UNIVERSIDAD DON BOSCO

Facultad de Ingeniería

Escuela de Ingeniería en Computación

BITCOIN EN EL SALVADOR
LEGISLACIÓN Y BUENAS PRÁCTICAS SEGÚN LA NORMA ISO 22301

Integrantes:

Daniel Eduardo Girón Díaz	GD201942
Oscar Napoleón Montiel Vidaurre	MV202584
Luis Alberto Villatoro Guzmán	VG201952

Asesor:

Magister Álvaro Hernán Zavala Ruballo

JULIO 2022 - EL SALVADOR - CENTRO AMÉRICA

Índice General.

Índice de Tablas.

Índice de Ilustraciones.

Introducción.

La Organización Internacional para la Estandarización (*International Organization for Standardization* en lo sucesivo abreviado ISO) es una organización internacional no gubernamental independiente que, a pesar de haber iniciado con 65 delegados de 25 países en la ciudad de Londres, en el año 1946; hoy día se establece en Ginebra, Suiza. Con un conglomerado de 167 países representados y con 804 diferentes Comités Técnicos cuyos miembros, son los mayores expertos de vanguardia con un alto grado de conocimientos y experiencia en desarrollar normas internacionales, basadas en el consenso y la voluntaria aceptación y uso por parte de grandes compañías, gobiernos, universidades, institutos, organizaciones públicas y privadas de todo nivel.

La ISO también colabora estrechamente con la Comisión Electrotécnica Internacional (*International Electrotechnical Commission* en lo sucesivo abreviado IEC) la cual es otra organización reconocida en la preparación y publicación de normas internacionales para todas las tecnologías eléctricas, electrónicas y ciencias relacionadas. De manera que sus publicaciones son estrechamente relacionadas y equivalentes en cuanto a las Tecnologías de la Información.

Con un catálogo de más de 24,227 normas internacionales publicadas y vigentes, la ISO cubre casi todos los aspectos de la tecnología y la manufactura. Y dentro de este conjunto de normas extraemos la ISO 22301:2019 sobre la seguridad y resiliencia, y los sistemas de gestión de la continuidad del negocio. Esta es la segunda edición en esta especialidad y está a cargo del Comité Técnico: ISO/TC 292 Seguridad y Resiliencia.

La continuidad del negocio permite identificar las estrategias necesarias para recuperar los principales productos y servicios de una empresa ante un evento de interrupción. La existencia de un programa de continuidad del negocio facilita mantener planes adecuadamente priorizados, coordinados y probados, además de preparar a la organización para responder a incidentes no esperados que generalmente impactan en los ingresos y en la imagen de la organización. La finalidad de este documento es proporcionar una guía de referencia, sobre la base de las buenas prácticas; para una organización o empresa que desee implementar el uso de Bitcoin de forma que se minimicen los riesgos e impactos que por su naturaleza le son inherentes, tomando como referencia la norma ISO22301 Continuidad de Negocio en su versión del año 2019.

Considerando el caso particular de El Salvador, donde el día 8 de junio de 2021 la Asamblea Legislativa ratificó la Ley Bitcoin, y con ello se convirtió en la primera nación a nivel mundial en adoptar el Bitcoin como moneda de curso legal. Dicha ley fue divulgada en el Diario Oficial número 110, tomo 431, de fecha 9 de junio 2021 y entro en vigencia 90 días más tarde; el 7 de septiembre de 2021.

De manera que abordaremos esta temática en 6 capítulos de la siguiente manera:
El Capítulo I presenta el Planteamiento del Problema, sus antecedentes y objetivos, así como la justificación y delimitación del estudio.
El Capítulo II se refiere al Marco Teórico de la Investigación, incluyendo los conceptos y términos de la Norma ISO 22301 y aquellos relacionados al Bitcoin.
El Capítulo III contiene la Metodología de la Investigación en la cual se define el tipo de investigación realizada, además de las unidades de análisis, las variables y su medición.
El Capítulo IV contine un Análisis y la Discusión de los Resultados obtenidos.
El Capitulo V presenta una Propuesta de Implementación, una guía genérica destinada a ser aplicable una organización que desee incursionar en forma resiliente al uso de Bitcoin.
El Capítulo VI contiene las conclusiones y recomendaciones.
Finalmente, las Referencias, Anexos y un Glosario de términos relacionados.

Capítulo I Planteamiento del Problema.

1.1 El problema de investigación.

En este documento se pretende dar una guía de posibles soluciones en el área de gestión de riesgos informáticos; plantear como medida de control la Norma Internacional ISO22301 Continuidad de Negocio y así como un marco de prevención, demostrar como las normas y estándares internacionales pueden ser aplicados.

Así mismo incluir algunos aspectos complementarios contenidos en las Técnicas para Facilitar la Participación de las Entidades Financieras en el Ecosistema Bitcoin NRP-29, emitida por el Banco Central de Reserva y la Ley de Bitcoin.

Ante la llegada del Bitcoin a El Salvador como moneda de curso legal que opera desde un punto de vista tecnológico y; sin que hubiera otro marco de referencia con el cual comparar, el país implementa una serie de servicios asociados los cuales se lanzaron a la población causando un impacto de opinión, sorpresa y escepticismo internacional al momento de su lanzamiento. Es entonces que las entidades financieras en El Salvador deben implementar una estrategia urgente para poder enfrentar el mandato presidencial y ofrecer como parte de sus productos internos, por lo menos un servicio digital de gama limitada de cobros y pagos de fondos públicos, impuestos, facturas, entre otros.

1.2 Antecedentes del problema.

En septiembre de 2021, El Salvador se convirtió en la primera nación del mundo en adoptar el Bitcoin como moneda de uso legal. Para muchos expertos esta decisión es controversial, por sus ventajas y desventajas. En el estudio se pretende abordar el tema desde la postura de una institución bancaria con un enfoque apegado a una norma internacional de buenas prácticas como la ISO 22301, la cual ayuda a las organizaciones a prevenir, prepararse, responder y recuperarse de incidentes inesperados.

El Salvador, al ser el primer país del mundo en adoptar el Bitcoin como moneda legal para uso comercial; se convierte en un referente de observación para economistas, analistas financieros, corredores de bolsa y gobiernos de otros países. Ya sea que se inclinen por su uso o lo rechacen. Hasta la fecha no existen otras implementaciones similares de Bitcoin como moneda de curso legal en la manera que ha sucedido en El Salvador; es ahí donde nace un punto de enfoque para diseñar una guía, que pueda respaldar su uso con base a un estándar internacional dentro de los términos de la continuidad del negocio, siendo esto el objetivo principal de este documento.

En este orden de ideas , es oportuno mencionar que la resiliencia es una parte importante de las operaciones comerciales hoy en día, para garantizar que se tiene capacidad de reacción y adaptación a las circunstancias cambiantes del medio, y para ello las empresas están implementado planes y procesos efectivos de continuidad del negocio para minimizar las interrupciones en sus servicios y mantener las operaciones críticas en un nivel aceptable de servicio para los usuarios en caso de incidentes disruptivos.

1.3 Objetivos.

1.3.1 Objetivo general:

Desarrollar una guía de buenas prácticas para la implementación de Bitcoin en El Salvador tomando como referencia la norma ISO22301.

1.3.2 Objetivos específicos:

- Documentar las buenas prácticas que se adoptaron al momento de la implementación de Bitcoin como moneda de pago por un ente financiero.
- Describir los aspectos técnicos y tecnológicos apegados a la Norma ISO 22301 para adoptar el uso del Bitcoin.
- Referenciar el marco legal y regulatorio sobre el uso de Bitcoin como medio de transacción, aplicables a instituciones financieras.

1.4 Justificación.

Los motivos que llevan a realizar la presente guía surgen debido a que El Salvador es el primer país en brindarle carácter legal al Bitcoin, aunque no hay antecedentes previos de implementación bajo este escenario en ninguna parte del mundo lo cual podría derivar en incertidumbre en los servicios ofrecidos y en la necesidad de establecer un sistema de gestión de la continuidad del negocio ante este escenario nuevo. De acá surge la iniciativa de crear una guía práctica, la cual pueda servir de apoyo a diferentes entidades u organizaciones en la implementación de esta nueva modalidad de flujo de capitales. Es importante destacar el reto emergente que representa debiendo resolver, superar y mantener al menos un criterio mínimo aceptable para la continuidad del negocio basado en un estándar internacional de buenas prácticas para su uso comercial en el mercado.

1.5 Delimitación del proyecto.

La delimitación geográfica es el territorio de El Salvador, en el período de enero a junio de 2022. De igual forma es pertinente destacar que en el ámbito de la tecnología y en particular, que el uso de Bitcoin requiere una aplicación de software diseñada para ejecutarse en teléfonos inteligentes, tabletas y otros dispositivos móviles y para desarrollar la guía, se ha utilizado el monedero digital oficial denominado *Chivo Wallet*. (Ver anexo 1 “Cronograma de trabajo”).

Capítulo II Marco de Investigación.

En este capítulo se presentan los conceptos teóricos básicos que nos ayudaran a comprender la terminología relacionada al Bitcoin y a las buenas prácticas.

2.1 Conceptos y términos más relevantes de la ISO22301.

2.1.1 Continuidad de Negocio es el nivel de preparación que tiene una empresa para mantener las funciones esenciales tras una emergencia o una interrupción. Estos eventos pueden incluir vulnerabilidades de seguridad, desastres naturales, cortes de energía, averías de los equipos o la salida repentina de un empleado clave (Vocabulario Bitcoin.org, 2022).

2.1.2 Sistema de Gestión de la Continuidad del Negocio (en lo sucesivo abreviado SGCN) es parte del sistema general de la organización que establece, opera, monitorea, revisa, mantiene y mejora la continuidad del negocio.

2.1.3 Análisis de Impacto de Negocio es un proceso especializado en la identificación de los tipos de impacto, orientado en conocer qué podría verse afectado y las consecuencias sobre los procesos de negocio (ISO 22301:2019, Tony Bevan, 2020).

2.1.4 Interrupción Máxima Aceptable es el tiempo máximo que la actividad puede estar detenida. Si se supera dicho límite habrá un daño inadmisible. Existencia del tiempo límite máximo para la restauración de los recursos, para la reparación y de la continuidad del negocio (ISO 22301:2019, Tony Bevan, 2020).

2.1.5 Período Máximo Admisible de Interrupción define el tiempo máximo tolerable de la indisponibilidad debido a una interrupción, por lo general desde la perspectiva del negocio o del equipo estratégico (ISO 22301:2019, Tony Bevan, 2020).

2.1.6 Punto Objetivo de Recuperación es la cantidad de tiempo máxima aceptable desde el último punto de recuperación de datos. Esto determina qué se considera una pérdida aceptable de datos entre el último punto de recuperación y la interrupción del servicio (ISO 22301:2019, Tony Bevan, 2020).

2.1.7 Tiempo Objetivo de Recuperación es el tiempo máximo aceptable que sus aplicaciones comerciales pueden estar inactivas, es decir la interrupción máxima tolerable que puede soportar la organización sin causar un daño significativo a la organización (ISO 22301:2019, Tony Bevan, 2020).

2.2 Conceptos y términos relacionados al Bitcoin.

2.2.1 Primitivas criptográficas es un algoritmo matemático de bajo nivel utilizado para establecer protocolos de cifrado para sistemas de seguridad. La contraseña del diseñador lo usa como el bloque de construcción más básico. Este componente es parte del sistema criptográfico, que es un conjunto de algoritmos cifrados necesarios para implementar servicios de seguridad específicos, como códigos de unidad o funciones picadillo. Debido a que estas áreas primitivas están construyendo bloques, están diseñados para realizar tareas precisas y confiables (Vocabulario Bitcoin.org, 2022).

2.2.2 Red entre pares hace referencia a un tipo de arquitectura para la comunicación entre aplicaciones que permite a individuos comunicarse y compartir información con otros individuos sin necesidad de un servidor central que facilite la comunicación (Vocabulario Bitcoin.org, 2022).

2.2.3 Algoritmo de prueba de trabajo es un sistema con el fin de desmotivar y dificultar comportamientos indeseados como ataques de denegación de servicio o correo electrónico masivo no solicitado. Requiere que el cliente del servicio realice algún tipo de trabajo que tenga cierto coste y que es verificado fácilmente en la parte del servidor. La característica clave de la estrategia es su asimetría: El trabajo debe ser moderadamente

difícil (pero factible) por el lado del cliente, pero fácil de verificar por el lado del servidor (Vocabulario Bitcoin.org, 2022).

2.2.4 Mecanismo de mejor esfuerzo es un tipo de servicio de red en el que la red no puede garantizar que los datos lleguen a su destino, ni ofrecer al usuario una determinada calidad de servicio en sus comunicaciones. En una red de mejor esfuerzo todos los usuarios reciben el mejor servicio posible en ese momento, lo que significa que obtendrán distintos anchos de banda y tiempos de respuesta en función del volumen de tráfico en la red (Vocabulario Bitcoin.org, 2022).

2.2.5 Función digesto de solo ida es una huella digital única de longitud fija, con las siguientes características (Vocabulario Bitcoin.org, 2022).

- Aceptar cualquier longitud del mensaje.
- Producir un digesto de longitud fija.
- Ocultar el mensaje de entrada.
- No producir un digesto predeterminado.
- Evitar colisiones.

2.2.6 Criptografía de clave pública es un sistema que utiliza pares de claves para cifrar y autenticar información. Una clave en el par es una clave pública que, como su nombre lo indica, puede distribuirse ampliamente sin afectar la seguridad. La segunda clave en el par es una clave privada que solo es conocida por el propietario (Vocabulario Bitcoin.org, 2022).

2.2.7 Firma digital es un mecanismo criptográfico que permite al receptor de un documento firmado digitalmente identificar al emisor del mismo, confirmar que el documento no ha sido alterado desde que fue firmado, y tener la certeza del control exclusivo del firmante sobre la utilización de los datos de creación de firma electrónica. Su funcionamiento se basa en los sistemas de clave pública, usando un par de claves para el envío del documento. Una de las claves es privada del propietario, y la

segunda es pública, que se entrega a los destinatarios para permitirles el acceso al documento (Vocabulario Bitcoin.org, 2022).

2.2.8 Estampa de tiempo es el sellado de tiempo que puede garantizar la integridad del conjunto de datos electrónicos que conforman la firma electrónica. Es decir, el sello de tiempo garantiza que una firma llevada a cabo en un momento dado no puede modificarse (Vocabulario Bitcoin.org, 2022).

El sello de tiempo también garantiza la no alteración de una serie de datos asociados con la firma electrónica, como la fecha, hora y lugar de realización de la firma, la dirección de correo del emisor del documento a firmar, la dirección de correo del firmante, entre otros.

