ITUPublications
Recomendaciones

Unión Internacional de Telecomunicaciones
Sector de la Normalización

Recomendación

UIT-T X.1411 (03/2023)

SERIE X: Redes de datos, comunicaciones de sistemas abiertos y seguridad

Aplicaciones y servicios con seguridad (2) – Seguridad en la tecnología de libro mayor distribuido (DLT)

Directrices sobre seguridad de la cadena de bloques como servicio (BaaS)

RECOMENDACIONES UIT-T DE LA SERIE X

Redes de datos, comunicaciones de sistemas abiertos y seguridad

REDES PÚBLICAS DE DATOS	X.1-X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.200-X.299
INTERFUNCIONAMIENTO ENTRE REDES	X.300-X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400-X.499
DIRECTORIO	X.500-X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	X.600-X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700-X.799
SEGURIDAD	X.800-X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.850-X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900-X.999
SEGURIDAD DE LA INFORMACIÓN Y DE LAS REDES	X.1000-X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD (1)	X.1100-X.1199
SEGURIDAD EN EL CIBERESPACIO	X.1200-X.1299
APLICACIONES Y SERVICIOS CON SEGURIDAD (2)	X.1300-X.1499
Comunicaciones de emergencia	X.1300-X.1309
Seguridad en las redes de sensores ubicuos	X.1310-X.1319
Seguridad en redes eléctricas inteligentes	X.1330-X.1339
Correo certificado	X.1340-X.1349
Seguridad en la Internet de las cosas (IoT)	X.1350-X.1369
Seguridad en los sistemas de transporte inteligentes (STI)	X.1370-X.1399
Seguridad en la tecnología de libro mayor distribuido (DLT)	**X.1400-X.1429**
Seguridad en las aplicaciones (2)	X.1450-X.1459
Seguridad en la web (2)	X.1470-X.1489
INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD	X.1500-X.1599
SEGURIDAD DE LA COMPUTACIÓN EN NUBE	X.1600-X.1699
COMUNICACIÓN CUÁNTICA	X.1700-X.1729
SEGURIDAD DE LOS DATOS	X.1750-X.1799
SEGURIDAD EN LAS REDES IMT-2020	X.1800-X.1819

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T X.1411

Directrices sobre seguridad de la cadena de bloques como servicio (BaaS)

Resumen

La Recomendación UIT-T X.1411 ofrece directrices genéricas de seguridad para la cadena de bloques como servicio (BaaS). En primer lugar, se analizan las amenazas de seguridad y las vulnerabilidades de la BaaS y, a continuación, se proporcionan las medidas de seguridad para la misma. La Recomendación también aborda los requisitos de seguridad y proporciona directrices para todas las actividades de construcción, funcionamiento y uso de la BaaS.

La cadena de bloques como servicio (BaaS) se ha convertido en la corriente principal en el desarrollo de la cadena de bloques debido a sus prometedoras capacidades y al amplio apoyo que ha recibido de la industria, especialmente de los principales proveedores en la nube. La BaaS proporciona el servicio y los recursos fundamentales para las aplicaciones de la cadena de bloques; sin embargo, se enfrenta a retos de seguridad derivados tanto de las tecnologías básicas de la cadena de bloques como de las plataformas en la nube. Por lo tanto, la orientación sobre la seguridad de BaaS es una necesidad y reviste gran importancia.

Historia[*]

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único
1.0	UIT-T X.1411	03-03-2023	17	11.1002/1000/15110

Palabras clave

Cadena de bloques como servicio, entorno de computación en la nube, protocolo de consenso, contrato inteligente, seguridad.

[*] Para acceder a la Recomendación, sírvase digitar el URL https://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación.

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no se pronuncia en lo que respecta a la existencia, validez o aplicabilidad de los derechos de propiedad intelectual reclamados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patentes/derechos de autor de *software*, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar las correspondientes bases de datos del UIT-T disponibles en el sitio web del UIT-T en http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Recomendación UIT-T X.1411

Directrices sobre seguridad de la cadena de bloques como servicio (BaaS)

1 Cometido

En esta Recomendación se especifican las directrices de seguridad para la cadena de bloques como servicio (BaaS). Describe las definiciones, las estructura, las amenazas y vulnerabilidades de seguridad y las medidas para la cadena de bloques como servicio. La seguridad de las aplicaciones de BaaS creadas a partir de la misma recae fuera del alcance de esta Recomendación.

