorismo, acción militar, …
4.21 Indisponibilidad del personal	4. Ataques Intencionales	Ausencia deliberada del puesto de trabajo: como huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos
4.22 Extorsión	4. Ataques Intencionales	Presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido
4.23 Ingeniería social	4. Ataques Intencionales	Abuso de la buena fe de las personas para que realicen actividades que interesan un tercero

3.2.2.2. Evaluación de Riesgos

Tabla 18
Matriz de Riesgos COAC "29 DE OCTUBRE"

VALORIZACIÓN SEVERIDAD DEL RIESGO						
AMENAZA	NIVEL DE PROB.	(P)	IMPACTO	(I)	SEVERIDAD RIESGO	(P x I)
1.1 Fuego	BAJO	2	ALTO	4	ALTO	8
1.2 Daños Por Agua	BAJO	2	MEDIO	3	MEDIO	6
1.3 Desastres Naturales	BAJO	2	ALTO	4	ALTO	8
2.3 Desastre Industriales	BAJO	2	MEDIO	3	MEDIO	6
2.4 Contaminación	BAJO	2	BAJO	2	BAJO	4
2.5 Avería de origen físico o lógico	BAJO	2	MEDIO	3	MEDIO	6
2.6 Corte de Suministro Eléctrico	BAJO	2	ALTO	4	ALTO	8
2.7 Condiciones Inadecuadas de temperatura y/o humedad	BAJO	2	MEDIO	3	MEDIO	6
2.8 Fallos de servicio de Comunicación	MEDIO	3	MUY ALTO	5	MUY ALTO	15
2.9 Interrupción de otro Servicios y Suministros Esenciales	BAJO	2	MEDIO	3	MEDIO	6
2.10 Degradación de los soportes de almacenamiento de la información	MUY BAJO	1	ALTO	4	ALTO	4
3.1 Errores de los Usuarios	MEDIO	3	BAJO	2	MEDIO	6
3.2 Errores del Administrador	MEDIO	3	BAJO	2	MEDIO	6

Continua

VALORIZACIÓN SEVERIDAD DEL RIESGO						
AMENAZA	NIVEL DE PROB.	(P)	IMPACTO	(I)	SEVERIDAD RIESGO	(P x I)
3.3 Errores de monitorización	MEDIO	3	BAJO	2	MEDIO	6
3.4 Errores de Configuración	BAJO	2	MEDIO	3	MEDIO	6
3.5 Deficiencias de la Organización	MUY BAJO	1	MEDIO	3	MEDIO	3
3.6 Difusión de software dañino	MUY BAJO	1	MEDIO	3	MEDIO	3
3.7 Errores de re-encaminamiento	MUY BAJO	1	BAJO	2	BAJO	2
3.8 Errores de secuencia	MUY BAJO	1	BAJO	2	BAJO	2
3.9 Escapes de Información	BAJO	2	MEDIO	3	MEDIO	6
3.10 Alteración de la Información	BAJO	2	MEDIO	3	MEDIO	6
3.11 Introducción de Información Incorrecta	BAJO	2	MEDIO	3	MEDIO	6
3.12 Degradación de la Información	BAJO	2	MEDIO	3	MEDIO	6
3.13 Destrucción de la Información	BAJO	2	MEDIO	3	MEDIO	6
3.14 Divulgación de la Información	BAJO	2	MEDIO	3	MEDIO	6
3.15 Vulnerabilidades de los programas (software)	BAJO	2	MEDIO	3	MEDIO	6
3.16 Errores de mantenimiento / actualización de	BAJO	2	MEDIO	3	MEDIO	6

Continua

VALORIZACIÓN SEVERIDAD DEL RIESGO						
AMENAZA	NIVEL DE PROB.	(P)	IMPACTO	(I)	SEVERIDAD RIESGO	(P x I)
programas (software)						
3.17 Errores de mantenimiento /actualización de equipos (hardware)	BAJO	2	BAJO	2	BAJO	4
3.18 Caída del sistema por agotamiento de recursos	MEDIO	3	ALTO	4	MUY ALTO	12
3.19 Indisponibilidad del personal	BAJO	2	BAJO	2	BAJO	4
4.1 Manipulación de la configuración	BAJO	2	BAJO	2	BAJO	4
4.2 Suplantación de la identidad del usuario	MUY BAJO	1	MEDIO	3	MEDIO	3
4.3 Abuso de privilegios de acceso	BAJO	2	MEDIO	3	MEDIO	6
4.4 Uso no previsto	BAJO	2	BAJO	2	BAJO	4
4.5 Difusión de software dañino	BAJO	2	MEDIO	3	MEDIO	6
4.6 Encaminamiento de mensajes	BAJO	2	BAJO	2	MEDIO	4
4.7 Alteración de secuencia	MUY BAJO	1	MEDIO	3	MEDIO	3
4.8 Acceso no autorizado	BAJO	2	ALTO	4	ALTO	8
4.9 Análisis de tráfico	BAJO	2	MEDIO	3	MEDIO	6
4.10 Repudio	BAJO	2	BAJO	2	BAJO	4

Continua

VALORIZACIÓN SEVERIDAD DEL RIESGO						
AMENAZA	NIVEL DE PROB.	(P)	IMPACTO	(I)	SEVERIDAD RIESGO	(P x I)
4.11 Intercepción de Información (escucha)	MUY BAJO	1	BAJO	2	BAJO	2
4.12 Modificación de la información	BAJO	2	MEDIO	3	MEDIO	6
4.13 Introducción de falsa información	MUY BAJO	1	MEDIO	3	MEDIO	3
4.14 Corrupción de la Información	BAJO	2	MEDIO	3	MEDIO	6
4.15 Destrucción de la Información	MUY BAJO	1	MEDIO	3	MEDIO	3
4.16 Divulgación de información	MUY BAJO	1	MEDIO	3	MEDIO	3
4.17 Manipulación de programas	MUY BAJO	1	MEDIO	3	MEDIO	3
4.18 Denegación de servicio	MUY BAJO	1	ALTO	4	ALTO	4
4.19 Robo	BAJO	2	MEDIO	3	MEDIO	6
4.20 Ataque destructivo	BAJO	2	MEDIO	3	MEDIO	6
4.21 Indisponibilidad del personal	BAJO	2	MEDIO	3	MEDIO	6
4.22 Extorsión	BAJO	2	MEDIO	3	MEDIO	6
4.23 Ingeniería social	BAJO	2	BAJO	2	BAJO	4

3.2.3. Análisis de Impacto del Negocio (BIA)

En este ítem se muestran los pasos necesarios para la realización del Análisis de Impacto del Negocio (BIA) tomando la referencia de los aspectos descritos en la norma internacional ISO/IEC 22301:2012 para la realización de BIA y las acciones necesarias para su aplicación e implementación en COAC “29 DE OCTUBRE”.

3.2.3.1. Síntesis BIA

El análisis B.I.A (Business Impact Analysis - Análisis de Impacto al Negocio) permite identificar los servicios críticos, listando todos los servicios provistos por el Departamento de Informática y Comunicación de COAC “29 DE COAC”, sus procesos y sistema de información que lo soporta así como también la categorización de los recursos para evaluar cuáles de ellos deben contar con procedimientos de Continuidad de negocio

La definición del Impacto por la interrupción de los servicios de la COAC “29 de Octubre” necesita de un proceso definido que permita evaluar la afectación en las actividades que soportan los procesos catalogados como críticos.

Es necesario que la organización logre:

- Identificar las actividades relevantes dentro de sus procesos críticos.
- Comprender el impacto potencial en el tiempo de una falta de operatividad de dichas actividades.
- Estimar un periodo máximo tolerable de interrupción (MTPD) para cada actividad crítica, es decir; el tiempo que le tomaría a los impactos adversos que pudieran surgir como consecuencia de no

ofrecer un servicio o la realización de una actividad en COAC, a ser inaceptable.

- Identificar todas las dependencias de las actividades, tanto internas como externas, de los propietarios de la gestión de cada proceso y el personal adecuado, como expertos en la materia, para proporcionar información sobre los procesos de negocios, así como proveedores externos.
- Priorizar las actividades de acuerdo a las necesidad de recuperación.
- Estimar los recursos que requiere cada actividad crítica para su reanudación.
- Decidir el tiempo de recuperación objetivo (RTO) para la reanudación de las actividades críticas dentro del periodo de interrupción máxima tolerable (MTPD), el RTO se determina en la etapa de diseño del ciclo de vida de BCM, ya que es una decisión (no es un hallazgo), pero una estimación inicial puede hacerse durante el BIA que se puede confirmar en la etapa posterior, una vez se dispone de toda la información.
- Desarrollar y Actualizar el Análisis de Impacto de Negocio (BIA) en periodos de tiempo previamente definidos, especialmente cuando se producen cambios relevantes en los procesos críticos del negocio.

Para la ejecución del BIA en la COAC “29 DE OCTUBRE es necesario cumplir con las siguientes especificaciones:

- Establecer la fase inicial de un BIA
  - Determinar los objetivos y alcance del BIA

- Escoger una metodología o herramienta adecuada para la planificación de la realización del BIA.
- Estimar la duración del proyecto BIA.
- Comunicar la necesidad de un BIA a la Alta Dirección y a las personas relacionadas a COAC “29 DE OCTUBRE.
- Planificar capacitaciones efectivas dentro de la organización.

- Determinar los resultados de las interrupciones, la estimación del daño y el impacto directo en la organización.
  - Resultados de las interrupciones: Incumplimiento de las regulaciones o leyes, interrupción de los servicios y /o productos críticos brindados, pérdida de activos tangibles e intangibles (incluye personal), pérdida de prestigio e imagen pública.
  - Estimar cualitativa y cuantitativamente el grado del daño a la organización.
  - Impacto directo en la organización en el ámbito: Legal, operacional, personal, externo (ciudadanos y proveedores), financiero entre otros.

- Desarrollar el BIA de acuerdo a la metodología escogida.

Establecer un procedimiento apropiado para la recopilación de la información dentro de COAC “29 DE OCTUBRE (entrevistas, juntas de trabajo, cuestionarios o la combinación de ellos).

Recopilación de información por medio de entrevistas, para ello es necesario: Respetar un formato general para todas las entrevistas realizadas, establecer qué datos son relevantes de obtener en la entrevista, presentar el formato de la entrevista días antes a los implicados, luego de la entrevista, de ser necesario, programar algunas nuevas para aclarar puntos no resueltos o no claros de los proporcionados inicialmente.

Recopilación de información por medio de cuestionarios, para ello es necesario: realizar formatos comunes para cada tipo de cuestionario, de acuerdo al rol del implicado, programar reuniones para la explicación y repartición de los cuestionarios, asistir a los participantes durante la realización del cuestionario, revisar y levantar información relevante, de ser necesario programar nuevas reuniones para aclarar o solicitar nuevos datos en el cuestionario.

Recopilación de información por medio de juntas de trabajo, para ello es necesario, evaluar la disponibilidad del personal, seleccionar la locación adecuada, establecer los objetivos de la junta y definir la fecha de la misma, durante la junta es importante, comprometer al cumplimiento de los objetivos acordados y determinar los puntos relevantes durante la junta.

- Establecer una metodología de análisis de la información.
- Desarrollar los resultados del BIA, es necesario: realizar una primera versión de los hallazgos de impacto del BIA para mostrárselos a la Alta Dirección y solicitar sus opiniones o comentarios, luego hacer las correcciones requeridas y preparar los resultados finales del Informe BIA y realizar la exposición final de los principales Hallazgos a la Alta Gerencia de COAC “29 DE OCTUBRE.

- Definir el nivel de criticidad de las actividades identificadas y priorizarlas.
- Establecer los registros vitales para la continuidad y reanudación del negocio.

- Establecer los límites de tiempo de recuperación para las actividades más relevantes de los procesos críticos

- Alinear el nivel de criticidad con las ventajas de reanudación de las actividades críticas.
- Establecer la prioridad de recuperación de funciones en la actividad crítica.
- Definir los recursos mínimos necesarios (internos, externos, adicionales, existentes) para la reanudación de las actividades.

Business Impact Analysis - BIA

Objetivo

El análisis B.I.A (Business Impact Analysis - Análisis de Impacto al Negocio) permite identificar y determinar de manera cuantitativa y/o cualitativa impactos, efectos, y pérdidas ocasionadas en los servicios críticos, los procesos asociados a estos servicios e infraestructura que los soportan, permitiendo, con las acciones definidas, mitigar los riesgos que ocasionan eventos de indisponibilidad.

Todo servicio provisto por COAC “29 DE OCTUBRE” debe contar con su respectivo análisis B.I.A previo su implantación.

Criterios de Calificación BIA

Para la evaluación de la criticidad de los servicios se utilizarán los criterios de calificación B.I.A (Business Impact Analysis), de la metodología de riesgos de COAC “29 DE OCTUBRE” (Metodología de Riesgo Operativo), así como los definidos en el Plan de Continuidad de Negocio.

Actualización BIA

La actualización y revisión del B.I.A estará a cargo del siguiente personal miembro del Comité de Continuidad de Negocio:

- Subgerencia Administrativa
- Subgerencia Comercial
- Subgerencia de Operaciones y Tecnología
- Subgerencia de Riesgos
- Dirección de DO y Procesos
- Dirección de Talento Humano

Responsables de Evaluación BIA

Los responsables de la evaluación, mantendrán reuniones de trabajo semestrales o cuando se requiera para identificar posibles impactos al negocio, actualizarán la matriz e informarán por medio de las respectivas actas de las reuniones al Comité de Continuidad de Negocio con los resultados de las revisiones realizadas. De ser necesario este equipo de trabajo emitirá informes para el Comité de Continuidad de Negocio.

Es responsabilidad del Comité de Continuidad de Negocio revisar las actas e informes presentados por el equipo de trabajo a cargo del mantenimiento y actualización del B.I.A y realizar las observaciones que sean necesarias para asegurar que el análisis realizado cumpla con los objetivos de COAC “29 DE OCTUBRE” para asegurar la disponibilidad de los servicios.

La aprobación final de los resultados del B.I.A será otorgada por la Alta Gerencia por medio de la elaboración de la respectiva acta.

Criterios BIA

El análisis identificará los servicios críticos considerando los siguientes criterios:

- Tolerancia: Identifica el tiempo que COAC “29 DE OCTUBRE” acepta la indisponibilidad de un determinado servicio y que deberá ser recuperado luego de ese período.
- Impacto: Es el nivel de la afectación económica, imagen y/o en la relación con los clientes.

La ponderación de estos dos criterios tendrá como resultado la criticidad del servicio que estará clasificada de la siguiente forma:

- Extrema: Son los servicios considerados como vitales, siendo fundamental la recuperación del servicio en el menor tiempo posible (a definirse en el procedimiento).
- Alta: Son servicios de importancia y que deberán recuperarse con segunda prioridad (a definirse en el procedimiento).
- Baja: Son servicios que deben recuperare en un tiempo mayor, una vez recuperados los servicios clasificados como extremos y altos (a definirse en el procedimiento).
- Inferior: Son servicios de baja prioridad y podrán ser recuperados en un tiempo mayor a los anteriores, sin que represente impacto al negocio (a definirse en el procedimiento).