2.2.9 Cadena de bloques es un gigantesco libro de cuentas inalterable al que únicamente los miembros autorizados tienen acceso, donde los registros o bloques están enlazados y cifrados para proteger la seguridad y privacidad de las transacciones, en otras palabras; es una base de datos distribuida y asegurada mediante cifrado que se puede aplicar a todo tipo de transacciones que no tienen por qué ser necesariamente económicas, pero con capacidad de ejercer control y seguimiento de pedidos, pagos, cuentas, detalles de producción y de legitimidad. Además, debido a que los usuarios comparten una única fuente fidedigna de información, puede ver todos los detalles de una transacción de principio a fin, lo que le permite generar mayor confianza y eficiencia, además de obtener más oportunidades (Vocabulario Bitcoin.org, 2022).

2.2.10 Elementos clave de la cadena de bloques:

- Tecnología de libro mayor distribuido.

Todos los participantes de la red tienen acceso al libro mayor distribuido y a su registro inmutable de transacciones. Con este libro mayor compartido, las transacciones se registran solo una vez, eliminando la duplicación del esfuerzo que es típico de las redes de negocios tradicionales (Vocabulario Bitcoin.org, 2022).

- Registros inalterables.

Ningún participante puede cambiar o falsificar una transacción una vez grabada en el libro mayor compartido. Si el registro de una transacción incluye un error, se debe añadir una nueva transacción para revertir el error, pero ambas transacciones serán visibles.

2.2.11 Funcionamiento de la cadena de bloques.

- A cada participante de la cadena se le llama nodo, que en realidad viene a ser un ordenador más o menos potente. Estos nodos se conectan en una red descentralizada, sin un ordenador principal. Son redes entre pares que hablan entre sí usando el mismo lenguaje o protocolo.
- Al mensaje que transmiten se le llama ficha o token, lo cual es una representación de la información que aloja la red. Esta información puede representar cualquier tipo de archivo digital.
- La información viaja encriptada, gracias a lo cual puede estar distribuida sin que se revele su contenido y se agrupa en bloques enlazados.
- Una cadena de bloques es esencialmente un registro, un libro mayor de acontecimientos digitales que está distribuido o es compartido entre muchas partes diferentes.
- Solo puede ser actualizado a partir del consenso de la mayoría de participantes del sistema y, una vez introducida, la información nunca puede ser borrada.
- La cadena de bloques de Bitcoin contiene un registro certero y verificable de todas las transacciones que se han hecho en su historia.

2.2.11 Beneficios de la cadena de bloques.

- Mayor confianza.

Si utiliza una red privada a la que solo los miembros tienen acceso, con la cadena de bloques se tiene la seguridad de que recibirá datos precisos y oportunos, además de que sus registros son confidenciales y se compartirán solo con miembros específicos de la red a los que se haya autorizado.

- Mayor seguridad.

Todos los miembros de la red deben llegar a un consenso acerca de la precisión de los datos y todas las transacciones validadas son inalterables ya que se registran de forma permanente. Nadie, ni siquiera un administrador del sistema, puede suprimir una transacción.

- Más eficiencia.

Con un libro mayor distribuido compartido entre los miembros de una red, se elimina el tiempo perdido en las acciones de conciliación de registros. Y para acelerar las transacciones, un conjunto de reglas, llamado contrato inteligente, se almacena en la cadena de bloques y se ejecuta automáticamente.

2.2.12 Bitcoin es una criptomoneda y un sistema de pago sin un banco central o administrador único (Vocabulario Bitcoin.org, 2022). En principio, los usuarios de Bitcoin pueden transferir dinero entre sí a través de una red entre iguales usando software libre y de código abierto. Las transacciones son verificadas y custodiadas criptográficamente por una red descentralizada de nodos voluntarios, que registran el historial de las cuentas en una base de datos pública llamada cadena de bloques, e impide el doble gasto o la falsificación de dinero. A cambio de dicho trabajo, que es computacionalmente costoso, el protocolo de red de bitcoin recompensa a los computadores verificadores creando nuevos bitcoins. Este trabajo es conocido como minería de bitcoin.

Bitcoin - con B mayúscula, se utiliza para describir el concepto de Bitcoin, o la totalidad de la red. Mientras que bitcoin – en minúscula, se utiliza para describir una unidad del mismo. Su símbolo es ₿ y a menudo se abrevia como BTC o XBT.

2.2.13 Funcionamiento de Bitcoin mediante tecnología de red entre pares para operar sin una autoridad central o bancos intermediarios. La gestión de las transacciones y la emisión de bitcoins es llevada a cabo de forma colectiva por la red. Bitcoin es de código abierto; su diseño es público, nadie es dueño o controla Bitcoin y todo el mundo

puede participar. Por medio de sus muchas propiedades únicas, Bitcoin permite usos interesantes no contemplados por ningún sistema de pagos anterior.

Consiste en una clave criptográfica que se asocia a un monedero virtual, el cual descuenta y recibe pagos. Para su utilización, primero se debe contar con un sistema para almacenarlos y poder operar con ellos. Un usuario de la red bitcoin debe poseer un monedero electrónico, el cual contiene pares de llaves criptográficas, es decir, una clave pública y otra privada, señala una investigación de la facultad de finanzas de la Universidad de Sevilla. Los monederos pueden ser utilizados desde computadores o desde dispositivos móviles, siempre y cuando se cuente con la aplicación que posee bitcoin para realizar las operaciones.

2.2.14 ¿Cuál es el incentivo de usar Bitcoin en El Salvador? La atracción de inversionistas, la movilidad de grandes capitales con comisiones relativamente bajas con menores trámites. Las criptomonedas se han colado en la agenda económica internacional tras la espectacular revalorización de aproximadamente un 1.500 por ciento que vivió el bitcoin en 2017. El bitcoin, creado en 2009, es la criptomoneda más conocida y de mayor valor, pero existen más de mil diferentes monedas virtuales, como *Ethereum, Ripple* y *Litecoin*, entre otras.

2.2.15 ¿Qué beneficios reporta el Bitcoin a la organización?

- Agiliza las transacciones.

Si trabajas con diferentes mercados y tienes clientes de otros países, la tardanza de las transacciones financieras puede ser un dolor de cabeza. En ese caso, comprar y pagar con bitcoin es una herramienta financiera muy interesante para las pymes puesto que agiliza las transacciones económicas. Las transacciones con bitcoin son casi instantáneas y no existe la posibilidad de revocar el pago ni de emitirlo sin tener fondos.

- Reduce los errores en las transacciones.

Las transacciones en bitcoin son muy seguras, y siempre quedan registradas en una extensa red descentralizada que no depende únicamente de algunos nodos importantes,

como sucede con las redes bancarias. Así se reduce considerablemente la posibilidad de que el dinero no llegue o que sea necesario repetir la operación. Además, Bitcoin puede detectar los errores tipográficos e impide enviar dinero por error a una dirección no válida.

- Comisiones más bajas.

Los costos que implican las transacciones financieras no son nada despreciables, tanto para las grandes empresas como para las pymes y autónomos. Cada transacción no solo implica pagar comisiones bancarias, sino también pérdidas a la hora de convertir de una moneda a otra. Con el bitcoin el costo de las transacciones se reduce al mínimo ya que las comisiones son muy bajas.

- Posibilidad de captar nuevos clientes.

El interés que ha despertado el bitcoin, una criptomoneda admitida en todo el mundo, puede ayudarte a captar nuevos clientes. Comprar bitcoin y usarlos en tus transacciones comerciales te permitirá adelantarte a la competencia transmitiendo una imagen de innovación empresarial. También podría impulsar el crecimiento de tu negocio permitiéndote establecer precios más competitivos.

- Sin comisiones.
- Compra en comercios.
- Envío de fondos sin intermediarios.
- Facilidad de intercambio a dólares en cualquier momento.
- Es opcional utilizar la moneda de su preferencia (BTC o USD).

2.2.16 Desventajas que trae consigo el uso de Bitcoin.

- Objeto de especulación en cuanto a la fijación del su precio.
- Susceptible de ser usado en casos de lavado de dinero.
- Facilidad para ser usado en actividades Ilícitas, como rescates por secuestro de datos, personas y otras actividades de la red profunda.
- Requiere acceso a Internet.
- Requiere uso de un dispositivo inteligente.

2.2.17 Chivo Wallet.

Chivo Wallet es la billetera digital oficial para uso de Bitcoin y dólares estadounidenses que lanzó el Gobierno de El Salvador a través de Casa Presidencial. Chivo Wallet es una aplicación para teléfonos inteligentes, tabletas o cualquier dispositivo Android, IOS, HarmonyOS. Este monedero digital permite enviar y recibir bitcoin o dólares, y es compatible con otras billeteras *Bitcoin On-chain* y *Lightning*. Se conecta con el sistema bancario de El Salvador para depositar o retirar dólares desde la plataforma, y se encuentra enlazada a una red de cajeros automáticos propios de la marca Chivo para comprar bitcoin, depositar y retirar dólares en efectivo. Funciona en una versión de uso para personas naturales y otra para empresas o negocios que facilita cobrar, asignar terminales de cobro para empleados, y pago de impuestos.

2.3 Normativas y regulaciones locales.

Nombre	***Entrada en Vigencia***	***Entidad Emisora***
Normas Técnicas para el Sistema de Gestión de la Continuidad del Negocio	Julio 2020	(NRP-24, Comité de Normas, Banco Central de Reserva, 2020)
Ley Bitcoin	Septiembre 2021	(Ley Bitcoin, Asamblea Legislativa de la República de El Salvador, 2021)
Fideicomiso Bitcoin	Septiembre 2021	(Fideicomiso, Asamblea Legislativa de la República de El Salvador, 2021)
Normas Técnicas para Facilitar la Participación de Entidades Financieras en el Ecosistema Bitcoin.	Septiembre 2021	(NRP-29, Comité de Normas, Banco Central de Reserva, 2021)

Tabla 1 Normativas y regulaciones locales
Fuente: Elaboración propia

2.4 Definición de buenas prácticas.

La ISO-22301 se redactó por los principales expertos en la materia y provee el mejor marco de referencia para la gestión de la continuidad del negocio en las empresas. Implementada lealmente, la gestión de la continuidad del negocio reducirá la posibilidad de suceso de un incidente y, en caso de darse, la organización estará preparada para responder de forma atenta y, así, reducir tajantemente el daño de ese incidente. ISO 22301 sirve para que su organización pueda seguir operando, incluidas

2.5 La Norma ISO 22301.

Fue el primer estándar internacional del mundo para implementar y mantener planes, sistemas y procesos efectivos de continuidad del negocio cuando se publicó en 2012. Ahora ha sido revisada para actualizarla con las últimas ideas y mejores prácticas desde su última publicación en octubre de 2019 ISO 22301:2019 Seguridad y resiliencia — Sistemas de gestión de la continuidad del negocio — Requisitos. La ISO 22301 es aplicable a todas las organizaciones, independientemente del tamaño, la industria o la naturaleza del negocio. También es relevante para los organismos reguladores y de certificación, ya que les permite evaluar la capacidad de una organización para cumplir con sus requisitos legales o reglamentarios. Basado en la Estructura de Alto Nivel de ISO, se alinea con muchos otros estándares de sistemas de gestión reconocidos internacionalmente, como ISO 9001 (gestión de calidad) e ISO 14001 (gestión ambiental). Como tal, está diseñado para integrarse en los procesos de gestión existentes de una organización.

La ISO 22301 es una herramienta útil para profesionales de riesgo y continuidad del negocio, directores de cadenas de suministro, gerentes de auditoría y asociados, desarrolladores de informes de responsabilidad social corporativa, organismos reguladores y cualquier otra persona involucrada o interesada en la continuidad del negocio.

2.6 El Ciclo de Edward Deming.

También conocido como ciclo PDCA (del inglés Plan-Do-Check-Act) o PHVA (de la traducción oficial al español como Planificar-Hacer-Verificar-Actuar) o espiral de mejora continua, es un método sistemático para la resolución de problemas con el fin de generar una mejora continua de la calidad, en cuatro pasos, según el concepto ideado por Walter A. Shewhart, amigo y mentor de William E. Deming que lo enseñó en el Japón de los años 1950 (Plan, Do, Check & Act. INCIBE, 2019). A veces también es, por ello, denominado Ciclo Deming-Shewhart.2. Es muy utilizado por los Sistemas de Gestión de la Calidad (SGC), los Sistemas de Gestión Ambiental (SGA) y los Sistemas de Gestión de la Seguridad de la Información (SGSI), regulados por ISO, así como en modelos de

Gestión de la Calidad Total (EFQM, Fundibeq, Malcolm Baldrige National Quality, etc). Los resultados de la implementación de este ciclo permiten a las organizaciones una mejora integral de la competitividad, de los productos y servicios, mejorando continuamente la calidad, reduciendo los costos, optimizando la productividad, reduciendo los precios, incrementando la participación del mercado y aumentando la rentabilidad.

2.7 Sistema de Gestión de Continuidad del Negocio.

Un Sistema de Gestión de Continuidad de Negocio (En lo sucesivo abreviado SGCN) certificado bajo la norma ISO 22301 es el estándar de mayor aceptación a nivel internacional, y ayuda a las organizaciones a prepararse para las emergencias, a gestionar las crisis y mejorar su capacidad de recuperación operacional, asegurar la cadena de suministro y protegerse, por ejemplo, su reputación ante una crisis (ISO 22301:2019, Tony Bevan, 2020).

2.8 Análisis de impacto del negocio.

Análisis de Impacto al Negocio (En lo sucesivo abreviado AIN): identifica, cuantifica y califica los impactos en el tiempo de una pérdida, interrupción o perturbación de las actividades de negocios en una organización a nivel estratégico, táctico y operativo; y proporciona los datos a partir de los cuales se pueden determinar estrategias de continuidad adecuadas (ISO 22301:2019, Tony Bevan, 2020). La decisión de qué productos y servicios están contenidos en el alcance del programa de Gestión de Continuidad de Negocio, se realiza antes del AIN, y debe estar documentado en la política de SGCN. Se debe determinar el Período Máximo Tolerable de Interrupción (en lo sucesivo abreviado PMTI), que es el período de tiempo dentro del cual, si no se pudieran reanudar las actividades, los impactos llegarían a ser inaceptables para la organización; amenazando su normal desempeño o haciendo que sus objetivos ya no sean alcanzables.

2.9 Plan de continuidad del negocio.

El Plan de Continuidad del Negocio, en lo sucesivo abreviado (PCN), es un plan que se diseña para mantener la operación normal de la compañía en caso de que se presente alguna eventualidad que pueda afectar de manera directa o indirecta las actividades cotidianas (ISO 22301:2019, Tony Bevan, 2020). Gracias a esto las empresas pueden contar con planes de contingencia que contribuyen a mitigar los riesgos y el impacto dentro de la compañía.

Este tipo de sistemas les permite a las empresas restablecer sus operaciones luego de sufrir un incidente que haya ocasionado problemas en el desarrollo de las actividades cotidianas. Así mismo, contribuye en la protección de la reputación de la institución, la prevención en pérdidas económicas, el servicio al cliente y el cumplimiento de plazos. Por otro lado, también permiten que se anticipen a los riesgos a los que están expuestos, pues ayuda a que se puedan preparar planes en caso de sufrir una emergencia catastrófica, y cómo actuar frente a esa crisis.