2 Referencias

Las siguientes Recomendaciones UIT-T y demás referencias indicadas contienen disposiciones que, por referencia a las mismas en este texto, constituyen disposiciones de esta Recomendación. Las ediciones citadas estaban en vigor en la fecha de publicación. Todas las Recomendaciones y demás referencias están sujetas a revisión; por lo tanto, se aconseja a todos los usuarios de esta Recomendación que estudien la posibilidad de aplicar la edición más reciente de las Recomendaciones y demás referencias que se indican a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T vigentes. La referencia a un documento en el marco de esta Recomendación no confiere al mismo, como documento independiente, el rango de Recomendación.

[UIT-T X.1401] Recomendación UIT-T X.1401 (2019), *Amenazas a la seguridad de tecnología de libro mayor distribuido*.

[UIT-T X.1601] Recomendación UIT-T X.1601 (2015), *Marco de seguridad para la computación en la nube.*

3 Definiciones

3.1 Términos definidos en otros documentos

En la presente Recomendación se utilizan los siguientes términos definidos en otros documentos:

3.1.1 cadena de bloques como servicio (BaaS) [b-UIT-T Y.3530]: una categoría de servicio en la nube en la que las capacidades disponibles para el cliente del servicio en la nube le permiten establecer plataformas de cadena de bloques y desarrollar aplicaciones descentralizadas mediante tecnologías de cadena de bloques.

3.1.2 cliente de servicios en la nube [b-UIT-T Y.3500]: parte que mantiene una relación empresarial a los efectos de utilizar servicios en la nube.

3.1.3 proveedor de servicio en la nube [b-UIT-T Y.3500]: parte que pone a disposición los servicios en la nube.

3.1.4 asociado de servicio en la nube [b-UIT-T Y.3500]: parte que da soporte o es auxiliar a las actividades de un proveedor de servicios en la nube, de un cliente de servicios en la nube, o de ambos.

3.1.5 consenso [b-UIT-T X.1400]: acuerdo de que un conjunto de transacciones es válido.

3.1.6 par a par [b-ISO 22739]: red de pares que comparten directamente recursos o información los unos con los otros, sin requerir una entidad central; que emplea una red así o relativo a ella.

3.1.7 prueba de trabajo [b-UIT-T X.1400]: procedimiento de consenso para resolver un problema difícil (costoso o que requiere mucho tiempo) por el que se obtiene un resultado fácil de verificar por parte de otros agentes.

3.1.8 contrato inteligente [b-UIT-T X.1400]: un programa escrito en el sistema del libro mayor distribuido que codifica la normativa aplicable a ciertos tipos de transacciones de dicho sistema, con miras a su validación y activación en condiciones específicas.

3.1.9 amenaza [b-ISO/CEI 27000]: una posible causa de un incidente no deseado que puede dañar un sistema o perjudicar a una organización.

3.2 Términos definidos en esta Recomendación

En la presente Recomendación se definen los siguientes términos:

3.2.1 ataque del 51%: un ataque en el que los atacantes controlan suficientes nodos de la cadena de bloques o suficientes recursos de computación como para anular o reescribir el sistema de libro mayor distribuido mediante el control de la generación de bloques.

3.2.2 partición de red: situación de conexión de red en la que esta está dividida en diversas partes desconectada.

4 Abreviaturas y acrónimos

En la presente Recomendación se utilizan las siguientes abreviaturas y acrónimos:

API Interfaz de programación de aplicación (*application programming interface*)

BaaS Cadena de bloques como servicio (*blockchain as a service*)

BSC Cliente de cadena de bloques como servicio (*blockchain as a service customer*)

BSD Diseñador de cadena de bloques como servicio (*blockchain as a service developer*)

BSP Proveedor de cadena de bloques como servicio (*blockchain as a service provider*)

BSS Desarrollador de seguridad de la cadena de bloques como servicio (*blockchain as a service security developer*)

CPU Unidad central de procesamiento (*central processing unit*)

CSC Cliente de servicios en la nube (*cloud service customer*)

CSN Asociado de servicio en la nube (*cloud service partner*)

CSP Proveedor de servicios en la nube (*cloud service provider*)

DDoS Denegación de servicio distribuida (*distributed denial-of-service*)

GPU Unidad de procesamiento gráfico (*graphics processing unit*)

IAM Gestión de identidad y acceso (*identity and access management*)

IIP Información de identificación personal

P2P Par a par (*peer-to-peer*)

PoW Prueba de trabajo (*proof of work*)

SDK Herramienta de desarrollo de *software* (*software development kit*)

5 Convenios

En esta Recomendación:

La expresión "**se requiere**" indica que el requisito es absolutamente obligatorio y debe aplicarse sin excepción si se pretende declarar la conformidad con este documento.

