



Government Blockchain Association

Modelo de Madurez para soluciones desarrolladas en *Blockchain (BMM)*

Introducción al BMM

Versión: 1.0
Fecha: Enero 14, 2023

Aprobaciones

Ver la versión original en Inglés para las firmas de aprobación.

Este documento fue desarrollado por el Grupo de Trabajo de Contenido en Español de GBA, tomando como base el documento original en Inglés desarrollado por el grupo de trabajo de Estándares y Certificaciones de GBA.

Alejandro Mandujano

Director Global Ops &
Región Ibero América

Cargo

Enero 14, 2023

Fecha

Ver la versión original en Inglés para las firmas de aprobación.

Este documento fue desarrollado por el Grupo de Trabajo de Contenido en Español de GBA, tomando como base el documento original en Inglés desarrollado por el grupo de trabajo de Estándares y Certificaciones de GBA.





Contenido

1. Introducción	1
1.1 ¿Por qué necesitamos el BMM?	1
1.2 ¿Qué es el BMM?	1
1.3 ¿Quién es el público del BMM?	1
1.3.1 Proveedores de solución	1
1.3.2 Inversionistas	1
1.3.3 Profesionales de Adquisiciones.....	1
1.3.4 Clientes	2
1.4 ¿Cómo se usa el BMM?	2
1.5 ¿Cómo se mantiene el BMM?	2
1.6 Términos y definiciones	2
2. Alcance de la serie BMM	2
2.1 Soluciones de <i>Blockchain</i>	2
2.2 Documentos de la Serie BMM	2
2.2.1 Introducción	3
2.2.2 Requerimientos	3
2.2.3 Recursos y herramientas	3
2.2.3.1 Profesionales Certificados en BMM	3
2.2.3.2 Herramientas de Consultoría	4
2.2.3.3 Metodología de Evaluación	4
2.2.3.4 Herramientas de Entrenamiento y Certificación	4
3. Principios guía	4
3.1 Principios del <i>Blockchain</i>	4
3.1.1 Principios primarios	4
3.1.2 Principios secundarios	5
3.2 Principio del Modelo de Madurez de <i>Blockchain</i> (BMM)	5
3.2.1 Ruta de mejora de la solución	5
3.2.2 Contexto del dominio	6
3.3 Evaluaciones	6
3.3.1 Socios Autorizados por GBA para realizar Evaluaciones de BMM (BAAs)	6
3.3.2 Preparación de la evaluación	7
3.3.3 Planeación de la evaluación	7
3.3.4 Objetividad vs. Perspectiva	7



3.3.5 Conflictos de interés	8
3.4 Realización de evaluaciones y reporte de resultados	8
4.Contenido y estructura del BMM	8
4.1 Elementos	8
4.1.1 Distribución	9
4.1.2 Gobernanza	9
4.1.3 Administración de Identidades	9
4.1.4 Interoperabilidad	9
4.1.5 Desempeño	9
4.1.6 Privacidad	9
4.1.7 Confiabilidad	10
4.1.8 Resiliencia (Tolerancia a fallas)	10
4.1.9 Seguridad	10
4.1.10 Sostenibilidad de la infraestructura	10
4.1.11 Sincronización	10
4.2 Niveles	10
4.2.1. Nivel 1: Inicial	11
4.2.2. Nivel 2: Documentación	11
4.2.3. Nivel 3: Validación	11
4.2.4. Nivel 4: Producción	11
4.2.5. Nivel 5: Optimización	11
5. Administración del Modelo de Madurez de <i>Blockchain</i>	11

Apéndices:

A	Términos y definiciones
B	Autores, colaboradores y reconocimientos
C	Historial de enmiendas y gestión de cambios



1. Introducción

El propósito de este documento es describir el contenido, estructura, uso y mantenimiento del Modelo de Madurez de Blockchain (BMM), que está integrado por requerimientos, recursos y herramientas aplicables a soluciones desarrolladas bajo Blockchain. Una Solución desarrollada bajo Blockchain incluye todas las capas (red, protocolo, aplicación y transacciones).

1.1 ¿Por qué necesitamos el BMM?

Algunos gobiernos y empresas están en proceso de comprar y desarrollar soluciones basadas en *Blockchain*. Sin embargo, tienen poca o ninguna experiencia en la adquisición, implantación o mantenimiento de soluciones basadas en *Blockchain*.

1.2 ¿Qué es el BMM?

El BMM es un marco estructurado para comparar una solución de Blockchain propuesta o un prototipo con los atributos o elementos de una solución tecnológica confiable. Incluye una evaluación tanto de las características del producto y los procesos empleados para el desarrollo y mantenimiento de la solución. Este modelo es una tecnología agnóstica y es igualmente aplicable a soluciones desarrolladas en Blockchains Públicas, Privadas o Híbridas. No está asociado con algún proveedor, dominio o industria. Está destinado a ser igualmente aplicable a todas las implantaciones de Blockchain.

