Políticas de Gobierno y Operación de la Red T Alastria

v.1.0

Document Control

Version history

Version	Date	Comments
0.1	15-feb-2019	Versión inicial usando referencia de un documento previo creado por Jesús Ruiz y la Comisión de Resiliencia
0.2	19-may-2019	Inclusión de sección de Documento de Aceptación de Compromiso de Ejecución de Nodos Críticos
0.3	22-may-2019	Inclusión de sección de Documento de Aceptación de Compromiso de Ejecución de Nodo Regular
0.4	31-may-2019	Cambios menores
0.5	23-sep-2019	Inclusión de referencias de documentos estándares
0.6	25-sep-2019	Refundición de los tres documentos de Políticas existentes anteriormente en uno solo y añadir comentarios del Equipo Core y varios revisores más
0.7	03-oct-2019	Revisión con Javier Ibáñez para incorporar aclaraciones de los comentarios realizados por Moisés
0.8	07-oct-2019	Incorporar comentarios de Domingo Gaitero en referencia a los estándares ISO 27001 y referencias a las Políticas de Propiedad Intelectual en el Estatuto; y las de Julio San José, pequeñas referencias de NTP y de guarda de claves.
0.9	18-nov-2019	Actualización según sugerencias de la última Junta Directiva (CML y JLG)
1.0	04-feb-2020	Cambios sugeridos por Ismael Arribas en relación con términos en el Glosario y a apartados del resto de la política
1.01	04-mar-2020	Inclusión de una aclaración en el apartado 3.1.2 “Este punto de libre acceso en lectura NO ocurre en el caso de la Red T de nodos de socios Alastria como se especifica más adelante.”

Issue Control

Owner: Juan Luis Gozalo

Reviewed by:

Miguel García – CPO Alastria - Fecha: 27/sept/2019

Jaime Cuesta – Responsable Proyectos Alastria - Fecha: 27/sept/2019

Cristina Martínez – CLO Alastria – Fecha: 27/sept/2019- 22/octubre/2019

Carlos Pastor – Líder Comisión Identidad – Fecha: 27/sept/2019

Nacho de la Vega – Equipo Core Plataforma y Core Identidad - Fecha: 27/sept/2019

Urko Larrañaga – Equipo Core Plataforma - Fecha: 27/sept/2019

Nacho Alamillo – Líder Comisión Estándares – Fecha: 30/sept/2019

Ismael Arribas – Líder Comisión Estándares – Fecha: 30/sept/2019, dic/2019
Javier Ibáñez – Sponsor CITT – Fechas: 21/sept/2019, 11/oct/2019
Julio San José – Líder Comisión Resiliencia – Fecha: 07/oct/2019
Domingo Gaitero – Proceso Social – Experto en Calidad – Fecha: 07/oct/2019
Comité Legal: Fecha: 17/oct/2019
Comité Legal: Fecha: 21/nov/2019

Approved by: Junta Directiva 28/nov/2019
Comité Legal: 21/nov/2019

Distribution:

None

File reference:

Change Log

Version	Status[1]	Changes on version
0.1	JLG	Versión Inicial
0.2	JLG	Inclusión de sección de Documento de Aceptación de Compromiso de Ejecución de Nodos Críticos
0.3	JLG	Inclusión de sección de Documento de Aceptación de Compromiso de Ejecución de Nodo Regular
0.4	JLG	Eliminar la palabra Telsius del apartado 2
0.5	JLG	Incorporar referencias de términos, políticas y definiciones a lo largo del texto. Reescritura de apartados de Política Permisionado e incluir Des-permisionado
0.6	JLG	Refundición: Este documento incorpora ahora la Política de Permisionado, la Política de Nodos Críticos y la Política de Nodos Regulares, todos en un único documento. Cambia además “Red Alastria” por “Red T de los socios de Alastria” Incluye las referencias al Comité de Emergencia y a las Políticas de Incidencias y de Cambios
0.6	NdLV	Aclaraciones sobre los nodos Bootnodes y el permisionado
0.6	IA, CML, MG, JC, CP	Aclaración Red T el software base “es” del software Quorum, indicando también que los equipos de trabajo de socios de Alastria han realizado las correspondientes modificaciones a este software. Cambios en Glosario Corrección en pag.17 sobre definición

[1] Juan Luis Gozalo (JLG); NdLV (Nacho de la Vega); IA (Ismael Arribas); NA (Nacho Alamillo); CML (Cristina Martínez Laburta); MG (Miguel García); JC (Jaime Cuesta), CP (Carlos Pastor); JI (Javier Ibáñez); JSJ (Julio San José); DG (Domingo Gaitero)

		Cambios en los gráficos de topología de Red T para darle mayor claridad Aclaración de tipo de red asignada a Red T según ITU Cambio de “Organizacionales” a “organizativos” y “Operacionales” Unificar los apartados de Glosario en uno único
0.7	JLG/JI	Incorporar aclaraciones en base a los comentarios recibidos de Moises para dejar claras responsabilidades y declaración de Red “Best Effort”
0.8	JSJ, DG	Cambiar NTP de nis.org a hora.roa.es Aclarar dónde se guardan las claves de los nodos Incorporar nota a pie de alineamiento con ISO 27001 Incorporar nota a pie de referencia a Propiedad Intelectual Incorporar nota a pie de referencia a Privacidad de Datos/GRPD
0.9	CML, JLG	Inclusión de las secciones 9.1 y 9.2 Ajuste del formato de secciones y tabla de contenidos Eliminar en varias secciones la especificación de “obligatoriedad” sustituyéndola por la “recomendación fuerte”.
1.0	IM, CML, JLG	Precisión de terminología en el glosario y en diferentes apartados según comentarios de IM.
1.01.	JLG, CML	Inclusión de una aclaración en el apartado 3.1.2 “Este punto de libre acceso en lectura NO ocurre en el caso de la Red T de nodos de socios Alastria como se especifica más adelante.”

Índice

Glosario

Asociado: miembro de la Asociación Consorcio Red Alastria.

AWS - Amazon Web Services: Proveedor de servicios de máquinas de infraestructura virtual donde alojar servicios de web, procesamiento, etc…

Bastionado de sistemas (o *hardening*): conjunto de políticas de seguridad, endurecimiento y delimitación clara de los privilegios de usuarios, grupos, roles y configuración de servicios de protocolo de internet (*Internet Protocol,* IP)[2].

CPD (Centro de Procesamiento de Datos): Ubicación física donde están instaladas las máquinas físicas donde se procesan las operaciones informáticas.

DLT (*Distributed Ledger Technology*[3])(Tecnología de Registro Distribuido): *Un registro distribuido es un registro compartido, replicado y sincronizado de una forma descentralizada y distribuida.*

Docker: Sistema de gestión de paquetes virtuales (contenedores) que permiten una instalación más automática y controlada.

Entornos Virtualizados: Técnicamente hablando es la posibilidad de tener máquinas (computadoras) ejecutándose de manera virtual (no en una máquina física) dentro de una máquina física o varias.

Equipo *Core*: Personas cedidas de manera voluntaria por los Asociados realizando funciones de soporte, desarrollo e investigación de nuevas funcionalidades a incorporar a la plataforma de la Red T.

Equipo de Motor de Gestión: Personas dependientes de la Dirección General de Alastria con la función de dinamizar y favorecer la colaboración de los asociados.

Guía de Bastionado: Instrucciones para realizar una securización (dotación de niveles técnicos de seguridad o aseguramiento) de una instalación informática.

---

[2] Cf. INSTITUTO NACIONAL DE CIBERSEGURIDAD (INCIBE), https://www.incibe.es/protege-tu-empresa/catalogo-de-ciberseguridad/listado-soluciones/bastionado-sistemas-y-servidores

[3] ITU (2019) ”Technical Specification FG DLT D1.1 - Distributed ledger technology terms and definitions”: “Distributed Ledger is a type of ledger that is shared, replicated and synchronised in a distributed and decentralized manner”

GitHub: Sistema de control de versiones, de gran uso por la comunidad de desarrolladores y que se usa por la Asociación Consorcio Red Alastria para ubicar, referenciar y acceder al *software* abierto creado colaborativamente por sus Asociados.