La expresión "**se recomienda**" indica que se trata de un requisito recomendado, pero que no es absolutamente obligatorio. Por lo tanto, su cumplimiento no es indispensable para poder declarar la conformidad.

La expresión "**(se) tiene la opción de**" indica que el requisito se permite, sin que ello signifique que se recomienda. No se pretende implicar que el fabricante deba ofrecer esta opción y que el operador de red/proveedor de servicio tenga la posibilidad de activarla. Significa, más bien, que el fabricante tiene la opción de proporcionar esta función sin que ello afecte a la conformidad con la presente especificación.

En el cuerpo de la presente Recomendación y en sus apéndices, aparecen algunas veces verbos y tiempos verbales que expresan obligación, prohibición, recomendación y posibilidad; en cuyo caso, deberán interpretarse en sus respectivos sentidos. Cuando estas expresiones o términos aparecen en apéndices o en partes incluidas explícitamente a título informativo no deben interpretarse en su sentido normativo.

6 Aspectos generales de la seguridad de la cadena de bloques como servicio

La cadena de bloques como servicio ofrece un entorno integrado de desarrollo, tanto para diseñadores como para clientes, que permite crear, desarrollar, probar, acoger, desplegar y explotar aplicaciones asociadas a la cadena de bloques. Así, los clientes de la BaaS pueden utilizar componentes básicos de la cadena de bloques de la plataforma de BaaS para utilizar eficientemente y desplegar fácilmente redes y aplicaciones de cadena de bloques.

Puesto que los servicios y la plataforma fundamental de la cadena de bloques están integrados en el servicio en la nube, en el funcionamiento de la BaaS intervienen tres actores principales, que se corresponden con los de los servicios en la nube.

- **Proveedor de cadena de bloques como servicio (BSP)**: correspondiente al proveedor de servicios en la nube (CS) en el entorno de computación en la nube, el BSP consta de proveedores de plataforma e infraestructura de cadena de bloques que ponen a disposición la cadena de bloques como servicio. El BSP simplifica el desarrollo y utilización de las cadenas de bloques y las aplicaciones con recursos y funciones fundamentales relacionados con la cadena de bloques, en términos de almacenamiento, comunicación, computación y compatibilidad de redes. El BSP es responsable de la seguridad de los recursos fundamentales de la cadena de bloques y las herramientas de desarrollo ofrecidas a otras funciones de la BaaS.
- **Diseñador de cadena de bloques como servicio (BSD)**: correspondiente al asociado del servicio en la nube (CSN) en el entorno de computación en la nube, el BSD participa en el desarrollo y operación de componentes básicos de la BaaS, con el fin de asistir al BSP en la prestación de sus servicios de cadena de bloques. El BSD es responsable de la seguridad de los componentes básicos desarrollados.
  - El **diseñador de seguridad de la cadena de bloques como servicio (BSS)** es un tipo específico de BSD. El BSS presta asistencia al BSP para mejorar la seguridad de la BaaS, en calidad de proveedor tercero de servicios de seguridad. Los servicios de seguridad facilitados por el BSS incluyen, entre otros, la gestión de identidades y acceso (IAM), auditorías o la detección de intrusiones.
- **Cliente de cadena de bloques como servicio (BSC)**: correspondiente al cliente de servicios en la nube (CSC) en el entorno de computación en la nube, son BSC aquellos clientes de la cadena de bloques que solicitan, utilizan y acceden al servicio o recurso de cadena de bloques a través de las funciones facilitadas directamente por el BSP, o a través de las aplicaciones y servicios ofrecidos indirectamente por el BSD. El BSC se responsabiliza de respetar las normas de seguridad indicadas por el BSP en lo que respecta al funcionamiento de sus propias aplicaciones y redes de cadena de bloques. Además, se alienta al BSC a cooperar con el BSP

en la supervisión de la seguridad de las redes personalizadas de cadena de bloques, así como en la comunicación de eventos de seguridad, en caso necesario.

Las interacciones entre estos actores aparecen representadas en la Figura 1.