1.3 ¿Quién es el público del BMM?

1.3.1 Proveedores de soluciones Blockchain

Los proveedores de soluciones utilizan el BMM como hoja de ruta para mejorar su solución y demostrar que cumple con las mejores prácticas de la industria y que los inversionistas, los profesionales de adquisiciones y los clientes pueden confiar en ella. La evaluación se utiliza para demostrar que la solución cumple con los criterios reconocidos internacionalmente para una solución de Blockchain confiable.

1.3.2 Inversionistas

El Inversionista de la solución utiliza los resultados de la evaluación del BMM para evaluar la madurez y el valor de las posibles inversiones en soluciones. Las evaluaciones de nivel uno y dos son aplicables a posibles soluciones y evalúan la viabilidad y solidez de los planes y diseños.

1.3.3 Profesionales de Adquisiciones

Los profesionales de adquisiciones usan el modelo para evaluar las soluciones propuestas y comparar las soluciones ofrecidas con un estándar común para respaldar selecciones de adquisiciones justas y efectivas.

1.3.4 Clientes

Los clientes de soluciones utilizan los resultados de las evaluaciones para respaldar que la evaluación y selección de soluciones de Blockchain cumplan con las expectativas de los clientes y confiar que cuentan con la integridad y sostenibilidad durante el ciclo de vida de la solución.



1.4 ¿Cómo se usa el BMM?

El BMM define un conjunto de expectativas para una variedad de atributos o elementos. Las expectativas se clasifican en niveles de madurez. Cada nivel tiene un conjunto único de criterios. Los criterios son utilizados por expertos en la materia, capacitados y calificados para realizar evaluaciones de acuerdo con un conjunto definido de criterios de evaluación. Los resultados se hacen públicos (si así lo desea el proveedor de la solución) y se pueden utilizar para comparar soluciones con un conjunto común de criterios.

1.5 ¿Cómo se actualiza el BMM?

El BMM se mantiene actualizado por el Grupo de trabajo de estándares y certificación de la Government Blockchain Association, GBA. El grupo está formado por expertos en diferentes materias, y que forman parte de organizaciones internacionales de normalización, organizaciones internacionales de gobernanza y organizaciones tecnológicas. Este es un grupo voluntario que revisa, implanta, evalúa y mejora de forma rutinaria los productos de trabajo relacionados con BMM.

1.6 Términos y definiciones

Los términos y definiciones utilizados en este modelo se registran en el Apéndice A: Términos y definiciones.

2. Alcance de la serie BMM

El alcance de este documento describe los componentes de la serie BMM aplicables a las soluciones de Blockchain en todas las capas (red, protocolo, aplicación y transacciones).

2.1 Soluciones de Blockchain

El alcance de esta serie se refiere a las soluciones de Blockchain. Se entiende que la tecnología de Blockchain puede ser parte de una solución que podría ser una solución confiable, transparente, confiable, inmutable, distribuida y sostenible. Sin embargo, para tener una evaluación integral de una solución para todos los atributos que se esperan de una solución de Blockchain, se requiere un examen integral (Full Stack) de tecnologías. Una solución de Blockchain incluye:

- Protocolo
- Aplicación o solución basada en un protocolo
- Tecnologías que interactúan con otras soluciones
- Personas, procesos e infraestructura de apoyo para sustentar la solución

Los componentes de la Blockchain, incluidos los activos, los datos, los nodos, los mecanismos de consenso/sincronización, la infraestructura/la red, el sistema, los participantes, los protocolos, los registros y los contratos inteligentes o los guiones del ciclo de vida, integran una solución de Blockchain.

2.2 Serie de documentos BMM

Los siguientes elementos están incluidos en el conjunto de productos de trabajo del BMM.



2.2.1 Introducción

Este documento da una descripción general del propósito, el contenido y la estructura de la serie de productos de trabajo del BMM. También establece principios rectores, definiciones y referencias a productos de trabajo relacionados que componen la Serie BMM.

2.2.2 Requerimientos

2.2.2.1. *Requerimientos del modelo*

Los Requerimientos del modelo BMM describen los criterios necesarios para cada elemento y nivel de madurez con el fin de lograr una calificación de nivel para cada elemento del BMM.

2.2.2.2. *Requerimientos de la evaluación*

Los requerimientos del programa de evaluación del BMM describen el método y los criterios mínimos necesarios para planear y realizar la evaluación, así como informar los resultados de la evaluación del BMM.