Una vez identificado la criticidad del servicio, se evaluaran los procesos, tecnología y proveedores que soportan la provisión del servicio, según el grado de afectación de cada componente, identificando los principales elementos que deberá contar con procedimientos de continuidad de negocio.

La clasificación de la criticidad ha sido considerada con referencia en las mejores prácticas de criticidad como punto de partida:

- Inferior: Son elementos que tienen una afectación igual o inferior al 10% de la disponibilidad del servicio.
- Bajo: Los elementos dentro de esta clasificación, tienen un afectación igual o menor al 20% en la disponibilidad del servicio.
- Medio: Los componentes de los servicios en esta categoría, tendrán una afectación a la disponibilidad del servicio de hasta el 40%.
- Alto: Los componentes de los servicios catalogados con esta criticidad, tienen una afectación superior al 40%.

Los componentes dentro de las clasificaciones de criticidad Media y Alta deben contar obligatoriamente con los procedimientos de continuidad de negocio para garantizar la recuperación de los procesos, tecnologías y/o proveedores que soportan los servicios considerados como críticos.

Las demás clasificaciones podrán o no disponer de los procedimientos de continuidad de negocio, según las necesidades de COAC “29 DE OCTUBRE”.

Tiempos del Negocio

Son los tiempos asociados a la atención de una interrupción en los cuales se enmarcaron las urgencias de los procesos, donde se puede establecer:

MTPD (Periodo Máximo Tolerable de Interrupción), es el plazo después del cual la viabilidad de una organización se verá amenazada de forma irrevocable (financiera, pérdida de reputación, etc.) si no puede reiniciar la entrega de un producto, proceso o servicio específico.

RTO (Tiempo de Recuperación Objetivo), es el tiempo objetivo en el que se debe reiniciar la entrega de un producto, proceso o servicio específico para que la viabilidad de la Organización no se vea amenazada, este tiempo comienza a partir de la invocación del plan. El RTO debe asegurar que no se excede el MTPD.

RPO (Punto de Recuperación Objetivo), es el punto desde el que la información debe ser restaurada para permitir la operación de una actividad una vez que ésta se haya reiniciado.

Tabla 19
BIA - Análisis de Servicios

# Serv.	Nombre Servicio	Descripción	Toler. (MTPD)	Impacto	Criticidad Servicio
18	Gestión de Tecnología de Información	* Planear, desarrollar y mantener hardware, software, infraestructura y datos. * Administrar las relaciones con las líneas de negocio y proveedores	Hasta 3 horas	Superior	Extrema

Tabla 20
BIA – Análisis Procesos

# Serv	Nombre Servicio	Critic.	Sub subproceso	Grado de afectación	Criticidad
18	Gestión de Tecnología de Información	Extrema	Monitoreo, seguimiento y control de hardware y software	Más de 75%	ALTO
18	Gestión de Tecnología de Información	Extrema	Disponibilidad de HD / SW	Más de 75%	ALTO
18	Gestión de Tecnología de Información	Extrema	Identificación de los servicios tecnológicos	Desde 26% hasta el 50%	MEDIO
18	Gestión de Tecnología de Información	Extrema	Atención y resolución de requerimientos de servicios tecnológicos	Desde 26% hasta el 50%	MEDIO

Continua

# Serv	Nombre Servicio	Critic.	Sub subproceso	Grado de afectación	Criticidad
18	Gestión de Tecnología de Información	Extrema	Identificación del inventario de Base de Datos	Desde 26% hasta el 50%	MEDIO
18	Gestión de Tecnología de Información	Extrema	Ejecución de mantenimiento preventivo de Base de Datos	Más de 75%	ALTO
18	Gestión de Tecnología de Información	Extrema	Solución de problemas detectados en el mantenimiento preventivo de Base de Datos	Más de 75%	ALTO
18	Gestión de Tecnología de Información	Extrema	Administración de Base de datos	Más de 75%	ALTO
18	Gestión de Tecnología de Información	Extrema	Disponibilidad de Base de datos	Más de 75%	ALTO
18	Gestión de Tecnología de Información	Extrema	Identificación de usuarios del sistema de los recursos tecnológicos	Desde 26% hasta el 50%	MEDIO
18	Gestión de Tecnología de Información	Extrema	Aseguramiento de los accesos a los recursos tecnológicos	Más de 75%	ALTO
18	Gestión de Tecnología de Información	Extrema	Gestión de los accesos a los recursos tecnológicos	Más de 75%	ALTO

Tabla 21
BIA – Análisis de Aplicativos

Servicio	Criticidad	Sistema/Equipo	Grado afectación	Criticidad de la Aplicativo
Gestión de Tecnología de Información	Extrema	Transaccionalidad de atm	Más de 75%	ALTO
Gestión de Tecnología de Información	Extrema	DGRV (Plan estratégico)	Del 0%	INFERIOR
Gestión de Tecnología de Información	Extrema	Presupuesto	Del 0%	INFERIOR
Gestión de Tecnología de Información	Extrema	Lavado de activos	Más de 75%	ALTO
Gestión de Tecnología de Información	Extrema	Riesgo Operativo	Desde 51% hasta el 75%	ALTO
Gestión de Tecnología de Información	Extrema	Riesgo de Crédito	Más de 75%	ALTO
Gestión de Tecnología de Información	Extrema	Tesorería	Más de 75%	ALTO
Gestión de Tecnología de Información	Extrema	Cash Management	Más de 75%	ALTO
Gestión de Tecnología de Información	Extrema	Web Informativa	Desde 26% hasta el 50%	MEDIO
Gestión de Tecnología de Información	Extrema	INTRANET	Del 0%	INFERIOR
Gestión de Tecnología de Información	Extrema	Core - Depósitos a Plazo	Más de 75%	ALTO
Gestión de Tecnología de Información	Extrema	Correo electrónico on-line	Desde 26% hasta el 50%	MEDIO
Gestión de Tecnología de Información	Extrema	Firewall	Más de 75%	ALTO

Continua 

Servicio	Criticidad	Sistema/Equipo	Grado afectación	Criticidad de la Aplicativo
Gestión de Tecnología de Información	Extrema	Telefonía IP	Desde 26% hasta el 50%	MEDIO
Gestión de Tecnología de Información	Extrema	CRM	Del 0%	INFERIOR
Gestión de Tecnología de Información	Extrema	DWH	Del 0%	INFERIOR
Gestión de Tecnología de Información	Extrema	SWITCH TRANSACCIONAL ATM	Más de 75%	ALTO
Gestión de Tecnología de Información	Extrema	Directorio Activo	Más de 75%	ALTO
Gestión de Tecnología de Información	Extrema	Cámara de Compensación	Desde 26% hasta el 50%	MEDIO
Gestión de Tecnología de Información	Extrema	Redetrans	Desde 26% hasta el 50%	MEDIO
Gestión de Tecnología de Información	Extrema	Riesgo Mercado y Liquidez	Desde 26% hasta el 50%	MEDIO
Gestión de Tecnología de Información	Extrema	Core -cajas	Más de 75%	ALTO
Gestión de Tecnología de Información	Extrema	Core - Certificados de aportación	Desde 1% hasta el 25%	BAJO
Gestión de Tecnología de Información	Extrema	Core - Depósitos a la vista	Más de 75%	ALTO
Gestión de Tecnología de Información	Extrema	Core - Crédito	Desde 26% hasta el 50%	MEDIO
Gestión de Tecnología de Información	Extrema	Core- Activos Fijos	Desde 1% hasta el 25%	BAJO
Gestión de Tecnología de Información	Extrema	Core Contabilidad	Desde 26% hasta el 50%	MEDIO

Continua

Servicio	Criticidad	Sistema/Equipo	Grado afectación	Criticidad de la Aplicativo
Gestión de Tecnología de Información	Extrema	Core- Tesorería	Desde 26% hasta el 50%	MEDIO
Gestión de Tecnología de Información	Extrema	Core-Nómina	Desde 26% hasta el 50%	MEDIO
Gestión de Tecnología de Información	Extrema	Core- Facturación Electrónica	Desde 51% hasta el 75%	ALTO
Gestión de Tecnología de Información	Extrema	Core -Compras y Proveedores	Desde 1% hasta el 25%	BAJO
Gestión de Tecnología de Información	Extrema	Core Seguridades	Más de 75%	ALTO
Gestión de Tecnología de Información	Extrema	Core Clientes	Desde 51% hasta el 75%	ALTO
Gestión de Tecnología de Información	Extrema	Core-Cobranzas	Más de 75%	ALTO
Gestión de Tecnología de Información	Extrema	Core-Firmas	Más de 75%	ALTO
Gestión de Tecnología de Información	Extrema	Switch S 29	Más de 75%	ALTO

Tabla 22
BIA - Evaluación de Riesgos Macro proceso Gestión Informática

PROCESOS	SUBPROCESOS	Sub-subprocesos	Proceso Crítico
Planificación de gestión de tecnología de la información	Gestión integral de proyectos de tecnología de la información	Recepción de propuestas de proyectos de Tecnología de Información	NO CRITICO
		Elaboración del Ante Proyecto	NO CRITICO
		Evaluación del Ante Proyecto por las áreas involucradas	NO CRITICO
		Aprobación y priorización del Ante Proyecto	NO CRITICO
		Diseño y planificación del proyecto	NO CRITICO
		Ejecución del proyecto	NO CRITICO
		Seguimiento del proyecto de TI	NO CRITICO
		Evaluación de cumplimiento del proyecto de TI solicitado	NO CRITICO
		Cierre del proyecto	NO CRITICO
GESTIÓN DE PLATAFORMA TECNOLÓGICA	Control y soporte de hardware y software	Identificación del Inventario de Hardware y Software	NO CRITICO
		Planificación de mantenimiento preventivo de hardware y software	NO CRITICO
		Ejecución de mantenimiento preventivo de hardware y software	NO CRITICO
		Solución de problemas detectados en el mantenimiento preventivo	NO CRITICO
		Monitoreo, seguimiento y control de hardware y software	CRITICO
		Disponibilidad de HD / SW disponible	CRITICO
		Identificación de los servicios tecnológicos	CRITICO

Continua

Gestión de producción	Administración de servicios de tecnología de información	Recepción de requerimientos de atención de incidentes y problemas	NO CRITICO
		Atención y resolución de requerimientos de servicios tecnológicos	CRITICO
		Medición de NAS y OLA del servicio tecnológico	NO CRITICO
Gestión de base de datos	Administración de base de datos	Identificación del inventario de Base de Datos	CRITICO
		Planificación de mantenimiento preventivo de Base de Datos	NO CRITICO
		Ejecución de mantenimiento preventivo de Base de Datos	CRITICO
		Solución de problemas detectados en el mantenimiento preventivo de Base de Datos	CRITICO
		Gestión de Minería de Datos (atención de requerimientos)	NO CRITICO
		Administración de Base de datos	CRITICO
		Disponibilidad de Base de datos	CRITICO
Gestión de seguridad y control de la información	Seguridad y control de la información	Identificación de usuarios del sistema de los recursos tecnológicos	CRITICO
		Aseguramiento de los accesos a los recursos tecnológicos	CRITICO
		Gestión de los accesos a los recursos tecnológicos	CRITICO
		Evaluación y seguimiento de control de accesos aplicados a los recursos tecnológicos	NO CRITICO
Gestión de desarrollo de software	Desarrollo e implementación de software	Recepción requerimiento de desarrollo de software	NO CRITICO
		Realizar levantamiento de información, evaluar y planificar requerimientos solicitados	NO CRITICO
		Ejecutar el desarrollo del requerimiento solicitado	NO CRITICO

Continua

		Verificar y validar funcionalidad del requerimiento y retroalimentar en caso de inconsistencias (pruebas)	NO CRITICO
		Gestión de aseguramiento de calidad	NO CRITICO
		Gestionar versionamiento de fuentes y ejecutables	NO CRITICO
		Puesta en producción	NO CRITICO
		Realizar seguimiento post producción del requerimiento	NO CRITICO

RIESGOS DEL MACROPROCESO GESTIÓN INFORMÁTICA

VALORACION DEL RIESGO

PROCESO: GESTIÓN DE PLATAFORMA TECNOLÓGICA

SUBPROCESO: CONTROL Y SOPORTE DE HARDWARE Y SOFTWARE

Tabla 23
Gestión de Plataforma Tecnológica

Descripción Riesgo	Escena.	Evento	Causa	Descripción Control	Oport	Aut	Efect. Control	Riesg. Res.
Daños de Hardware y Software (destrucción y/o deterioro de equipos, centrales de Comunicaciones, equipos de Monitoreo, equipos Seguridad, equipos Almacenamiento) debido a un incendio	Incendio	Alto grado de afectación de HD/SW (Data Center) de la Cooperativa debido a la exposición al fuego.	No disponibilidad de HD/SW (Data Center) que ofrece los servicios tecnológicos de la Cooperativa incluidos monitoreo, seguimiento y control.	Backup de equipos críticos en el Sitio Alterno	CV	AT	OPTIMO	BAJO
				Sensores de humo, alarmas y sistema automático de extinción de incendios	CV	AT	OPTIMO	
				Supervisión y mantenimientos periódicos del cableado Eléctrico del Data Center principal y alterno y mal uso de los toma corrientes.	PV	MA	OPTIMO	

Continua

Descripción Riesgo	Escena.	Evento	Causa	Descripción Control	Oport	Aut	Efect. Control	Riesg. Res.
				Equipo de personal de emergencia (Brigadistas).	PV	MA	OPTIMO	
				Capacitación a los brigadistas sobre la ubicación y uso de los equipos contra incendio (grifos, gabinetes de manga, extinguidores).	PV	MA	REGULAR	
				Mantenimiento y conservación del sistema y equipos de extinción de incendios.	PV, CV	MA	OPTIMO	
Daños en el Hardware (equipos, Centrales de Comunicaciones, Servidores) por alojamiento de ceniza debido a una	Erupción volcánica	Afectación a los servicios tecnológicos que ofrece la DIC debido al alojamiento de ceniza en los equipos, centrales de	No disponibilidad de equipos, centrales de comunicación y servidores	Backup de equipos críticos en el Sitio Alterno	CV	AT	OPTIMO	BAJO
				Sistema de ventilación adecuada	PV, CV	AT	OPTIMO	
				Supervisión y Mantenimiento	PV	MA	OPTIMO	

Continua

Descripción Riesgo	Escena.	Evento	Causa	Descripción Control	Oport	Aut	Efect. Control	Riesg. Res.
erupción volcánica		comunicación y servidores (Data Center).	que provoca errores en los servicios tecnológicos de la Cooperativa incluido monitoreo, seguimiento y control de Hardware.	de ductos de ventilación				
				Simulacros de Evacuación a sitio seguro	PV	MA	OPTIMO	
				Capacitación al personal sobre las afectaciones de la erupción volcánica como (salud, equipos).	PV	MA	REGULAR	
Daño en la Infraestructura Tecnológica de la Administración Central debido a un de terremoto	Terremoto	Daño en la Infraestructura del (servicios de comunicaciones, abastecimiento eléctrico)	No disponibilidad de servicios tecnológicos de la Cooperativa incluido monitoreo, seguimiento y control HD/SW.	Tener backup de equipos críticos en el Sitio Alterno	CV	AT	OPTIMO	BAJO
				Alimentación de energía secundaria (UPS, Planta Generadora) para todos los Equipos Críticos (de Comunicación, Servidores, etc.)	CV	AT	OPTIMO	