Un buen plan de contingencia debe incluir escenarios para anticipar desastres naturales como terremotos, incendios y huracanes. Crisis de personal; incluidas lesiones y accidentes en el lugar de trabajo, así como huelgas y muertes de empleados. Pérdida de datos; problemas de productos, como reubicaciones de planes, mala gestión, como destrucción accidental y robo. Generalmente se compone de un conjunto de otros planes como los mencionados a continuación:

- Plan de Contingencia, que incluye el detalle de actividades a realizar.
- Plan de Emergencia, incluyendo el manejo de desastres naturales o accidentes.
- Plan de Crisis, que incluye manejo de la crisis por el Comité de Crisis.
- Plan de Reanudación, que contiene la guía para volver a las actividades operativas normales.
- Plan de Restauración, que se refiere a como operar la contingencia.
- Plan de Comunicación, relacionado a las actividades de comunicación a las partes interesadas.
- Plan de Ejercicios y Pruebas, con su respectivo cronograma.

- Plan de Mitigación, con el detalle de mitigación de riesgos.
- Plan de Manejo de Incidentes, esperados e inesperados.

2.10 Fases de un Plan de Continuidad de Negocio.

2.10.1 Determinación delimitante.

Se debe clasificar cada una de las áreas dándole una clasificación de prioridad a cada una de ellas, con el fin de entender cuáles son las más vulnerables y de esta manera poder ir trabajando en la continuidad de la organización, en este punto es clave la participación de la dirección (Plan, Do, Check & Act. INCIBE, 2019).

2.10.2 Análisis de la empresa.

Se debe recoger toda la información de la organización con el fin de identificar cuáles son los procesos de negocios críticos (activos), cómo se les dará soporte y cuáles son las necesidades que se presentan (Plan, Do, Check & Act. INCIBE, 2019).

2.10.3 Determinación de la estrategia.

Una vez estén definidos los activos se debe establecer que si en caso de que se llegue a presentar una amenaza están en la capacidad de recuperar estos activos en corto plazo, si por el contrario requiere de un tiempo mayor se deben establecer estrategias (Plan, Do, Check & Act. INCIBE, 2019).

2.10.4 Respuesta a la contingencia.

Se elegirán las estrategias necesarias que se podrán en marcha en caso de presentarse un desastre y se creará un plan de crisis en donde se documentará toda la información (Plan, Do, Check & Act. INCIBE, 2019).

2.10.5 Pruebas, mantenimiento y revisión.

En este punto es demasiado importante contar con recursos tecnológicos que permitirán crear planes de prueba, mantenimiento y revisión, para identificar cuáles son las buenas prácticas y en qué se debe mejorar (Plan, Do, Check & Act. INCIBE, 2019).

2.10.6 Concienciación.

Se debe crear una cultura dentro de la organización para que todos los empleados conozcan el plan de acción y se apropien de la situación, al igual que entiendan cuál será su rol dentro de este plan. Tener un Plan de Continuidad de Negocio bien estructurado,

con estrategias para reaccionar ante diferentes escenarios puede ser la diferencia entre reaccionar a tiempo y de forma eficiente a una eventualidad o no ser capaces de mantener la operación en la empresa. Además, lo ideal es que cada cierto periodo se revise el Plan de Continuidad de Negocio y se adecue a los cambios que haya tenido la organización en los equipos de trabajo o en los sistemas implementados.

2.11 Plan de Recuperación de Desastres.

El plan de recuperación ante desastres es una parte del plan de continuidad de negocio (ISO 22301:2019, Tony Bevan, 2020). Está relacionado con el área de Tecnologías de la Información, (en lo sucesivo abreviado TI) y se refiere a las acciones que se van a emprender para resolver cualquier eventualidad que impida que el personal pueda acceder al sistema, ya sea un desastre natural, un ataque informático o una contingencia.

El Plan de Recuperación de Desastres también contempla establecer el tiempo objetivo de recuperación, que es el periodo máximo que puede tardar el negocio en reanudar operaciones; y el punto objetivo de recuperación, es decir; el punto máximo de datos que se pueden perder en el evento sin comprometer el resto de la información.

Por su parte, el Plan de Continuidad de Negocio establece toda la estrategia para hacer frente a una eventualidad, no sólo ante un evento repentino. Por ejemplo, también puede abarcar el Plan de Gestión de Incidentes, que contempla algún incidente de seguridad, sin que haya una interrupción total de la operación o una gran pérdida de datos.

Capítulo III Metodología de la Investigación.

3.1 Tipo de investigación.

La investigación a realizar es de tipo Análisis de Contenido la cual tendrá como base principal el estándar ISO22301:2019 así como las normativas NRP-24 y NRP-29 de las cuales cualitativamente se propondrá exponiendo el uso de las buenas prácticas. El enfoque cualitativo está dado por lo que se encuentra dictaminado en el marco legal, así como también los funcionamientos de los procesos. Y una vez realizado el análisis de contenido de la norma, se identificarán los controles que servirán mayormente como una guía que podrá adoptada en una entidad financiera. (Ver anexo 2 “Organigrama Institucional”).

3.2 Unidades de análisis.

Las Unidades de Análisis son la documentación sobre implementación de Bitcoin en El Salvador, como la Ley Bitcoin, Normas Técnicas para el Sistema de Gestión de la Continuidad del Negocio NRP-24, Normas Técnicas para Facilitar la Participación de las Entidades Financieras en el Ecosistema Bitcoin NRP-29 y la Internacionalmente aceptada ISO22301 Seguridad y resiliencia, Sistemas de gestión de la continuidad del negocio.

3.3 Variables y su medición.

3.3.1 Variable 1: Buenas prácticas referentes a la implementación del bitcoin.

3.3.2 Variable 2: Aspectos Técnicos y Tecnológicos.

3.3.3 Variable 3: Implicaciones en la forma de declarar impuestos y patrimonio

Para esta terna de variables su utilizará los instrumentos Cuadro de Comparativo y Hoja de Observaciones.

Matriz de Congruencia.

Unidad de análisis	Variables	Técnica	Instrumento
Documentación sobre implementación de Bitcoin	V1 - Buenas prácticas referentes a la implementación del bitcoin.	Entrevista	Cuestionario
			Cuestionario
Norma ISO 22301	V2 - Aspectos Técnicos y Tecnológicos.		Cuestionario
Ley Bitcoin			
NRP-24			Cuestionario
NRP-29			
Ley Bitcoin	V3 - Implicaciones en la forma de declarar impuestos y patrimonio.		Cuestionario
NRP-24			
NRP-29			Cuestionario

Tabla 2 Matriz de Congruencia
Fuente: Elaboración propia.

3.4 Procesamiento y análisis de la información.

Los elementos de análisis de información se basan por un lado en la Norma ISO 22301 y por otro lado también en la Ley Bitcoin. La revisión de registros consiste en la lectura y análisis de las leyes, regulaciones y normativas locales como; Ley Bitcoin, NRP-24, NRP-29 y Norma ISO 22031.

Entrevista semiestructurada: Es un método especial en la recolección de la información, aplicada principalmente a personas que no poseen el tiempo para llenar un cuestionario. Consiste en la realización de diálogos con las personas interesadas, el investigador propone temas de manera estratégica de tal forma que la conversación fluya acorde a los temas. NRP-24, y NRP-29. (Ver anexo 3 “Guía de entrevista”).

Capítulo IV Análisis y Discusión de Resultados.

Con el propósito de dar respuesta al objetivo de “Desarrollar una guía de buenas prácticas para la implementación de Bitcoin en El Salvador tomando como referencia la norma ISO22301”, se plantearon tres objetivos específicos; con el fin de lograr cada uno de estos se identificaron unidades de análisis o sujetos de estudio, de los cuales se derivaron variables que ayudaran al cumplimiento de los objetivos específicos.

4.1 Resultados del objetivo específico 1.

Documentar las buenas prácticas que se adoptaron al momento de la implementación de Bitcoin como moneda de pago por un ente financiero.

La unidad de análisis que se estudió para dar respuesta al primer objetivo específico relacionado a la documentación de las buenas prácticas en la implementación de Bitcoin fue la “Documentación sobre la implementación de Bitcoin”.

Unidad de Análisis	Variable	Resultado
Documentación sobre la implementación de Bitcoin	NRP-29 Normas Técnicas para facilitar la participación de entidades financieras en el Ecosistema Bitcoin.	Entendimiento del marco documental y buenas prácticas relacionadas al ecosistema Bitcoin, obligaciones de las entidades, registro de las entidades y disposiciones generales.

Tabla 3 Resultados del objetivo específico 1.
Fuente: Elaboración propia.

Se ha tomado como referencia una entidad financiera a través de una aplicación tercerizada como lo es Chivo Wallet, así mismo se entrevistó al encargado de Continuidad del Negocio el cual comentó que la normativa fue implementada de manera muy rápida ya que, a nivel global, ningún país ha utilizado el Bitcoin como una moneda de curso legal y aunque el BCR regula su uso en el sector financiero, estas no avalan su total valor monetario para intercambio de operaciones.

4.2 Resultados del objetivo específico 2.

Describir los aspectos técnicos y tecnológicos apegados a la Norma ISO 22301 para adoptar el uso del Bitcoin.

Las unidades de análisis que se estudiaron para dar respuesta al segundo objetivo específico relacionado a la descripción de aspectos técnicos y tecnológicos apegados a la Norma ISO 22301, fueron la ISO22301 como estándar o buena práctica internacional, la Ley Bitcoin, La normativa NRP-24 “Normas Técnicas para el Sistema de Gestión de la Continuidad del Negocio” y la NRP-29 “Normas Técnicas para Facilitar la Participación de las Entidades Financieras en el Ecosistema Bitcoin”.

Unidad de Análisis	Variable	Resultado
ISO22301	Aspectos Técnicos y Tecnológicos	Guía de implementación de buenas prácticas relacionadas al sistema de Gestión de Continuidad del Negocio
Ley Bitcoin	Aspectos Técnicos y Tecnológicos	Definición de Bitcoin, método de intercambio de Bitcoin mediante clave criptográfica por medio del método Peer To Peer, exclusiones y vigencia.
NRP-24	Aspectos Técnicos y Tecnológicos	Roles y responsabilidades de Junta Directiva, Comités y Unidad de Riesgo en la Gestión de Continuidad del Negocio.
NRP-29	Aspectos Técnicos y Tecnológicos	Sujetos obligados al cumplimiento de las disposiciones establecidas: Bancos, Bancos Cooperativos, Sociedades de Ahorro y Crédito, Proveedores de dinero electrónico. Obligaciones pertinentes para Ley de Bitcoin y reglamento, relaciones contractuales con Proveedor del servicio de Bitcoin, capacidad operativa, reporte de operaciones sospechosas y sanciones por incumplimiento.

Tabla 4 Resultados del objetivo específico 2.
Fuente: Elaboración propia.

4.3 Resultados del objetivo específico 3.

Referenciar el marco legal y regulatorio sobre el uso de Bitcoin como medio de transacción, aplicables a instituciones financieras.

Las unidades de análisis utilizadas para dar respuesta a este objetivo son la Ley Bitcoin y como regulación emitida por la Superintendencia la NRP-29: Normas Técnicas para Facilitar la Participación de las Entidades Financieras en el Ecosistema Bitcoin.

Unidad de Análisis	Variable	Resultado
Ley Bitcoin	Disposiciones generales, finales y transitorias.	Conceptos y partes involucradas en el proceso de transacciones mediante Bitcoin. Disposiciones Generales, finales y transitorias
NRP-29	Herramientas de detección de lavado de activos, financiación al terrorismo.	Reporte de operaciones sospechosas

Tabla 5 Resultados del objetivo específico 3.
Fuente: Elaboración propia.

Adicionalmente para dar respuesta a este objetivo, se elaboró una entrevista a experto de continuidad en una institución financiera, el cual nos mencionó como principales regulaciones aplicables La Ley bitcoin y la NRP-29: Normas Técnicas para Facilitar la Participación de las Entidades Financieras en el Ecosistema Bitcoin, las cuales son de obligatorio cumplimiento y de las mismas se apoyan para la implementación de su Sistema.

Capitulo V Propuesta de Implementación de Buenas Prácticas según la Norma ISO 22301

5.1 Identificar requisitos legales y reglamentarios.

Para nuestro análisis propuesto, las normativas y leyes aplicables a las entidades Bancarias y al ecosistema Bitcoin, se resumen en tres principales:

- NRP-24 Normas Técnicas para el Sistema de Gestión de la Continuidad del Negocio. El Banco Central de Reserva (en lo sucesivo abreviado BCR) cuenta con normativas para la implementación de sistemas de gestión, entre ellas la NRP-24, la cual entra en vigor a partir del día uno de julio del dos mil veinte y comprende todo el marco normativo de SGCN que permite mejorar de manera significativa el nivel de resiliencia de las organizaciones. A continuación, se presenta un diagrama resumen de la normativa.

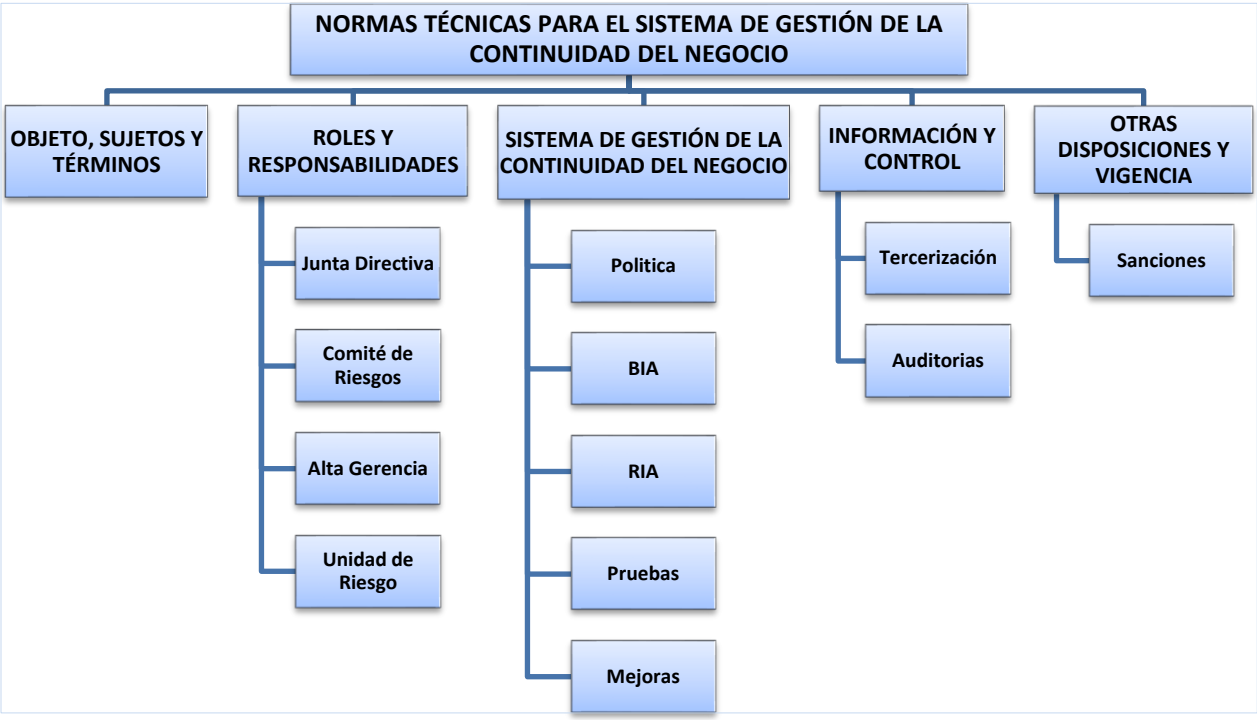


Ilustración 1 Diagrama resumen de la normativa NRP24
Fuente: Elaboración propia.