2.2.2.3. *Requerimientos de capacitación y certificación*

El Documento de requerimientos de capacitación y certificación del BMM describe el método y los criterios para garantizar que las personas hayan recibido la capacitación adecuada y hayan demostrado la competencia necesaria para implantar y evaluar el cumplimiento del BMM.

2.2.3 Recursos y herramientas

GBA pone recursos y herramientas a disposición del público en la [página de Recursos del BMM de GBA](#). Esto incluye información general como videos, texto general, descargas del modelo, Requerimientos de evaluación y un directorio de Asesores Certificados en BMM.

2.2.3.1 *Profesionales Certificados del BMM*

GBA mantiene un directorio de profesionales acreditados. Estas personas incluyen:

- **Consultores:** los miembros de GBA que completan un curso de GBA de Fundamentos de Blockchain, el curso GBA BMM, un taller BMM, y son participantes activos en el programa de educación continua GBA BMM, se enumeran en el sitio de GBA como Consultores BMM.
- **Evaluadores:** las personas que cumplen con los criterios de consultor y han completado con éxito el curso de miembro del equipo de evaluación de GBA y han sido aceptados en el programa de evaluación del BMM y se enumeran en el sitio de GBA como Evaluadores del BMM.
- **Evaluadores Principales:** personas que han cumplido con los Requerimientos de un evaluador BMM y han:
 - Participado en al menos dos evaluaciones como miembros del equipo de evaluación
 - Sido observados, por un Evaluador Principal certificado de GBA, liderando con éxito una evaluación BMM.
- **Instructor BMM:** personas que han sido calificadas por GBA.



2.2.3.2. Herramientas de consultoría

GBA desarrolla recursos y herramientas que pone a disposición de personas certificadas que han cumplido con los criterios descritos en el Documento de Requerimientos de capacitación y certificación del BMM. Estos recursos incluyen listas de verificación, plantillas y documentos de orientación para respaldar las actividades de consultoría e implantación de soluciones de Blockchain. También incluye herramientas para ayudar a una organización a prepararse para una evaluación. Estos recursos y herramientas están disponibles en la Biblioteca de documentos para profesionales del BMM de GBA¹.

2.2.3.3. Metodología de evaluación

La Metodología de Evaluación es un documento de proceso que detalla las actividades, secuencias y criterios de las tareas requeridas para realizar una evaluación de acuerdo con los Requerimientos de Evaluación del BMM. Define las funciones y responsabilidades de todas las actividades que constituyen el proceso de evaluación.

2.2.3.4. Herramientas de capacitación y certificación

Las herramientas de capacitación y certificación incluyen presentaciones de capacitación, guías para instructores, folletos para estudiantes y herramientas de prueba necesarias para capacitar y evaluar de manera consistente el conocimiento, las destrezas y las habilidades personales (KSA, por sus siglas en inglés: Knowledge, Skills & Abilities).

3. Principios guía

Estos principios guía son verdades fundamentales o proposiciones que sirven como base para la serie BMM. Los siguientes principios se utilizan para interpretar y guiar la implantación y la mejora continua de la serie BMM y las soluciones que se implanten y evalúen.

3.1 Principios de Blockchain

Los principios primarios, la descentralización y la distribución son los fundamentos de una solución de Blockchain. Los principios secundarios apoyan el logro de los principios primarios o son el resultado de los principios primarios.

3.1.1 Principios primarios

La razón principal por la que se estableció la primera Blockchain a principios de la década de los 90s fue el resultado de la preocupación de que, a medida que el mundo dependía cada vez más de los registros digitales, esos registros electrónicos podrían alterarse sin ser detectados. Los investigadores reflexionaron sobre cómo sería vivir en un mundo donde no se puede confiar en los registros. Utilizando el trabajo del documento técnico de David Chaum "Sistemas informáticos establecidos, mantenidos y de confianza por grupos mutuamente sospechosos" (Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups"), desarrollaron un sistema que era descentralizado y distribuido. En 1991 Scott Stornetta y Stuart Haber desarrollaron e implantaron la primera Blockchain, quienes son considerados por muchos como los fundadores de Blockchain. Su solución empleó el concepto de datos ligados unidos por criptografía y confirmados por testimonio colectivo. En 2008, Satoshi Nakamoto², refirió a su trabajo en el Documento

¹ El acceso a la Biblioteca de documentos para profesionales del BMM de GBA es limitado a miembros profesionales GBA BMM



técnico (white paper)³ incluyendo el concepto de carga que incluía el libro mayor y un token (Bitcoin).

Desde la primera conceptualización de la tecnología hasta el crecimiento explosivo de la Blockchain, la confianza ha sido el factor más importante en los requerimientos para las soluciones de Blockchain. Por esa razón, a veces se le denomina "Protocolo de confianza". Los fundadores de la tecnología Blockchain identificaron dos principios fundamentales que garantizarían la confianza de los registros digitales: descentralización y distribución. Estos dos principios forman la base de la tecnología Blockchain.