IBFT (*Istanbul Byzantine Fault Tolerance)*: Mecanismo de consenso establecido entre los nodos de una red *blockchain* para tomar la decisión de unir o no un bloque a la cadena de bloques, donde se persigue una tolerancia eficiente de faltas o incumplimientos, esto es, un algoritmo que logre consenso entre un mayor número de nodos honestos (tolerantes a faltas) que deshonestos (incumplidores, fraudulentos, fallidos o *faulty nodes).*[4] y [5]. Forma parte de la familia de mecanismos de consenso BFT.

Lista de Permisionado: Lista de nodos que han sido habilitados en una red *blockchain*.

Mecanismo de Consenso[6]: Reglas y procedimientos por los cuales los nodos de una red determinan y acuerdan cómo validar un conjunto de transacciones.

Mecanismo de Permisionado: Función que habilita o no la comunicación entre los nodos de la red en base a una serie de reglas manuales o automáticas, dentro de un ámbito de red pública permisionada.

Mejores Esfuerzos (*Best Efforts*): Estándar de responsabilidad civil por culpa o negligencia de los gestores de nodos que les obliga a vigilar la actividad del nodo conforme a las reglas y políticas de la red y a seguir las buenas prácticas profesionales y estándares de los operadores (*lex artis*), a fin de prevenir cualquier daño nodal a terceros.

Nodo: Computadora o proceso que se conecta a una red DLT y utiliza el protocolo *peer-to-peer* (P2P, por sus siglas en inglés) que permite que dichas máquinas se comuniquen entre sí dentro de la red, así como difundir información sobre transacciones y bloques. Según ITU, es "un proceso o dispositivo que participa en una DLT"[7]

---

[4] ITU (2019), ITU-T Technical Specification FG DLT D3.1, *DLT Reference Architecture,* Agosto, sub 6.1.5.3.

[5] Consensys Inc.(jun-2018) https://media.consensys.net/scaling-consensus-for-enterprise-explaining-the-ibft-algorithm-ba86182ea668

[6] ITU (2019) "Technical Specification FG DLT D1.1 - Distributed ledger technology terms and definitions": "Consensus mechanisms are the rules and procedures by which consensus is reached" and "Consensus is an agreement that a set of transactions is valid"

[7] ITU (2019) "Technical Specification FG DLT D1.1 - Distributed ledger technology terms and definitions": "node is a device or process that participates in a distributed ledger network".

Nodos Críticos: En la Red T se definen como aquellos nodos sin los que la red no puede funcionar, dada la naturaleza de la función que realizan.

Nodos Permisionadores: Ejecutan la función de *bootnode* de Quorum[8] para permitir el descubrimiento de nodos en una red peer to peer. Sin la aceptación por parte de uno de estos nodos, un nuevo nodo no puede unirse a la red.

Nodos Regulares: Participan replicando la *blockchain*, aceptando los bloques generados por los validadores y ejecutando las transacciones incluidas en los mismos. También se les permite inyectar transacciones en la Red a partir de fuentes externas al *blockchain*.

Nodos Validadores: Nodos que se encargan de garantizar el consenso de la red y de la generación de bloques. Para ello, ejecutan el algoritmo de consenso (IBFT)[9].

Permisionado: Autorización o habilitación de los Nodos Permisionadores a los Nodos Regulares para que, empleando el límite de gas concedido, propongan (inicien), realicen (escriban), o consulten (lean) transacciones.

Quorum: *Software* de JPMorgan, cliente de la red *Ethereum* que incorpora características propias de una *blockchain* permisionada, como permitir transacciones privadas y cambiar el modo en el que se decide la inclusión de bloques en la cadena *blockchain*.

Repositorio Público de *Software*: Espacio centralizado donde se almacena, organiza, mantiene y difunde información digital, habitualmente archivos informáticos, que pueden contener trabajos científicos, conjuntos de datos o *software*.

Resiliencia: Capacidad de un sistema para recuperarse de las incidencias que pueda sufrir.

RTO (*Recovery Time Objective)*: Tiempo deseado para la recuperación de un activo informático tras una incidencia.

RPO (*Recovery Point Objective*) - Punto de recuperación objetivo entendido como la cantidad de datos que se puede asumir perder en caso de una incidencia tras un fallo del sistema. Se define como tiempo por ser el periodo que transcurre entre el momento del desastre y el último punto de restauración de los datos en una copia de seguridad.

[8] Quorum está desarrollado por JPMorgan y se puede encontrar en https://www.goquorum.com/

[9] IBFT – Istanbul Bizantine Fault Tolerance

Sistema Operativo: Elemento de *software* que gestiona los recursos de hardware de una máquina.

Solidity Command Line Interface (solc): Solidity es un lenguaje de programación de *smart Contracts* en *Ethereum*. *Solc* es un tipo de compilador de línea de comandos sin interfaz gráfica para ese lenguaje.

Transacción privada: Transacción sólo conocida entre emisor y receptor.

Validación: Proceso por el que los Nodos Validadores verifican que las transacciones recibidas cumplen el protocolo IBFT establecido, aseguran la formación de bloques de transacciones, la correspondencia de claves criptográficas en la cadena de bloques y, en última instancia, la unidad de esta.

VPN (*Virtual Private Network*): Conexión telemática entre dos ordenadores usando técnicas criptográficas que permiten garantizar la privacidad de la comunicación entre ellas.

Web3j: Librería ligera de Java y Android, altamente modular, para trabajar con *Smart Contracts* e integrar clientes (nodos) sobre redes tipo *Ethereum*[10].

[10] https://docs.web3j.io/

1. Introducción, Objetivos y Alcance

El Consorcio Red Alastria (en lo sucesivo, ALASTRIA, la ASOCIACIÓN o el CONSORCIO) se constituye como asociación al amparo de la Ley Orgánica 1/2002, de 22 de marzo, reguladora del Derecho de Asociación. ALASTRIA cuenta con plena capacidad de obrar y ha sido inscrita en la Sección Primera del Registro Nacional de Asociaciones con el número 616096.

ALASTRIA opera sin ánimo de lucro y tiene como objetivo fundamental crear una comunidad integrada por todo tipo de organizaciones públicas y privadas, así como expertos individuales, para favorecer la implantación, estandarización, protección y utilización de las tecnologías tipo Distributed Ledger Technologies (DLT), fomentando el conocimiento y el uso por la sociedad española de esta tecnología, promoviendo su uso entre las administraciones, las empresas y demás agentes sociales.

ALASTRIA, en su calidad de comunidad sin ánimo de lucro dedicada a la promoción de redes e infraestructuras distribuidas (*blockchain*), bajo los principios de ausencia del interés comercial y de neutralidad tecnológica, gracias a la colaboración de sus asociados (Los Asociados), ha desarrollado la infraestructura denominada Red T (la "Red" o la "Red de Socios de Alastria") con la finalidad de que sus asociados puedan realizar en ella pruebas de concepto/producto/actividad, en las condiciones que en cada caso se determinen.

El artículo 3 de los estatutos de ALASTRIA ("Fines y actividades") establece que las Guías Básicas Tecnológica y Operativa, bajo forma documental primaria o principal de Políticas de Gobierno y Operación de la Red ("Políticas de Gobierno"), establecerán los protocolos y estándares *blockchain* que adoptarán las redes que sigan los estándares de ALASTRIA (Guía Tecnológica) y se completarán cuando sea necesario con sub-políticas técnicas de gobierno de nodos (críticos o regulares) y permisionado. En todo momento se dará prioridad a criterios de neutralidad tecnológica (ausencia de preferencias sobre una tecnología concreta) y universalidad (intento de habilitar el máximo de protocolos tecnológicos que permita el uso y mayor adopción posible de la red).