- NRP-29 Normas Técnicas para facilitar la participación de entidades financieras en el Ecosistema Bitcoin. La cual entra en vigor a partir del 7 de septiembre del año dos mil veintiuno y comprende todo el marco normativo relacionado al Bitcoin. A continuación, se presenta un diagrama resumen del contenido de la norma expuesta.

Ilustración 2 Diagrama resumen de la normativa NRP29
Fuente: Elaboración propia.

- Ley Bitcoin. El nuevo marco legal, reconoce a esta divisa digital como una moneda de curso legal en el país. La ley ampara, además, que la criptomoneda sea con irrestricto poder liberatorio, ilimitada en cualquier transacción y a cualquier título. Dicha Ley entra en vigor a partir del 7 de septiembre de 2021 entra en vigor en El Salvador la Ley Bitcoin.

Ilustración 3 Diagrama resumen de la Ley Bitcoin.
Fuente: Elaboración propia.

5.2 Establecer el alcance y las exclusiones del SGCN.

En esta sección se debe definir dónde se implementará el Sistema de Gestión de Continuidad del Negocio, incluyendo los límites del lugar o lugares físicos incluidos, los grupos de empleados internos y externos incluidos, los procesos relacionados, actividades a desarrollar, productos o servicios internos y externos incluidos. Si se requiere priorizar los recursos mediante la creación de un sistema de gestión de continuidad de negocio que no cubra toda su organización o sus actividades, la selección de un alcance limitado a la gestión de los intereses de las partes interesadas clave es un enfoque pragmático. Para ello, se pueden incluir sólo centros, activos, procesos, productos y unidades de negocio o departamentos específicos.

Alcance: Establecer los procedimientos técnicos, así como los mecanismos oportunos para lograr la recuperación de la disponibilidad de los activos clave de la organización y garantizar su alineamiento estratégico, así como su capacidad de poder ser auditado y hacerlo de obligado cumplimiento a todas las dependencias de la organización.

El propósito del sistema de Gestión de Continuidad del Negocio, aplicado a entidades bancarias que deben hacer uso del ecosistema Bitcoin dentro de sus procesos debe buscar prioritariamente:

5.2.1 Proteger la integridad física de los colabores, clientes, activos y partes interesadas de la organización antes cualquier escenario de interrupción.

5.2.2 Preparar a la organización en las acciones necesarias para mantener la disponibilidad de sus servicios ante interrupciones de alto impacto.

5.2.3 Cumplir con los requerimientos regulatorios legales relacionados a la gestión de continuidad.

5.2.4 Aplicar el ciclo de mejora continua en las actividades críticas de entidad ante evento disruptivos.

5.2.5 Gestionar los riesgos relacionados a la continuidad de negocio. Dentro de su alcance se deben establecer los procedimientos técnicos, así como los mecanismos oportunos para lograr la recuperación de la disponibilidad de los activos clave de la organización y garantizar su alineamiento estratégico, así como su capacidad de poder ser auditado y hacerlo de obligado cumplimiento a todas las dependencias de la organización bajo el marco regulatorio establecido en las normativas NRP-24 y 29, así como en las leyes locales (Ley Bitcoin) apoyadas en el estándar ISO22301:2019.

Las exclusiones por considerar serán los procesos que después del análisis la organización determine que no son críticos o indispensables para su operación.

5.3 Definir la política de continuidad del negocio

En esta sección es importante definir las responsabilidades principales y la intención de la gerencia. Una responsabilidad vital de la dirección es establecer y documentar una Política de Continuidad de Negocio que esté alineada con la dirección estratégica de la organización, es por ello que para poder implementar el SGCN en una organización, además de establecer las políticas y procedimientos, es importante entender hacia dónde va la entidad, es decir, conocer la estrategia principal (Ver anexo 4 “Política de

Continuidad de negocio"). Los requisitos del SGCN deben integrarse en los procesos de negocio y contar con los recursos adecuados.

5.3.1 El perfil de la política deberá:

- Ser apropiada para el propósito de la organización.
- Proporcionar un marco referencial para establecer los objetivos de continuidad de las operaciones.
- Incluir el compromiso de cumplir los requisitos aplicables.
- Incluir el compromiso de mejorar continuamente el SGCN.
- Comunicar disposiciones con la organización.
- Estar a disposición de las partes interesadas, según proceda.
- La Política de Continuidad de Negocio puede referirse a, o incluir sub-políticas que cubran, procesos y actividades clave que son importantes para la provisión continua de productos y servicios clave en caso de un incidente disruptivo y la recuperación de las operaciones normales. Para demostrar la importancia de la Política de Continuidad de Negocio, ésta debe ser autorizada por la Alta Dirección. (ver anexo 5 "Políticas Generales de la Organización").

5.3.2 Los principios y compromisos de la política de continuidad del negocio sustentada en:

- La protección y seguridad de las personas es la primera premisa y el objetivo prioritario, tanto en situación normal como en situación de crisis derivada de un desastre, con respecto a la seguridad ocupacional.
- El nombramiento de representantes de las distintas áreas con la debida experiencia y conocimiento, para que participen activamente en la elaboración, implantación, revisión, prueba y actualización de los Planes de Continuidad de Negocio.
- El desarrollo e implantación de Planes de Continuidad de Negocio será teniendo en cuenta las áreas y departamentos internos, proveedores y servicios y empleando sistemas, recursos y procedimientos adecuados y proporcionados.
- El aprovechamiento de las sinergias generadas en el desarrollo e implantación de los Planes de Continuidad de Negocio, contemplando los medios y recursos comunes de los que dispone toda la organización.

- La adopción de medidas razonables para la continuidad operativa de los procesos y actividades, en función de la criticidad de los mismos establecida por la Organización.
- La inclusión de criterios de seguridad, privacidad y fiabilidad que garanticen de forma razonable la continuidad de los servicios críticos proporcionados por terceros, en caso de su externalización.
- La elaboración, dentro de los Planes de Continuidad de Negocio, de procedimientos de comunicación apropiados, tanto internos como externos, que posibiliten la correcta ejecución de los mismos, así como el suministro oportuno de información a todas las partes interesadas.
- La comunicación a todo el personal de sus responsabilidades y de los procedimientos que le competen, en el marco de la continuidad de negocio, mediante labores de concienciación y formación.
- El desarrollo de un SGCN que contemple la realización de revisiones, pruebas y actualizaciones de los Planes de Continuidad de Negocio de forma periódica o ante cambios significativos, en un proceso de mejora continua de los mismos.
- La permanente disposición a colaborar con las autoridades en cuanto a la prevención de lavado de dinero, y cualquier otra solicitud judicial debidamente diligenciada.

5.3.3 Establecer los objetivos de continuidad del negocio.

Es importante en esta sección, definir los objetivos medibles que deben lograrse con la continuidad del negocio. Los objetos de continuidad de la actividad deben establecerse en las funciones y niveles pertinentes de una organización; los objetivos pueden ser a nivel organizativo o departamental.

Los objetivos deben ser:

- Coherentes con la política de continuidad de las actividades.
- Ser medibles.
- Tener en cuenta los requisitos aplicables.
- Ser comunicados.
- Se supervisa y se actualiza según proceda.

5.3.4 Los objetivos de continuidad de negocios y la planificación para lograrlos.

- Diseñar, planificar y ejecutar un análisis de riesgos de disponibilidad sobre los diferentes activos de la organización, cuya continuidad resulte imprescindible para que la misma pueda prestar sus servicios a un nivel mínimo aceptable.
- Diseñar, planificar y ejecutar la Estrategia de Continuidad del Negocio en los diferentes niveles, así como los procedimientos y mecanismos que llevará a cabo la organización para hacer frente a los riesgos detectados y lograr el alineamiento con la estrategia con los Objetivos de la Organización
- Establecer y definir los niveles de recuperación aceptables del Servicio, así como los mecanismos oportunos para lograr la recuperación de la disponibilidad de los activos clave de la organización y garantizar su alineamiento estratégico, eficacia, así como su capacidad de poder ser auditado.
- Restablecer el Servicio a la situación anterior al imprevisto, donde se debe diseñar los diferentes procedimientos a seguir para garantizar una transición ordenada desde la situación actual una vez ocurrida la contingencia, hacia la actividad habitual de la organización, previa a la ocurrencia de la contingencia.
- Mantener actualizado del Plan de Continuidad de Negocio, de manera continua y permanente mediante métodos y procedimientos, tales que permitan la fluidez y de la continuidad del negoció en la misma proporción de crecimiento de la organización.
- Diseñar, planificar y ejecutar las respectivas pruebas, ensayos y simulaciones tanto a nivel organizativo como técnico, para asegurar una adecuada gestión de la Continuidad del Negocio de acuerdo con los parámetros de la ISO22301.

Los objetivos deben ser comunicados a las personas pertinentes dentro de la organización; deben ser supervisados y actualizados según sea necesario. Para ello se debe establecer un plan para alcanzar sus objetivos; el plan debe tener en cuenta:

- Lo que se debe hacer.
- Los recursos necesarios.
- Quién es responsable.
- Fecha de consecución.

- Cómo evaluar los resultados.

5.4 Definir las competencias requeridas del personal.

Definir el conocimiento y las habilidades necesarias. La implantación de un SGCN eficaz depende en gran medida de los conocimientos y las capacidades de sus empleados, proveedores y contratistas. Para tener la certeza de contar con una base de conocimientos y habilidades adecuada, es necesario:

- Definir los conocimientos y las competencias necesarias.
- Determinar quién debe tener los conocimientos y las habilidades.
- Verificar que las personas adecuadas tienen los conocimientos y las habilidades correctas.

A continuación, se presentan las principales competencias identificadas, del personal que deberá intervenir en el desarrollo del SGCN:

PRIORIDAD	CARGO	ROL EN TI	COMPETENCIAS
1. Critico	Coordinador de Continuidad del negocio	Líder plan de Contingencia	Conocimientos ISO22301 Leyes y Regulaciones Locales relacionadas a Continuidad del Negocio Licenciatura en administración de empresas, Ingeniería en sistemas o similares Deseable Maestría en Riesgos Informáticos Experiencia de 1 año en puestos similares
1. Critico	Especialista de Continuidad de negocios TI	Colaborador	Conocimientos ISO22301 Leyes y Regulaciones Locales relacionadas a Continuidad del Negocio Graduado en Ingeniería en sistemas informáticos o similares Deseable Maestría en informática Experiencia de 1 año en puestos similares
2.Medio	Incident Manager	Colaborador	Graduado en Ingeniería en sistemas informáticos o similares Experiencia de 1 año en puestos similares
2.Medio	Problem Manager	Colaborador	Ingeniería en sistemas informáticos o similares Experiencia de 1 año en puestos similares
1. Critico	Gerente de TI	Gerente	Conocimientos de Leyes y Regulaciones Locales bancarias Graduado en Ingeniería en sistemas informáticos o similares Deseable Maestría en informática Experiencia de 5 años en puestos similares

1.Critico	Gerente Negocio	Colaborador	Conocimientos de Leyes y Regulaciones Locales bancarias Graduado en licenciatura o Ingeniería Deseable Maestría Experiencia de 5 años en puestos similares
1.Critico	Líder especialista de Negocio	Colaborador	Conocimientos de Leyes y Regulaciones Locales bancarias Graduado en licenciatura o Ingeniería Experiencia de 3 años en puestos similares

Tabla 6 Competencias identificadas del personal de gestión de continuidad de negocio.
Fuente: Elaboración propia.

5.5 Realizar el análisis de impacto empresarial y evaluación de riesgos.

Una organización debe implantar y mantener un proceso para analizar el impacto al negocio y evaluar el riesgo de interrupción de sus actividades clave. Los resultados del análisis del impacto en el negocio y de la evaluación del riesgo permitirán a una organización determinar la estrategia y la solución adecuadas necesarias para responder a un incidente disruptivo. Dicho análisis debe tomar en cuenta todos los productos que la entidad financiera ofrecerá a los clientes, así como los procesos relacionados. Además, debe identificar, cuantificar los impactos regulatorios, financieros, reputacionales, legales y operativos que se generen a raíz de eventos de interrupción. Así mismo dentro del análisis se deben identificar la Interrupción Máxima Aceptable, el Período Máximo Admisible de Interrupción, Punto Objetivo de Recuperación y Tiempo Objetivo de Recuperación.

También se recomienda que el análisis de impacto del negocio debe ser actualizado periódicamente a un máximo plazo de un año, de preferencia en ciclos menores de tiempo, con el objetivo de identificar cambios en los procesos o servicios. (Ver anexo 6 “Listado de servicios que pueden ser pagados con Bitcoin en El Salvador”). En primera instancia, realizar la evaluación de Riesgos relacionados a incidentes disruptivos que impacten a la herramienta que nos brinda el servicio, como canal de servicio: Chivo Wallet.

Los resultados del análisis del impacto en el negocio y de la evaluación del riesgo permitirán a una organización determinar la estrategia y la solución adecuadas

necesarias para responder a un incidente disruptivo. El riesgo consiste en la probabilidad de que, la ocurrencia de un suceso adverso afecte a la entidad e impacte en su habilidad para lograr sus objetivos y por ende la capacidad de cumplir su misión y visión.

Identificar los incidentes disruptivos relacionados a Chivo Wallet. Riesgos Identificados:

- Manejo de usuarios y contraseña Chivo Wallet.
- Errores en la ejecución de tareas operativas.
- Problemas de software que afectan servicios críticos.
- Inadecuado esquema de contingencia de software.
- Términos y condiciones de uso de Chivo Wallet.

Identificar los incidentes disruptivos relacionados al Bitcoin.

- Gestión de riesgos de las amenazas concretas.
- En caso de Denegación de Servicio de Chivo Wallet, se puede remediar mediante otras formas de transacción como el dinero en efectivo, Tarjetas de Crédito, Tarjetas de Débito, Cheques y Cobro de Remesas, entre otros.

Otros riesgos a considerar son detallados a continuación:

- Riesgo de Crédito: Es la posibilidad de pérdida, debido al incumplimiento de las obligaciones contractuales asumidas por una contraparte, entendida esta última como un prestatario o un emisor de deuda.
- Riesgo de Liquidez: Es la posibilidad de incurrir en pérdidas por no disponer de los recursos suficientes para cumplir con las obligaciones asumidas, incurrir en costos excesivos y no poder desarrollar el negocio en las condiciones previstas.
- Riesgo de Mercado: Es la posibilidad de pérdida, producto de movimientos en los precios de mercado que generan un deterioro de valor en las posiciones dentro y fuera del balance o en los resultados financieros de la entidad.