- **Descentralización** – Los datos son distribuidos entre una red integrada por participantes independientes que validan las transacciones.
- **Distribución** - La función de registrar información en una solución de Blockchain se distribuye entre una red para mitigar el riesgo de interrupciones de la red y manipulación de datos.

3.1.2 Principios secundarios

Los principios secundarios son el resultado de lograr la descentralización y la distribución. Estos principios secundarios pueden utilizarse para determinar el grado de descentralización y distribución. Se describen a continuación:

- **Consenso:** el estado de la información verificada es confirmado por un grupo de entidades que acuerdan mutuamente la integridad de la información. Esto puede realizarse mediante una amplia variedad de mecanismos de consenso y sincronización.
- **Criptografía:** las soluciones de Blockchain utilizan criptografía para asegurar transacciones y registros.
- **Inmutabilidad:** la información registrada en una Blockchain nunca se puede cambiar. Sin embargo, se puede agregar nueva información para registrar un cambio de estado. Toda la información y cualquier información agregada se registra de forma permanente.
- **Mecanismo de incentivos:** las soluciones de Blockchain incluyen un mecanismo de incentivos para motivar a las partes interesadas a mantener la solución.
- **Entre iguales (Peer to Peer):** las soluciones de Blockchain de igual a igual utilizan comunicaciones directamente entre las partes interesadas sin la participación de un tercero.
- **Resiliencia:** ninguna entidad o evento individual puede interrumpir o impedir el acceso a la solución de Blockchain.
- **Transparencia:** cualquier cambio en la información registrada en una solución de Blockchain es visible y transparente para todos los usuarios y administradores de la solución.

3.2. Principio del Modelo de Madurez de Blockchain (BMM)

3.2.1 Ruta de mejora de la solución

Ninguna solución es perfecta desde el principio. Las soluciones cambian con el tiempo a medida que cambian el entorno, las necesidades y la tecnología. Las soluciones pueden mejorar o degradarse con el tiempo. Requieren seguimiento, mantenimiento y mejoras. Por

² La identidad de Satoshi Nakamoto es ampliamente discutida

³ <https://bitcoin.org/bitcoin.pdf>



lo tanto, el BMM debe ser utilizado como una herramienta de capacitación y entrenamiento. Los consultores, evaluadores y evaluadores principales deben centrarse en ayudar a los proveedores de soluciones a mejorar su solución.

3.2.2 Contexto del dominio

Si bien el BMM identifica los Requerimientos básicos que se aplican a todas las soluciones de Blockchain, debe entenderse que algunos dominios tienen diferentes expectativas, especificaciones y requerimientos. Por ejemplo, las expectativas de gestión de identidades son muy diferentes según el dominio:

- Los sistemas bancarios y financieros son industrias reguladas que requieren una estricta observancia de las regulaciones contra el lavado de dinero (AML, por sus siglas en inglés: Anti-Money-Laundering) y del conocimiento del cliente (KYC, por sus siglas en inglés: Know-Your-Customer).
- Las soluciones de ensayos médicos requieren que se sepa que los datos provienen de un identificador de paciente específico. Sin embargo, es posible que sea necesario ocultar su identidad específica.
- La mayoría de los sistemas electorales requieren una separación permanente entre el votante y la boleta de votación.

Los profesionales del BMM deben tener la flexibilidad, la experiencia y el juicio para aplicar los requerimientos de manera adecuada en el contexto del dominio.

3.3 Evaluaciones

Las evaluaciones del BMM son un proceso. Este proceso se basa en requerimientos específicos para:

- La Preparación
- La Planeación y realización de las evaluaciones
- El Reporte de resultados

3.3.1 Asociados Autorizados por GBA para realizar Evaluaciones de BMM (BAAs – por sus siglas en inglés, BMM Authorized Associates)

GBA reconoce y publica los resultados de las Evaluaciones de BMM realizadas tanto por GBA como por los Asociados Autorizados por GBA (BAAs). El procedimiento para ser un BAA – BMM Assessment Associate incluye los siguientes criterios:

- Ser Miembro Empresarial Activo de GBA
- Ser recomendado por el Líder Regional de GBA
- Ser Aprobado por el Director de Estándares & Certificaciones de GBA

Los BAAs son encargados de establecer relaciones de negocio con las diferentes entidades para realizar Evaluaciones de BMM. Sin embargo, los BAAs no podrán establecer o tener relaciones actuales de negocio para realizar funciones de Consultoría y Evaluaciones en la misma entidad.