La "**Red T" es una red permisionada pública**[11] accesible a cualquier usuario con un ordenador y una conexión a Internet. Los Nodos Regulares que participan en ella han de ser aceptados por los Nodos Permisionadores, pero las transacciones por defecto son públicas. Eso quiere decir que los Nodos Críticos participan en el mantenimiento y seguridad de la Red y que todas las transacciones, salvo que decidan usar características de Transacción Privada, son visibles para los distintos Nodos.

[11] Según la clasificación de la ITU(International Telecommunications Union): https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d12.pdf Apartado 4 la Red T sería un tipo de red permisionada

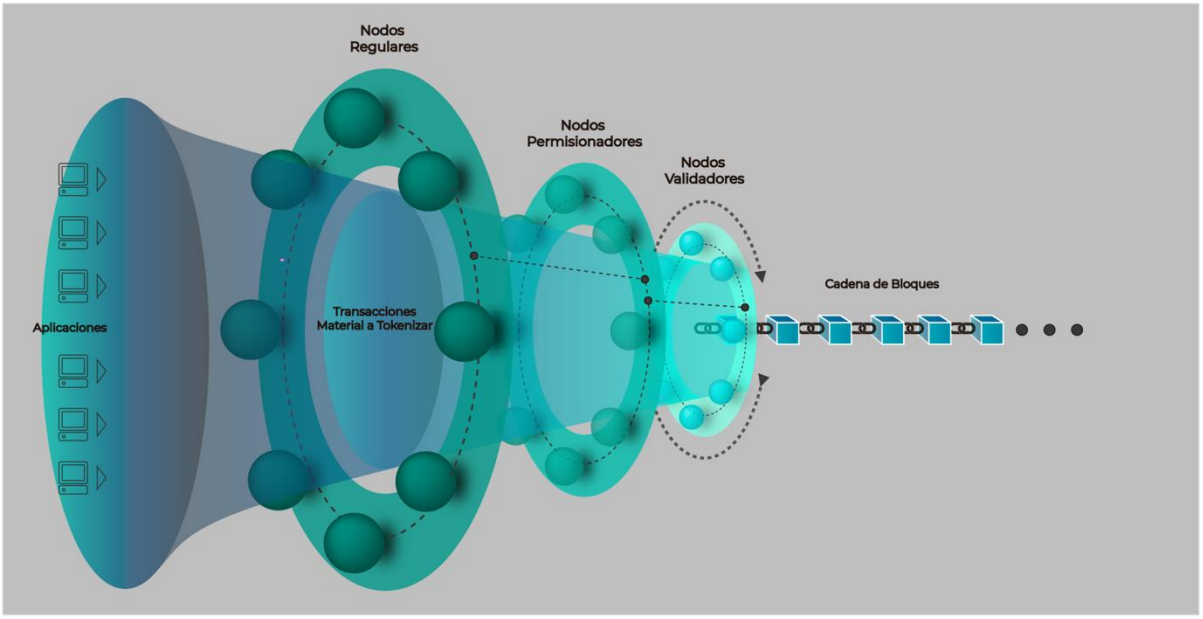
El presente documento se redacta en cumplimiento de lo dispuesto en los estatutos de la ASOCIACIÓN, teniendo en cuenta las diferentes tipologías de nodo que existen y su función dentro de la Red.

En este documento se define cómo se establecen los elementos operativos y de gobierno en la Red T, incluyendo la Política de Permisionado[12], define qué se debe tener en cuenta a la hora de instalar un Nodo Crítico[13] y operarlo por parte del Asociado al instalarlo en la Red, qué cuestiones deben tenerse en cuenta en la gestión de un Nodo Regular y, por último, el funcionamiento del Comité de Emergencia de Nodos Críticos.

[12] Ver glosario para definición de “Permisionado”.

[13] Ver glosario para definición de Nodo Crítico.

2. Descripción de la Arquitectura de la Red tipo Quorum[10] de los socios de Alastria (Red T)



En la red Tipo Quorum ("Red T") existen básicamente tres tipos de nodos, según su función en la red:

Validador (block-maker)	Los nodos validadores ejecutan el algoritmo de consenso, que en el caso de esta Red T es el IBFT.
Permisionador (Bootnode)	Son nodos cuyas direcciones físicas ("enodes") son perfectamente conocidas por toda la red. Los nodos de la red sólo conocen los bootnodes que tengan en su fichero de permisionado. A través de un bootnode, los nodos de la red no pueden conocer más nodos.
Regular (general)	Un nodo que participa replicando la blockchain, aceptando los bloques generados por los validadores y ejecutando las transacciones incluidas en los mismos. También se le permite inyectar transacciones en la red, a partir de fuentes externas al blockchain.

El *software* necesario para todos los nodos[14], su instalación y conexión a la Red T de los socios de Alastria está descrito en las herramientas GitHub[15] y Docker[16] que se han creado en el repositorio público de *software* de ALASTRIA.

[14] La Política de Propiedad Intelectual aplicable a todo el *software* de los Nodos de la Red T existente en los repositorios oficiales viene referenciada en el Anexo IV de los Estatutos Oficiales de Alastria.

[15] https://github.com/alastria/alastria-node

[16] https://hub.docker.com/r/alastria/alastria-node-general.

2.1. Nodo Validador

Los **Nodos Validadores**[17] de la Red T ejecutan el algoritmo de consenso IBFT de Quorum[18] que hace que los nodos vayan de modo consecutivo ejerciendo la labor de propuesta de adición de un nuevo bloque a añadir a la cadena. Dada la criticidad de estos nodos en el buen funcionamiento de la Red se ha determinado que los nodos validadores **realicen exclusivamente la ejecución del algoritmo de consenso** y no se permita su utilización para otras funciones. En concreto, aquel Asociado que opera un Nodo Validador, no podrá usarlo para desplegar contratos, iniciar transacciones o realizar operaciones de lectura de la cadena blockchain: únicamente podrá utilizarlo para ejecutar el algoritmo de consenso.

En otras palabras, los Nodos Validadores no deben tener ningún tipo de conectividad con sistemas empresariales, ejecutar software ajeno al del nodo validador o compartir recursos con otras funciones corporativas. El software[19] que se ejecuta por los Nodos Validadores es el especificado[20] y recomendado por estas políticas técnicas. Los Nodos Validadores se comprometen a no alterar o modificar el software recomendado sin conocimiento del equipo técnico de la Asociación y de los restantes Asociados operadores de nodos críticos. Cualquier modificación del software indicado se hará bajo la exclusiva responsabilidad del gestor del nodo crítico, sin que en ningún caso pueda quedar comprometidos ni el funcionamiento ni la seguridad de la Red.

Los Nodos Validadores solo se podrán conectar a otros Nodos Validadores y a uno o más Nodos Permisionadores. Es decir, los Nodos Validadores se configurarán para que no acepten conexiones de ningún nodo regular, vía el mecanismo de permisionado de Quorum. De esta manera, se limita el número de conexiones de un Nodo Validador con otros Nodos, independiente del tamaño de la red y, de esta forma, se pueden gestionar más fácilmente los requerimientos técnicos para la ejecución del algoritmo de consenso y de las medidas de seguridad a implantar en el Nodo.

2.2. Nodo Permisionador

Un **Nodo Permisionador es un nodo que ejecuta la función de *bootnode* de Quorum**[21], pero que además en la Red tiene otras funciones y restricciones en cuanto a conectividad con otros Nodos.

---

[17] En este documento, usaremos el término “validador”, pero es equivalente a “block-maker” o “constructor” o “minador” en otras referencias.

[18] Quorum está desarrollado por JPMorgan y se puede encontrar en https://www.goquorum.com/.

[19] La Política de Propiedad Intelectual aplicable a todo el software de los nodos Alastria existente en los repositorios oficiales viene referenciada en el Anexo IV de los Estatutos Oficiales de Alastria.

[20] El repositorio oficial está en https://github.com/alastria/alastria-node.

[21] Quorum está desarrollado por JPMorgan y se puede encontrar en https://www.goquorum.com/.