Continua

Descripción Riesgo	Escena.	Evento	Causa	Descripción Control	Oport	Aut	Efect. Control	Riesg. Res.
				Señalización y supervisión de rutas de evacuación (puertas, escaleras, salidas de emergencia, punto de encuentro seguro)	PV	MA	REGULAR	
				Formación de Brigadas de Evacuación	PV	MA	REGULAR	
				Telecomunicaciones Backup con las mismas características en los Enlaces de Comunicación de proveedores.	CV	AT	OPTIMO	
Daños en la Infraestructura Eléctrica de la Administración	Corte de suministro	Daños en DATA CENTER y	No disponibilidad de servicios	Tener backup de equipos críticos en el Sitio Alterno	CV	AT	OPTIMO	BAJO

Continua

Descripción Riesgo	Escena.	Evento	Causa	Descripción Control	Oport	Aut	Efect. Control	Riesg. Res.
Central debido a una sobrecarga de energía.	ELECTRICO	equipos de Computo	tecnológicos de la Cooperativa incluido monitoreo, seguimiento y control HD/SW.	Alimentación de energía secundaria (UPS, Planta Generadora) para todos los Equipos Críticos (de Comunicación, Servidores, etc.)	CV	AT	OPTIMO	
				Interruptores con reguladores de voltaje, que no permite el paso de sobretensión y cortocircuito.	PV	AT	OPTIMO	
				Mantenimiento de infraestructura eléctrica	PV	MA	BUENO	
Falla y caída de enlaces de Telecomunicación y	FALLA SERVICIO DE	Falla y caída de Telecomunicación en la	No disponibilidad de servicios	Tener backup de equipos críticos en el Sitio Alterno	CV	AT	OPTIMO	BAJO

Continua

Descripción Riesgo	Escena.	Evento	Causa	Descripción Control	Oport	Aut	Efect. Control	Riesg. Res.
capacidad de trasmitir datos de un sitio a otro	COMUNICACIÓN	Administración Central	tecnológicos de la Cooperativa.	Proveedor de Telecomunicaciones Backup con las mismas características en los Enlaces de Comunicación.	PV	AT	OPTIMO	
				Mantenimiento y revisión de equipos y enlaces de comunicación.	PV	MA	BUENO	
La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada	CAIDA DEL SISTEMA	Caída del CORE Bancario	No disponibilidad e interrupción de servicios tecnológicos de la Cooperativa	Tener backup de equipos críticos en el Sitio Alterno	CV	AT	OPTIMO	BAJO
				Soporte de proveedores de emergencia para caída del sistema	CV	AT	OPTIMO	
				Procedimiento de restablecimiento de sistema	CV	AT	OPTIMO	
				Mantenimiento de Hardware (Servidores, equipos de	PV	MA	BUENO	

Continua

Descripción Riesgo	Escena.	Evento	Causa	Descripción Control	Oport	Aut	Efect. Control	Riesg. Res.
				cómputo) que soportan el CORE				
Sobrecarga en los recursos computacionales provoca la caída del CORE por la pérdida de la conectividad de la red por el consumo del ancho de banda	Deneg. de servicio	Caída del CORE y negación de Servicio a usuarios legítimos	No disponibilidad e interrupción de servicios tecnológicos de la Cooperativa	Tener backup de equipos críticos en el Sitio Alterno	CV	AT	OPTIMO	BAJO
				Políticas de acceso mediante Firewall	PV	AT	OPTIMO	
				Asignación de IPs aisladas de la red para evitar accesos no permitidos	PV	AT	OPTIMO	
				Escaneo de vulnerabilidades (Ethical Hacking)	DT	MA	DEFICIENTE	

Continua

PROCESO: GESTIÓN DE PRODUCCIÓN

SUBPROCESO: ADMINISTRACIÓN DE SERVICIOS DE TECNOLOGÍA DE INFORMACIÓN

Tabla 24
Gestión de Producción

Descripción riesgo	Escen	Evento	Causa	Descripción	Opor	Aut	Efect. Ctrl.	Riesg res.
Daños de hardware y software (destrucción y/o deterioro del ambiente de producción debido a un incendio	Incendio	Alto grado de afectación de hd/sw del ambiente de producción debido a la exposición al fuego.	No disponibilidad de servicios tecnológicos de producción para la identificación, atención y resolución de requerimientos	Backup de equipos críticos en el sitio alterno	Cv	At	Optimo	Bajo
				Sensores de humo, alarmas y sistema automático de extinción de incendios	Cv	At	Optimo	
				Supervisión y mantenimientos periódicos del cableado eléctrico del data center principal y alterno y mal uso de los toma corrientes.	Pv	Ma	Optimo	
				Equipo de personal de emergencia (brigadistas).	Pv	Ma	Optimo	

Continua

				Capacitación a los brigadistas sobre la ubicación y uso de los equipos contra incendio	Pv	Ma	Regular	
				Mantenimiento y conservación del sistema y equipos de extinción de incendios.	Pv, cv	Ma	Optimo	
daños en el hardware (equipos, centrales de comunicaciones, servidores) por alojamiento de ceniza en el ambiente de producción debido a una erupción volcánica	Erupción volcánica	Afectación a los servicios tecnológicos de producción debido al alojamiento de ceniza en los equipos, centrales de comunicación y servidores.	No disponibilidad de equipos, centrales de comunicación y servidores que provoca errores en la identificación, atención y resolución de los servicios tecnológicos de la producción.	Backup de equipos críticos en el sitio alterno	Cv	At	Optimo	Bajo
				Sistema de ventilación adecuado	Pv, cv	At	Optimo	
				Supervisión y mantenimiento de ductos de ventilación	Pv	Ma	Optimo	
				Simulacros de evacuación a sitio seguro	Pv	Ma	Optimo	
				Capacitación al personal sobre las afectaciones de la erupción volcánica como	Pv	Ma	Regular	

Continua 

Daño en la infraestructura tecnológica de producción a causa de terremoto	Terrem.	Daño en la infraestructura de producción	No disponibilidad de servicios tecnológicos de producción para la identificación, atención y resolución de requerimientos,	Tener backup de equipos críticos en el sitio alterno	Cv	At	Optimo	Bajo
				Alimentación de energía secundaria	Cv	At	Optimo	
				Señalización y supervisión de rutas de evacuación	Pv	Ma	Regular	
				Formación de brigadas de evacuación	Pv	Ma	Regular	
				Telecomunicaciones backup con las mismas características en los enlaces de comunicación de proveedores.	Cv	At	Optimo	
Daños en la infraestructura eléctrica de producción a	Corte de sum. Eléctrico	Daños a equipos de cómputo del ambiente de	No disponibilidad de servicios	Tener backup de equipos críticos en el sitio alterno	Cv	At	Optimo	Bajo

Continua

causa de una sobrecarga de energía.		producción y soporta servicios tecnológicos.	tecnológicos de producción para la identificación, atención y resolución de requerimientos,	Alimentación de energía secundaria	Cv	At	Optimo	
				Interruptores con reguladores de voltaje, que no permite el paso de sobretensión y cortocircuito.	Pv	At	Optimo	
				Mantenimiento infraestructura eléctrica	Pv	Ma	Bueno	
Falla y caída de enlaces de telecomunicación y capacidad de trasmitir datos producción.	Falla servicio de comunicación	Falla y caída de telecomunicación en el ambiente de producción	No disponibilidad de servicios tecnológicos de producción para la identificación, atención y resolución de requerimientos,	Tener backup de equipos críticos en el sitio alterno	Cv	At	Optimo	Bajo
				Proveedor de telecomunicaciones backup con las mismas características en los enlaces de comunicación.	Pv	At	Optimo	
				Mantenimiento y revisión de equipos y enlaces de comunicación.	Pv	Ma	Bueno	

Continua

La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada en producción	Caida del sistema	Caída del core bancario con afectación a los servicios tecnológicos de producción	No disponibilidad de servicios tecnológicos de producción para la identificación, atención y resolución de requerimientos,	Tener backup de equipos críticos en el sitio alterno	Cv	At	Optimo	Bajo
				Soporte de proveedores de emergencia para caída del sistema	Cv	At	Optimo	
				Procedimiento de restablecimiento de sistema	Cv	At	Optimo	
				Mantenimiento de hardware (servidores, equipos de cómputo) que soportan el core	Pv	Ma	Bueno	
sobrecarga en los recursos computacionales provoca la caída del core por la pérdida de la conectividad de la red por el consumo del ancho de banda	Denegación de servicio	Caída del core y negación de servicio a usuarios legítimos de producción	No disponibilidad de servicios tecnológicos de producción para la identificación, atención y resolución de requerimientos,	Tener backup de equipos críticos en el sitio alterno	Cv	At	Optimo	Bajo
				Políticas de acceso mediante firewall	Pv	At	Optimo	
				Asignación de ips aisladas de la red para evitar accesos no permitidos	Pv	At	Optimo	

Valoración del riesgo

PROCESO: GESTIÓN DE BASE DE DATOS

SUBPROCESO: ADMINISTRACION DE BASE DE DATOS

Tabla 25
Gestión de Base de Datos

Descripción riesgo	Escenario	Evento	Causa	Descripción	Oportunidad	Automatización	Efectividad control	Riesgo residual
Daños de hardware y software (destrucción y/o deterioro de los servidores de bases de datos) a causa de un incendio	Incendio	Alto grado de afectación de hd/sw de (bases de datos) de la cooperativa debido a la exposición al fuego.	No disponibilidad de servidores de base de datos donde se encuentra almacenado información de la cooperativa	Replica de base de datos en el sitio alterno	Cv	At	Optimo	Bajo
				Sensores de humo, alarmas y sistema automático de extinción de incendios	Cv	At	Optimo	
				Supervisión y mantenimientos periódicos del cableado eléctrico del data center principal y alterno y mal uso de los toma corrientes.	Pv	Ma	Optimo	

Continua

Descripción riesgo	Escenario	Evento	Causa	Descripción	Oportunidad	Automatización	Efectividad control	Riesgo residual
				Equipo de personal de emergencia (brigadistas).	Pv	Ma	Optimo	
				Capacitación a los brigadistas sobre la ubicación y uso de los equipos contra incendio (grifos, gabinetes de manga, extinguidores).	Pv	Ma	Regular	
				Mantenimiento y conservación del sistema y equipos de extinción de incendios.	Pv, cv	Ma	Optimo	
daños en el hardware (servidores de base de	Erupción volcánica	Afectación a los servidores	No disponibilidad de servidores	Replica de base de datos en el sitio alterno	Cv	At	Optimo	Bajo

Continua

Descripción riesgo	Escenario	Evento	Causa	Descripción	Oportunidad	Automatización	Efectividad control	Riesgo residual
datos) por alojamiento de ceniza debido a una erupción volcánica		de base de datos	de base de datos que provoca errores en la administración, mantenimiento y solución de problemas detectados en el almacenamiento de información.	Sistema de ventilación adecuado	Pv, cv	At	Optimo	
				Supervisión y mantenimiento de ductos de ventilación	Pv	Ma	Optimo	
				Simulacros de evacuación a sitio seguro	Pv	Ma	Optimo	
				Capacitación al personal sobre las afectaciones de la erupción volcánica como (salud, equipos).	Pv	Ma	Regular	
Daño en la infraestructura tecnológica de los servidores de bases de datos debido a un de terremoto	Terremoto	Daño en la infraestructura de los servidores de base de datos	No disponibilidad de servidores de base de datos para la administración, mantenimiento y	Replica de base de datos en el sitio alterno	Cv	At	Optimo	Bajo
				Alimentación de energía secundarias (ups, planta generadora) para todos los servidores de	Cv	At	Optimo	

Continua

Descripción riesgo	Escenario	Evento	Causa	Descripción	Oportunidad	Automatización	Efectividad control	Riesgo residual
			solución de problemas detectados en el almacenamiento de información.	las bases de datos				
				Señalización y supervisión de rutas de evacuación (puertas, escaleras, salidas de emergencia, punto de encuentro seguro)	Pv	Ma	Regular	
				Formación de brigadas de evacuación	Pv	Ma	Regular	
				Telecomunicaciones backup con las mismas características en los enlaces de comunicación de proveedores.	Cv	At	Optimo	

Continua

Descripción riesgo	Escenario	Evento	Causa	Descripción	Oportunidad	Automatización	Efectividad control	Riesgo residual
Daños en la infraestructura eléctrica de los servidores de base de datos debido a una de una sobrecarga de energía.	Corte de suministro electrico	Daños en servidores de base de datos	No disponibilidad de servidores de base de datos para la administración, mantenimiento y solución de problemas detectados en el almacenamiento de información.	Replica de base de datos en el sitio alterno	Cv	At	Optimo	Bajo
				Alimentación de energía secundarias (ups, planta generadora) para servidores de las bases de datos	Cv	At	Optimo	
				Interruptores con reguladores de voltaje, que no permite el paso de sobretensión y cortocircuito.	Pv	At	Optimo	
				Mantenimiento infraestructura eléctrica de servidores de	Pv	Ma	Bueno	

Continua

Descripción riesgo	Escenario	Evento	Causa	Descripción	Oportunidad	Automatización	Efectividad control	Riesgo residual
				las bases de datos				
Falla y caída de enlaces de telecomunicación y capacidad de trasmitir datos de los servidores de base de datos.	Falla servicio de comunicación	Falla y caída de telecomunicación en los servidores de base de datos	No disponibilidad de servidores de base de datos.	Replica de base de datos en el sitio alterno	Cv	At	Optimo	Bajo
				Proveedor de telecomunicaciones backup con las mismas características en los enlaces de comunicación.	Pv	At	Optimo	
				Mantenimiento y revisión de equipos y enlaces de comunicación de las bases de datos.	Pv	Ma	Bueno	
Daños y falla en la capacidad de los soportes	Degradación de los soportes de almacena	Falla en el almacenamiento de información	No disponibilidad de base de datos para su	Respaldo de bases de datos en cintas	Pv	Ma	Bueno	Bajo

Continua

Descripción riesgo	Escenario	Evento	Causa	Descripción	Oportunidad	Automatización	Efectividad control	Riesgo residual
almacenamiento de información	miento de la información	en base de datos	administración, mantenimiento y solución de problemas	Comprobación de la información respaldada de las bases de datos	Pv	Ma	Bueno	
				Mantenimiento y revisión de soportes de almacenamiento	Pv	Ma	Bueno	
La carencia de recursos suficientes provoca la caída de la base de datos cuando la carga de trabajo es desmesurada	Caida del sistema	Caída de la base de datos	No disponibilidad de base de datos para su administración, mantenimiento y solución de problemas	Replica de base de datos en el sitio alterno	Cv	At	Optimo	Bajo
				Soporte de proveedores emergentes para caída de bases de datos	Cv	At	Optimo	
				Procedimiento de restauración de bases de datos	Cv	At	Optimo	