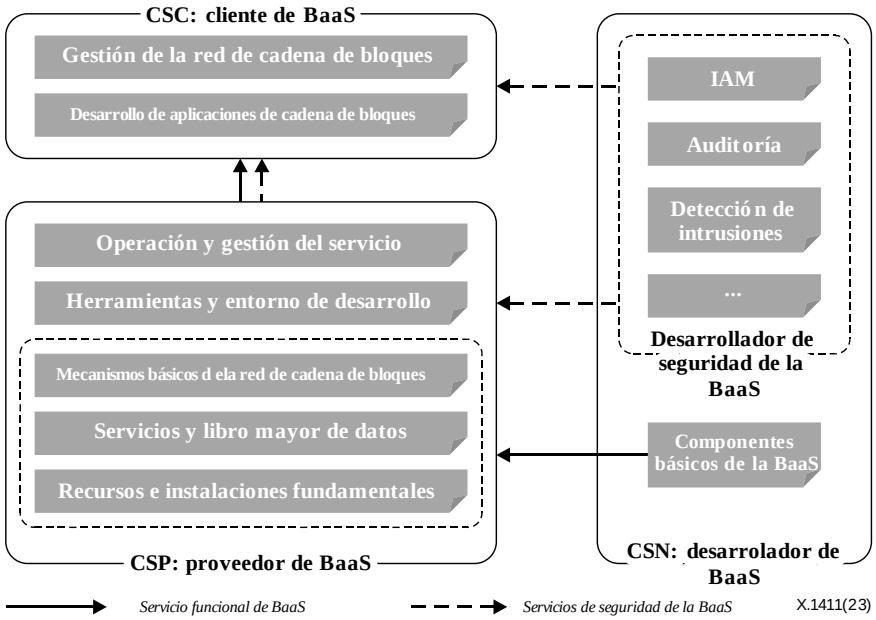

Figura 1 – Funciones e interacciones de los actores en la cadena de bloques como servicio

6.1 Aspectos generales de la seguridad del BSP

El BSP ofrece funciones básicas de la cadena de bloques, entre las que se encuentran los contratos inteligentes, los protocolos de consenso, las conexiones par a par (P2P), los algoritmos criptográficos, los registros de transacciones, la gestión de libro mayor, la gestión de nodos y recursos y el soporte de interfaces normalizadas de desarrollo y servicios de seguridad. A continuación se indican las funciones del BSP y los retos de seguridad asociados.

6.1.1 Instalaciones y recursos fundamentales

El BSP facilita instalaciones fundamentales para ofrecer recursos básicos de computación, comunicación y de otros tipos para el fomento del desarrollo de las redes y las aplicaciones de cadena de bloques. Estas instalaciones pueden ser dispositivos físicos o virtualizados, como las máquinas o los contenedores virtuales.

Entre los retos que presentan las instalaciones fundamentales se encuentran los riesgos medioambientales que pueden afectar a las instalaciones físicas, las inyecciones de puerta trasera, los recursos compartidos entre usuarios, etc.

6.1.2 Servicios y libro mayor de datos

El BSP ofrece servicios de datos en la cadena y fuera de ella, como servicios de almacenamiento, gestión, resolución de consultas de los clientes y datos de sistema para BSC. En este caso, el libro mayor de datos en la cadena garantiza la resistencia contra la manipulación, mientras que la base de datos fuera de la cadena fomenta los servicios de datos eficaces.

En términos de seguridad de datos, el BSP afronta los siguientes retos de seguridad:

– indisponibilidad de los servicios de datos, incluyendo el almacenamiento incoherente de datos en la cadena y fuera de ella a causa de las particiones de red, la pérdida de datos causada por la distribución de las instalaciones de almacenamiento y las bases de datos, revisiones no autorizadas del libro mayor de datos, etc.;

– vulneraciones de la privacidad, incluyendo el acceso no autorizado a datos individuales, la derivación de información sensible a partir de los datos, la eliminación errónea de datos privados, etc.

6.1.3 Mecanismos básicos de la red de cadena de bloques

El BSP ofrece un conjunto de opciones de mecanismos básicos de la red de cadena de bloques para simplificar la configuración de redes personalizadas de cadena de bloques. Los mecanismos básicos de la red de cadena de bloques incluyen los protocolos de consenso, los protocolos de conexión P2P y los algoritmos criptográficos. El BSC puede optar por un conjunto específico de componentes de red entre todas las opciones y configurar los parámetros correspondientes para establecer rápidamente una red personalizada de cadena de bloques.