- Riesgo Operacional: Es la posibilidad de incurrir en pérdidas, debido a las fallas en los procesos, el personal, los sistemas de información y a causa de acontecimientos externos; incluye el riesgo legal.
- Riesgo Reputacional: Es la posibilidad de incurrir en pérdidas, producto del deterioro de imagen de la entidad, debido al incumplimiento de leyes, normas internas, códigos de gobierno corporativo, códigos de conducta, lavado de dinero, entre otros.

El análisis del impacto en el negocio se realiza una vez finalizada la evaluación de riesgos, y para la realización de dicho análisis se deberá completar de acuerdo con las siguientes etapas:

DATOS DEL SERVICIO	
Fecha de análisis	10 de abril 2022
Servicio afectado	Recepción de pagos
Procesos críticos	Pago de Tarjeta en Bitcoin Pago de Préstamo en Bitcoin Pago de Colectores en Bitcoin Pago de Pólizas de seguros en Bitcoin Abono a Cuenta en Bitcoin
Área responsable	Operaciones
Especialista de negocio	Jefatura de Pagos
Especialista de tecnología	Desarrollo de sistemas
Descripción del servicio	Pagos y abonos en Bitcoin

Tabla 7 Datos del servicio
Fuente: Elaboración propia.

En la sección datos del servicio, se deben colocar los datos generales tales como, fecha de análisis, servicio afectado, procesos críticos, área responsable, especialista de negocio, especialista de tecnología, descripción del servicio.

Establecer Fechas Criticas	
Meses Críticos	Junio y diciembre
Fechas Criticas	15 y 30 de cada mes
Días Críticos	Lunes y sábado
Horas Críticas	12:00 del medio día

Tabla 8 Establecer fechas críticas.
Fuente: Elaboración propia.

Se deben establecer las fechas más críticas del calendario en las que se presentarían mayor impacto en caso de interrupción, como fechas de pago de salarios, temporadas festivas.

Definir Tiempo de Recuperación Objetivo	
RTO de Negocio	30 minutos de traslado en agencias más cercanas
RTO de Tecnología	1 hora en levantar el servicio en caso de interrupción
RTO de Proveedor	30 minutos en levantar aplicación Chivo Wallet
RTO Real	1:00 Se toma el mayor tiempo (1 hora)

Tabla 9 Tiempo de Recuperación Objetivo.
Fuente: Elaboración propia.

Parte esencial del análisis es el establecimiento del Tiempo de Recuperación Objetivo, el cual nos indica el tiempo máximo disponible para levantar el servicio a su estado normal sin exponer a la organización, considerando como RTO Real, el mayor o más prolongado de entre todos los tiempos de las diferentes áreas, en este caso 1 hora por el RTO de Tecnología.

Identificación de Canales	
Agencias	Si Aplica
Aplicación Móvil	Si Aplica
Portal Web	No Aplica
Chat de asistencia	No Aplica
Call Center	No Aplica
Cajeros Automáticos	No Aplica
Sistemas de Puntos de Venta (POS)	No Aplica

Tabla 10 Identificación de Canales.
Fuente: Elaboración propia.

Así mismo, es importante identificar los canales que intervienen en la prestación del servicio.

Cálculo del máximo periodo tolerable de disrupción.		
Impacto Financiero*	Monto de Transacciones en Agencias $15,954 Total de Transacciones en Bitcoin: 31 Impacto Financiero: $15,954/150 días = $ 106.36 /8 horas Total Impacto Financiero por Hora: $13.30	Alto
Impacto Legal	Ley Bitcoin,	Medio
Impacto Regulatorio	NRP-29 NRP-24	Medio
Impacto Reputacional	Accionistas (X) Colaboradores (X) Clientes (X) Proveedores (X) Socios estratégicos Gobiernos (X) Entes reguladores (X) Comunidades Público en General Generadores de opinión (X) Medios de Comunicación (X)	Medio

Tabla 11 Cálculo del máximo periodo tolerable de disrupción.
Fuente: Elaboración propia.

Valores obtenidos de Informe Interno Chivo Wallet Empresarial del periodo noviembre 2021 a marzo 2022. Para obtener el nivel de impacto financiero por cada hora de interrupción del servicio, se divide el monto total de transacciones en Bitcoin en agencias entre el total de días en el periodo mencionado.

Recursos	
Mobiliario	Acceso a sistemas internos Conexión a Internet Acceso a correo interno Escritorio Sillas Teléfono Computadora Impresora Office Puntos de RED Celular
Personal Critico	Coordinador de Continuidad del negocio Especialista de Continuidad de negocios TI Incident Manager Problem Manager Gerente de TI

	Gerente Negocio Líder especialista de Negocio
Edificios	40 agencias a nivel Nacional

Tabla 12 Recursos críticos.
Fuente: Elaboración propia.

Se deben identificar los recursos críticos que ayudaran al personal critico a garantizar y mantener la estrategia mínima de funcionamiento establecida.

Identificación de Sitios Alternos			
Ubicación de sitio operativo principal	**Ubicación de sitio operativo alterno**	**Distancia en KM**	**Tiempo de traslado**
Edificio/Sede principal	Edificio/Sede alterno 1	10 KM	30 minutos
Edificio/Sede principal	Edificio/Sede alterno 2	20 KM	60 minutos
Edificio/Sede principal	Edificio/Sede alterno 3	30 KM	90 minutos

Tabla 13 Identificación de Sitios Alternos
Fuente: Elaboración propia.

En caso de que el sitio operativo principal este inhabilitado es muy útil tener identificado los sitios alternos para traslado del personal y equipo.

Actividades de a realizar por procesos identificados				
Pago de Tarjeta en Bitcoin.	**Pago de Préstamo en Bitcoin.**	**Pago de Colectores en Bitcoin.**	**Pago de Pólizas de seguros en Bitcoin.**	**Abono a Cuenta en Bitcoin.**
Cajero Solicita los fondos por medio de Chivo Wallet Web según petición del Cliente.	Cajero Solicita los fondos por medio de Chivo Wallet Web según petición del Cliente.	Cajero Solicita los fondos por medio de Chivo Wallet Web según petición del Cliente.	Cajero Solicita los fondos por medio de Chivo Wallet Web según petición del Cliente.	Cajero Solicita los fondos por medio de Chivo Wallet Web según petición del Cliente.
Cajero se asegura que los Fondos estén aplicados en Chivo Wallet	Cajero se asegura que los Fondos estén aplicados en Chivo Wallet	Cajero se asegura que los Fondos estén aplicados en Chivo Wallet	Cajero se asegura que los Fondos estén aplicados en Chivo Wallet	Cajero se asegura que los Fondos estén aplicados en Chivo Wallet
Cajero procesa Transacción solicitada por el cliente en aplicativo y entrega comprobante.	Cajero procesa Transacción solicitada por el cliente en aplicativo y entrega comprobante.	Cajero procesa Transacción solicitada por el cliente en aplicativo y entrega comprobante.	Cajero procesa Transacción solicitada por el cliente en aplicativo y entrega comprobante.	Cajero procesa Transacción solicitada por el cliente en aplicativo y entrega comprobante.

Cuadratura diaria de comprobantes procesados	Cuadratura diaria de comprobantes procesados	Cuadratura diaria de comprobantes procesados	Cuadratura diaria de comprobantes procesados	Cuadratura diaria de comprobantes procesados
Desglosador realiza nota de abono a cuenta con finalización XXXXXXXX5471	Desglosador realiza nota de abono a cuenta con finalización XXXXXXXX5471	Desglosador realiza nota de abono a cuenta con finalización XXXXXXXX5471	Desglosador realiza nota de abono a cuenta con finalización XXXXXXXX5471	Desglosador realiza nota de abono a cuenta con finalización XXXXXXXX5471
Liberación de Lote Contable	Liberación de Lote Contable	Liberación de Lote Contable	Liberación de Lote Contable	Liberación de Lote Contable

Tabla 14 Actividades de a realizar por procesos identificados
Fuente: Elaboración propia.

En esta sección se deben identificar cada una de las actividades que intervienen en cada una de las partes críticas del servicio.

Aplicativos críticos que intervienen en proceso		
Core Bancario	**Chivo Wallet**	**Interfaz Core Bancario Chivo**
Descripción: Core Banking basado en AS400 con base de datos ORACLE 19c, IIS 10, Framework 3.5 con C#.	Descripción: Aplicación que permite la transaccionalidad de Bitcoin a dólares y viceversa.	Descripción: Permite a las Agencias alimentar al Core Bancario con las transacciones emitidas por Chivo Wallet, IIS 10, Framework 3.5 con C#.
Tipo de esquema alterno: Contrato con Proveedor GBM, sitio Alterno.	Tipo de esquema alterno: Proveedor del Servicio garantiza tener su resiliencia en un 100%, con un down time de 99% al año.	Tipo de esquema alterno: Contrato con Proveedor GBM, sitio Alterno.
Limitantes: Sitio primario 100% y Resiliencia 100%	Limitantes: Administrado por Proveedor Chivo.	Limitantes: Sitio primario 100% y Resiliencia 100%
Ubicación: CPP: Pirámide Sta Tecla. CPA: Edificio GBM Colonia Roma	Ubicación: Instalaciones del Proveedor.	Ubicación: CPP: Pirámide Sta Tecla. CPA: Edificio GBM Colonia Roma
Tiempo de habilitación de esquema: 3 horas	Tiempo de habilitación de esquema: 30 minutos (inmediato)	Tiempo de habilitación de esquema: 3 horas
Descripción: Core Banking basado en AS400 con base de datos ORACLE 19c, IIS 10, Framework 3.5 con C#.	Descripción: Aplicación que permite la transaccionalidad de Bitcoin a dólares y viceversa.	Descripción: Permite a las Agencias alimentar al Core Bancario con las transacciones emitidas por Chivo Wallet, IIS 10, Framework 3.5 con C#.

Tabla 15 Análisis de Aplicativos críticos que intervienen en proceso
Fuente: Elaboración propia.

Se deben identificar los aplicativos críticos que intervienen en el servicio. Es importante identificar el nivel de blindaje para cada uno y así establecer mecanismos automatizados de respuesta o un proceso manual para restablecer las actividades según corresponda.

Análisis de Proveedores			
Proveedor de Enlaces	**Proveedor Servicio**	**Proveedor de Infraestructura**	**Proveedores Base de Datos**
• Nombre: Tigo • Descripción: Proveedor de enlace primario principal • Proveedor Único: No • Dependencia de Proveedor: Si • Proveedor regulatorio: Si, SIGET, NRP-24 • Proveedor Multiservicios: No	• Nombre: Chivo Wallet • Descripción: Proveedor de plataforma de transacción en Bitcoin • Proveedor Único: Si • Dependencia de Proveedor: Si, Totalmente • Proveedor regulatorio: Si, Ley Bitcoin • Proveedor Multiservicios: No	• Nombre: GBM • Descripción: Proveedor de infraestructura Servidor y Software. • Proveedor Único: No • Dependencia de Proveedor: Si • Proveedor regulatorio: Si, NRP-24 • Proveedor Multiservicios: Si, infraestructura, Software, sistemas operativos.	• Nombre: DATUM • Descripción: Asesoria y soporte especializado Base de Datos ORACLE • Proveedor Único: No • Nivel de dependencia de Proveedor: No • Proveedor regulatorio: No • Proveedor Multiservicios: No
• Nombre: Claro • Descripción: Proveedor de enlace secundario principal y sucursales • Proveedor Único: No • Nivel de dependencia de Proveedor: Si • Proveedor regulatorio: Si, SIGET • Proveedor Multiservicios: No	• -	• -	• Nombre: GSSA • Descripción: Proveedor de enlace secundario principal y sucursales • Proveedor Único: No • Nivel de dependencia de Proveedor: No • Proveedor regulatorio: No • Proveedor Multiservicios: No
• Nombre: IBW • Descripción: Proveedor de enlaces sucursales • Proveedor Único: No • Nivel de dependencia de Proveedor: Si • Proveedor regulatorio: Si, SIGET • Proveedor Multiservicios: No	• -	• -	• -

Tabla 16 Análisis de Proveedores
Fuente: Elaboración propia.

5.6 Establecer los planes y procedimientos de continuidad del negocio.

Se deben establecer planes y procedimientos para las actividades de respuesta, comunicación, recuperación (incluidos los planes de recuperación ante desastres), restauración y devolución. Basándose en los resultados de las estrategias y soluciones de continuidad de negocio seleccionadas, una organización debe establecer una estructura de respuesta e implementar planes y procedimientos para gestionar la organización durante un incidente perturbador que requiera la activación de sus soluciones de continuidad de negocio.

5.6.1 Los procedimientos deberán:

- Identificar las medidas inmediatas adoptadas durante una interrupción.
- Ser capaces de adaptarse a los cambios en las condiciones internas y externas como consecuencia de las perturbaciones.
- Centrarse en el impacto de los incidentes que podrían provocar una interrupción.
- Minimizar el impacto de las perturbaciones.
- Asignar funciones y responsabilidades para las tareas dentro de ellas.
- Se elaborarán y mantendrán planes y procedimientos documentados de continuidad de la actividad que proporcionen orientación e información para que los equipos puedan responder a un incidente perturbador y recuperar el funcionamiento normal.
- Los planes deberán estar fácilmente disponibles donde y cuando sea necesario.

5.6.2 Los planes de continuidad de negocio deberán contener colectivamente:

- Detalles de las medidas que tomará cada equipo para continuar o recuperar las actividades prioritarias, supervisar el impacto de la interrupción y la respuesta de las organizaciones.
- Referencia a los umbrales y procesos predefinidos para activar la respuesta.
- Procedimientos para permitir la entrega de productos y servicios a una capacidad acordada.

- Detalles para gestionar las consecuencias inmediatas de una perturbación teniendo en cuenta el bienestar de las personas, la prevención de nuevas perturbaciones en las actividades prioritarias y el impacto en el medio ambiente.

5.6.3 Cada plan deberá:

- Indicar la finalidad, el alcance y los objetivos.
- Las funciones y responsabilidades del equipo que aplicará el plan.
- Identificar las acciones para aplicar las soluciones.
- Contener la información necesaria para activar, operar, coordinar y comunicar las acciones del equipo
- Identificar las dependencias internas y externas necesarias.
- Identificar los recursos necesarios.
- Incluir requisitos de información.
- Incluir un proceso de renuncia y establecer un perfil del futuro candidato.