Continua

Descripción riesgo	Escenario	Evento	Causa	Descripción	Oportunidad	Automatización	Efectividad control	Riesgo residual
				Mantenimiento de hardware (servidores, equipos de cómputo) que soportan las bases de datos	Pv	Ma	Bueno	
sobrecarga en los recursos computacionales provoca la caída de base de datos por la pérdida de la conectividad de la red por el consumo del ancho de banda	Denegación de servicio	Caída de la base de datos y negación de servicio a usuarios legítimos	No disponibilidad de base de datos para su administración, mantenimiento y solución de problemas	Replica de base de datos en el sitio alterno	Cv	At	Optimo	Bajo
				Políticas de acceso mediante firewall de base de datos	Pv	At	Optimo	
				Asignación de ips aisladas de la red para evitar accesos no permitidos	Pv	At	Optimo	

PROCESO: GESTIÓN DE SEGURIDAD Y CONTROL DE LA INFORMACIÓN

SUBPROCESO: SEGURIDAD Y CONTROL DE LA INFORMACIÓN

Tabla 26
Gestión de Seguridad y Control de la Información

Descripción riesgo	Escenario	Evento	Causa	Descripción	Oportunidad	Autom	Efect control	Riesgo resid
Daños de hardware y software (destrucción y/o deterioro de los equipos, centrales de comunicaciones, ambiente de producción, equipos de monitoreo, seguridad, almacenamiento) a causa de un incendio	Incendio	Alto grado de afectación de hd/sw (data center) de la cooperativa debido a la exposición al fuego.	No disponibilidad de hd/sw (data center) que ofrece los servicios tecnológicos de la cooperativa incluido identificación de usuarios, aseguramiento y gestión de accesos a los recursos tecnológicos	Backup de equipos críticos en el sitio alterno	Cv	At	Optimo	Bajo
				Sensores de humo, alarmas y sistema automático de extinción de incendios	Cv	At	Optimo	
				Supervisión y mantenimientos periódicos del cableado eléctrico del data center principal y alterno y mal uso de los toma corrientes.	Pv	Ma	Optimo	
				Equipo de personal de emergencia	Pv	Ma	Optimo	

Continua

				Capacitación a los brigadistas sobre la ubicación y uso de los equipos contra incendio	Pv	Ma	Regular	
				Mantenimiento y conservación del sistema y equipos de extinción de incendios.	Pv, cv	Ma	Optimo	
daños en el hardware (equipos, centrales de comunicaciones, servidores) por alojamiento de ceniza debido a una erupción volcánica	Erupción volcánica	Afectación a los servicios tecnológicos que ofrece la dic debido al alojamiento de ceniza en los equipos, centrales de comunicación y servidores (data center).	No disponibilidad de equipos, centrales de comunicación y servidores que provoca errores en los servicios tecnológicos de la cooperativa incluido identificación de usuarios,	Backup de equipos críticos en el sitio alterno	Cv	At	Optimo	Bajo
				Sistema de ventilación adecuado	Pv, cv	At	Optimo	
				Supervisión y mantenimiento de ductos de ventilación	Pv	Ma	Optimo	
				Simulacros de evacuación a sitio seguro	Pv	Ma	Optimo	
				Capacitación al personal sobre las afectaciones de la erupción volcánica como (salud, equipos).	Pv	Ma	Regular	

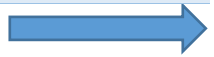
Continua

			aseguramiento y gestión de accesos a los recursos tecnológicos				
Daño en la infraestructura tecnológica de la administración central a causa de terremoto	Terremoto	Daño en la infraestructura del data center (servicios de comunicaciones, abastecimiento eléctrico)	No disponibilidad de servicios tecnológicos de la cooperativa incluido identificación de usuarios, aseguramiento y gestión de accesos a los recursos tecnológicos	Tener backup de equipos críticos en el sitio alterno	Cv	At	Optimo	Bajo
				Alimentación de energía secundaria para todos los equipos críticos	Cv	At	Optimo	
				Señalización y supervisión de rutas de evacuación	Pv	Ma	Regular	
				Formación de brigadas de evacuación	Pv	Ma	Regular	

Continua

				Telecomunicaciones backup con las mismas características en los enlaces de comunicación de proveedores.	Cv	At	Optimo	
Daños en la infraestructura eléctrica de la administración central a causa de una sobrecarga de energía.	Corte de suministro electrico	Daños en data center y equipos de computo	No disponibilidad de servicios tecnológicos de la cooperativa incluido identificación de usuarios, aseguramiento y gestión de accesos a los recursos tecnológicos	Tener backup de equipos críticos en el sitio alterno	Cv	At	Optimo	Bajo
				Alimentación de energía secundaria para todos los equipos críticos	Cv	At	Optimo	
				Interruptores con reguladores de voltaje, que no permite el paso de sobretensión y cortocircuito.	Pv	At	Optimo	
				Mantenimiento infraestructura eléctrica	Pv	Ma	Bueno	
Falla y caída de enlaces de telecomunicación y	Falla servicio de comunicación	Falla y caída de telecomunicación en la	No disponibilidad de servicios	Tener backup de equipos críticos en el sitio alterno	Cv	At	Optimo	Bajo

Continua



capacidad de trasmitir datos de un sitio a otro		administración central	tecnológicos de la cooperativa.	Proveedor de telecomunicaciones backup con las mismas características en los enlaces de comunicación.	Pv	At	Optimo	
				Mantenimiento y revisión de equipos y enlaces de comunicación.	Pv	Ma	Bueno	
La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada	Caida del sistema	Caída del core bancario	No disponibilidad e interrupción de servicios tecnológicos de la cooperativa	Tener backup de equipos críticos en el sitio alterno	Cv	At	Optimo	Bajo
				Soporte de proveedores de emergencia para caída del sistema	Cv	At	Optimo	
				Procedimiento de restablecimiento de sistema	Cv	At	Optimo	
				Mantenimiento de hardware (servidores, equipos de cómputo) que soportan el core	Pv	Ma	Bueno	

Continua

Acceso indebido, sin autorización o contra derecho a sistemas de tratamiento de la información	Acesso no autorizado	Desciframiento de los códigos de acceso o passwords y violación de programas y sistemas	Sabotaje informático, borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del core, espionaje informático o fuga de datos.	Tener backup de equipos críticos en el sitio alterno	Cv	At	Optimo	Bajo
				Políticas de acceso mediante firewall	Pv	At	Optimo	
				Asignación de ips aisladas de la red para evitar accesos no autorizados	Pv	At	Optimo	
				Escaneo de vulnerabilidades (ethical hacking)	Dt	Ma	Deficiente	
sobrecarga en los recursos computacionales provoca la caída del core por la pérdida de la	Denegación de servicio	Caída del core y negación de servicio a usuarios legítimos	No disponibilidad e interrupción de servicios tecnológicos de la cooperativa	Tener backup de equipos críticos en el sitio alterno	Cv	At	Optimo	Bajo
				Políticas de acceso mediante firewall	Pv	At	Optimo	

Continua

conectividad de la red por el consumo del ancho de banda		incluido identificación de usuarios, aseguramiento y gestión de accesos a los recursos tecnológicos	Asignación de ips aisladas de la red para evitar accesos no permitidos	Pv	At	Optimo
			Escaneo de vulnerabilidades (ethical hacking)	Dt	Ma	Deficiente

CAPÍTULO IV
DISEÑO Y APLICACIÓN

En este capítulo se presentara el planteamiento de los planes de acción en caso de presentarse un evento que comprometa el correcto flujo de los procesos de la COAC “29 de Octubre” para esto se considerara los procedimientos de comunicación y gestión de incidentes necesarios para un adecuada activación y ejecución del plan de continuidad del negocio. En tal sentido en este capítulo se presentaran los siguientes ítems

- Plan de Comunicación de Crisis
- Estrategias de Continuidad de negocio
- Procedimientos de Continuidad y Reanudación
- Plan de Pruebas

4.1. PLAN DE COMUNICACIÓN DE CRISIS

En esta sección se detallara los procesos de comunicación necesarios en caso de presentarse un incidente de crisis, así como también la forma de ejecutarlos y sus respectivos responsables. Mismos que servirán de base para la activación del plan de continuidad del Negocio

4.1.1 Síntesis

En la COAC 29 de Octubre es de suma importancia crear, validar y ejecutar planes de comunicación que incluyan a todos los responsables de la ejecución de actividades incluidas en el plan de continuidad es por ello que se han definido ciertas actividades que aportaran al correcto flujo de la comunicación:

a. Identificar y estructurar un equipo que se encargue de la comunicación de los eventos de crisis.

b. Establecer las vías de comunicación más factibles para la comunicación de entes internos y externos la compañía de tal forma las notificaciones se den de una forma adecuada

c. Contemplar dentro de los planes de comunicación a todo el personal que pueda verse afectado por un evento de crisis dentro de las instalaciones de la organización.

4.1.2 Objetivo

Establecer vías de comunicación efectivas que nos permitan alcanzar al mayor porcentaje de personal que pudiera verse afectado en caso de presentarse un evento o incidente que obligue a la COAC 29 de Octubre a detener sus actividades y operación normal.

4.1.3 Alcance

El plan de comunicación incluirá a todas las áreas de negocio de la Administración Central de la COAC “29 de Octubre” así como también a los proveedores externos considerados como claves para la ejecución del plan de continuidad

Escenarios considerados para comunicación:

- Fuego
- Terremoto
- Erupción Volcánica
- Corte de Suministro Eléctrico

- Fallos de servicio de Comunicación
- Degradación de los soportes de almacenamiento de la información
- Caída del sistema por agotamiento de recursos
- Acceso no autorizado
- Denegación de servicio

Equipo de Comunicación

El personal de Comunicación de Crisis consta de:

- Coordinador de Comunicación de Crisis: es el responsable de gestionar los recursos de comunicación para la notificación de eventos de crisis de una forma organizada y oportuna
- Asesor Legal: Encargado de ejecutar e informar sobre normativas legales y requerimientos de entes de control en caso de presentarse un evento de crisis
- Staff de Comunicación: encarado de la parte operativa de la comunicación
- Voceros internos y externos: encargados de transmitir la información pertinente al público relacionado

Estrategias de Comunicación en Crisis.- Las estrategias a tomar se dividen en:

Antes.- Actividades de prevención y preparación

Informarse y dimensionar los posibles eventos de crisis que puedan afectar al correcto flujo de las operaciones de la Administración central de la COAC “29 de Octubre”.

Mantener una base actualizada del personal así como también asegurarse que los mecanismos de comunicación habilitados en caso de un incidente operen de una forma adecuada

Durante.- actividades de control y operación alterna

- **Análisis de la situación.**

Ejecución de un análisis objetivo del incidente presentado el cual tiene como propósito identificar el origen del problema así como también las consecuencias internas y externas a la organización dimensionando el impacto final que tendrá sobre la operación del negocio.

.

- **Planteamiento de estrategias de comunicación.**

Una vez realizado el análisis de la situación y tomando en cuenta el posible impacto sobre la organización se deberá evaluar cuales son los recursos necesarios y la forma más adecuada de comunicación del incidente.
Al momento de identificar la mejor estrategia de comunicación se deben considerar ciertas pautas como son:

- Todos los incidentes tienen una repercusión en la imagen de la compañía por lo cual el canal de comunicación debe permitir brindar un mensaje acorde a la magnitud del incidente y ser capaz de llegar a la mayor cantidad de personas.

- El coordinador de comunicación en crisis es el responsable de proveer el mensaje que será entregado a todos los involucrados, mismo que deberá corresponder a la versión oficial de lo ocurrido.

- La cobertura del mensaje dependerá de la magnitud del incidente por lo que este únicamente deberá llegar a los puntos o personal que se vea afectado de una forma prudente y cautelosa tomando en cuenta que los vacíos pueden dar cabida a la tergiversación de la información

- Los comentarios de los clientes son fundamentales por lo que se deberán iniciar procesos de retroalimentación que permitan estabilizar los procesos.

- **Prioridades a la hora de informar**

Una vez activado el plan de comunicación se debe asegurar que nuestro mensaje llegue a todos nuestros grupos de interés procurando que nuestra versión sea la primera que conozcan priorizando la comunicación con entes de control, entes de socorro, autoridades y funcionarios claves de la organización.

Después.- actividades de estabilización

Fin de la crisis, evaluación y retroalimentación.

Una vez que se ha logrado estabilizar los procesos de negocio es necesario iniciar un proceso de evaluación que nos permita identificar fortalezas y deficiencias durante cada una de las fases del proceso de comunicación estableciendo cambios que nos permitan mejorar la capacidad de respuesta del personal.

Adicionalmente se debe monitorear el impacto de la crisis sobre la confianza de nuestros grupos de interés a fin de implementar procedimientos de mejora y optimización.

Organización de Comunicación de Crisis

Tabla 27

Descripción general de los grupos de recuperación

Posición / Rol	Prioridad	Crítico (S/N)
Coordinador de Comunicación en Crisis	1	S
Staff de Comunicación	2	S
Asesor Legal	1	S
Voceros	3	S

Leyenda:

Posición: Posición o Rol perteneciente al grupo de Comunicación en Crisis.

Prioridad: Orden de importancia de las posiciones.1 es el primero en ejecutar, 2 el segundo y así sucesivamente.

Criticidad: Determina si es una posición crítica/indispensable dentro del Grupo. S=Sí, N=No Crítico.

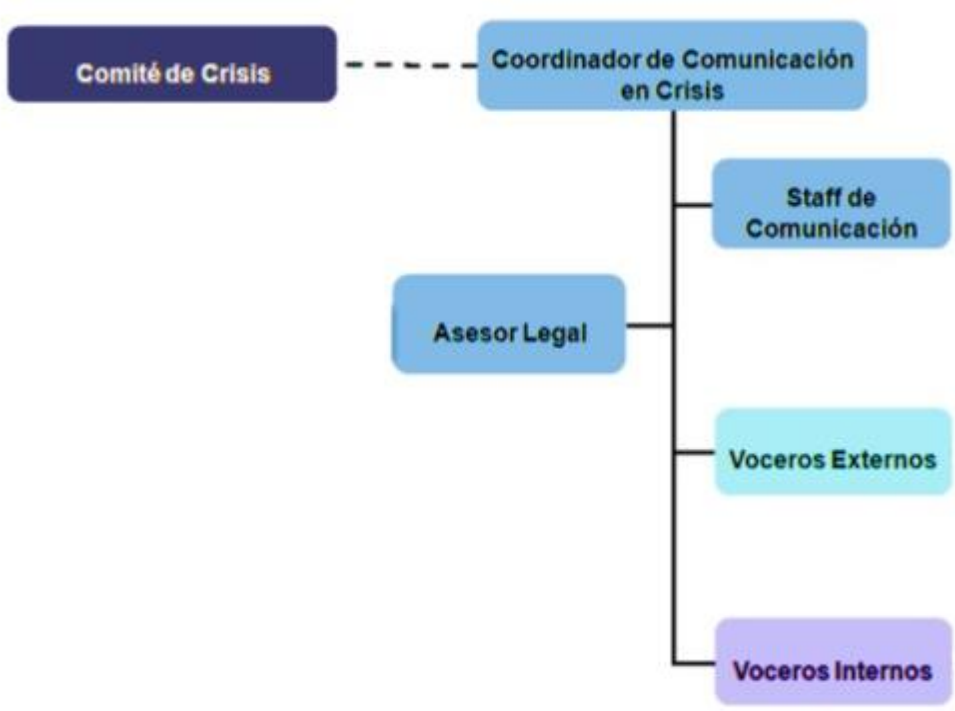


Figura 17 Organigrama de Comunicación de Crisis

Para el caso del presente ejercicio y tomando en cuenta que se analizaran únicamente los eventos de crisis que afecten a la provisión de servicios por parte de la Dirección de Informática y Comunicaciones los roles representados en el organigrama serán ocupados por el siguiente personal:

- Coordinador de Comunicación en Crisis: Sub Gerencia de Operaciones y Tecnología
- Staff de comunicación en crisis: personal de Comité de Crisis
- Asesor Legal: Representante de la Dirección Jurídica

Fase Antes: Actividades de Preparación

Leyenda:

Nro.: Número correlativo de la tarea.