Se requiere que el BAA registre cualquier Evaluación de BMM con el Director de Estándares & Certificaciones de GBA en un plazo no mayor a 30 días naturales de iniciar la relación de negocios con la entidad. Al concluir con la Evaluación de BMM, el BAA entregará los



entregables de la Evaluación del BMM al Director de Estándares & Certificaciones para su revisión y aprobación junto con el pago de la cuota por el servicio de Revisión de la Evaluación de BMM. Una vez aprobado, el resultado de la Evaluación de BMM será publicado en la Página Web del BMM.

3.3.2 Preparación de la evaluación

Los proveedores de soluciones pueden descargar recursos del sitio de GBA para prepararse para la evaluación. Buscar el consejo de un Asesor profesional de BMM puede optimizar y acelerar los resultados positivos. GBA no participa en servicios de consultoría. Sin embargo, capacita y acredita a expertos de BMM que estén disponibles para ofrecer asesorías a organizaciones que buscan apoyo para su proceso de mejora de soluciones basadas en el BMM.

3.3.3 Planeación de la evaluación

Las evaluaciones se planifican para maximizar el valor de una evaluación y minimizar los costos y gastos administrativos. La planificación implica las siguientes consideraciones:

3.3.3.1. Equipos de evaluación

Los equipos de evaluación se integran por un grupo de por lo menos cuatro miembros calificados del equipo de evaluación, uno de los cuales es un evaluador principal. El equipo combinado debe tener las habilidades y capacidades para realizar una evaluación desde las siguientes perspectivas:

- Técnica
- Legal
- Gestión de Activos Digitales
- Industria/Dominio

Es responsabilidad del Evaluador principal validar que el equipo esté adecuadamente capacitado para realizar la evaluación.

3.3.3.2. *Preparación para la Auto-Evaluación*

Previo a la conformación del equipo para realizar la evaluación, el evaluador principal y el punto de contacto de la solución verifican que la documentación con la adecuada evidencia objetiva haya sido recopilada para sustentar la evaluación y que se encuentre disponible durante la revisión del equipo. Esto puede ser realizado por un consultor. Sin embargo, se recomienda utilizar un consultor autorizado por GBA para minimizar sorpresas durante la revisión realizada por el equipo de evaluación.

3.3.4 Objetividad vs perspectiva

Los equipos de evaluación necesitan objetividad y perspectiva para realizar una evaluación de manera efectiva. Por lo general, la perspectiva se logra al tener personas dentro del equipo que conocen de cerca la solución. Sin embargo, esas personas suelen carecer de objetividad. La objetividad es absolutamente necesaria en un equipo de evaluación. Para equilibrar estas dos importantes consideraciones, el equipo puede estar compuesto por personas internas y externas a la organización que buscan la evaluación. Sin embargo, se aplican las siguientes restricciones:



- Los miembros del equipo interno no pueden representar más del 50% del equipo de evaluación.
- Nadie que sea responsable del resultado positivo de la evaluación puede formar parte del equipo de evaluación. Esto incluye a cualquier consultor, gerente o cualquier persona dentro de la cadena de liderazgo relacionada con la solución.
- Ningún miembro interno del equipo de evaluación puede tener autoridad de supervisión sobre otro miembro interno del equipo.

3.3.5 Conflictos de intereses

Los conflictos de intereses son casi inevitables. Sin embargo, el asesor principal es responsable de garantizar que se identifiquen y mitiguen todos los posibles conflictos de interés.

3.4 Realización de evaluaciones y reporte de resultados

Los equipos de evaluación revisarán la evidencia y realizarán entrevistas para realizar la evaluación. El equipo logrará un consenso sobre los resultados de la evaluación. Los resultados de la evaluación incluyen una calificación para cada elemento. La calificación más baja de un elemento representará la calificación general del nivel del resto de los elementos de la solución. Junto con las calificaciones, hay debilidades/oportunidades de mejora identificadas por el equipo para ayudar a la organización a madurar la solución al siguiente nivel de madurez para cada elemento. Una vez que la Solución basada en Blockchain sea Evaluada y con un resultado positivo será publicada en la Página Web de GBA.

4. Contenido y estructura del BMM

Las capacidades definidas en el Modelo de Madurez de Blockchain (BMM), se articulan en dos tipos de requerimientos y expectativas de evaluación. Hay requerimientos y expectativas genéricos, y requerimientos y expectativas específicos del dominio.

- Los requerimientos y expectativas genéricos se refieren al conjunto de elementos que debe tener una solución de Blockchain para que sea una solución confiable.
- Los requerimientos y expectativas específicas son un conjunto de elementos que son necesarios para la aplicación de la tecnología Blockchain a dominios específicos.