Establecer roles y cargos críticos			
Cargo	**Teléfono**	**Correo**	**Ubicación**
Coordinador de Continuidad del negocio			
Especialista de Continuidad de negocios de TI			
Administrador de Incidentes			
Administrador de Problemas			
Gerente de TI			
Gerente Negocio			
Líder especialista de Negocio			

Tabla 17 Roles y Cargos Críticos
Fuente: Elaboración propia

Recursos	
Mobiliario	• Acceso a sistemas internos • Conexión a Internet • Acceso a correo interno • Escritorio • Sillas

	• Teléfono • Computadora • Impresora • Office • Puntos de RED • Celular

Tabla 18 Recursos
Fuente: Elaboración propia

Actividades por realizar durante un incidente		
Escenario	**Causas**	**Actividades**
Fallas en sistemas	Errores en sistemas Fallas en infraestructura Falla en la Red	Generar incidente en herramienta establecida Contactar a los especialistas de negocio y Tecnología Análisis del incidente Activar sitio de contingencia del CORE Bancario y/o Interfaz
Fallas energía Eléctrica	Corte de energía Desastre Natural Elementos Medioambientales	Contactar a personal de mantenimiento y Data Center Activación de Ups principal para mantener energía eléctrica en equipos. Activación de Planta Eléctrica para darle energía al Ups Principal. En caso de arranque automático de planta eléctrica falle, se procede con el arranque manual de la planta electica por parte del personal de mantenimiento al edificio y/o Agencia. En caso de que la luz no regrese en 8 horas aprox, se procede a verificar el estado de los carburantes de la planta y se procede con inyectar destilados de petróleo para que dure lo necesario.
Sitio Operativo Inhabilitado	Disturbios públicos Evacuaciones Delincuencia Conato de incendio Orden Sanitaria	Activación de Call Tree de llamada para recibir indicaciones Activación de Sitio físico Alterno para operaciones ya establecidos.
Incidentes de Ciberataques	Secuestro de Datos Ataque DOS Código Malicioso	Analizar el nivel de tráfico de red que llega a los servicios para establecer una referencia clara. Activación de panel de control para monitorizar los servicios. Identificación del ataque y enviar a HoneyPot al atacante. Identificar los posibles procesos afectados para proceder con el bloqueo de IPs atacantes. En última instancia de ser necesario se procede a desconectar el servicio de ISP. Identificar los procesos maliciosos y eliminarlos para evitar un futuro ataque o una posible infección (Ramsonware, spyware, Back door, etc).
Incidentes de Proveedor	Indisponibilidad de personal Errores en sistemas o Tecnología Mal soporte de proveedor	Se contacta con Proveedor sobre incidencia Pedir análisis de la situación, verificación de enlaces, acceso a red. Activar velo o marquesina del anuncio de mantenimiento o solución de incidencia por parte del proveedor.

		Cajero Chivo procede a indicar a cliente que la pagina actualmente esta en mantenimiento y que se debe esperar a que proveedor reestablezca. Si el proveedor lo considera oportuno, se debe realizar el traslado a sitio de contingencia vía DNS. En caso de indisponibilidad del personal, proveedor debe responder ante la demanda y activar su estrategia de teletrabajo.
Liquidez	Corrida Bancaria Disposiciones Gubernamentales Reputación	No se identifican actividades a realizar en caso exista problemas de liquidez.
Ausencia de personal	Por pandemia Aislamiento preventivo Por enfermedad	Cajero Chivo indica a Subgerente de Agencia su estado de salud, por medio de una constancia de salud. En caso de contagio por pandemia, enviar prueba con resultado positivo. Subgerente procede a indicar a Cajero Chivo de respaldo que debe de sustituir al Cajero Principal mientras se recupera de su estado de salud.
Fallas por errores operativos	Errores Operativos Información Física	En caso de que Cajero Chivo no verifique el monto requerido por cliente, ya sea por pago de préstamo, pago de tarjeta, etc, y asigne una cantidad errónea, se procede a solicitar la aprobación a subgerente para revertir el pago. Subgerente brinda aprobación para proceder.
Eventos climáticos	Inundaciones Tormentas Eléctricas Terremotos	Verificar las Agencias afectadas por evento climático suscitado. Se procede con el cierre temporal de la agencia afectada Se indica a clientes por medio de los canales digitales las agencias cerradas por evento, y cuales serían las agencias aledañas para que puedan realizar sus transacciones en BTC.

Tabla 19 Actividades por realizar durante un incidente
Fuente: Elaboración propia

Actividades a realizar después de un incidente		
Escenario	**Causas**	**Actividades**
Fallas en sistemas	Errores en sistemas Fallas en infraestructura Falla en la Red	Revisar que la sincronización de las bases de datos y aplicaciones se encuentren trabajando en tiempo real. Equipo técnico informa que el incidente a sido superado y que ya se puede proceder con el traslado a sitio productivo. El equipo técnico procede con traslado de sitio de Contingencia a Producción (Switch over). Se realizan las pruebas respectivas y se certifica que ya se ha superado el inconveniente.
Fallas energía Eléctrica	Corte de energía Desastre Natural Elementos Medioambientales	Cuando el servicio de energía eléctrica es reestablecido, se procede con el apagado de la planta eléctrica. Se verifica el nivel de combustible y si es necesario se procede con el llenado de tanque a su máxima capacidad, con el objetivo de poder prever nuevo evento futuro. Se realiza una inspección de los componentes de la planta para verificar su optimo estado.

Sitio Operativo Inhabilitado	Disturbios públicos Evacuaciones Delincuencia Conato de incendio Orden Sanitaria	Cuando las autoridades confirmen que la situación se ha controlado, se procede a indicar a los colaboradores que el día siguiente pueden retornar a su agencia principal.
Incidentes de Ciberataques	Secuestro de Datos Ataque DOS Código Malicioso	Equipo de Ciberseguridad Bancaria informa a Alta Gerencia que la situación ha sido controlada. Se procede con una validación de disponibilidad de sistemas. Verificar si hay data disponible. Se procede con el levantamiento de informe a la Alta Gerencia Si hay necesidad de realizar parchado o hardening de OS se realiza un change de emergencia para corregir. Activar monitoreo en tiempo real de aplicaciones y bases de datos. Se procede si es necesario con la restauración de la data afectada o la reinstalación de aplicaciones dañadas con soporte del Proveedor.
Incidentes de Proveedor	Indisponibilidad de personal Errores en sistemas o Tecnología Mal soporte de proveedor	Proveedor informa al área correspondiente sobre la solución de incidencia. Proveedor procede a eliminar mensaje o velo de mantenimiento, ya que el servicio ha sido reestablecido. Cajero Chivo procede a indicar a cliente que la aplicación ha sido reestablecida por parte del proveedor. Se procede a realizar pruebas en la aplicación.
Liquidez	Corrida Bancaria Disposiciones Gubernamentales Reputación	No se identifican actividades a realizar en caso exista problemas de liquidez.
Ausencia de personal	Por pandemia Aislamiento preventivo Por enfermedad	Cajero principal Chivo envía constancia de salud o prueba negativa de contagio a subgerente para poder retornar a sus labores diarias. Subgerente indica a Cajero Chivo de respaldo que el día siguiente retorna cajero principal a sus labores diarias.
Fallas por errores operativos	Errores Operativos Información Física	Cajero procede a procesar la cantidad correcta indicada por Cliente.
Eventos climáticos	Inundaciones Tormentas Eléctricas Terremotos	Cuando las autoridades de protección Civil indiquen que ya no hay amenazas del evento climático percibido, se procede a indicar a los colaboradores sobre su retorno a su sitio principal. Se indica a departamento de comunicaciones que retire el comunicado de las agencias cerradas y que se cambie la información indicando la fecha de reapertura.

Tabla 20 Actividades a realizar después de un incidente
Fuente: Elaboración propia

5.7 Comunicar a las partes interesadas, dejando constancia.

Pueden ser correos electrónicos, pero también comunicaciones oficiales de fuentes como agencias gubernamentales y otras. En este apartado se deben realizar un levantamiento de números de contactos, correos, contactos en Teams (o en herramienta de comunicación interna) de las partes interesadas o principales involucrados en el desarrollo del plan de continuidad. Apoyarse en CallTree.

Establecer roles y cargos críticos			
Cargo	**Teléfono**	**Correo**	**Ubicación**
Coordinador de Continuidad del negocio			
Especialista de Continuidad de negocios de TI			
Administrador de Incidentes			
Administrador de Problemas			
Gerente de TI			
Gerente Negocio			
Líder especialista de Negocio			

Tabla 21 Formato Call Tree
Fuente: Elaboración propia

5.8 Registrar una bitácora sobre interrupciones, acciones y decisiones tomadas.

Normalmente estos registros se realizan a través de actas o completando listas de verificación de actividades realizadas. Una organización debe tener procesos documentados para volver a las operaciones normales después de un incidente de continuidad del negocio.

5.9 Calendarizar ejercicios, pruebas o ensayos.

Para garantizar que sus estrategias, soluciones y planes de continuidad de la actividad siguen siendo válidos, una organización debe establecer un programa de ejercicios para probar la eficacia de sus disposiciones de continuidad de la actividad. No es necesario que una organización pruebe la totalidad de sus disposiciones de continuidad de la actividad durante cada ejercicio.

Los exámenes son para:

- Verificar la coherencia con sus objetivos de continuidad de la actividad.
- Basarse en escenarios adecuados con fines y objetivos claramente definidos.
- Desarrollar el trabajo en equipo y la competencia de los equipos de continuidad de la actividad y de quienes tienen funciones que desempeñar durante una interrupción.
- Validar sus estrategias, soluciones y planes de continuidad empresarial.
- Elaborar informes posteriores al ejercicio que contengan resultados, recomendaciones y acciones de mejora.
- Realizar a intervalos planificados o cuando se produzcan cambios significativos en la organización o en el contexto en el que opera.

5.10 Evaluar la documentación y las capacidades de continuidad de negocio.

Una organización debe evaluar la adecuación y eficacia de su análisis de impacto en el negocio, evaluación de riesgos, estrategias, soluciones, planes y procedimientos a intervalos planificados, después de un incidente o invocación y cuando se produzcan cambios significativos.

Dicha evaluación se realiza mediante los ejercicios o pruebas controladas, las cuales se clasifican de la siguiente manera:

Tipos de Pruebas

- Pruebas de Servicio: Pruebas de Servicio del lado de negocio.
- Pruebas de tecnología: Prueba de componentes Tecnológicos.
- Pruebas de Proveedor: Ejercicio que realiza Proveedor para probar el servicio brindado.
- Pruebas de Sitio Alterno: Pruebas de traslado a sitio alterno
- Pruebas Unitarias: Pruebas de componentes de Tecnología que soportan el servicio.

- Pruebas Completas: Prueba que contempla todos los tipos de pruebas de Servicio, Tecnológicas, unitarias y de sitio alterno en un solo Ejercicio. Normalmente se conocen como pruebas integrales.

Aplicación del sistema / probado		***Sistemas críticos***		**Tipo de prueba**	***Integral***
fecha de prueba	*5/4/2022*	**Tiempo de Inicio**	*4:00 p. m.*	**Tiempo final**	*5:00 p.m.*
Facilitador				**Firma**	
Escenario de prueba		*Validar el correcto funcionamiento de las contingencias tecnológicas (Transición de ambiente Productivo a Contingencia) en conjunto con proveedor Chivo Wallet, en sitio alterno operativo y la capacidad de respuesta por parte del negocio ante un escenario de caída de sistemas.*			

Pasos	**Descripción de paso**	**Resultado esperado**	**Resultado actual**	**Evaluación de resultados**	
				Satisfactorio	**Insatisfactorio**
1	Tras la notificación de que ha ocurrido un evento, el Coordinador pondrá en contacto con el personal clave (utilizando Lista de Notificación).	Coordinador deberá ponerse en contacto con los miembros del equipo, propietario del sistema/aplicación, y otros en la Lista de notificaciones, e informarles sobre el evento de contingencia y transmitir toda la información conocida. Coordinador debería dirigir los esfuerzos de notificación.	Se identifica un problema y se contacta rápidamente con el responsable buscando su contacto en el directorio actualizado	***x***	

2	Personal (Administrador del sistema) iniciarán proceso de solicitud del árbol de llamadas.	Personal (Administrador del sistema) iniciarán proceso árbol de llamadas.	El coordinador sabedor de la situación se encontrará disponible y llevará a cabo la evaluación inicial del árbol de llamadas.	***x***	
3	Coordinador recibe informe de evaluación de áreas en curso (Administrador del sistema. Evaluar el daño a la aplicación y / o hardware de soporte.).	Coordinador debe determinar si el contacto volverá a actualizar su perfil en 1 horas	Coordinador determina que la solicitud se realizó con éxito al hacer contacto	***x***	
4	Actividades del coordinador	Coordinador deberá notificar a la gestión, propietario del sistema/aplicación, Personal (Administrador del sistema. Evaluar el daño a la aplicación y / o hardware de soporte y restaurar las comunicaciones de red.), y que se ha activado el árbol de llamadas.	Coordinador notificó al Gerente del área	***x***	

4	Actividades del coordinador	Después de la activación, Coordinador debería notificar al Depto. de Sistemas y (otros encargados), informarle que proporcione toda la información conocida	Coordinador notificó al Gerente del área	***x***	
4	Actividades del coordinador	Coordinador deberá notificar al comité de crisis para efectuar todos los procedimientos necesarios para revisar los servicios que provee el sistema.	Coordinador notificó al Gerente del área	***x***	
5	Actividades del coordinador	Después de la activación, Coordinador deberá notificar a Sistemas, informarle, que proporcione toda la información conocida	Coordinador contactó Les informó del evento de contingencia, transmitió toda la información conocida y sugiere un curso de acción. Y que es necesaria la actualización	***x***	

6	Coordinador procede con activar traslado a sitio alterno de colaboradores según manual de sitios alternos documentado	El traslado a sitio alterno debe de ser en orden y respetando el tiempo definido de traslado de 30 min	Traslado en tiempo	***x***	
7	Personal procede a traslado a Sitio Alterno operativo	El traslado a sitio alterno debe de ser en orden y respetando el tiempo definido de traslado de 30 min	Traslado en tiempo	***x***	
8	Personal de Tecnología procede con el Switcheo de Producción CORE Bancario a Contingencia	Switcheo deberá realizarse en 15 minutos máximo	El Switcheo se realizó en 10 minutos	**x**	
9	Cajero de Chivo Wallet procede a procesar en ambiente alterno CORE y en sitio alterno establecido	Procesar en ambiente alterno de manera transparente y notificar fallas	No se presentaron inconvenientes y Cajeros procesaron sus operaciones de manera trasparente durante 1 hora	**x**	
10	Personal de Tecnología procede con el Switcheo de Contingencia CORE Bancario a Producción	Switcheo deberá realizarse en 15 minutos máximo	El Switcheo se realizó en 10 minutos	**x**	

11	Personal procede a traslado a Sitio principal operativo	El traslado a sitio principal debe de ser en orden y respetando el tiempo definido de traslado de 30 min	Traslado en tiempo	**x**	
12	Coordinador notifica que incidente ha finalizado	Correo de notificación a involucrados	Se envió correo a los involucrados	**x**	
Resultado		**98%**		**Exitosa**	
Comentarios		*La prueba se realizó correctamente y los resultados son satisfactorios a la hora de recuperar la información desde los directorios*			
Recomendación Del Facilitador		*La necesidad de mantener actualizados los directorios de contactos y sitios alternos para establecer una rápida comunicación con todos los miembros de la empresa en caso de eventos no esperados*			

Tabla 22 Prueba Integral
Fuente: Elaboración propia

5.11 Revisar datos y resultados de seguimiento y medición.

Esta evaluación determina si su SGCN cumplió con los objetivos. Una organización necesita evaluar el rendimiento y la eficacia de su SGCN para asegurarse de que puede alcanzar los resultados previstos. Para ello, debe determinar qué es lo que hay que supervisar y medir, los métodos de supervisión y medición y cómo se evaluarán los resultados.