Tarea Descripción: Descripción de la tarea o actividad.

Duración: Tiempo necesario para la ejecución de la tarea

R1, R2, R3, R4: Roles responsables

Tabla 28
Actividades de Preparación

Tarea, descripción	Frec.	R 1	R 2	R 3	R 4
Establecer cuáles serán las locaciones alternas que serán utilizadas durante los eventos de crisis.	Anual	x			
Asegurar que el listado de locaciones externas se encuentre actualizado y que sea de conocimiento del personal de comunicación en crisis.	Anual	x			
Asegurar la existencia y disponibilidad de los insumos requeridos para la recopilación de toda la información necesaria sobre los posibles eventos de crisis.	Anual	x			

Continua

Identificar y asegurarse que el personal que conforma los organismos de acción en caso de crisis conozca sus responsabilidades.	Anual	x	x
Mantener actualizada y disponible la lista de los participantes y el directorio telefónico de los miembros del equipo de comunicación en crisis.	Trimestral	x	
Validar y actualizar el directorio interno de la compañía especificando al personal clave de cada una de las áreas.	Anual	x	
Asegurar la actualización, distribución y entendimiento del Plan de Comunicación en Crisis.	Semestral	x	
Programar ejercicios o simulacros periódicos en los que se active el plan de comunicación en crisis	Semestral	x	

Fase Durante: Actividades de Respuesta y Operación Alterna

Leyenda:

- **Rol:** Nombre del rol del grupo de Comunicación en Crisis
- **Nro.:** Número correlativo de tarea o actividad
- **Tarea:** Descripción de la tarea o actividad
- **Frecuencia:** Frecuencia de ejecución de tareas
- **Duración**: Tiempo de aplicación de la tarea o actividad.

Coordinador de Comunicación en Crisis

Tabla 29
Actividades de Respuesta y Operación Alterna

Rol: Coordinador de Comunicación en Crisis		
Nro.	Tarea, descripción	Duración
Actividades de Respuesta (DURANTE)		
1	Una vez activado el Comité de Crisis, esperar la notificación para la activación del Plan conjuntamente con la información detallada del evento de crisis analizado por el comité	Dentro la primera hora.
2	En conjunto con el Staff de Comunicación, evaluar la información compartida por el comité de crisis a fin de evaluar si la imagen de la cooperativa se verá comprometida	Dentro la primera hora
3	Informar sobre el evento presentado al staff de comunicación y a los voceros respectivos utilizando el listado de contactos previamente definido	Dentro la primera hora.
5	Dirigirse a la ubicación seleccionada para la comunicación en crisis y notificar a los responsables de cada área sobre las locaciones alternas a ser ocupadas.	Dentro de las primeras 3 horas.
6	Confirmar que las actividades definidas en el plan de gestión de crisis se llevan a cabo de acuerdo a lo establecido	Dentro de la primera hora.
7	Discutir con el Staff de Comunicación la información presentada por el comité de crisis a fin de validar las causas y los posibles impactos sobre la reputación de la COAC 29 de Octubre ante sus clientes	Dentro de las primeras 3 horas.

Continua

8	Convocar al Asesor Legal para la elaboración de los mensajes a ser transmitidos a las audiencias afectadas.	Dentro de las primeras 2 horas.
9	Establecer un cronograma de comunicación en el que se incluya el orden de difusión hacia las áreas de negocio afectadas	Dentro de las primeras 6 horas.
11	Solicitar al Comité de Crisis la definición de los canales de comunicación para los mensajes previamente aprobados.	Dentro de la primera hora.
12	Una vez recibida la aprobación del comité de crisis, comunicar a los voceros para que hagan llegar los mensajes específicos a cada una de las audiencias	Dentro de la primera hora.
14	Monitorear la respuesta del público a fin de valorar el impacto que ha tenido la crisis sobre el negocio	Desde el envío del comunicado hasta que concluya la crisis
15	Identificar y ejecutar las acciones correctivas en función de la respuesta de provista por los involucrados	Desde el envío del comunicado hasta que concluya la crisis
18	Desactivar el estado de comunicación de crisis.	

En cada una de estas fases el coordinador de comunicación en emergencia interactuara con los diferentes miembros encargados de la ejecución del plan de comunicación por lo que las tareas serán compartidas variando únicamente el grado de responsabilidad de cada uno de ellos.

Fase Después: Restauración y Retorno

Leyenda:

- **Nro.**: Número correlativo de la tarea.
- **Tarea:** Descripción de la tarea o actividad.
- **Duración:** Tiempo necesario para la ejecución de la tarea
- **R1, R2, R3, R4**: Roles responsables

Rol	Descripción del Rol
R1	Coordinador de Comunicación en Crisis
R2	Staff de Comunicación
R3	Asesor Legal
R4	Voceros

Tabla 30
Restauración y Retorno

N°	Tarea, descripción	Duración	R1	R2	R3	R4
A.	REPARACIÓN: Establece el conjunto de actividades necesarias para minimizar los daños ocasionados como producto del evento de crisis así como también la línea base para el retorno a la normalidad					
Estado de la Situación: Desastre Controlado						
1	Esperar la notificación del comité de crisis en la que indica que el evento de crisis ha sido controlado.	Dentro de la primera hora.	X	X	X	X
B.	VUELTA A LA NORMALIDAD: Establece el conjunto de actividades para reestablecer el correcto funcionamiento de la organización desactivando los ambientes alternos y activando en entorno normal.					
Estado de la Situación: Fin del Desastre						

Continua

2	Documentar los procesos de comunicación ejecutados durante el evento de crisis.	Dentro de las 48 horas.	X	X		
3	Dimensionar el impacto del evento de crisis en la imagen institucional	Dentro de las 48 horas.	X	X		
4	Presentar el informe al comité de crisis	Dentro de las 48 horas.	X			
5	Implementar planes de remediación para subsanar los daños producto del evento de crisis	Dentro de las 72 horas.	X			
6	Esperar la notificación de finalización del evento de crisis por parte del comité de Crisis	Dentro de las 72 horas.	X	X	X	X
7	Reestructurar en caso de ser necesario el plan de comunicación de crisis en base al conocimiento adquirido producto del evento de crisis	Dentro de las 72 horas.	X	X	X	X
8	Actualizar el plan de continuidad la documentación soporte	Dentro de las 72 horas.	X			

4.2. ESTRATEGIAS DE CONTINUIDAD DE NEGOCIO

En este capítulo se presentara el planteamiento del BCP para la COAC “29 de Octubre” el cual se ha realizado en base a los análisis ejecutados en el capítulo anterior y que buscan asegurar la continuidad de los procesos de la Dirección de Tecnología y Comunicaciones.

4.2.1 Establecer Estrategias de Recuperación de Continuidad de Negocios

En este punto se explicaran los procedimientos y estrategias identificadas como más viables como producto de la ejecución de los análisis de impacto y factibilidad. Dichos procedimientos y estrategias tienen como finalidad determinar cuál será el camino adecuado y más óptimo para el aseguramiento de la continuidad de los procesos así como también para la recuperación ante incidentes que generen un alto impacto.

Adicionalmente se señalaran los puntos específicos señalados por la norma ISO/IEC 22301:2012 en la cual se basa este trabajo para la identificación de Estrategias de Recuperación así como también los procedimientos y acciones necesarias para implementarlas en la COAC “29 de Octubre”

4.2.2 Síntesis

Para este trabajo se tendrá como propósito el diseño, definición y selección de las estrategias necesarias para el aseguramiento de la continuidad del negocio, mediante el establecimiento de Tiempos Estimados de Recuperación (RTO) y Tiempos máximos Tolerables de Interrupción (MTD) los cuales deben estar alineados con los objetivos de la organización, el mercado en el que se desenvuelve y los recursos disponibles para estos propósitos

4.2.3 ISO/IEC 22301:2012 – Procesos y Actividades Fundamentales

La norma ISO/IEC 22301:2012 establece que la organización debe identificar cuáles son sus procesos fundamentales así como también las actividades críticas dentro de cada uno de ellos para de esta forma enfocar sus esfuerzos en la implementación de controles y estrategias de mitigación de riesgos que ayuden a generar un estado de continuidad para el negocio.

En tal sentido es de suma importancia que la institución logre:

- Determinar cuáles serán los tiempos objetivos de recuperación (RTO), así como también las estrategias, planes y recursos disponibles que permitirán que estos tiempos se cumplan, para esto los encargados de este proceso deben tener en cuenta que los RTO no pueden ser mayores que los Plazos máximos Tolerables de interrupción (MTPD) de cada uno de los servicios ofrecidos por el área de TI, mismos que soportan los procesos y actividades de cada uno de los ciclos de negocio.

- Identificar al personal clave para las tareas de recuperación ya sea personal interno o externo (proveedores)

- Documentar el organigrama del comité de recuperación así como también la estructura del equipo encargado de la ejecución de las tareas operativas necesarias para la reanudación de los servicios, tomando en cuenta las pérdidas económicas y de información que la organización está dispuesta a asumir.

4.2.4 Aplicación en la COAC “29 de Octubre”

- Identificar las necesidades específicas de estrategias de continuidad para cada proceso critico ofrecido por TI:

  - Validar los mecanismos disponibles que aseguren continuidad para el negocio en torno a las comunicaciones y el personal.
  - Establecer los parámetros necesarios para asegurar la continuidad de los recursos, el personal y la infraestructura de TI que soportan el negocio.
  - Identificar procedimientos alternativos capaces de soportar la continuidad de los procesos que soportan los servicios de TI del negocio.

Para esto se puede contar con estrategias capaces de contemplar actividades preventivas y de recuperación, las cuales deben estar ligadas a las capacidades económicas, operacionales y de personal de la organización pudiendo contemplarse las siguientes:

- **Diversificación:** Estrategia adecuada cuando se dispone de recursos de recursos técnicos y económicos necesarios y cuando el RTO está definido en minutos o un par de horas.

- **Replicación:** Está sujeto a la capacidad económica de la organización y de los recursos de infraestructura y comunicaciones que soportan el servicio de replicación de datos ofrecido por TI, adicionalmente se debe contemplar la disponibilidad de espacios físicos para el alojamiento de la infraestructura, es muy aplicable cuando el RTO es menor de un día.

- **Stand by:** Una de las estrategias más adoptadas por los especialistas de TI cuando se trata de ofrecer continuidad a costos moderados. Este consiste en la implementación de sites alternos con capacidades básicas pero capaces de soportar los principales aplicativos de la compañía así como también los procesos que automatizan. Estos servicios pueden ser tercerizados, por el momento existen varios proveedores que ofrecen el arrendamiento de servidores e infraestructura para contingencia. Esta estrategia es viable cuando el RTO está definido en un par de días.

- **Adquisición Post Incidente:** En el caso que se adopte esta estrategia es necesario realizar una evaluación de proveedores en la que se califique su criticidad y se evalué las capacidades de respuesta ante los requerimientos de la organización. Esta estrategia es viable cuando los RTO están definidos en varios días o semanas.

- Definir una estrategia de continuidad que se encuentre alineada con el BIA y sus resultados, a fin de enfocar los esfuerzos en los servicios críticos del área de TI mismos que soportan el giro del negocio.
- Analizar los factores necesarios para la elaboración de una estrategia de continuidad fiable, eficaz y alineada las macro estrategias y objetivos de la organización. Proveyendo a la Alta Gerencia los fundamentos para tomar la decisión más óptima.
- Definir cuál será la estructura de respuesta necesaria para una adecuada ejecución de las estrategias de continuidad establecidas.

➢ Analizar los acuerdos contractuales con los proveedores, para identificar requerimientos incluidos y no incluidos en los estándares sugeridos.

ESTRATEGIAS DE CONTINUIDAD DE NEGOCIO

Objetivo

Validar y definir estrategias de continuidad capaces de alinearse con los tiempos objetivos de recuperación definidos como parte del BIA, mismas que deben ser capaces de ofrecer continuidad en torno a los servicios de TI y los procesos de negocio que estos soportan

Componentes

Entre los principales componentes necesarios para una adecuada definición de una estrategia de continuidad viable tenemos: Infraestructura, Personal, Recursos, Proveedores Críticos e Información Sensitiva. Adicionalmente hay que considerar algunos puntos clave como son: la seguridad de la información, de los sitios alternos donde se levantaran los servicios críticos y más que toda la seguridad del personal encargado de la ejecución de las tareas de recuperación y continuidad.

Tipos de Sites Alternos

Hot Site: La mayor ventaja de este tipo de solución es que ofrece una recuperación casi inmediata de los servicios, sin embargo se requiere de una inversión económica bastante fuerte ya que son necesarios canales de replicación de datos en tiempo real a fin de alimentar las bases de datos del site alterno. Los tiempos estimados de recuperación para una estrategia basada en este tipo de sitio alterno es de 0 a 4 horas.

Warm Site: Solución basada en el levantamiento de respaldos de información, lo que se traduce en costos de implementación más accesibles ya que el Site Alterno no requiere de recursos para la replicación en línea sino que

únicamente debe disponer de conectividad base, enlaces con entes externos y equipos básicos capaces de soportar los servicios críticos de TI. Los tiempos estimados de recuperación con este tipo de solución van desde las 24 hasta las 48 horas.