La Lista de Permisionado de cada uno de los Nodos Permisionadores contendrá, además de los Nodos Validadores, la lista de los Nodos Regulares que han sido aceptados en la Red.

De esta manera, los Nodos Permisionadores **se conectarán por un lado con los Nodos Validadores y por el otro con los Nodos Regulares**, aislando a los nodos validadores de la gestión del permisionado y de las conexiones con los nodos regulares.

Las direcciones físicas de los Nodos Permisionadores (similares en concepto a las direcciones IP de Internet) serán públicas y bien conocidas, para que los Nodos Regulares puedan conectarse inicialmente a la Red.

Los beneficios obtenidos con esta configuración son los siguientes:

- Los recursos necesarios para conectividad de Red de los Nodos Validadores se mantienen constantes pudiendo dedicar todos los recursos de las máquinas a la ejecución del algoritmo de consenso IBFT, independientemente del número de Nodos Regulares de la red.
- Los cambios de configuración de los Nodos Validadores se reducen al mínimo necesario, y siempre relacionados con la ejecución del algoritmo de consenso. En concreto, no es necesaria la actualización de la lista de permisionado en estos nodos, aunque cambien los Nodos Regulares. Una reducción de los cambios necesarios en los Nodos Validadores redunda en una mayor estabilidad de estos nodos. Podría ser necesario una actualización del fichero de permisionado en el caso que se añada al consenso IBFT un nuevo validador que se ha permisionado más tarde que la última actualización del fichero de permisionado.
- Al reducirse la exposición de los Nodos Validadores al resto de la Red, es más eficiente la implementación técnica de las políticas de seguridad y bastionado de los Nodos Validadores descritas en el apartado correspondiente de este documento.

2.3. Nodo Regular

Los **Nodos Regulares[22] son los que permiten a los Asociados la participación en la Red, desplegando contratos, iniciando transacciones, ejecutando los Smart Contracts[23] y realizando operaciones de lectura de la cadena de bloques**.

Los Nodos Regulares están conectados a los sistemas empresariales de las entidades que las

[22] En este documento usaremos el término “regular” para referirnos a este tipo de nodo. En otros documentos se le denomina “general”.

[23] Smart Contract - Technical Specification FG DLT D1.1Distributed ledger technology terms and definitions, definición 6.51, y apartado A.7.

operan (Asociados) y no tienen mayores restricciones técnicas que las de las propias políticas internas de cada una de las entidades propietarias y gestoras de los mismos, asociadas a ALASTRIA.

3. Política de Permisionado

3.1. Consideraciones preliminares

Según los criterios de estandarización, la **Red T se clasifica como una red Permisionada[24]/Pública**, en contraste con las redes Públicas/No-permisionadas (Bitcoin[25], Ethereum[26]), y a diferencia también de las redes privadas.

No obstante, en otros ámbitos se usan otras clasificaciones que utilizan criterios similares, pero no idénticos, lo que puede generar algún malentendido en la discusión sobre ciertas características todavía no totalmente definidas de este tipo de redes y que pueden influir en las propiedades de *inclusividad* y en las políticas de uso de redes como la Red T. De hecho, el modelo exacto de Permisionado implementado en la Red tiene implicaciones en el modelo de Identidad Digital Soberana[27] (ID_Alastria), que precisa proporcionar acceso de la persona física al *blockchain*, ya sea directa o indirectamente.

Para aclarar conceptos, a continuación, se exponen algunas de las características e implicaciones más importantes sobre Permisionado.

3.1.1. Permisionado de todos los nodos o de solo algunos nodos

En algunos ámbitos se realiza una distinción entre redes permisionadas y redes públicas, distinción basada en si se requiere el permisionado de todos los nodos de la red o de sólo algunos de ellos.

Se puede considerar que, si se requiere que todos los nodos se permisionen, independientemente de si su actividad es de escritura o lectura, entonces se trata de redes privadas.

---

[24] Es decir, que "requiere autorización para desarrollar una o varias actividades" en la red (sic, ITU (2019), ITU-T Technical Specification, FG DLT D1.1, *Distributed ledger technology terms and definitions,* 1 august 2019, sub 6.42. Conforme a estos estándares Alastria es un "permissioned DLT system" (ITU, ibid., sub. 6.41) donde "se requieren permisos para mantener y operar un nodo"; siendo además público (ibid., 6.49) y por tanto "accesible al público para su uso".

[25] Bitcoin https://bitcon.org/.

[26] Ethereum https://www.ethereum.org/.

[27] Self-Sovereign Identity (Digital). En Technical Report FG DLT D1.3 (DLT Landscape Standardization puede encontrarse una referencia al DID de ID_Alastria.

De igual modo, se puede considerar que una red permisionada-pública es aquella que requiere el permisionado de un subconjunto de los nodos (por ejemplo, los nodos que tienen capacidad de escritura), no requiriendo el permisionado de otros nodos (por ejemplo, los nodos que solo tienen acceso de lectura).

3.1.2. *Inclusividad* de la Red

Con este último enfoque, una red de estas características requiere permisionado solo para los nodos que pueden modificar el *blockchain*, mientras que el estado es completamente público y cualquiera puede acceder en modo lectura y, por lo tanto, auditar la Red. Este punto de libre acceso en lectura NO ocurre en el caso de la Red T de nodos de socios Alastria como se especifica más adelante.

3.1.3. Consideraciones de implementación

Desde el punto de vista técnico, **con la tecnología Quorum derivada de *Ethereum*, no es fácil implementar un Permisionado limitado a los Nodos que modifiquen el estado de la *blockchain***. Actualmente**, en Quorum el Permisionado es a nivel de nodo y es todo-o-nada**, es decir un nodo que participe en la red ya no tiene ninguna limitación de lectura/escritura, siempre que el actor que use ese nodo tenga una cuenta con suficiente gas para iniciar transacciones.

El mecanismo actual de permisionado de Quorum implica que **todos los nodos tienen que estar permisionados aun cuando sólo realicen consultas**, ya que deben replicar la *blockchain* en su disco.

En esta situación, un actor que quiera consultar y que no tenga un nodo permisionado debería acceder a la red a través del nodo de alguna otra entidad que sí cuenta con un nodo ya permisionado. Sería entonces responsabilidad de esta última entidad el control de la actividad transaccional en la red de la entidad "*delegada*".

Esto ya ocurre en redes completamente privadas, donde las entidades participantes en la *blockchain* proporcionan actividades a sus clientes (personas físicas o empresas) sin requerir que éstos tengan nodos en la red. Aunque en la mayor parte de los casos, la entidad cliente no tiene nunca acceso directo a la *blockchain*, y todas las transacciones son iniciadas y firmadas por la entidad que opera o gestiona el nodo.

3.1.4. Modelo de permisionado de Alastria

Volviendo a la clasificación elaborada en diversos organismos de normalización (UNE, W3C,

ISO…) como, por ejemplo, ITU-T FGDLT, puede definirse la Red T como una red permisionada-pública. El caso de ALASTRIA se opta por requerir que todos los nodos estén permisionados[28].

Las implicaciones derivadas de esta consideración son las que siguen:

1. No pueden existir nodos "anónimos" que permiten acceso a actores anónimos en escritura y lectura.
2. Si una entidad permite acceso a la *blockchain* (tanto lectura como escritura) a otras entidades a través del nodo que opera en la Red, **ésta (la entidad que opera el nodo) es responsable** de todas las acciones que se realizan a través de su nodo en la *blockchain*, con las implicaciones que de ello se deriven.

Con la versión actual de Quorum, el permisionado es a nivel de nodo y no a nivel de entidad. Es decir, **una entidad puede tener más de un nodo siendo necesario permisionar cada uno de ellos de manera independiente**. Ya está previsto evolucionar en el futuro a un sistema más sofisticado de permisionado, basado en Smart Contracts que automaticen el modelo actual y que permita gestionar de manera más eficiente el permisionado.