Se planificarán las ocasiones en las que se llevará a cabo la actividad de seguimiento y medición, y se identificará y seleccionará al personal encargado de la actividad de seguimiento y medición teniendo en cuenta su competencia e imparcialidad. Deberán conservarse las pruebas adecuadas de la actividad de seguimiento y medición y los resultados de la actividad de seguimiento y medición.

Las pruebas o ejercicios que evalúan los planes nos sirven para medir el nivel de efectividad del sistema y el nivel de robustez de los planes de acción elaborados. Para ello, se deben establecer umbrales de calificación de los ejercicios y las acciones a realizar, dependiendo de la nota obtenida.

Exitosa	Satisfactoria	Fallida
Nota Entre 90%-100%	Nota Entre 80%-89%	Nota abajo de 80%
No necesita realizar acciones	Establecer planes de acción y seguimiento	Establecer planes de acción, seguimiento y se debe repetir el ejercicio luego de cerrados los planes de acción.

Tabla 23 Escala de resultados
Fuente: Elaboración propia

5.12 A continuación, veremos un ejemplo hipotético de informe de pruebas a la alta dirección.

Estimados miembros de Junta Directiva,

Mediante el presente se presentan los resultados de los ejercicios realizados durante el periodo de febrero a abril 2022.

Tipo de Prueba	Servicio	Nota	Diagnostico
Integral	Recepción de Pagos en BTC	98%	Exitosa
Unitaria (TI + Negocio)	Abono a Cuenta en BTC	100%	Exitosa
TI	Interfaz de conexión	79%	Fallida
Emergencia	Evacuación de Edificios	85%	Satisfactoria

Tabla 24 Tabla de resultados
Fuente: Elaboración propia

Para la prueba fallida de Componentes de TI “Interfaz de conexión”, se establecen los siguientes planes de acción:

Servicio	Causa de la falla	Planes de acción
Interfaz de conexión	Interfaz caída debido a falla en Servidor Principal	Implementar alta disponibilidad por medio de la adición de un nodo extra. Implementar monitoreo en tiempo real con la herramienta Spot Ligth.

		Tercerizar la administración de los servidores para garantizar máxima disponibilidad y soporte Third Party. Actualizar Plan de Continuidad.

Tabla 25 Planes de acción por prueba fallida.
Fuente: Elaboración propia.

5.13 Programar auditorías internas.

El objetivo de las auditorías internas es confirmar que el SGCN se ha implantado eficazmente e identificar cualquier debilidad y oportunidad de mejora.

Las auditorías internas deben comprobar:

- Si el SGCN satisface las necesidades de la organización.
- Cumple los requisitos de la norma ISO 22301:2019.
- La coherencia con la que se aplican los procesos y procedimientos.
- Si los procesos y procedimientos logran los resultados previstos.

Una organización debe realizar auditorías internas a intervalos planificados. El programa de auditoría deberá:

- Tener en cuenta la importancia de los procesos en cuestión y los resultados de las auditorías anteriores.
- Definir los criterios y el alcance de cada auditoría.
- Seleccionar a los auditores y realizar las auditorías para garantizar la objetividad e imparcialidad del proceso de auditoría.
- Garantizar que los resultados de las auditorías se comuniquen a los responsables correspondientes.
- Conservar pruebas documentadas de la aplicación del programa de auditoría y de los resultados de esta.
- Garantizar que se adopten sin demora las medidas correctoras necesarias para subsanar las no conformidades y sus causas.

5.14 Verificar los resultados de la revisión por la dirección.

Por lo general, esto se presenta en forma de actas o tal vez decisiones documentadas. La alta dirección debe revisar el SGCN de la organización a intervalos planificados para evaluar su adecuación, conveniencia y eficacia para satisfacer las necesidades de la organización.

Las entradas y salidas de las reuniones de revisión de la gestión deben cumplir los requisitos de la cláusula 9.3 de la Norma ISO22301:2019 Los resultados incluirán decisiones relacionadas con las oportunidades de mejora continua y cualquier cambio necesario para mejorar la eficiencia y la eficacia del SGCN.

Una organización debe conservar la información documentada como prueba de los resultados de las revisiones de la gestión y comunicar los resultados a las partes interesadas pertinentes.

5.15 Analizar las no conformidades y acciones correctivas tomadas.

Esta es una descripción de las no conformidades y su causa. El objetivo principal de la implantación de un SGCN es garantizar que una organización pueda responder a un incidente perturbador de manera oportuna y continuar con la entrega de sus productos y servicios claves a un nivel predefinido hasta que se pueda afectar el retorno a las operaciones normales.

Las organizaciones deben determinar las oportunidades de mejora e implementar acciones para lograr los resultados previstos de su SGCN. Las organizaciones deben reaccionar ante las no conformidades y tomar medidas para controlar y corregir las no conformidades y hacer frente a las consecuencias.

5.16 Analizar resultados de las acciones correctivas.

Esta es una descripción de lo que se ha hecho para eliminar la causa de una no conformidad. Las organizaciones deben investigar las no conformidades para:

- Establecer si la disconformidad existe en otro lugar.
- Identificar la causa raíz de la no conformidad.
- Identificar cualquier acción correctiva necesaria para evitar que se repita la no conformidad.
- Identificar los cambios necesarios en el SGCN.
- Cualquier acción correctiva identificada para abordar las no conformidades debe aplicarse sin demora indebida. La acción correctiva implementada debe ser revisada para determinar su efectividad.

5.17 Retroalimentación y mejora continua.

- Comenzar identificando el "¿Por qué?". Asegúrese de que las razones para implantar un SGCN son claras y están en consonancia con su dirección estratégica; de lo contrario, corre el riesgo de no obtener la aceptación crítica de la alta dirección.
- Luego, considerar el "¿Para qué?". Implantar y mantener un SGCN requiere un compromiso importante, así que asegúrese de que su alcance es lo suficientemente amplio como para abarcar la información crítica que hay que proteger, pero no es tan amplio como para no disponer de recursos suficientes para implantarlo y mantenerlo.
- Consiga que todas las partes interesadas clave participen en el momento adecuado. La alta dirección para el establecimiento del contexto, los requisitos, la política y los objetivos; los directivos y empleados con valiosos conocimientos para las evaluaciones de riesgos, el diseño de procesos y la redacción de procedimientos.
- Comuníquese ampliamente a lo largo del proceso con todas las partes interesadas. Hágales saber lo que está haciendo, por qué lo está haciendo, cómo piensa hacerlo y cuál será su participación. Proporcione actualizaciones periódicas sobre el progreso.
- Consiga ayuda externa cuando la necesite. No fracase por falta de conocimientos técnicos internos. La gestión de los riesgos de seguridad de la información suele requerir conocimientos especializados. Sin embargo, asegúrese de comprobar las credenciales de un tercero antes de contratarlo.

- Mantenga la sencillez de sus procesos y la documentación de apoyo. Puede desarrollarse para ser más extensa con el tiempo si es necesario.
- Diseñe y aplique reglas que pueda seguir en la práctica. No cometas el error de documentar una norma demasiado elaborada que nadie pueda seguir. Es mejor aceptar un riesgo y seguir buscando formas de gestionarlo.
- Recuerde a sus proveedores. Algunos proveedores le ayudarán a mejorar su SGCN, otros aumentarán su riesgo. Debe asegurarse de que los proveedores de alto riesgo tienen controles al menos tan buenos como los suyos. Si no es así, busque alternativas.
- Formar, formar y volver a formar. Es probable que la continuidad del negocio sea un concepto nuevo para muchos o la mayoría de sus empleados. Es posible que la gente tenga que cambiar hábitos arraigados durante muchos años. Es poco probable que una sola sesión informativa de concienciación sea suficiente.
- Recuerde que debe asignar recursos suficientes para probar rutinariamente sus controles. Las amenazas a las que se enfrenta su organización cambiarán constantemente y debe comprobar si es capaz de responder a ellas.

Capítulo VI Conclusiones y Recomendaciones.

6.1 Conclusiones.

1 Para establecer un SGCN, es necesario en primer lugar contar con un Gobierno de Continuidad basado en la política de continuidad del negocio, que involucre a la alta dirección, quienes son los que tienen la autoridad de aprobar las políticas, planes, y exigir el cumplimiento de la estrategia.

2 Para establecer un SGCN, es necesario conocer y tener clara la Estrategia del Negocio, ya que, por medio de la estrategia de negocio se define la metodología de gestión, en cuanto a la creación de planes y políticas.

3 Mediante el resultado del Análisis de Impacto podemos concluir que bitcoin tiene baja transaccionalidad, es decir, un volumen de operaciones tan bajo que no representa un aspecto crítico.

6.2 Recomendaciones.

1 Para que las entidades financieras se adapten al ecosistema de Bitcoin, deben apoyarse al menos en marcos fundamentales como las buenas prácticas ISO 22301 y el marco regulatorio local de los países en particular.

2 El SGCN debe basarse en 4 pilares fundamentales:

- El Gobierno de Continuidad (Política de Continuidad de Negocio, y Comités de apoyo a la Gestión).
- La Ejecución de la Metodología (Análisis de Impacto del Negocio, Análisis de Riesgos, Planes y Procedimientos de Continuidad, Capacitaciones y concientización).
- El Control y el Monitoreo de la Metodología (Pruebas de Continuidad, Manejo de Incidentes).
- Los Planes de Respuesta (Plan de Recuperación de Desastres, Plan de Continuidad del Negocio y Plan de Recuperación y restauración de Sistemas, Gestión de Incidentes y Gestión de Crisis)

Referencias.

Fideicomiso, Asamblea Legislativa de la República de El Salvador. (31 de agosto de 2021). *https://www.asamblea.gob.sv*. Recuperado el febrero de 2022, de https://www.asamblea.gob.sv/sites/default/files/documents/decretos/91A41A63-1796-4BA0-B969-9C16E505304F.pdf

ISO 22301:2019, Tony Bevan. (8 de mayo de 2020). *nqa.com*. Recuperado el 1 de febrero de 2022, de https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-22301-Guia-de-implantacion.pdf

ISOTools Excellence Chile. (febrero de 2022). *https://www.isotools.cl/*. Recuperado el febrero de 2022, de https://www.isotools.cl/iso-22301-continuidad-negocio-ciclo-pdca/

Ley Bitcoin, Asamblea Legislativa de la República de El Salvador. (9 de junio de 2021). *https://www.asamblea.gob.sv*. Recuperado el febrero de 2022, de https://www.asamblea.gob.sv/sites/default/files/documents/decretos/8EE85A5B-A420-4826-ABD0-463380E2603B.pdf

NRP-24, Comité de Normas, Banco Central de Reserva. (1 de julio de 2020). *bcr.gob.sv*. Recuperado el febrero de 2022, de https://www.bcr.gob.sv/regulaciones/upload/NRP-24.pdf?v=1657294190

NRP-29, Comité de Normas, Banco Central de Reserva. (7 de septiembre de 2021). *https://www.bcr.gob.sv/*. Recuperado el febrero de 2022, de https://www.bcr.gob.sv/regulaciones/upload/NRP-29.pdf?v=1657295247

Plan, Do, Check & Act. INCIBE. (26 de septiembre de 2019). *https://www.incibe.es/*. Recuperado el febrero de 2022, de https://www.incibe.es/protege-tu-empresa/blog/fases-plan-continuidad-negocio

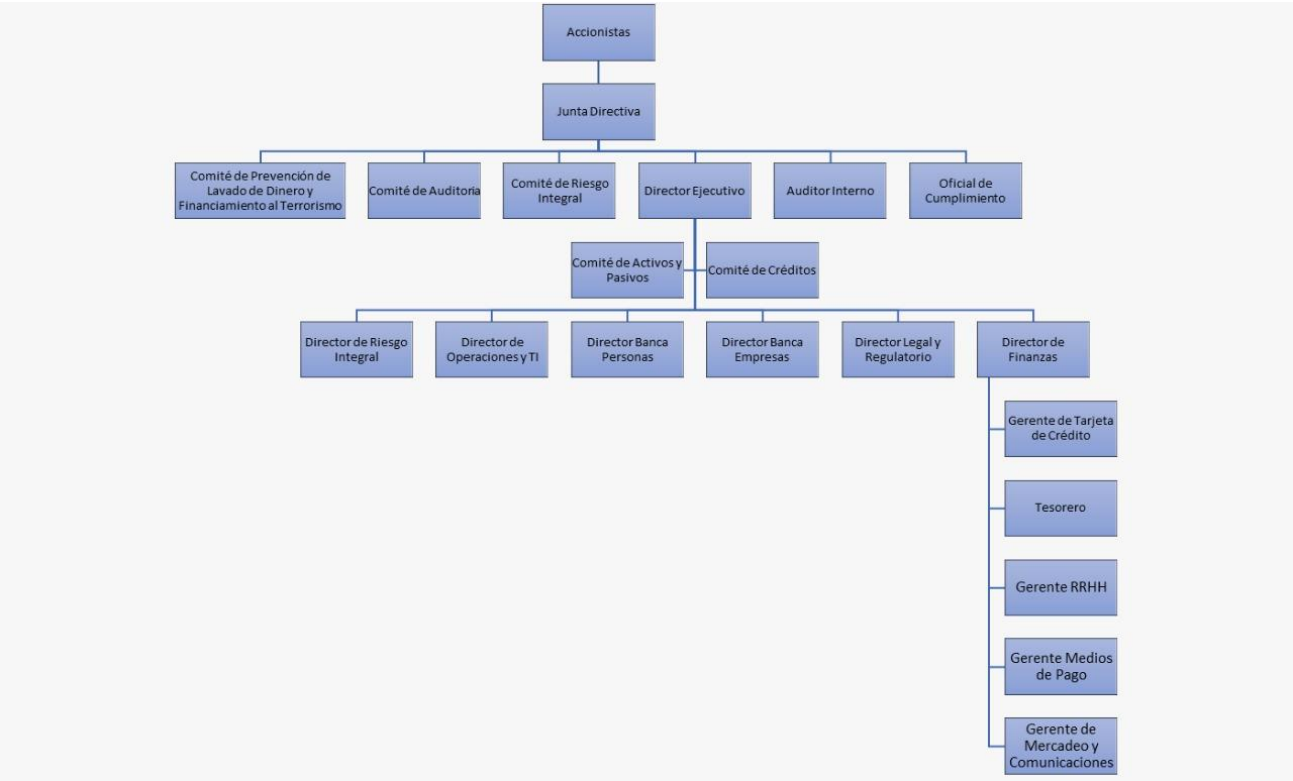
Vocabulario Bitcoin.org. (febrero de 2022). *Bitcoin Project 2009-2022*. Obtenido de https://bitcoin.org/es/vocabulario

Anexos.