4.1 Elementos

Para que una solución sea confiable para el uso en las organizaciones, debe ser capaz de cumplir con los requerimientos y expectativas en los siguientes elementos:

- Distribución
- Gobernanza
- Administración de Identidades
- Interoperabilidad
- Desempeño
- Privacidad
- Confiabilidad
- Resiliencia
- Seguridad
- Sostenibilidad de la infraestructura
- Sincronización

Los siguientes subpárrafos describen los objetivos asociados con cada elemento:



4.1.1 Distribución

El objetivo de la distribución es evaluar el riesgo de concentración de hospedaje de homogéneo a heterogéneo.

4.1.2 Gobernanza

El objetivo de la gobernanza en una solución de Blockchain es proporcionar una administración eficaz de los componentes clave, incluidos los activos, los nodos, los mecanismos de sincronización, la infraestructura/red, el sistema, los participantes, los protocolos, los registros y los contratos inteligentes o las descripciones (scripts) del ciclo de vida. La gobernanza puede ser realizada por una variedad de mecanismos que van desde una autoridad centralizada hasta uno o más acuerdos de red mutualizados.

4.1.3 Administración de Identidades

El objetivo de la administración de identidades en una solución de Blockchain es garantizar que existan controles para la administración de identidades y accesos. Los controles incluyen:

- Métodos para identificar a los usuarios de un sistema y establecer un perfil de usuario, dirección u otro identificador
- Definir las actividades y los procesos para vincular a un usuario a una identidad conocida o disociar a un usuario de una identidad real para proteger el anonimato.
- Asociar perfiles de usuario con uno o más roles y/o permisos
- Asociar roles y niveles de acceso y permisos
- Asignar usuarios a grupos
- Realizar Altas, Bajas y Cambios (ABCs) de usuarios, roles, grupos y permisos
- Limitar el acceso a individuos y grupos según las reglas definidas.

4.1.4 Interoperabilidad

El objetivo de la interoperabilidad es facilitar la capacidad de una solución de Blockchain para compartir y utilizar información y activos con otras soluciones heredadas y de otras soluciones de Blockchain.

4.1.5 Desempeño

El objetivo del Desempeño en una solución de Blockchain es garantizar que los volúmenes de transacciones y la velocidad de transmisión sean adecuados para el uso de la Blockchain. Esto se mide sobre la base de una comprensión de los requerimientos de la demanda y la utilización de los recursos. Incluye la consideración de la capacidad, el costo, la latencia, la memoria, las velocidades de transacción y la finalización de la transacción.

4.1.6 Privacidad

El objetivo de la privacidad en una solución de Blockchain es garantizar que la solución tenga el cifrado y la protección adecuados de la información de identificación personal (PII por sus siglas en inglés: Personal Identifiable Information) de acuerdo con los estándares internacionales, como la Regulación general de privacidad de datos (GDPR; por sus siglas en inglés: General Data Privacy Regulation) y demás regulaciones y códigos nacionales y / o locales. Las protecciones se requieren tanto interna como externamente a la red debido a los componentes clave, compuestos por nodos, mecanismos de



sincronización, infraestructura/red, sistema, scripts determinísticos y contratos inteligentes.

4.1.7 Confiabilidad

El objetivo de la confiabilidad en una solución de Blockchain es proporcionar la seguridad de que los controles adecuados aborden y mitiguen la resolución de duplicidad de bloques, bloques, errores o fraudes en disputa en la red.

4.1.8 Resiliencia (tolerancia a fallas)

El objetivo de la resiliencia en una solución de Blockchain es garantizar la continuidad de las operaciones durante eventos imprevistos, limitaciones y fallas. La Administración de la resiliencia tiene como objetivo optimizar la capacidad y disponibilidad de los componentes críticos. Los componentes críticos pueden incluir nodos, mecanismos de sincronización, infraestructura/red, sistema, contratos inteligentes y scripts determinísticos.

4.1.9 Seguridad

El objetivo de la seguridad en una solución de Blockchain es garantizar que los controles adecuados aborden y mitiguen los riesgos de seguridad de extremo a extremo de la solución compuesta por nodos, mecanismos de sincronización, infraestructura/red (*hardware/software*), interfaces de red, dispositivos conectados a red, sistema, scripts determinísticos y contratos inteligentes.

4.1.10. Sostenibilidad de la infraestructura

El objetivo de la sostenibilidad de la infraestructura es garantizar la disponibilidad de todos los recursos necesarios para mantener las capacidades y satisfacer los requerimientos a lo largo de la vida útil de la solución.

4.1.11. Sincronización

El objetivo de la sincronización en una solución de Blockchain es evaluar los medios para que la red logre consistencia e integridad para lograr la irrevocabilidad de los registros distribuidos e inmutables. La sincronización cubre muchos mecanismos que incluyen, entre otros, algoritmos de consenso, competencias como minado, validadores elegidos o seleccionados con soluciones de prueba de participación (*proof of stake*).