Cold Site: Solución más económica basada en el ahorro durante la implementación de recursos de contingencia para el site alterno, ya que este deberá contemplar comunicaciones estrictamente críticas y los equipos necesarios para el levantamiento de los servicios de TI fundamentales, al igual que la solución anterior está basada en el levantamiento de copias de respaldo. Los tiempos estimados de recuperación son de aproximadamente una a dos semanas

Tabla 31
Estrategias Propuestas a Nivel de Infraestructura

Estrategia	Tipo	Responsable
Espacio Físico		
1. Seleccionar Sites Alternos para el levantamiento de los servicios críticos de TI que soportan los procesos críticos de negocio.	Táctico	Subgerencia de Operaciones y Tecnología
2. Seleccionar una locación adecuada para la ubicación del Site Alterno. Misma que debe contener los recursos mínimos para el levantamiento de los servicios críticos de TI que soportan el giro del negocio.	Táctico	Subgerencia de Operaciones y Tecnología
Ordenamiento de aplicaciones/servidores		
3. Identificar en base a las necesidades específicas de cada ciclo de negocio las aplicaciones críticas que las automatizan, así como también los servidores o recursos de	Táctico	Dirección de Informática y comunicaciones

Continua

infraestructuras necesarios para su adecuado funcionamiento, a fin de agilizar los procesos de continuidad.		
4. Evaluar los procedimientos de la empresa para la compra e implementación de aplicaciones, así como también los procedimientos de evaluación para determinar la criticidad de las mismas sus respectivos RTO y MTDs.	Táctico	Dirección de Informática y comunicaciones
Asegurar enlaces de comunicación		
5. Asegurar la existencia de canales de comunicación dedicados con velocidades de conexión adecuadas, las cuales aseguren el correcto funcionamiento de las aplicaciones críticas durante los procesos de continuidad.	Táctico	Dirección de Informática y comunicaciones

Tabla 32
Estrategias Propuestas a Nivel de Personal

Estrategia	Tipo	Responsable
Identificación de roles primarios y alternos		
1. Establecer estructuras jerárquicas adecuadas para el comité de continuidad de negocio, así como también la estructura de TI (personal) necesaria para la ejecución de los procesos de levantamiento de servicios críticos, los conocimientos técnicos necesarios de cada uno de ellos y sus responsabilidades dentro de cada actividad. Adicionalmente se deberá identificar al personal clave de cada una de	Estratégico	Comité de Continuidad

Continua

	las áreas de negocio los cuales se encargaran de la operación de sistemas.		
2.	Identificar personal alterno para asegurar la continuidad de las operaciones de la COAC “29 de Octubre” en caso que el personal primario no esté disponible a causa de un desastre. Se debe identificar más de un alterno que cuente con las características necesarias para cumplir las funciones del personal primario. Además se debe considerar el trabajar desde casa en caso no se pueda contar con algún ambiente de trabajo.	Estratégico	Comité de Continuidad
3.	Identificar características similares entre el personal de la COAC “29 de Octubre” para definir posibles roles alternos en los procesos que demanden mayor cantidad de personal, el personal no tiene que ser necesariamente de las misma área o ubicación geográfica.	Estratégico	Comité de Continuidad
4.	Designar un responsable del BCP, el cuál tenga una dedicación exclusiva a ello. Dicho responsable se encargará de la gestión del BCP, los elementos tecnológicos requeridos por el negocio y deberá contar con conocimientos avanzados para el manejo de la Continuidad de Negocios.	Estratégico	Subgerencia de Riesgos
Capacitación de personal			
5.	Promover a través de un calendario de capacitación que cada subgerencia y dirección gestione capacitaciones sobre los	Estratégico	Subgerencia de Riesgos

Continua

	Planes de Continuidad de Negocios tanto a personal primario como alterno con el fin de reducir brechas de conocimiento entre estos.		
6.	Efectuar un programa de capacitación virtual para el personal en general que incluya la prevención de emergencias, protección a la familia, reporte de incidentes en casos de desastre, entre otros.	Estratégico	Subgerencia Administrativa
7.	Realizar talleres para el manejo de situaciones de crisis por parte del personal para asegurar una respuesta adecuada durante un desastre. Invitar autoridades como bomberos, defensa civil o policía nacional para que participen de los talleres	Estratégico	Subgerencia Administrativa
8.	Establecer un Plan de Capacitación Anual propio del área de tecnología para los roles primarios y alternos, que considere temas técnicos y de procesos, y la recuperación en sí de los componentes tecnológicos, con el fin de reducir las brechas de conocimiento que se puedan tener entre personal primario y alterno.	Estratégico	Subgerencia de Tecnología y Operaciones
Comunicación entre el personal			
9.	Asegurar que cada área defina un árbol de llamadas integrado a nivel de la COAC “29 de Octubre” para garantizar la comunicación efectiva entre el personal en caso de desastre.	Estratégico	Cada Área del Negocio

Continua 

10. Incluir dentro de la política de vacaciones una cláusula que prevenga que personal primario y alterno tengan vacaciones o capacitaciones en las mismas fechas, de modo que siempre se contará con un rol disponible.	Estratégico	Dirección de Talento Humano
11. Identificar posibles canales de comunicación entre la COAC “29 de Octubre” y el personal. Definir un responsable que administre y difunda cada canal (mensajes telefónicos usando un software o tercerizando, canales virtuales, plataforma virtual).	Estratégico	Dirección de Informática y Comunicaciones
12. Identificar posibles canales de comunicación adecuados para la coordinación entre los integrantes del equipo de recuperación de Sistemas involucrados. Se debe definir un responsable que administre y difunde cada canal. a. Utilizar celulares y/o radios. b. Evaluar el uso de mensajes telefónicos masivos. Se debe apoyar en la evaluación y posible de selección alguna que brinde dicho servicio. c. Crear grupos de chat de comunicación y/o grupos de correo en dónde se agreguen los roles de recuperación del área, para utilizarlo como herramienta de comunicación en caso de desastre.	Estratégico	Dirección de Informática y Comunicaciones

Continua

Políticas		
13. Implementar un mecanismo que permita disponer de dinero (efectivo, cheques, vales de consumo, crédito) para poder apoyar económicamente a los colaboradores afectados por un desastre.	Operativo	Dirección de Talento Humano
14. Evaluar la asignación de Tablet o Smartphone para los Líderes de recuperación de cada plan y sus respectivos colaboradores.	Operativo	Subgerencia Administrativa
15. Propiciar que todos los personales primarios y alternos tengan acceso al correo electrónico.	Operativo	Dirección de Informática y Comunicaciones
16. Establecer indicadores de continuidad del Negocio que midan el desempeño del personal al personal que participa en las actividades de recuperación.	Operativo	Subgerencia de Riesgos
Brigadas de emergencia		
17. Mantener un listado de brigadistas actualizado y organizado por funciones y sedes para Evacuación, Seguridad, Incendio y Primeros Auxilios.	Operativo	Subgerencia Administrativa
18. Replicar el esquema de brigadistas en otras instalaciones de Pacífico donde no esté implementado.	Operativo	Subgerencia Administrativa

Continua 

Responsabilidad social		
19. Realizar un plan de responsabilidad social que incluya los siguientes puntos: a. Definir un Kit básico para la asistencia a la comunidad compuesto principalmente por: Alimentos no perecibles, carpas, abrigos, medicinas básicas según primeros auxilios. b. Identificar posibles almacenes para el kit básico de asistencia. c. Identificar alternativas de reutilización del kit básico. d. Presentar un presupuesto total para actividades a implementar.	Operativo	Subgerencia Administrativa
20. Definir líderes de responsabilidad social (es independiente a los brigadistas del apoyo interno de la COAC “29 de Octubre”) cuyo objetivo sea gestionar las actividades orientadas a velar por el bienestar de los familiares de personal y de la comunidad en general.	Operativo	Subgerencia Administrativa

Tabla 33
Estrategias Propuestas a Nivel de Recursos

Estrategia	Tipo	Responsable
Equipos de cómputo / equipos de comunicaciones		
1. Elaborar un mapa de distribución de los equipos de cómputo y de comunicaciones como impresoras, computadoras o teléfonos que estarán ubicados en el Sitio Alterno de Operación.	Operativo	Dirección de Informática y comunicaciones
2. Considerar el stock actual de computadoras y laptop como stock en caso de desastre, las cuales deberán estar configuradas y listas para ser usadas por los	Operativo	Dirección de Informática y comunicaciones
3. Distribuir el stock actual de computadoras entre las diferentes instalaciones de la COAC “29 de Octubre”.	Operativo	Dirección de Informática y comunicaciones
4. Revisar el procedimiento de gestión de inventarios para incluir recursos para la Continuidad del Negocio.	Operativo	Dirección de Informática y comunicaciones
5. Asegurar que todo el personal clave de los procesos de TI cuenten con computadores para el desarrollo de las actividades de recuperación a nivel de configuración, monitoreo, entre otros. Además, se debe considerar como recurso adicional un computador que permita realizar pruebas y/o validaciones de interconectividad, entre otras pruebas.	Estratégico	Dirección de Informática y comunicaciones
6. Considerar el uso de switches inalámbricos para lograr acelerar la disponibilidad de la red. Esto sería importante para lograr que las portátiles se conecten de manera rápida, en el caso de que el Sitio	Operativo	Dirección de Informática y comunicaciones

Continua

Alterno requiera habilitarse para más personal.		
Insumos y suministros (Compras)		
7. Implementar inventario mínimo en el Sitio Alterno de Operación hasta un determinado número de Horas. para insumos y suministros identificados en el BIA.	Operativo	Dirección de Informática y Comunicaciones
8. Definir listado de proveedores alternos de insumos y suministros.	Operativo	Dirección de Informática y Comunicaciones
Enseres		
9. Elaborar un mapa de distribución de las posiciones del personal que estará ubicado en el Sitio Alterno de Operación.	Operativo	Subgerencia de Tecnología y Operaciones

Tabla 34
Estrategias Propuestas a Nivel de Proveedores Críticos

Estrategia	Tipo	Responsable
Relación con autoridades y organismos públicas		
1. Tener un acercamiento con las autoridades	Operativo	Subgerencia Administrativa
2. Identificar los protocolos actuales que utiliza el estado para tomar control de los recursos y/o servicios necesarios para atender desastres	Operativo	Subgerencia Administrativa
Acuerdos y/o cláusulas en los contratos		
3. Incorporar en los contratos de mantenimiento del edificio, acuerdos de prioridad que permitan formalizar el compromiso de los proveedores para realizar una primera evaluación de los	Operativo	Subgerencia Administrativa

Continua

daños y determinar la posibilidad de continuar las operaciones en la instalación afectada.		
4. Identificar proveedores para la reconstrucción/reparación de las instalaciones y establecer contratos que contengan acuerdos de nivel de servicio requerido.	Operativo	Subgerencia Administrativa
5. Revisar los contratos firmados con los proveedores para asegurar que existan acuerdos de niveles de servicio (SLA) que definan penalizaciones en ellos por incumplimientos, de tal manera que se pueda contar con sus servicios en caso de desastre.	Operativo	Subgerencia Administrativa
Políticas		
6. Revisar la política de proveedores existente para contar con un contrato base que considere la inclusión de la cláusula de Riesgo Operacional, se establezcan los requisitos mínimos con los que debe cumplir un proveedor y contemple la auditoría de los esquemas de continuidad de negocios de los proveedores críticos.	Operativo	Dirección Jurídica
7. Definir una política que permita realizar gastos adicionales para emergencia en una eventual situación de desastre. Se deben considerar los siguientes aspectos como definir un esquema por área o local y coordinar con otras entidades públicas como SUNARP y ONPE sobre las políticas y/o procedimientos que serán establecidos en la COAC “29 de Octubre” para	Operativo	Subgerencia de Financiera

Continua

que reconozcan las operaciones realizadas por los usuarios autorizado.		
Evaluación de esquemas de continuidad		
8. Indagar cuáles son los esquemas de contingencia manejados por los proveedores más críticos, y evaluar si éstos pueden asegurar el servicio brindado. Adicionalmente, identificar los contactos claves y al menos dos opciones de comunicación con ellos. En caso que el proveedor no cuente con un Plan de Continuidad, se debe solicitar de manera expresa la implementación de planes de contingencia que puedan ser usadas en caso de desastre.	Operativo	Subgerencia Administrativa
9. Establecer visitas periódicas a las instalaciones de los proveedores para poder censar/revisar los esquemas de continuidad ofrecidos por ellos.	Operativo	Subgerencia Administrativa
Pruebas de contratos y acuerdos de niveles de servicio		
10. Definir un Plan Anual de Pruebas de los servicios y/o aplicaciones relacionados a los procesos de alcance que involucre a los proveedores más críticos, definiendo pruebas y ejercicios que evalúen diferentes escenarios y niveles de estrés. Se tomará como insumo un formato de Esquema de Pruebas proporcionado por Continuidad de Negocios.	Operativo	Subgerencia Tecnología y Operaciones

4.3. PROCEDIMIENTOS DE CONTINUIDAD Y REANUDACIÓN

4.3.1. Procedimientos de Continuidad de Negocio COAC 29 De Octubre

Descripción: En el caso de que se presente un evento de indisponibilidad, los responsables de las áreas según sea el caso proceden de la siguiente forma, e informan a la Subgerencia de Riesgos:

1. Evaluar las causas del incidente, identificando los servicios, los procesos y sistemas informáticos afectados.
2. Declaratoria de Continuidad de Negocio según el nivel de afectación considerando lo descrito en el numeral correspondiente de este documento.
3. Comunicar por los medios disponibles al personal responsable de los procedimientos de continuidad de negocio la activación del Plan y los procedimientos a ejecutar y el respectivo orden de ejecución de los procedimientos.
4. Los responsables ejecutarán lo procedimientos de continuidad de negocio para restablecer los servicios afectados.
5. De ser necesario se solicitará a los proveedores la aplicación de sus procedimientos de continuidad de negocio acordados para restablecer los servicios afectados.
6. En caso de requerirse movilizar el personal crítico de LA COOPERATIVA y/o de los proveedores se activará el Anexo 10 – Procedimiento de movilización del personal clave.
7. La Gerencia General definirá la necesidad y los términos para comunicar a los clientes afectados por la indisponibilidad del servicio, incluyendo el tiempo estimado en que se restablecerán.
8. Los miembros del Comité de monitorearán en todo momento la activación de la continuidad de negocio, de identificarse inconvenientes deberá tomar las decisiones que sean necesarias para la reanudación del servicio.

9. Los responsables de la ejecución de los procedimientos informarán al Comité de Continuidad de Negocio la aplicación de los procedimientos o cualquier novedad en su cumplimiento.
10. Una vez restablecidos los servicios con los procedimientos de continuidad de negocio se realizará el monitoreo del servicio en períodos de máximo 1 hora, buscando identificar posibles inconvenientes en la prestación del servicio y tomar los correctivos del caso.
11. Una vez que los servicios se han restablecido, se evaluará las acciones necesarias para habilitar la infraestructura afectada por el incidente y se iniciarán las acciones de restauración y/o recuperación, según corresponda.

4.3.2. Consideraciones Generales

- Todos los integrantes del Comité de Continuidad de negocio deben tener una copia impresa actualizada de todos los documentos referentes al Plan de Continuidad.
- Una vez difundido los procedimientos de continuidad de negocio aprobados, el Director de Informática y Comunicaciones deberá tener en custodia los procedimientos en medio físicos y deberá sociabilizar al personal de la dirección.
- Los responsables principales y alternos de aplicar los procedimientos deben tener en su poder todos los documentos actualizados y los procedimientos a su cargo para ejecutar sus actividades dentro del Plan de Continuidad de Continuidad.
- Todos los documentos del Plan de Continuidad de negocio bajo custodia del personal de la Cooperativa debe mantenerse bajo los respectivos niveles de confidencialidad, sin que esto limite su fácil acceso para el responsable de su aplicación y actualización.