Anexo 1 “Cronograma de Trabajo”

Actividad	***Inicio***	***Fin***	***Indicador de Logro***
Recopilar las declaraciones y reportes del Banco Central de Reserva, Super Intendencia del Sistema Financiero y Ministerios de Hacienda y Economía con respecto al uso del Bitcoin.	31 enero	13 febrero	Contar con las publicaciones oficiales de las instituciones especificadas. Revisión.
Recopilar y evidenciar las acciones tomadas por la Banca Nacional, para sistematizar y adoptar el uso de Bitcoin desde la norma ISO 22301	14 febrero	27 febrero	Contar con la lista de acciones, medidas y controles pertinentes para garantizar la resiliencia ante el uso de Bitcoin. Revisión.
Recopilar incidentes y su impacto positivo y negativo relacionado al Bitcoin	28 febrero	13 marzo	Lista de incidentes y acciones relacionadas. Revisión.
Redacción Final y presentación	14 marzo	18 marzo	Documento listo y revisado.

Anexo 2 “Organigrama Institucional”



Anexo 3 "Guía de Entrevista"

Esta entrevista está diseñada para conocer los aspectos relacionados al BITCOIN y su uso en las instituciones financieras en El Salvador, con el objetivo de tomar en cuenta la realidad de su aplicación y a obtener de una fuente idónea de información. Los datos obtenidos serán manejados de manera confidencial y anónima.

Lugar y fecha: ***San Salvador, 14 de febrero 2022.***
Nombre: ***Daniel Eduardo Girón Diaz.***
Puesto, cargo o función que desempeña: ***Encargado de Continuidad de Negocio.***
Institución u organización: ***Banco El Salvador.***

1. *¿Cuánto tiempo lleva desempeñando sus funciones en el puesto actual?*
   R/ 20 meses.

2. *¿Dentro de sus actividades laborales, existe alguna relación directa o indirecta con el Bitcoin o con su uso en general?*
   R/ Efectivamente, de manera indirecta. Ya que la Gestión de Continuidad evalúa los procesos críticos de la organización. Actualmente las transacciones mediante Bitcoin no se consideran como un proceso crítico por tener una baja frecuencia de transacciones y las pocas operaciones con Bitcoin son de valores menores a USD 1,000 De manera que no sobrepasan los USD 5,000 al mes.

3. *¿Cuál es la postura de su organización en relación al uso de Bitcoin?*
   Debido a la obligatoriedad de las leyes y reglamentos establecidos por la Asamblea Legislativa de El Salvador, impulsadas por el gobierno local, todo agente económico deberá aceptar bitcoin como forma de pago cuando así le sea ofrecido por quien adquiere un bien o servicio. Es decir que todas las instituciones en general, publicas y privadas, nos vemos en la necesidad de adaptar políticas, de operación y desarrollo de software adecuado para dar cumplimiento a las regulaciones impuestas.

4. *¿Cuenta actualmente su organización con un Plan de Continuidad de Negocio en caso de que se presente un evento disruptivo?*
   R/ Al ser una entidad regulada por la Super intendencia del Sistema Financiero es de carácter obligatorio la implementación o adopción de técnicas de continuidad de negocio para garantizar la operatividad.

5. *¿De qué marco regulatorio, buenas prácticas, políticas se apoyaron en su institución financiera para el levantamiento o la implementación del SGCN?*
   R/ Para la implementación del SGCN nos apoyamos principalmente de la ISO22301 como estándar internacional, de la normativa NRP-24 que

regula a las instituciones financiera en lo relacionado a la Gestión de Continuidad del Negocio.

6. *¿Apegado a la política actual de continuidad de negocio implementada en su institución financiera, se han incluido las transacciones mediante Bitcoin dentro de sus planes actuales?*
R/ Las transacciones mediante Bitcoin desde una implementación no se han considerado como un servicio critico como tal debido a su poca transaccionalidad, sin embargo, se han establecido planes alternos documentados en manuales operativos con el objetivo de al menos tener documentado algunos procedimientos alternos en caso haya algún incidente que detenga dichas operaciones, mas que todo a nivel de Agencias y Sucursales.

7. *¿De acuerdo con su experiencia cuál cree que sería la aceptación o rechazo de parte de los clientes ante su posible utilización como reemplazo a las transacciones normales mediante dólares en un futuro?*
R/ De momento la utilización de la moneda electrónica Bitcoin no ha tenido mucha aceptación por parte de los clientes, ya que hemos visto según estadísticas internas que la transaccionalidad es muy poca, no obstante, en un futuro no descartamos que este nuevo modelo transaccional pueda tomar más auge, por ellos debemos estar siempre preparados para cuando suceda.

8. *¿De acuerdo con su experiencia, cuales cree que deberían de ser los elementos mínimos que se deben considerar para la implementación de un SGCN en una institución financiera?*
R/ A mi forma de ver es importante considerar la ISO22301 como marco referencial para implementación de un SGCN en una institución financiera. Elementos tales como análisis BIA con importantes para evaluar el nivel de impacto al negocio que tienen los servicios considerados como críticos en su organización, a partir del establecimiento del nivel de impacto se deben crear planes o procedimientos de continuidad para garantizar la continuidad de las operaciones, Planes de Recuperación de Desastres para entender que hacer en caso se materialice un evento disruptivo y a parte de esto evaluar o realizarle pruebas al Plan elaborado, medir el nivel de satisfacción del ejercicio y si hay que hacer mejoras implementarlas, con esto se cumple el ciclo de Deming o PDCA. Es importante mencionar que en una institución financiera deben de existir comités y Juntas Directivas que aprueben toda la metodología y comités de manejo de crisis que serán los encargados del manejo de esta.

9. *¿Cómo hizo su organización para adaptarse a una aplicación tercerizada?*
R/ Para poder hacer uso de los servicios de Chivo Wallet fue necesario considerarlo como una aplicación desarrollada, operada y con soporte de terceros, la cual permite al core bancario descargar las transacciones realizadas y agregarlas a una base de datos interna del core bancario la cual registra las transacciones realizadas.

Anexo 4 “Política de Continuidad de Negocio”

La Política de Continuidad de Negocio se sustenta en el conjunto de principios y compromisos siguientes:

1. La protección y seguridad de las personas es la primera premisa y el objetivo prioritario, tanto en situación normal como en situación de crisis derivada de un desastre, con respecto a la seguridad ocupacional.

2. El nombramiento de representantes de las distintas áreas con la debida experiencia y conocimiento, para que participen activamente en la elaboración, implantación, revisión, prueba y actualización de los Planes de Continuidad de Negocio.

3. El desarrollo e implantación de Planes de Continuidad de Negocio será teniendo en cuenta las áreas y departamentos internos, proveedores y servicios y empleando sistemas, recursos y procedimientos adecuados y proporcionados.

4. El aprovechamiento de las sinergias generadas en el desarrollo e implantación de los Planes de Continuidad de Negocio, contemplando los medios y recursos comunes de los que dispone toda la organización.

5. La adopción de medidas razonables para la continuidad operativa de los procesos y actividades, en función de la criticidad de los mismos establecida por la Organización.

6. La inclusión de criterios de seguridad, privacidad y fiabilidad que garanticen de forma razonable la continuidad de los servicios críticos proporcionados por terceros, en caso de su externalización.

7. La elaboración, dentro de los Planes de Continuidad de Negocio, de procedimientos de comunicación apropiados, tanto internos como externos, que posibiliten la correcta ejecución de los mismos, así como el suministro oportuno de información a todas las partes interesadas.

8. La comunicación a todo el personal de sus responsabilidades y de los procedimientos que le competen, en el marco de la continuidad de negocio, mediante labores de concienciación y formación.

9. El desarrollo de un SGCN que contemple la realización de revisiones, pruebas y actualizaciones de los Planes de Continuidad de Negocio de forma periódica o ante cambios significativos, en un proceso de mejora continua de los mismos.

10. La permanente disposición a colaborar con las autoridades en cuanto a la prevención de lavado de dinero, y cualquier otra solicitud judicial debidamente diligenciada.

Anexo 5 “Políticas Generales de la Organización”

Establecimiento de políticas generales para un plan de trabajo anual.

1. Identificar Competencias.

   Se debe garantizar que el personal dispone de la competencia para desempeñar su función, así como facilitar su capacitación, y mantener evidencias de esto.

2. Elaborar un Plan de Comunicación.

   Se debe documentar a quien se comunicara una disrupción, incluyendo todas las partes interesadas.

3. Elaborar un Proceso de Análisis de Riesgos e Impacto en el Negocio.

   Documento en el que se establece el contexto, criterios y evaluación de potenciales riesgos, tratamientos y salidas del proceso.

4. Elaborar el Análisis de Impacto de Negocio.

   En el que se identifiquen las actividades críticas del negocio y se evalúen el impacto de no realizar dichas funciones en el tiempo, así como la identificación de RTO, RPO, MTPD, etc.

5. Elaborar los Procedimientos de Continuidad de Negocio.

   Estos se derivan de la información recolectada en el BIA y RA su propósito es indicar los principales pasos a seguir por cada rol en caso de disrupción.

6. Elaborar Procedimientos de Respuesta a Incidentes.

   La finalidad de estos procedimientos es dejar en claro los roles y responsabilidades de las personas involucradas, así como la metodología de gestión de los incidentes, entre otros requerimientos.

7. Elaborar Procedimientos de vuelta a la normalidad.
   Una vez se ha finalizado la contingencia, la vuelta al servicio habitual debe ser lo más ágil posible en un inicio para los servicios y posteriormente para los colaboradores, elaborando una serie de procedimientos en los que se indiquen los pasos a seguir para volver a la operación normal.

8. Recolectar Resultados de monitorización y evaluación.
   Dentro de un proceso de mejora continua, se recomienda realizar monitoreo de las actividades, analizarlas y evaluarlas, los resultados deben mantenerse como evidencia del proceso.

9. Recolectar Evidencia de no conformidades.
   Como resultado de las no conformidades detectadas, se deben tomar las medidas para dar tratamiento a las no conformidades, registrando las acciones a tomar como evidencia.

10. Evaluar y Revisar acciones post-incidentes.
    Tras un incidente que detone la activación del Plan de Continuidad, se debe realizar una revisión documentada las acciones tomadas, como evidencia.

11. Plantear una Auditoría Interna.
    Se deben realizar auditorías internas bajo un plan de acción. Conservando los informes como evidencia.

12. Mantener Revisiones por parte de la Alta Dirección.
    La Alta Dirección debe estar involucrada revisando el SGCN bajo un plan de trabajo registrando las revisiones.

13. Detectar No conformidades y acciones tomadas.

    Es recomendable mantener un registro de la evaluación de las no conformidades y las acciones que decidan tomarse.

14. Generar Resultados de acciones correctivas.

    Es recomendable mantener un registro de los cambios que se generan con las auditorias y las acciones tomadas.

15. Elaborar Plan de Capacitación.

    Identifica las capacitaciones que son necesarias en función a los roles y las responsabilidades plasmadas en los documentos anteriores. Sigue la planeación establecida por la organización.

16. Diseñar Plan de Pruebas.

    Es el ejercicio fundamental de la validez de los sistemas de gestión, con la realización de las pruebas, las organizaciones se sitúan en un estatus de madurez en la toma de decisiones frente a un evento disruptivo, los planes de pruebas constan de elementos como una planeación y entregables de sanción y acciones correctivas ante los hallazgos detectados.

17. Gestionar un Plan de Mantenimiento.

    Que permita dar una revisión a la documentación de forma periódica permite garantizar que la información está acorde a los objetivos de la Organización, así como se revisan que los procedimientos estén actualizados. Por otro lado, la revisión y actualización de las pruebas y procedimientos garantiza que se dispone de información reciente en caso de que haya que activar el Plan de Continuidad.

Anexo 6 "Listado de servicios que pueden ser pagados con Bitcoin en El Salvador"

SERVICIOS		***INCIDENTES***				
Agua	Pago de recibo	Fallas en servidores ***Chivo Wallet Proveedor***	Fallas en ***Chivo Wallet Usuario*** de lado usuario	Fallas en ***Chivo Wallet Comercio*** de lado del Banco	Datos erróneos de transacción* ***incidente de saldos***	Transacción no aplicada
Electricidad	Pago de recibo					
Teléfono	Pago de recibo					
Internet	Pago de recibo					
Impuestos	Pago de Impuestos					
AFP´s	Pago de Cuotas					
Pagos en comercios	Compras					
Pagos de tarjetas	Abonos					
Pago de prestamos	Abonos					
Colegiaturas	Pago de Mensualidades					
Aseguradoras	Pago de Pólizas					
Servicios funerarios	Pago de Servicios					
Donaciones a fundaciones	Donaciones					
Préstamos Personales	Abonos					
Abonos a cuentas de ahorros	Abonos					

Glosario.

Continuidad del negocio: capacidad de una organización para continuar con la entrega de productos o servicios a niveles predefinidos aceptables tras una interrupción.

Gestión de la continuidad del negocio: proceso de gestión integral que identifica las amenazas potenciales para una organización y el impacto que esas amenazas, si se materializan, pueden causar en las operaciones del negocio, y proporciona un marco para construir la resistencia de la organización con la capacidad de una respuesta eficaz que salvaguarde los intereses de las partes interesadas clave, la reputación, la marca y las actividades de creación de valor.

Plan de continuidad del negocio: procedimientos documentados que guían a una organización para responder, recuperar, reanudar y restablecer un nivel de funcionamiento predefinido tras una interrupción.

Análisis del impacto en el negocio: proceso de análisis de las actividades y del efecto que puede tener en ellas una interrupción del negocio.

Equipo de gestión de crisis: grupo de funcionalidad individual responsable de dirigir el desarrollo y la ejecución del plan de respuesta y continuidad operativa, de declarar una interrupción operativa o una situación de crisis de emergencia, y de proporcionar dirección durante el proceso de recuperación, tanto antes como después del incidente perturbador.

Interrupción: acontecimiento, ya sea previsto (por ejemplo, una huelga laboral o un huracán) o imprevisto (por ejemplo, un apagón o un terremoto), que causa una desviación negativa no planificada de la entrega prevista de productos o servicios de acuerdo con los objetivos de una organización.

Invocación: acto por el que se declara la necesidad de poner en marcha los mecanismos de continuidad de la actividad de una organización para seguir suministrando productos o servicios clave.

Periodo máximo de interrupción tolerable: tiempo que tardaría en ser inaceptable el impacto adverso que puede surgir como resultado de no suministrar un producto/servicio o realizar una actividad.

Objetivo mínimo de continuidad del negocio: nivel mínimo de servicios y/o productos que es aceptable para que una organización logre sus objetivos de negocio durante una interrupción.

Objetivo del punto de recuperación: punto hasta el que se restablece la información utilizada por una actividad para que ésta pueda funcionar al reanudarse.

Objetivo de tiempo de recuperación: periodo de tiempo tras un incidente en el que se reanuda un producto o servicio o una actividad o se recuperan los recursos.