4.2 Niveles

Dentro de cada elemento, hay cinco niveles. Los cinco niveles se relacionan con los grados de confiabilidad y cumplimiento para el elemento dado o el elemento específico del dominio. Los cinco niveles son:

- Level 1: Inicial
- Level 2: Documentación
- Level 3: Validación
- Level 4: Producción
- Level 5: Optimización

Para ser evaluado en cualquier nivel, todas las expectativas de ese nivel e inferiores deben cumplirse para todos los requerimientos especificados en cada nivel.



4.2.1. Nivel 1: Inicial

El nivel inicial es el nivel de referencia. Representa el estado de tener alguna parte del elemento documentado e implantado. Para que una solución alcance el nivel uno, debe haber alguna evidencia de que las actividades descritas en la descripción del elemento han sido documentadas y/o implantadas.

4.2.2. Nivel 2: Documentación

Los elementos se evalúan como "Documentados" cuando hay evidencia de que las actividades descritas en la descripción del elemento BMM se han incorporado en las especificaciones detalladas, los planes, los diseños u otra documentación de la solución. La documentación debe ser suficiente para brindar confianza a los inversionistas, usuarios potenciales y clientes de que la solución (o solución potencial) tiene la capacidad de implantar el elemento cuando se implanta en un entorno de producción.

4.2.3. Nivel 3: Validación

Los elementos se evalúan como "Validados" cuando existe evidencia adecuada de que la solución demuestra que funciona según lo previsto, genera el resultado esperado y es una prueba de concepto. El sistema demuestra que cada elemento del sistema tiene la capacidad de satisfacer sus Requerimientos operativos durante el ciclo de vida de la solución.

4.2.4. Nivel 4: Producción

Los elementos se evalúan como "Producción" cuando existe evidencia adecuada de que funcionan según lo previsto, generando el resultado esperado, junto con todas las demás partes de la solución de Blockchain. Por lo tanto, la solución tiene la capacidad de implantación operativa, con documentación de respaldo y registro de su desempeño.

4.2.5. Nivel 5: Optimización

Los elementos se evalúan como "optimizados" cuando existe evidencia adecuada de que pueden mantener la continuidad de sus operaciones, con un desempeño consistente y confiable, durante un período prolongado. También se espera que las soluciones demuestren evidencia adecuada de que pueden adaptarse a la escala adecuada de implantación, mientras mantienen un Desempeño consistente y confiable.

5. Administración del Modelo de Madurez de Blockchain

GBA es responsable de revisar y mejorar periódicamente la Serie BMM de documentos, recursos y herramientas. Con ese fin, GBA estableció un Director de Estándares y Certificaciones que es responsable de la supervisión del programa BMM y de las actividades relacionadas. Estas actividades incluyen:

- Establecimiento de grupos e individuos de supervisión
- Programar y realizar revisiones periódicas y revisiones de los documentos y herramientas de la serie BMM



Apéndice A: Términos y definiciones

Término	Definición
Administrative Control (Control administrativo)	La capacidad de realizar cambios en el hardware del nodo o en las actualizaciones del libro mayor.
Asset (Activo)	Cualquier cosa que tenga valor para una parte interesada. Ver ISO/TS 19299:2015 3.3
Block (Bloque)	Datos estructurados que comprenden datos de bloque y un encabezado de bloque
Block Data (Bloque de datos)	Datos estructurados que comprenden cero o más registros de transacciones o referencias a registros de transacciones.
Block Header (Encabezado de bloque)	Datos estructurados que incluyen un enlace criptográfico al bloque anterior a menos que no haya un bloque anterior
Block Reward (Recompensa por bloque)	Recompensa otorgada a los mineros o validadores después de que se confirma un bloque en un sistema de Blockchain
Blockchain	Libro mayor distribuido con transacciones confirmadas, organizadas en una cadena secuencial de "solo registrar" usando enlaces criptográficos
Blockchain System (Sistema Blockchain)	Sistema que implanta una Blockchain
Charter (Carta)	El término "carta" o "carta del proyecto" se refiere a uno o más documentos que describe cómo se Implantará la solución blockchain. Podría ser una propuesta, libro blanco, plan de proyecto, documento de diseño, paquete técnico de datos o cualquier otra combinación de productos de trabajo que definan las intenciones de las partes de Implantar una solución Blockchain.
Components (Componentes)	Referente a nodos, mecanismos de consenso, infraestructura/red, sistema, scripts determinísticos y contratos inteligentes.
Consensus (Consenso)	Acuerdo entre los nodos DLT (Distributed Ledger Technology por sus siglas en inglés) de que se valida una transacción y que el libro mayor distribuido contiene un conjunto coherente y ordenado de transacciones validadas
Consensus Mechanism (Mecanismo de consenso)	Acuerdo entre los nodos DLT de que se valida una transacción y que la Contabilidad distribuida contiene un conjunto consistente y un orden de transacciones validadas.
Crypto-asset (Cripto-activo)	Activo digital generado mediante técnicas criptográficas