El proceso de permisionado actual en la Red T consta de dos partes manuales que irán evolucionando hacia procesos automáticos basados en *Smart Contracts*: una primera parte técnica y una segunda administrativa. Con la primera, la parte técnica, el Asociado debe realizar una petición a través de GitHub, formalizando una solicitud de actualización de ficheros[29] para incorporar los datos del Nodo dentro de los ficheros de declaración de Nodos. Estos ficheros están ubicados bajo el repositorio *alastria/alastria-node* y son los tres ficheros siguientes:

- DIRECTORY_REGULAR.md
- data/regular-nodes.json
- data/constellation-nodes.json (este fichero es necesario únicamente si hemos activado Constellation, el mecanismo de transacciones privadas de Quorum en nuestro nodo).

Una vez que el Asociado realiza esta petición en la herramienta GitHub, de modo automático le llega al Equipo *Core* un aviso para realizar una verificación técnica en la que se comprobará que los ficheros han sido correctamente modificados, que el Nodo se visualiza correctamente y está adecuadamente instalado.

Además debe realizarse una petición via formulario https://portal.r2docuo.com/alastria/forms/noderequest donde se solicita el permisionado

[28] V. supra, nota 21.

[29] Esta solicitud de actualización es denominada "Pull Request" en GitHub.

formal a la Asociación. Si esto es todo correcto a nivel técnico, se procede a esta segunda revisión, la administrativa, para comprobar que el Asociado cumple los requisitos previos exigidos (ser socio de ALASTRIA sin ningún tipo de problema administrativo o legal que impida al nodo ser incorporado). En caso de que todo sea correcto, el Equipo *Core* procede a incorporar los cambios de ficheros al sistema y el Nodo acaba siendo visible a la Red en cuanto uno de los Nodos Permisionadores (*bootnode)* actualiza los ficheros de configuración.

En los próximos meses está previsto automatizar esta funcionalidad usando Smart Contracts[30], para así permitir una gestión descentralizada de la función de Permisionado, basándose en una petición de credenciales de los Nodos que solicitan su inclusión y una autorización automática de la Red. Los criterios que sean establecidos para llevar a cabo esa automatización, una vez aprobados, serán plasmados en una nueva versión de este documento.

3.1.5. Modelo de Des-Permisionado de la Red

Puede ser necesario realizar un des-permisionado, inhabilitación, desautorización, revocación o extinción de la validez de la autorización o permiso del Nodo que ha sido incluido en la Red T. Las causas pueden ser voluntarias e involuntarias. Las primeras causan efecto a petición del Asociado gestor del nodo en cuestión (por ejemplo, el Asociado se da de baja en la ASOCIACIÓN) y las segundas tienen efecto a instancia de la propia ASOCIACIÓN (por causa del incumplimiento de las obligaciones inherentes a la condición de Asociado gestor del Nodo, bien a nivel administrativo (como un impago de una cuota) o bien a nivel técnico (como puede ser el uso inadecuado de la Red o por incumplimiento de las normas y políticas de uso de la Red. En estos casos, el Equipo *Core* procederá a modificar los tres ficheros indicados antes eliminando las referencias al nodo al que se ha solicitado des-permisionar, y finalmente, se reiniciarán los *bootnodes* tras actualizar sus ficheros de configuración.

En el caso de que un Asociado quiera des-permisionar un nodo debe notificarlo con al menos, 15 días hábiles de antelación a la fecha de su efectividad.

Cuando se desarrolle la gestión automática del Permisionado y Des-permisionado basada en *Smart Contracts,* este proceso quedará automatizado cumpliendo con el objetivo de máxima descentralización del gobierno de Red. Como se ha indicado más arriba, los criterios que sean establecidos para llevar a cabo esa automatización, una vez aprobados, serán plasmados en una nueva versión de este documento.

[30] Contrato inteligente consistente en un “programa escrito en el sistema de registro distribuido que codifica las reglas para tipos específicos de transacciones de un modo que puede ser validado y ejecutado bajo condiciones específicas” (ITU (2019), FG DLT D1.1, sub 6.51.

4. Políticas Técnicas de Operación y Recomendaciones ligadas al Permisionado

4.1. Política técnica de operación para Nodos Permisionadores

Los Asociados deben cumplir con la "Política de Permisionado" siguiente:

- **Todo Nodo que quiera tener acceso a la Red debe estar permisionado** en la Red T (por diseño técnico) aunque puede que en futuros tipos de redes se pueda permitir acceso en modo lectura a nodos no permisionados como en otras redes (ej. LacChain).
- La solicitud de permisionado se realiza a través de la herramienta GitHub mediante un Pull Request y un formulario online. Esta solicitud es evaluada, a nivel técnico, por el Equipo *Core* de soporte de la plataforma y, a nivel administrativo, por el equipo de Motor de Gestión, tras lo cual se realiza la autorización o denegación de uso de la red. Estas solicitudes quedan registradas en el control de versiones existente en dicha herramienta.
- La función crítica de los Nodos Permisionadores es no permitir conexión unilateral de nodos no identificados y autorizados en la lista oficial mantenida por ALASTRIA.
- Los Nodos Permisionadores deben protegerse de las conexiones externas mediante las normas de Bastionado[31].
- Los Asociados que gestionen Nodos Permisionadores **deben necesariamente cumplir las Condiciones establecidas en el Documento "Condiciones de Operación de la Red T por parte de Nodos Críticos"[32]**.
- Se recomienda utilizar las versiones de *software* del Nodo Permisionador existente especificadas en el repositorio oficial de ALASTRIA y mantener actualizados sus nodos con las últimas versiones.
- Por motivos de seguridad no deben ejecutarse otros procesos en la misma máquina donde se esté ejecutando el *software* del Nodo Permisionador, entendiendo por máquina la parte virtual de una máquina física, si la hubiese, de modo que esté absolutamente compartimentado el uso de dicho espacio de máquina entre el Nodo y otros procesos del Asociado Gestor del Nodo Validador.
- Se recomienda no modificar de modo particular el *software* del Nodo Validador, aceptándolo en todos sus términos y sin propósito de cambios con el compromiso de asumir las actualizaciones en todos sus términos. En su caso, la modificación habrá de llevarse a cabo usando los mecanismos establecidos a través del Pull Request en GitHub.
- Asegurar previamente a la solicitud de inclusión del Nodo Validador que la herramienta de visualización de la Red "*netstats*"[33], ve el nuevo nodo y que su actividad se refleja

[31] Por Bastionado se entienden las instrucciones y acciones técnicas que se deben tomar para la protección física y lógica de la seguridad del nodo.

[32] https://portal.r2docuo.com/alastria/document?L62DE71FFF

[33] https://netstats.telsius.alastria.io/

adecuadamente.

- En caso de que el Asociado operador del Nodo Validador quiera dar de baja su nodo de la función de permisionado, debe comunicarlo por el procedimiento establecido de Pull Request en GitHub con al menos 15 días hábiles de antelación que permitan evaluar si es necesario activar algún plan de contingencia ante una posible indisponibilidad de la Red.

5. Políticas Técnicas de Operación y Recomendaciones para Nodos Críticos (Validadores o Permisionadores)

5.1. Requisitos de Resiliencia

Los requisitos de Resiliencia aplican principalmente a los Nodos Críticos, por su criticidad e importancia en el buen funcionamiento de la Red.

5.2. Seguridad física de Nodos Críticos[34]

Los Nodos Validadores **realizan exclusivamente la ejecución del algoritmo de consenso**, quedando prohibida su utilización para otras funciones. Esta exclusividad se aplica a la porción de máquina donde se está ejecutando el *software* del nodo en cuestión, debiendo quedar perfectamente compartimentado.

Los Nodos Críticos no deben tener ningún tipo de conectividad con sistemas empresariales, ni ejecutar *software* ajeno al del Nodo Crítico o compartir recursos con otras funciones corporativas del Asociado. El *software* recomendado para su utilización por los nodos críticos es el especificado por estas Políticas Técnicas de ALASTRIA.