- La Dirección de Desarrollo Organizacional y Procesos es el responsable de velar por la distribución de las actualizaciones y de garantizar el acceso a la documentación del Plan.
- La Dirección de Informática y Comunicaciones pondrá a disposición el Plan de Continuidad de negocio en formato digital, sea en CD, computadores y/o servidores documentales, garantizando el acceso solo al personal autorizado.
-

4.3.3. EJECUTAR PROCEDIMIENTOS DE RECUPERACIÓN Y RESTAURACIÓN COAC 29 DE OCTUBRE

Descripción: Una vez que el servicio está restablecido bajo los procedimientos de continuidad de negocio, los miembros de Comité de acuerdo al tipo de evento evalúan los daños ocasionados en la infraestructura principal y presenta el Comité quién activa la aplicación de procedimientos de restauración y/o recuperación según sea el caso, en seguida se iniciarán las acciones en coordinación con los responsables de las áreas involucradas de la Dirección de Informática y Comunicaciones para restaurar y/o recuperar las instalaciones, sistemas informáticos y procesos principales hasta lograr la operatividad normal.

Los responsables de ejecutar los procedimientos informan al Comité cuando se realicen las actividades previstas en los documentos y los servicios se encuentren restaurados.

Una vez que el servicio se encuentra restablecido con los procesos y sistemas informáticos principales, el Comité confirma y declara el fin de la Continuidad de negocio a todos los responsables de la ejecución del Plan.

Consideraciones Generales:

- El Comité de Continuidad de negocio a través de la Subgerencia de Riesgos por los medios disponibles instruirá de activar los procedimientos

de recuperación y restauración, informando el orden de aplicación de los procedimientos y a los respectivos responsables para su inmediata puesta en marcha.

- El Comité mantendrá una reunión para evaluar los resultados, en un plazo no mayor a 3 días laborables de declarado el fin de la continuidad de negocio.

PROCEDIMIENTOS DIRECCIÓN DE INFORMÁTICA Y COMUNICACIONES

Tabla 35: Incendio

Responsable Directo	Otros responsables:
Jefe de Infraestructura	Administrador de Redes y Seguridades - Operador de turno

Procedimiento de Incendio dentro DATA CENTER

En caso de presentarse una alarma de Incendio dentro del Data Center se considera que debido al estructura del mismo el incendio no se extenderá fuera del Data Center por tal motivo se debe seguir el siguiente procedimiento:

a) Dar aviso al Director de Informática y Comunicaciones y/o Jefe de Infraestructura.
b) Monitorear la activación automática del sistema de extinción de incendios utilizando el sistema de monitoreo o visualmente mediante la ventana reforzada del Data Center, en caso de que no se active el sistema de extinción de incendios automáticamente se lo debe hacer de forma manual utilizando los pulsadores manuales para descarga ubicados en el departamento de Producción de sistemas.

c) Verificar que el incendio se haya extinguido por completo ya sea mediante el sistema de monitoreo o mediante la ventana reforzada del Data Center.
d) Ejecutar procedimiento de apagado de Servidores (VER ANEXO 13).
e) Cortar el suministro de energía.

Procedimiento de Reanudación de Incendio dentro DATA CENTER

a) Solicitar el proveedor del enlace de contingencia que enrute el tráfico de datos hacia el Site alterno.
b) Activar el Site Alterno
c) Realizar un diagnóstico del sistema eléctrico del Data Center (Conexiones, Cableado, Fuentes de energía) para detectar la causa del incendio.
d) Realizar el cambio de la parte afectada.
e) Reanudar el suministro de energía. Realizar un diagnóstico de todos los equipos para determinar si el incendio causo algún daño en los mismos
f) Iniciar el proceso de Contacto con proveedores para solicitar soporte en caso de que algún equipo necesite ser cambiado o parcial o totalmente
g) Iniciar el proceso de cobro de seguro para cubrir los costos relacionados con el incendio.

Tabla 36
Erupción Volcánica

Responsable Directo	Otros responsables:
Jefe de Infraestructura	Administrador de Redes y Seguridades - Operador de turno

Procedimiento en caso de alarma de falla de aire acondicionado principal

a) Verificar mediante sistema de monitoreo el encendido automático del Aire Acondicionado de Contingencia.

b) En caso de que el encendido automático no se ejecute, realizar el encendido manual.
c) En caso de que el encendido manual no se ejecute, realizar el encendido del aire acondicionado secundario.
d) Verificar que no exista acumulación de ceniza en las ranuras de ventilación.
e) Comunicarse con el proveedor para solicitar soporte técnico

Procedimiento en caso de alarma de falla de aire acondicionado principal y secundario

a) Comunicarse con el proveedor para solicitar soporte técnico en sitio.
b) Iniciar el procedimiento de Diagnóstico y solución de problema del Aire acondicionado. (VER ANEXO 14)
c) En caso que el apagado del Aire acondicionado se mantenga por más de 15 minutos utilizar el Aire acondicionado Portátil y realizar el apagado de los equipos no críticos.
d) En caso de que la temperatura del Data Center supere los 30° C iniciar el procedimiento de apagado de los servidores (VER ANEXO 13) para evitar el daño de los mismos.

Procedimiento Reanudación en caso de apagado de equipos por falla de aire acondicionado

a) Solicitar el proveedor del enlace de contingencia que enrute el tráfico de datos hacia el Site alterno.
b) Activar el Site Alterno.
c) Una vez que el proveedor haya realizado la reparación de al menos un aire acondicionado encender el aire acondicionado
d) Esperar que las alarmas de temperatura del sistema de monitoreo desaparezcan.
e) Encender todos los equipos

f) Una vez verificado que todos los sistemas funcionan adecuadamente activar nuevamente el Data Center Principal
g) Configurar los aires acondicionados nuevamente en modo de contingencia activo-pasivo

Tabla 37
Terremoto

Responsable Directo	Otros responsables:
Jefe de Infraestructura	Administrador de Redes y Seguridades - Operador de turno

Procedimiento de Terremoto

a) Dar aviso al Director de Informática y Comunicaciones y/o Jefe de Infraestructura.
b) Si la seguridad personal de los miembros de la DIC no corre peligro iniciar el procedimiento de apagado de Servidores (VER ANEXO 13)
c) Cortar el suministro de energía

Procedimiento de Reanudación de Terremoto

a) Solicitar el proveedor del enlace de contingencia que enrute el tráfico de datos hacia el Site alterno.
b) Activar el Site Alterno.
c) Identificar la agencia más que se encuentre operativa cercana a matriz para informar a gerencia para el traslado del personal operativo para que se reanuden las actividades de los procesos críticos.
d) Revisar las instalaciones eléctricas que alimentan al Data Center siempre y cuando sea seguro ingresar nuevamente a las instalaciones.
e) Realizar un diagnóstico de todos los equipos para determinar si el siniestro causo algún daño en los mismos.

f) Iniciar el proceso de Contacto con proveedores para solicitar soporte en caso de que algún equipo necesite ser cambiado parcial o totalmente.
g) Una vez verificado que todos los sistemas funcionan adecuadamente activar nuevamente el Data Center Principal
h) Iniciar el proceso de cobro e seguro para cubrir los costos relacionados con el siniestro.

Tabla 38
Corte de Suministro Eléctrico

Responsable Directo	Otros responsables:
Jefe de Infraestructura	Administrador de Redes y Seguridades - Operador de turno

Procedimiento falla de energía de la red Pública

a) Dar aviso al Director de Informática y Comunicaciones y/o Jefe de Infraestructura
b) Verificar el encendido automático del Generador de energía en caso de no encender el Generador de manera automática iniciar el encendido manual.
c) Verificar la transferencia automática de energía, si no se realiza iniciar la transferencia manual en el tablero de trasferencia principal ubicado en la entrada del parqueadero interno.
d) Verificar el nivel de combustible cuando el corte supere las 6 horas de duración, si es necesario realizar el apagado manual del generador, cargar el combustible y encender nuevamente el generador.

Procedimiento Falla de energía de Red Pública y generador

a) Dar aviso al Director de Informática y Comunicaciones y/o Jefe de Infraestructura Apagar los equipos y servidores que no son considerados críticos.

b) Si no se restaura el suministro de energía en 20 minutos iniciar el procedimiento de apagado de los equipos (VER ANEXO 2).

Procedimiento de Reanudación de falla de energía de la red Pública y Generador

a) Solicitar el proveedor del enlace de contingencia que enrute el tráfico de datos hacia el Site alterno.
b) Activar el Site Alterno.
c) Cuando se reanude el suministro de energía de la red pública, realizar el prendido de los UPS.
d) Iniciar el procedimiento de encendido de los servidores y equipos
e) Verificar que todos los servicios se levanten correctamente
f) Iniciar el proceso de Contacto con proveedores para solicitar soporte en caso de que algún equipo necesite ser cambiado o parcial o totalmente.
g) Una vez verificado que todos los sistemas funcionan adecuadamente activar nuevamente el Data Center Principal
h) Iniciar el proceso de cobro de seguro para cubrir los costos relacionados con el siniestro.

Tabla 39
Falla Servicio de Comunicación

Responsable Directo	Otros responsables:
Jefe de Infraestructura	Administrador de Redes y Seguridades - Operador de turno

Procedimiento en caso de falla de Firewall

a) Dar aviso al Director de Informática y Comunicaciones y/o Jefe de Infraestructura.
b) Solicitar el proveedor del enlace de contingencia que enrute el tráfico de datos hacia el Site alterno.

c) Activar la conexión al Data Center alterno
d) Iniciar el procedimiento de contacto con el proveedor. (VER ANEXO 15).

Procedimiento de Reanudación en caso de falla de Firewall

a) Una vez instalado el nuevo equipo cargar las configuraciones y reglas
b) Probar la conectividad con las redes de los proveedores
c) Solicitar al proveedor de comunicaciones que se enrute nuevamente el trafico al edificio Matriz

Procedimiento en caso de falla de enlace de comunicación principal en agencias.

a) Comunicarse con el proveedor de enlace de Datos para pedir informe del evento y tiempo de solución
b) Verificar que se realice la conmutación automática al enlace alterno, en caso de no hacerlo comunicarse con la agencia para guiarles en la desconexión física del enlace principal.
c) Comunicarse con el departamento de Seguridad para que se apague el monitoreo de cámaras que se realiza utilizando el enlace de contingencia, con el fin de se utilice todo el canal de contingencia para transaccionalidad en la agencia.

Procedimiento en caso de falla de enlace de comunicación con edificio Matriz.

a) Comunicarse con el proveedor de enlace de Datos para pedir informe del evento y tiempo de solución.
b) Solicitar el proveedor del enlace de contingencia que enrute el tráfico de datos hacia el Site alterno.
c) Activar el Site alterno

Tabla 40
Caída Del Sistema

Responsable Directo	Otros responsables:
Jefe de Infraestructura	Administrador de Redes y Seguridades - Operador de turno

Procedimiento en caso de falla de BLADE ESXi

a) Dar aviso al Jefe de Infraestructura.
b) Verificar que todas las máquinas virtuales que residen en el Blade con daño se migren correctamente a los Blades restantes.
c) En caso de que una máquina virtual no se haya podido migrar, encender el respaldo de la máquina virtual y verificar que todos los servicios asociados a ella se levanten correctamente.
d) Iniciar el procedimiento de contactar al proveedor (VER ANEXO 15) para dar solución definitiva al problema.

Procedimiento en caso de falla de una máquina virtual

a) Dar aviso al Jefe de Infraestructura.
b) Encender la máquina virtual de respaldo y verificar que todos los servicios asociados a ella se levanten correctamente.
c) Revisar los logs de la herramienta VMware Vsphere para encontrar el origen de la falla (Falta de recursos computacionales, errores provocados por el aplicativo o servicio que corre en la máquina virtual, fallas causadas por una configuración mal ejecutada.), de acuerdo al Instructivo de Monitoreo de Infraestructura Virtual
d) En caso de Falta de recursos computacionales aumentar los recurso de la máquina virtual
e) En caso de falla causada por el aplicativo o servicio iniciar el procedimiento de contacto con el proveedor. (VER ANEXO 15)

Procedimiento de Reanudación en caso de falla de BLADE ESXi

a) Una vez superada la falla del Blade iniciar la migración de máquinas virtuales al Blade.
b) Verificar que todos los servicios funcionen adecuadamente.

Procedimiento de Reanudación en caso de falla de una máquina virtual

a) Una vez superado la falla de la máquina virtual, actualizar los datos y verificar que los servicios funcionen adecuadamente.
b) Apagar la máquina de respaldo.

DEGRADACIÓN DE LOS SOPORTES DE ALMACENAMIENTO DE LA INFORMACIÓN

Tabla 41
Procedimientos en caso de falla de Base de Datos de Producción

Responsable Directo	Otros responsables:
Jefe de Producción	Administrador de Base de Datos - Operador de turno

Procedimiento en caso de falla total del servidor de Base de Datos

a) Dar aviso al Director de Informática y Comunicaciones y/o Jefe de Producción.
b) Habilitar el servidor de contingencia ubicado en el Data Center Alterno (VER ANEXO 16).
c) Enrutar las peticiones a la base de datos principal hacia el servidor de contingencia.
d) d) Iniciar el procedimiento de contacto de proveedores para solicitar soporte técnico (VER ANEXO 15).

Procedimiento en caso de falla de la data de la base de datos Producción

a) Dar aviso al Director de Informática y Comunicaciones y/o Jefe de Producción.
b) Recuperar la información almacenada en cintas o en la base de contingencia de acuerdo a las Políticas de respaldo del Departamento de Producción, pudiendo tomar dichos respaldos de la bóveda de la matriz o de la agencia según lo amerite.
c) En caso de que no se pueda recuperar la Data habilitar el servidor de contingencia ubicado en el Data Center Alterno (VER ANEXO 16)
d) Enrutar las peticiones a la base de datos principal hacia el servidor de contingencia.
e) Iniciar el procedimiento de contacto de proveedores para solicitar soporte técnico. (VER ANEXO 15)

Tabla 42
Procedimiento en caso de falla de la Base de Datos de Desarrollo

Responsable Directo	Otros responsables:
Jefe de Desarrollo	Administrador de Base de Datos - Operador de turno

a) Dar aviso al Jefe de Producción.
b) Recuperar la información almacenada en cintas de acuerdo a las Políticas del Departamento de Producción, pudiendo tomar dichos respaldos de la bóveda de la matriz o de la agencia según lo amerite.
c) De no ser posible la recuperación coordinar con el proveedor de servidores de base de datos para que se active un servidor temporal y proceder con la migración total / actualización de base de datos de desarrollo.
d) Notificar a los usuarios del sistema la indisponibilidad/disponibilidad de la base de datos.

Tabla 43
Procedimiento de Reanudación en caso de falla de Base de Datos

Responsable Directo	Otros responsables:
Jefe de Producción	Administrador de Base de Datos
Jefe de Desarrollo	Técnicos DPSoft

Procedimiento de Reanudación en caso de falla total del servidor

a) Verificar que todas las conexiones a la base de datos funcionen adecuadamente
b) Una vez solventado el problema iniciar el procedimiento de levantamiento de la base de datos principal (VER ANEXO 16).