Cryptocurrency (Criptomoneda)	Cripto activo diseñado para funcionar como un medio de intercambio de valor
Cryptographic hash function (Función de algoritmo criptográfico)	Función de mapear cadenas binarias de longitud arbitraria a cadenas binarias de longitud fija, de modo que es computacionalmente costoso encontrar un resultado dado, una entrada que genere el mismo resultado. Es computacionalmente inviable encontrar para una entrada dada una segunda entrada que se asigne al mismo resultado, y es computacionalmente inviable encontrar dos entradas distintas que se asignen al mismo resultado
Cryptographic link (Enlace criptográfico)	Una referencia, construida utilizando una función técnica de un algoritmo criptográfico, que apunta a datos.
Cryptography (Criptografía)	Una Disciplina que incorpora los principios, medios y métodos para la transformación de datos con el fin de ocultar su contenido semántico, impedir su uso no autorizado o impedir su modificación inadvertida.
Decentralization (Descentralización)	Este término se utiliza para describir el grado en que una sola parte puede tomar decisiones o acciones en comparación con una población general de partes interesadas.
Decentralized Application (Aplicación descentralizada DApp)	Aplicación que se ejecuta en un sistema descentralizado
Decentralized System (Sistema descentralizado)	Este es un sistema distribuido en el que el control se distribuye entre las personas u organizaciones que participan en su funcionamiento.
Digital Asset (Activo Digital)	Un activo que existe sólo en forma digital o que es la representación digital de otro activo.
Domain Area (Area Dominio)	El conjunto de funciones que son necesarias para la aplicación de tecnología blockchain para usos específicos.
Element (Elemento)	Una de las características que debe tener una solución blockchain para que sea una solución confiable.
Inmutability (Inmutabilidad)	Una propiedad del libro mayor en la que los registros no se pueden modificar ni eliminar una vez que se agregan al libro mayor distribuido.
Interoperability (Interoperabilidad)	La capacidad de dos o más sistemas o aplicaciones para intercambiar información y activos. También incluye la capacidad de utilizar mutuamente la información y los activos que se han intercambiado.
Key Components (Componentes Clave)	Un componente que, si falla o se degrada, afectaría negativamente el Desempeño general de la solución de Blockchain.
Blockchain Node (Nodo)	Un Nodo de Blockchain es un dispositivo, normalmente una



de Blockchain)	<p>computadora, que participa en la red de blockchain. Opera con un Software bajo el protocolo de Blockchain, que le permite ayudar en la validación de transacciones y mantener la red segura. Los nodos de Blockchain se intercomunican entre ellos.</p> <p>Mientras más nodos sean controlados de forma independiente, más Descentralizada la red de Blockchain será.</p>
Smart Contracts (Contratos Inteligentes)	<p>Código de software que automatiza la ejecución de un acuerdo. Nota: Un Smart Contract puede representar los términos legales en un contrato legal y crear una obligación legal exigible de acuerdo a alguna ley aplicable dentro de una jurisdicción.</p>
Solution Point of Contact – SPoC (Punto de Contacto de la Solución)	<p>El Punto de Contacto de la Solución, es la persona dentro de la organización que colabora con el Evaluador Principal para planear y conducir la Evaluación. El Spoc recibe del Equipo de Evaluación el informe de la Evaluación. Es considerado el Cliente de la Evaluación.</p>
Transaction Finality (Finalización de Transacción)	<p>El momento en que es imposible revertir o alterar una transacción que es registrada en la Blockchain.</p>



Apéndice B: Autores, colaboradores y reconocimientos.

Un agradecimiento especial a las siguientes personas por su arduo trabajo, contribuciones y aportaciones:

- [Alejandro Mandujano](#)
- [Allyson R. Ugarte](#)
- [Dino Cataldo Dell'Accio](#)
- [Frederic de Vault](#)
- [Gerard Dache](#)
- [Lori Souza](#)
- [Meiyappan Masilamani](#)
- [Paul Dowding](#)
- [Steve Henley](#)



Apéndice C: Registro de Control de cambios

Historial de enmiendas y gestión de cambios				
Versión	Cambios/ Razones	Referencia del cambio	Modificado por	Fecha
1.0	Versión Inicial			Enero 14, 2023