Dadas sus características técnicas, los Nodos Críticos han de estar alojados en Entornos Virtualizados, bien dentro de los sistemas físicos del Asociado operador del nodo en cuestión (CPDs[35]), o en sistemas ubicados en la Nube y administrados únicamente por el Asociado.

En función de la ubicación, se deberán tomar ciertas consideraciones adicionales sobre la seguridad del Nodo Crítico para garantizar su integridad física, así como establecer un control de acceso monitorizable y un sistema de aislamiento suficiente para evitar su manipulación no deseada:

- **Nodos Críticos ubicados en CPD:** el CPD en sí deberá contar con acceso restringido, esto es, habrá de estar ubicado en una zona controlada y monitorizada bien dentro de

[34] Se está trabajando para asegurar un alineamiento total con la norma ISO 27001.

[35] Centro de Procesamiento de Datos.

las instalaciones u oficinas del Asociado o bien subcontratando el servicio siempre que cumpla con las siguientes condiciones de seguridad y transparencia con ALASTRIA, con algún tipo de sistema de control acceso automatizado y centralizado que, además, tenga definida una lista de usuarios y/o administradores autorizados para acceder al CPD.

La monitorización deberá registrar los accesos al CPD, así como los intentos de acceso no autorizados. Además, los registros deberán ser accesibles al personal acreditado por ALASTRIA para la realización de las tareas de auditoría que sean necesarias.

Por otra parte, el acceso físico en sí a la plataforma (servidor) que ejecuta el Sistema Operativo (virtualizado o no) deberá estar a su vez limitado, su acceso deberá estar aislado y, aún más, restringido al personal administrador a cargo de las actividades de administración, soporte y mantenimiento del Nodo Crítico en la Red.

Es recomendable que la plataforma donde se aloje el Nodo Crítico esté separada físicamente de los otros sistemas IT del Asociado o, al menos, sea dedicada exclusivamente a dar cobertura a la actividad del Nodo Crítico instalado en la Red, con el fin de prevenir su manipulación accidental o intencional por parte de personal ajeno a las actividades de administración, soporte y mantenimiento del Nodo Crítico.

- **Nodos Críticos ubicados en la Nube**: Los Nodos Críticos que se encuentren ubicados en la Nube de alguno de los proveedores de servicios (AWS, Google, MS..), aunque físicamente estén ubicados dentro de las instalaciones físicas (CPD) de un tercero, deberán contar igualmente con las medidas de seguridad físicas que garanticen un acceso restringido, monitorización de accesos y el aislamiento suficiente para evitar manipulaciones no deseables del Nodo Crítico.

  Para asegurar que el Nodo Crítico cuenta con las medidas de seguridad física suficientes, será necesario que los proveedores de servicio indicados dispongan también de políticas de seguridad que garanticen la protección física del nodo crítico de la misma forma que para los nodos críticos ubicados en un CPD en las instalaciones u oficinas del Asociado propietario y operador del Nodo Crítico.

  Además, cada Asociado operador de Nodo Crítico en la Red deberá monitorizar, verificar o comprobar periódicamente que las políticas de seguridad de acceso físico de los proveedores se encuentren actualizadas, que los controles que realizan los proveedores a sus sistemas físicos sean suficientes para asegurar el apetito de riesgo para los Nodos Críticos, y que las auditorías y certificaciones de cumplimiento sean realizadas satisfactoriamente. De esta manera se podrá verificar una correcta gestión de la seguridad física de los CPDs de los proveedores de servicios en la Nube.

5.3. Bastionado

Dado el tipo de sistema operativo ejecutado por los Nodos Críticos (Linux de 64bits), se deberá realizar el Bastionado de estos sistemas siguiendo la Guía de Bastionado. Es obligatorio usar Ubuntu 16.04[36], y muy recomendable usar *Red Hat* como sistema operativo en los Nodos Críticos[37].

La siguiente lista de comprobación[38] recoge los principales aspectos a tener en cuenta en un Bastionado (principalmente, en propias instalaciones) basado en RedHat pero se puede adaptar fácilmente a:

	Acción	CIS
	Preparación y Seguridad Física	
1	Si el equipo es una instalación nueva, se debe proteger del tráfico de red hostil hasta que el sistema operativo sea instalado y bastionado.	
2	Definir una contraseña para el BIOS/firmware.	
3	Configurar el orden de arranque de los dispositivos para evitar el inicio desde dispositivos externos.	
4	Usar la última versión posible de RHEL (si se usa RedHat como Sistema Operativo) o usar la última versión de Software de Ubuntu, CentOs, etc. teniendo en cuenta que los scripts de instalación creados han sido pensados para Ubuntu 16.04	1.7
	Configuración del Sistema de Ficheros	
5	Crear una partición separada con las opciones nodev, nosuid, and noexec establecidas para /tmp.	1.1.1-.4
6	Crear particiones separadas para /var, /var/log, /var/log/audit y /home.	1.1.{5,7,8,9}
7	Enlazar el montaje de /var/tmp a /tmp.	1.1.6
8	Establecer la opción nodev a /home.	1.1.10
9	Establecer las opciones nodev, nosuid, and noexec en /dev/shm.	1.1.14-.16
10	Configurar la opción “sticky bit” en todos los directorios escribibles.	1.1.17
	Actualización del Sistema	
11	Registrar el sistema en Red Hat Satellite Server para poder recibir actualizaciones y parches o activar actualizaciones automáticas en los otros sistemas operativos diferentes de RedHat	1.2.1
12	Instalar la clave GPG de Red Hat y habilitar el servicio gpgcheck en caso de usar Red Hat	1.2.2-.3
	Configuración Segura de Arranque	
13	Establecer Root como propietario de user/group y dar permisos de	1.5.1-.2

[36] Decisión Comisión de Resiliencia de 19feb2019.

[37] En caso de elegir *Red Hat* es importante señalar que el procedimiento de instalación automático existente en el repositorio alastria/alastria-node no es válido y será necesario realizar la instalación del nodo de modo manual.

[38] Esta lista de comprobación ha sido facilitada por la Comisión de Resiliencia en 2018.

	lectura y escritura únicamente a Root en /boot/grub2/grub.cfg.	
14	Establecer las password del boot loader.	1.5.3
15	Eliminar el sistema X Window.	3.2
16	Deshabilitar el servidor X Font.	
	Bastionado de Procesos	
17	Restringir core dumps.	1.6.1
18	Habilitar el Randomized Virtual Memory Region Placement.	1.6.2
	Bastionado del Sistema Operativo	
19	Eliminar servicios legacy (e.g., telnet-server; rsh, rlogin, rcp; ypserv, ypbind; tftp, tftp-server; talk, talk-server)	2.1.{1,3-10}
20	Deshabilitar cualquier servicio lanzado por xinetd o inetd que no vayan a ser utilizados.	
21	Eliminar xinetd, si es posible.	2.1.11
22	Eliminar otros servicios legacy (e.g., chargen-dgram, chargen-stream, daytime-dgram, daytime-stream, echo-dgram, echo-stream, tcpmux-server)	2.1.{12-18}
23	Deshabilitar servicios por defecto que no vayan a ser utilizados (e.g., FTP, DNS, LDAP, SMB, DHCP, NFS, SNMP, etc.)	
24	Habilitar Daemon umask	3.1
	Configuración de la Seguridad de red y de Cortafuegos	
25	Limitar conexiones a los servicios habilitados a aquellos usuarios autorizados utilizando firewalls u otras tecnologías de control de acceso.	4.7
26	Deshabilitar el IP forwarding.	4.1.1
27	Deshabilitar el envío de paquetes de redirección.	4.1.2
28	Deshabilitar la aceptación de paquetes con la ruta de redirección establecida en origen.	4.2.1
29	Deshabilitar la aceptación de paquetes de redirección ICMP.	4.2.2
30	Ignorar paquetes de peticiones Broadcast.	4.2.5
31	Habilitar la protección contras mensajes Bad error.	4.2.6
32	Habilitar las cookies TCP/SYN.	4.2.8
	Gestión remota usando SSH	
33	Establecer el protocolo SSH a 2.	6.2.1
34	Establecer el nivel de logs de SSH a INFO.	6.2.2
35	Deshabilitar el login de Root por SSH.	6.2.8
36	Establecer SSH PermitEmptyPasswords a No.	6.2.9
	Integridad del sistema y detección de intrusiones	
37	Instalar y configurar AIDE.	1.3.1-.2
38	Configurar SELinux.	1.4.1-.6
39	Instalar y configurar OSSec HIDS.	
	Registro de eventos	
40	Configurar Network Time Protocol (NTP). Establecer el huso horario español (GMT +1) basado en el servidor hora.roa.es	3.6
41	Habilitar la auditoría del sistema (auditd).	5.2
42	Instalar y configurar rsyslog.	5.1.1-.4
43	Todos los accesos Root deben ser auditados.	