Procedimiento de Reanudación en caso de falla de la data de la base de Datos Desarrollo o Producción

a) Realizar copia de la data de la Base de Datos de Contingencia.
b) Cargar la data en la base de Datos de Producción o Desarrollo.
c) Iniciar el procedimiento de levantamiento de la base de Datos principal

4.4. PLAN DE PRUEBAS COAC 29 DE OCTUBRE

4.4.1. Planificar Pruebas

Descripción: Para el desarrollo del plan de pruebas, previamente el Analista de Riesgo Operativo se alinea al cumplimiento de las fases descritas en el mismo, para lo cual planifica y realiza el levantamiento de información conforme los diferentes formatos (ANEXOS 2 al 8), enseguida desarrolla la evaluación de la situación actual y análisis de impacto al negocio (B.I.A) para el Plan de Continuidad de Negocio con los responsables de las áreas involucradas.

Para la planificación de pruebas, el Analista de Riesgo Operativo de acuerdo a los servicios críticos del análisis BIA, desarrolla el Plan de Pruebas que es registrado en el ANEXO 11: “Plan de Pruebas”, dicho Plan permite ejecutar los

diferentes procedimientos de forma controlada y organizada, identificando las mejoras al procedimiento, fechas y tiempos de ejecución, y necesidades de capacitación, que es presentado en el primer Comité de Continuidad de Negocio del año.

Las diferentes pruebas previstas a ejecutar se detallan a continuación:

- **Pruebas de los Procedimientos de Continuidad de Negocio:** Considera la activación de los procedimientos y validación de la efectividad para la recuperación de los servicios afectados. La planificación de las pruebas estará a cargo de la Subgerencia de Riesgos.
- **Pruebas de los Procedimientos de Continuidad y Restauración:** Para validar la efectividad de los procedimientos, integridad de los sistemas y su información, así como la disponibilidad de la infraestructura tecnológica designados para la contingencia. La planificación de las pruebas estará a cargo de la Subgerencia de Operaciones y Tecnología.
- **Pruebas de los procedimientos de apoyo:** Los procedimientos de apoyo podrán validarse de forma conceptual o práctica, según sea el caso y su planificación estará a cargo de uno o varios delegados del Comité de Continuidad de Negocio designados en el último Comité del año que termina.

Consideraciones Generales:

- Se deberá considerar los procesos, proveedores, aplicaciones tecnológicas y personal critico relacionados con los servicios críticos, resultado del análisis BIA.
- La planificación de las pruebas se realizará a inicios de cada año.

- Las Pruebas de los Procedimientos de Continuidad y Recuperación y Pruebas de los Procedimientos de Continuidad y Restauración deben realizarse al menos 3 veces al año, y las Pruebas de los procedimientos de apoyo deben realizarse al menos 1 vez al año.
- Se deberán realizar anualmente al menos 2 pruebas parciales y 1 prueba total.
- En caso de existir modificaciones a los procesos principales o a la infraestructura tecnológica y que afecte a un servicio considerado como crítico, se deberá realizar las respectivas actualizaciones a los procedimientos del Plan de Continuidad de Negocio y al menos una prueba parcial y una total adicional a la definida en la planificación anual.

4.4.2. Revisar y Aprobar Plan de Pruebas

Descripción: El Comité de Continuidad de Negocio revisa y aprueba o solicita modificación según las sugerencias de los integrantes del Comité, el Plan de Pruebas describe las actividades, responsables, fechas y horario estimado de aplicación de las pruebas incluyendo tiempos adicionales en caso de eventualidades.

Consideraciones Generales:

- El responsable de la ejecución de las pruebas, previa la ejecución de las pruebas evaluará el impacto que podrá ocasionar a las normales operaciones de la Cooperativa y se procederá en horarios que la afectación sea la menor posible y que garantice el total restablecimiento de la gestión normal de la Cooperativa.
- El responsable de la ejecución de las pruebas, para la aplicación de las pruebas se notificará al personal involucrado con al menos 5 días de anticipación.

4.4.3. Ejecutar y evaluar pruebas

Descripción: El Analista de Riesgo Operativo para la ejecución de las pruebas, realiza la convocatoria al personal involucrado (interno o externo) identificando fecha y lista del personal convocado según ANEXO 9: “Responsables de Ejecución de Procedimientos del Plan de Continuidad de Negocio”, a fin de validar la asistencia y participación.

Durante la ejecución de las pruebas se aplicará las actividades descritas en los procedimientos del Plan de Continuidad de Negocio, finalizadas las pruebas, el personal involucrado registra los resultados en los formatos: ANEXO 12: “Formulario de Prueba de Continuidad de Negocio”.

El Analista de Riesgo Operativo presenta los formatos 22 mediante informe y presenta en el Comité de Continuidad de Negocio para su revisión. Cualquier observación a las pruebas realizadas por el Comité se registra en las respectivas actas para el respectivo seguimiento e implementación.

Para la evaluación de las pruebas, el Comité de Continuidad de Negocio considerando los criterios detallados en los formularios, concluye si las pruebas son satisfactorias o insatisfactorias, este análisis se registra en acta del Comité para poner en conocimiento del CAIR y posteriormente del Consejo de Administración.

Si las pruebas son insatisfactorias, es decir no cumplen las expectativas, el Analista de Riesgo Operativo realiza los ajustes necesarios en los procedimientos y/o en la planificación para repetir la prueba hasta lograr el objetivo, considerando principalmente el tiempo de ejecución para restablecer el servicio.

Consideraciones Generales:

- El Comité de Continuidad de Negocio tendrá la potestad de solicitar en cualquier momento, la realización pruebas adicionales a las detalladas en el Plan de Pruebas, sean estas totales y/o parciales.

- Se deberá comunicar al Comité de Continuidad de Negocio la realización de las pruebas con al menos 15 días de anticipación de las pruebas, de tal forma que pueda solicitarse el aplazamiento de las pruebas por algún imprevisto o actividad de la Cooperativa que pueda afectar el normal desempeño de las pruebas o del negocio. En este caso se definirá una nueva fecha para su realización que no podrá ser mayor a 15 días.
- El Plazo máximo para presentar los informes de resultados de pruebas será de 20 días de realizadas las pruebas, incluyendo las mejoras identificadas y los plazos de implementación.
- Si las pruebas no son satisfactorias, estas deberán repetirse una vez identificadas las mejoras a los procedimientos que viabilicen el éxito de la prueba.

4.5 ANÁLISIS DE RESULTADOS DE PRUEBAS

El análisis de la posible ocurrencia de una amenaza se la realizó de acuerdo a su severidad y afectación de la continuidad de negocio de COAC “29 DE OCTUBRE” los cuales son:

- Incendio
- Terremoto
- Erupción Volcánica
- Corte de Suministro Eléctrico
- Fallos de servicio de Comunicación
- Degradación de los soportes de almacenamiento de la información
- Caída del sistema por agotamiento de recursos
- Acceso no autorizado
- Denegación de servicio

Para la evaluación se escogió escenarios fijos para el desarrollo de pruebas de Continuidad de Negocio con el objetivo de medir su impacto en la institución.

Al ejecutar el análisis aplicado a la realidad de COAC “29 DE OCTUBRE”, se identificó los escenarios de riesgo con mayor probabilidad de ocurrencia e impacto en el negocio siendo estos: Fallos de servicio de comunicación y Caída del sistema por agotamiento de recursos.

Estos escenarios provocan la pérdida de continuidad del negocio e interrupciones en los servicios que ofrece COAC “29 DE OCTUBRE”, los cuales son detallados de acuerdo a su importancia.

Para los casos se establece el **MTPD** (Periodo Máximo Tolerable de Interrupción), que fue definido dentro del análisis BIA donde se estipula el tiempo en el cual la institución puede permanecer sin ejecutar las actividades ligadas directamente a los servicios que ofrece la Dirección de Informática y Comunicaciones de COAC “29 DE OCTUBRE” sin verse amenazada de manera (financiera, pérdida de reputación, etc.) es de 3 horas para la recuperación de los enlaces de comunicación, se deben realizar las acciones descritas en los procedimientos de continuidad y reanudación descritos en el capítulo anterior conforme al **RTO:** Tiempo objetivo de recuperación definido.

4.5.1. Análisis del primer caso de prueba: Fallos de servicio de comunicación

Hipótesis: COAC “29 DE OCTUBRE” queda sin enlaces de comunicación en el edificio Matriz.

El tiempo de recuperación objetivo para realizar las actividades de reanudación de los enlaces de comunicación es de 30 minutos a 3 horas, al revisar los valores obtenidos del ejercicio de prueba se invirtieron los siguientes tiempos.

Tabla 44
Caso de Prueba 1

Área del Negocio	Actividades	Servicio o Aplicaciones Críticas	Tiempo Invertido
Gestión de Tecnología de la Información	Comunicación Procedimientos de continuidad y reanudación Vuelta a la normalidad	Internet Telefonía IP	5 Minutos 20 Minutos 10 Minutos

Dentro de la etapa de Comunicación al Comité de Continuidad se invirtió 5 minutos, 20 minutos para la ejecución de procedimientos de continuidad de negocio y reanudación donde se detalla la revisión y contacto con el proveedor para la solución del problema y 10 minutos para la estabilización de los enlaces lo que da un total de 35 minutos.

Los tiempos demuestran que los procedimientos de continuidad y reanudación se enmarcan en los tiempos definidos por COAC “29 DE OCTUBRE” lo que refleja un correcto despliegue de las actividades de continuidad para la solución del caso propuesto como incidente.

4.5.2. Análisis del segundo caso de prueba: Caída del sistema por agotamiento de recursos

Hipótesis: COAC “29 DE OCTUBRE” queda sin Core Bancario en el edificio Matriz.

El tiempo de recuperación objetivo para realizar las actividades de reanudación del sistema es de 30 minutos a 2 horas, al revisar los valores obtenidos del ejercicio de prueba se invirtieron los siguientes tiempos.

Tabla 45
Caso de Prueba 2

Área del Negocio	Actividades	Servicio o Aplicaciones Críticas	Tiempo Invertido
Gestión de Tecnología de la Información	Comunicación Procedimientos de continuidad y reanudación Vuelta a la normalidad	CORE Bancario	5 Minutos 45 Minutos 10 Minutos

Dentro de la etapa de Comunicación al Comité de Continuidad se invirtió 5 minutos, 45 minutos para la ejecución de procedimientos de continuidad de negocio y reanudación donde se detalla la revisión y contacto con el proveedor para la solución del problema y 10 minutos para la estabilización de los enlaces lo que da un total de 1 hora.

Los tiempos demuestran que los procedimientos de continuidad y reanudación se enmarcan en los tiempos definidos por COAC “29 DE OCTUBRE” lo que refleja un correcto despliegue de las actividades de continuidad para la solución del caso propuesto como incidente.

CAPÍTULO V
CONCLUSIONES Y RECOMENDACIONES

Una vez finalizado el análisis de la situación actual, el análisis de Riesgo, la elaboración del Plan de Continuidad de Negocio, la definición de procedimientos continuidad y reanudación y la realización de pruebas de los principales escenarios de riesgo en COAC “29 DE OCTUBRE”, ha dado como resultado las siguientes conclusiones y recomendaciones.

Conclusiones

La metodología de análisis de riesgo utilizada para este caso ha sido ajustada a la realidad económica de la empresa con sus riesgos particulares, orientada a la pérdida financiera soportable por la institución y alineada a las necesidades normativas e institucionales proporcionando beneficios para la protección de información e infraestructura.

El Análisis de Impacto en el Negocio BIA es la base fundamental para el desarrollo de este tipo de estudios por lo que su correcta realización asegura la correcta implementación del Plan de Continuidad de Negocio.

El éxito de un Plan de Continuidad del Negocio depende directamente del compromiso de la Alta Gerencia y de la colaboración de los funcionarios directamente involucrados con la continuidad.

Las instituciones sin importar su tamaño tienen que garantizar la continuidad de los servicios críticos que ofrecen a sus clientes, la inactividad de los servicios es proporcional al impacto y pérdidas de imagen, económicas y legales que sufren al no poder realizar sus actividades normales.

La evaluación y mejora continua es indispensable para la correcta gestión de la continuidad del negocio con el fin de obtener un nivel de madurez aceptable para satisfacer las necesidades normativas e institucionales.

Recomendaciones

Para futuros trabajos se debe utilizar la metodología de análisis de riesgo definida y alineada a la pérdida económica soportable por la Institución con sus riesgos particulares a fin de no mal gastar esfuerzos en una nueva personalización.

Actualizar permanentemente el Análisis de Impacto en el Negocio BIA en base de los cambios organizacionales que presente la Institución y de los nuevos riesgos en cuanto a amenazas y vulnerabilidades que se puedan suscitar.

Mantener el interés y compromiso de la Alta Gerencia con la Continuidad del Negocio con el fin de tener facilidades para futuros análisis, simulacros y capacitaciones que involucren al personal de la Institución para generar una cultura de Riesgo y continuidad.

Los incidentes que involucren a servicios que no son administrados en su totalidad por COAC “29 DE OCTUBRE” deben ser comunicados directamente al proveedor para buscar la mejor estrategia de solución a fin de garantizar la continuidad del negocio en el menor tiempo posible.

La Dirección de Informática y Comunicaciones debe realizar al menos 2 veces al año la revisión del plan de continuidad de negocio para evaluar su vigencia realizando simulacros y pruebas con el personal responsable para reforzar conocimientos y retroalimentar lo aprendido.

BIBLIOGRAFÍA

Alexander, A. (2013). *Nuevo Estándar Internacional en Continuidad del Negocio ISO 22301:2012.* Retrieved from ISO 22301: http://www.ariescg.com/iso22301.pdf

Cooperativa de Ahorro y Crédito 29 de Octubre. (2015). *Metodología de Administración de Riesgo operativo.*

Cooperativa de Ahorro y Crédito 29 de Octubre. (2016). *Cooperativa de Ahorro y Crédito 29 de Octubre Ltda*. Retrieved Abril 2016, from https://www.29deoctubre.fin.ec/conoce-la-institucion/

Cooperativa de Ahorro y Crédito 29 de Octubre. (2016). *Planificación Estrategica Cooperativa de Ahorro y Crédito 29 de Octubre 2016.*

Ferrer, R. (2015). *sisteseg.* Retrieved from sisteseg: https://www.google.com.ec/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjkhf7aybXOAhXOdSYKHcjpCtYQFggaMAA&url=http%3A%2F%2Fwww.sisteseg.com%2Ffiles%2FMicrosoft_PowerPoint_-_PLANES_DE_CONTINUIDAD_NEGOCIO_V_3.0.pdf&usg=AFQjCNGiTGWpwRdFJ

Hotchkiss, S. (2010). *Business Continuity Management: A Practical Guide.* Reino Unido: BCS, the Chartered Institute for IT.

International Standard organization. (2012). *ISO 22301 Bussiness continuity managment systems.* ISO.

Superintendencia de Bancos. (2015). Normativa para las Instituciones del Sistema Financiero.