El BSP es responsable de abordar los problemas de seguridad que afectan a los mecanismos básicos de la red de cadena de bloques. Estos desafíos afectan a la seguridad de las redes de cadena de bloques personalizadas e incluso a las aplicaciones de cadena de bloques construidas sobre la base de la plataforma de la BaaS, ya que el BSC utiliza directamente los mecanismos básicos de la red de cadena de bloques para desarrollar redes y aplicaciones de cadena de bloques. En este ámbito, los problemas de seguridad incluyen el acceso no autorizado a los recursos de la cadena de bloques, las particiones de red, los nodos perniciosos, etc. Por ejemplo, las particiones de red causadas por los servicios no disponibles de la cadena de bloques pueden provocar un retraso inaceptable en la obtención del consenso entre la red distribuida de la cadena de bloques.

6.1.4 Herramientas y entorno de desarrollo

El BSP facilita un entorno integrado de desarrollo provisto de una interfaz de programación de aplicación (API), un paquete de herramientas de desarrollo y otras herramientas, todo ello con el fin de simplificar el desarrollo de aplicaciones de cadena de bloques. Dado que el contrato inteligente es un mecanismo instintivo de cadena de bloques para el desarrollo de aplicaciones de cadena de bloques, el BSP también simplifica el despliegue de los contratos inteligentes y facilita un conjunto de contratos inteligentes para funciones comunes, como la gestión de identidad y acceso.

Entre los problemas asociados se encuentran el control inadecuado de accesos de la API, las interfaces incompatibles, la ejecución inesperada de contratos inteligentes, etc.

6.1.5 Operación y gestión del servicio

El BSP es responsable de supervisar y comunicar las alarmas pertinentes sobre el estado del servicio de la cadena de bloques, en términos de instalaciones físicas, nodos de la cadena de bloques, conexiones de red y recursos asignados, así como la IAM y otras funciones de gestión de la seguridad. El BSP también soporta y gestiona las funciones asociadas a la cadena de bloques facilitadas por el BSP.

Entre los problemas de seguridad asociados se encuentran las funciones de gestión no disponibles, la gestión de acceso inapropiada, los accesos de administración no autorizados, el aumento pronunciado de los recursos consumidos y los riesgos en los componentes asociados a la cadena de bloques facilitados por el BSD.

6.2 Aspectos generales de la seguridad del BSD

El BSD desarrolla componentes básicos de BaaS para el BSP o facilita servicios de seguridad para todos los actores.

6.2.1 Desarrollo de componentes básicos de BaaS

El BSD facilita componentes básicos de BaaS, como contratos inteligentes, algoritmos criptográficos, protocolos de consenso y criptoalgoritmos, en calidad de proveedor tercero.

Entre los problemas y las amenazas de seguridad asociados se encuentran las interfaces incompatibles, los diseños de protocolo inseguros, las puertas traseras en las ejecuciones de protocolos, etc.

6.2.2 Servicios de seguridad

El BSS hace las veces de proveedor tercero de servicios de seguridad para todos los actores en el ecosistema de la BaaS. Por ejemplo, el BSS puede ofrecer servicios de detección de intrusiones para el BSP, auditorías básicas para los BSD y servicios de IAM para el BSC.

Entre los problemas de seguridad se encuentran las normas obsoletas de seguridad, las operaciones inadecuadas de los empleados del BSS, etc.

6.3 Aspectos generales de la seguridad del BSC

El BSC utiliza servicios facilitados por el BSP y el BSD para establecer una red de cadena de bloques y aplicaciones de cadena de bloques personalizadas. Existen dos tipos de BSC: uno es el administrador que establece y gestiona las redes personalizadas de cadena de bloques; el otro, un miembro que se une a una red personalizada de cadena de bloques. Un BSC específico puede ser el administrador de una red personalizada de cadena de bloques y miembro de otra red personalizada de cadena de bloques.

Todos los tipos de BSC afrontan retos de seguridad en aspectos esenciales de la gestión y utilización. El administrador también afronta retos de seguridad en el establecimiento y la gestión de redes personalizadas de cadena de bloques, como, por ejemplo, la configuración inadecuada de nodos, conexiones y otros recursos de la cadena de bloques.

7 Amenazas de seguridad de la cadena de bloques como servicio

Las amenazas que afectan a BSP, BSD y BSC se pueden clasificar en tres tipos:

– diseños técnicos inseguros, fallos de ejecución y gestión inapropiada de recursos fundamentales, funciones básicas y sistemas de servicios de la cadena de bloques;

– interacciones inseguras entre BSC, BSD y BSP, incluyendo las interfaces incompatibles y la cadena de suministro no segura;

– operaciones inadecuadas de empleados, incluyendo el uso y el almacenamiento indebidos de contraseñas.