44	Configurar el envío de logs a un sistema externo (e.g. Splunk).	5.1.5
	Acceso a directorios y ficheros	
45	Habilitar y probar los chequeos de integridad sobre cuentas del sistema, membresía a grupos y permisos asociados.	
	Configuración PAM	
46	Asegurar que los ficheros de configuración de PAM, /etc/pam.d/* son seguros.	6.3
47	Establecer el algoritmo de hasheado de passwords a SHA-512.	6.3.1
48	Establecer medidas de robustez en la creación de passwords.	6.3.2
49	Restringir al acceso de Root únicamente a la consola del sistema.	6.4
	Paneles de Advertencia	
50	Establecer un banner de advertencia en los accesos físicos a la consola del sistema.	6.2.14, 8.1
51	Establecer un banner de advertencia en los accesos remotos a la consola del sistema	8.3
	Consideraciones sobre Antivirus	
52	Instalar y habilitar un software Anti-Virus.	
53	Configurar la actualización diaria de firmas del Anti-Virus.	

5.4. Integridad

La integridad y mantenimiento o continuidad de la funcionalidad del Nodo Crítico deberá estar protegida y asegurada teniendo en consideración los siguientes puntos:

- **Número mínimo de Nodos Críticos activos en la red:** para que la Red T pueda operar correctamente, garantizando una actividad óptima y segura, es necesario que se encuentren activos al menos **5 Nodos Validadores y 2 Permisionadores**.

- **Número óptimo de Nodos Críticos activos en la Red:** en la Red, el número óptimo de Nodos Críticos sería de veintiún (21) Nodos Validadores activos, 6 Nodos Validadores en *stand-by* y 8 Nodos Permisionadores.

- **Versionado y compatibilidad del *software*:** el *software* que se ejecuta en los Nodos Críticos, tanto el *software* propio de la Red T como el resto del *software* que use la Red o sea necesario para la operación segura y correcta del nodo en cuestión **deberá estar actualizado a la última versión**[39]. Las actualizaciones deberán utilizar repositorios de *software* certificados por sus propios desarrolladores, siguiendo los respectivos controles de integridad (verificación HASH, certificados digitales, etc.).

- **Monitorización del Nodo Crítico:** El funcionamiento del Nodo Crítico, así como el estado de su integridad y seguridad, deberá estar continuamente monitorizado y **bajo**

[39] La última versión del software a disposición de los socios de Alastria se encuentra en https://github.com/alastria/ y se instala por cada socio por su propia cuenta y riesgo.

control de un equipo administrador dedicado que haya sido notificado a la Asociación. El acceso local de los Nodos Críticos deberá ser habilitado a nivel de Sistema Operativo, así como de *software* de seguridad y/o de gestión remota.

- **Inclusión y decomisado de nodos:** Será necesario que el alta y la baja de los Nodos Críticos sea **notificada por el Asociado con antelación de dos (2) semanas y validada por personal acreditado por el CONSORCIO**. Las actividades de inclusión o decomisado de los Nodos Críticos deberá ser planificada, controlada y probada al finalizar, en ventanas de mantenimiento que garanticen la no afectación de la Red. Dichas actividades deberán ser documentadas, registrando cualquier tipo de incidencia, siguiendo los protocolos y actuaciones pertinentes de marcha atrás en caso de fallo o incidente grave que pueda afectar al resto de la Red.
- **Parada ordenada de Red (apagado de red):** Cuando por causas organizativas o de fuerza mayor, se decida que la Red debe pararse (apagarse), se procederá a la notificación a los Asociados gestores de Nodos en dicha Red, solicitando su aprobación mediante una nota firmada, indicándoles el procedimiento a seguir para guardar una copia de la cadena de bloques existente que puedan guardar como respaldo.

5.5. Disponibilidad

Para garantizar niveles óptimos de disponibilidad de la Red y su correcto funcionamiento, será necesario que los Nodos Críticos tengan habilitados los sistemas de monitorización correspondientes de cada Asociado y, asimismo, los mecanismos de respaldo y procedimientos de recuperación efectivos.

- **Monitorización**: como se ha detallado en el apartado anterior, además de monitorizar la integridad y seguridad del Nodo, éste deberá contar con mecanismos de monitorización que permitan verificar la correcta operación de este, tanto a nivel de Sistema Operativo y *hardware*, como del *software* propio de la Red.

  El *software* deberá ejecutar su protocolo de monitorización, verificando que el puerto de monitorización (TCP 8443) se encuentre abierto y a disposición de la Red T Para protección adicional, este puerto debe estar restringido a una o varias IPs que se establecerán por el Comité de Nodos Críticos, y que estarán en poder del Equipo *Core*.

  Además, se deberá contar con un mecanismo de alerta y monitoreo de Red en caso de ataques de denegación de servicio (DoS[40]) que puedan afectar la disponibilidad de la actividad o del acceso del Nodo Crítico a la Red T.

[40] Denial of Service.

- **Respaldo**: Aunque la necesidad de un respaldo tradicional de los Nodos Críticos no es necesaria *per se* dado que los datos de la *blockchain* están respaldados *de facto* en todos y cada uno de los demás Nodos de la Red, es recomendable que cada Asociado gestor de un Nodo cuente con algún mecanismo de respaldo del mismo tanto en el *software* como en los datos (copia de seguridad, snapshot[41], etc.) que garantice la total recuperación de la información necesaria para la reactivación del Nodo Crítico, dentro del tiempo máximo de indisponibilidad, después de un fallo o daño (intencional o accidental) del mismo, garantizando de esta forma que no se pierda información o datos importantes. Lo anterior es especialmente crítico para asegurar que no es necesario sincronizar la cadena de bloques desde su inicio.

  La gestión de los mecanismos de respaldo es una responsabilidad del Asociado operador del Nodo en cuestión, en caso de que el Nodo se aloje dentro del CPD del mismo. En caso de estar alojado en un sistema virtualizado en la Nube, el Asociado operador del Nodo es responsable de verificar que el proveedor disponga de las opciones de respaldo necesarias para cubrir con las necesidades de disponibilidad del Nodo Crítico.

- **Tiempos de recuperación:** el Asociado operador del Nodo Crítico deberá contar con un plan de recuperación y tiempos de recuperación RTO/RPO bien definidos, de forma tal que en un fallo que afecte a uno de los Nodos Validadores, se logre recuperar y reactivar al 100% el funcionamiento de dicho nodo dentro de los tiempos definidos afectando lo mínimo posible el funcionamiento de la Red. Este tiempo dependerá de si el nodo a recuperar es el único con el fallo y no afecta a la Red, o bien si es el Nodo que puede hacer que la Red falle en su conjunto.

  El plan de recuperación referido habrá de contar con procedimientos técnicos detallados dirigidos a lograr la recuperación y reactivación del Nodo Crítico afectado, así como la definición de las responsabilidades del personal del Asociado encargado de llevar a cabo las tareas de recuperación.

5.6. Privacidad

Para que los Nodos Críticos cuenten con el nivel de privacidad necesario para cumplir con las políticas de privacidad y el tratamiento de la información sensible[42], manteniendo la operación correcta de la red, será necesario que se disponga de lo siguiente:

[41] Copia (imagen) del software del nodo en un momento concreto del tiempo.

[42] El uso de la Red debe ser respetuoso con el Reglamento General de Protección de Datos y demás normas aplicables sobre el particular que se hallen en vigor.

- **Conexión a Internet:** con una IP pública que permita la visibilidad de la Red y todos sus Nodos, verificando que los Nodos Críticos ejecuten las funcionalidades que le corresponden en los puertos dedicados a ella según los requerimientos técnicos. Dado que la visibilidad del Nodo en cuestión será al internet público, deberán tomarse las precauciones necesarias, utilizando las metodologías, mecanismos y tecnologías necesarias para evitar enumeración de los servicios IP, procesos u otra información sensible diferente de aquella necesaria para su conexión con la Red T.

- **Cifrado de datos**: Tanto los datos en tránsito como los datos almacenados en los Nodos Críticos deberán estar cifrados utilizando algoritmos de cifrado fuertes que no presenten vulnerabilidades conocidas y que sean compatibles con las tecnologías y *software* necesarios para ejecutar las actividades relacionadas con la Red T sin afectar al rendimiento de esta.

  Los datos en tránsito incluyen el propio tráfico de datos de la Red T, el tráfico generado por comunicaciones de *softwares* de gestión, seguridad o respaldo que se ejecuten en el Nodo y comunicaciones de accesos remoto desde redes (redes de los Asociados) internas o redes públicas (Internet o terceros).

- **Comunicación remota**: en caso de que se necesite realizar conexiones desde redes o equipos remotos al Nodo Validador para el intercambio de datos con información sensible, monitorización de datos del sistema, control y acceso remoto, etc., se deberá utilizar una conexión de red privada virtual VPN entre el Nodo Validador y la red o sistema remoto.

  La VPN deberá ser gestionada y mantenida por personal acreditado por Asociado operador del Nodo, teniendo un riguroso control de usuarios que puedan acceder a ella mediante listas de usuarios, administradores y sistemas permitidos y un control de acceso eficaz que utilice dicha lista de usuarios.

5.7. Requisitos organizativos

Será necesario que el Asociado que administre u opere un Nodo Crítico en sus instalaciones cumpla con un proceso de certificación independiente con el cual se verifique el cumplimiento de cada uno de los elementos expuestos en ese documento y que se pueda aportar a los demás miembros del Consorcio.

En caso de que el Asociado disponga de un certificado SAS70, ISAE3402 o SSAE16 en vigor, o esté catalogada como una infraestructura crítica de acuerdo con la Ley 8/2011, se eximirá de cumplir con el proceso de certificación independiente, siempre que acredite a la ASOCIACIÓN el cumplimiento de lo indicado en este párrafo.

6. Políticas Técnicas de Operación y Recomendaciones para Nodos Regulares

6.1. Política técnica de operación para Nodos Regulares

El Asociado gestor de un Nodo Regular debe cumplir con la "Política Técnica para Nodos Regulares" siguiente:

- No permisionar ni permitir conectarse a otros Nodos no autorizados en la lista oficial mantenida por la ASOCIACIÓN.
- Mantener actualizada de modo permanente una lista de elementos permitidos a conectarse al Nodo desde accesos de elementos externos, en un fichero denominado "whitelist" ubicado dentro del componente *Alastria Open Access*[43] y que permite mantener la seguridad general de la Red.
- Utilizar las versiones especificadas en el repositorio oficial[44] y mantener actualizados sus correspondientes Nodos Regulares.
- Realizar la instalación de su Nodo bajo el directorio de instalación especificado.
- No modificar el *software* del Nodo de la Red. En caso de necesitar una modificación, esta deberá realizarse usando los métodos establecidos en GitHub[45].
- Asegurar que la herramienta de visualización de la Red "*netstats*"[46] visualiza adecuadamente su Nodo y que su actividad se refleja adecuadamente, habilitando los puertos IP[47] necesarios en la red de acceso para proporcionar dicha información de estadísticas de uso.
- Limitar la carga de la Red dentro de los límites establecidos en cada momento dentro de la política técnica en vigor, inicialmente fijada en 25.000 transacciones al día. Y en caso de necesitar superar este límite, solicitar y obtener una autorización por parte del Equipo Core.
- Los Asociados que gestionen Nodos Regulares **deben necesariamente cumplir las condiciones establecidas en el Documento de Condiciones de Uso de la Red por parte de Nodos Regulares**[48].
- Comunicar inmediatamente al equipo técnico de Alastria y al Comité de Emergencia de Nodos Críticos[49] las posibles vulnerabilidades que se pudieran encontrar en la Red y en su caso, no explotarlas en beneficio propio.

[43] https://github.com/alastria/alastria-access-point
[44] https://github.com/alastria/alastria-node
[45] https://github.com
[46] https://netstats.telsius.alastria.io/
[47] Los puertos necesarios se describen en https://github.com/alastria/alastria-node/README.md
[48] Este documento de Condiciones de Uso de la Red por parte de Nodos Regulares está disponible en https://portal.r2docuo.com/alastria/document?LAA4CC6A0B

Se recomienda además que se active el componente "Monitor"[50], protegido por firewall y accesible únicamente desde una IP concreta gestionada por el Equipo Core y que, activada por el Comité de Emergencia de Nodos Críticos sirve para permitir acciones de emergencia, tales como un reinicio del nodo en caso de mal funcionamiento y no atención por parte del Asociado gestor del mismo.

7. Comité de Emergencia de Nodos Críticos

7.1. Objetivo

El objetivo de este Comité como parte de la gestión de incidencias es actuar como línea de defensa, tal y cómo se ha solicitado por la Comisión de Resiliencia en caso de mal funcionamiento o ataques a la Red.

7.2. Constituyentes

Será parte un responsable designado de cada uno de los Asociados que han instalado un Nodo Crítico en la Red, un miembro de la Junta Directiva de Alastria y un miembro del equipo Motor de Gestión designado por la Dirección General de Alastria.

7.3. Función

El Comité se reunirá presencial o remotamente cuando se convoque a petición de cualquiera de sus miembros. Su función principal es evaluar una posible amenaza al funcionamiento de la Red, bien por malfuncionamiento de los Nodos Críticos o bien por detección de un ataque contra la Red.

Entre sus posibles acciones puede estar el realizar una intervención remota sobre un Nodo Crítico de la Red (a través de la herramienta Monitor) para ejecutar un reinicio o un apagado de un Nodo o la de solicitar un des-permisionado de urgencia de un Nodo.

[50] Este componente se puede instalar desde https://github.com/alastria/monitor o bien en el proceso estándar de instalación del nodo contestando "S" a la pregunta correspondiente.

8. Condiciones de Operación y Uso de la Red por parte de Nodos Críticos y Regulares

8.1. Condiciones de Operación de la Red por parte de los Nodos Críticos

Documento en cuya virtud el ASOCIADO declara expresamente conocer y se compromete al cumplimiento de la totalidad de las normas internas de la ASOCIACIÓN (Estatutos, sus anexos, políticas de gobierno, códigos de conducta, especificaciones técnicas y otros acuerdos operativos entre miembros y éstos y la ASOCIACIÓN) y a desplegar sus mejores esfuerzos conforme a los estándares profesionales, para la operación y mantenimiento de un Nodo Crítico (bien permisionador o validador).

Este documento constituye un compromiso para con la ASOCIACIÓN y para con los demás Asociados.

8.2. Condiciones de Uso de la Red por parte de los Nodos Regulares

Documento en cuya virtud el ASOCIADO declara expresamente conocer y se compromete al cumplimiento de la totalidad de las normas internas de la ASOCIACIÓN (Estatutos, sus anexos, políticas de gobierno, códigos de conducta, especificaciones técnicas y otros acuerdos operativos entre miembros y éstos y la ASOCIACIÓN) y a desplegar sus mejores esfuerzos conforme a los estándares profesionales, para la operación y mantenimiento de un Nodo Regular.

Este documento constituye un documento de buen uso de la red para con los demás Asociados.