Las cláusulas 7.1 a 7.3 presentan las amenazas de seguridad que afectan a cada uno de los actores.

7.1 Amenazas a la seguridad del BSP

7.1.1 Amenazas al servicio en la nube

Dado que el BSP ofrece recursos fundamentales de la cadena de bloques basados en servicios en la nube, se enfrenta a desafíos y amenazas heredados del propio servicio en la nube, tal y como se indica en las cláusulas 7 y 8 del documento [UIT-T X.1601]. Por ejemplo, el acceso no autorizado a una partición de un recurso de otro usuario en el entorno compartido de servicios en la nube podría provocar bifurcaciones de la cadena de bloques en el sistema de dicho usuario, por medio de la reescritura o la revisión de sus libros mayores de datos.

7.1.2 Amenazas a los mecanismos básicos de red de la cadena de bloques

Las amenazas a los protocolos de consenso, los protocolos de conexión P2P y los motores criptográficos pueden obedecer a vulnerabilidades en los diseños de los protocolos, fallos de ejecución de los mecanismos o una gestión inadecuada. Para más detalles, véase la cláusula 6 del documento [UIT-T X.1401].

7.1.3 Servicio de datos no fiable

Entre las amenazas al libro mayor distribuido de datos se encuentran los recursos insuficientes de la cadena de bloques, los fallos en el sistema de almacenamiento y la gestión no segura del almacenamiento; todos estos factores pueden causar incoherencias en el registro, pérdidas, manipulación o fugas de datos. Por ejemplo, el sistema y los datos de la cadena de bloques de una red personalizada de cadena de bloques se amplían cuando la red está en funcionamiento. Si un BSP no ofrece suficientes recursos de almacenamiento para que la red personalizada de cadena de bloques pueda hacer frente a la ampliación de datos, la red empieza a sobrescribir los datos antiguos con otros nuevos, o prescinde directamente de los nuevos datos, lo que puede provocar la pérdida de datos en la red personalizada de cadena de bloques. Otro ejemplo se da cuando, a causa de fallos de comunicación o de almacenamiento, se produce un almacenamiento incoherente de datos en los libros mayores distribuidos de datos. Si los fallos persisten durante mucho tiempo, las particiones resultantes de la red pueden provocar retrasos inesperados en las generaciones de bloques, las solicitudes de datos y otros servicios de datos.

7.1.4 Amenazas al entorno de desarrollo

El entorno integrado de desarrollo, el entorno de recopilación, los contratos inteligentes, las API, las herramientas de desarrollo de *software* (SDK) y otras funciones de accesibilidad para el desarrollo facilitadas por el BSP afrontan amenazas que afectan a los procesos de diseño, ejecución, configuración y operación de dichas funciones de desarrollo. Por ejemplo, los fallos de autenticación de las API pueden provocar accesos y usos no autorizados de los recursos fundamentales de la cadena de bloques. Además, los contratos inteligentes afrontan vulnerabilidades de seguridad en el diseño lógico, las ejecuciones de los contratos y la gestión del código, como los desbordamientos o la infrautilización de enteros en un contrato inteligente, que tienen como consecuencia resultados de funcionamiento inesperados.

7.1.5 Funciones inseguras de terceros

El BSP soporta funciones de terceros facilitadas por el BSD y las integra en la plataforma de BaaS por medio de API. En este ámbito, los fallos y los programas malignos en las funciones de terceros, así como las API incompatibles y el control de accesos inapropiado a las API, pueden provocar el desorden en el sistema de la BaaS.

7.1.6 Acceso no seguro al sistema

El acceso no seguro al sistema comprende la falta de control de acceso o un control de acceso inapropiado a los medios de la cadena de bloques, el libro mayor de datos, la red y las aplicaciones. Puede tener como resultado la manipulación de los datos de la cadena de bloques, intrusiones en redes personalizadas de cadena de bloques y fugas de información privada.

7.1.7 Amenazas internas

Existe la posibilidad de que los empleados del BSP, de forma accidental o deliberada, incurran en conductas maliciosas, como la compartición de contraseñas con personas no autorizadas, el olvido negligente de contraseñas en zonas no seguras, la exposición de información personal, etc. Las amenazas internas pueden provocar la fuga de información privada, el acceso no autorizado a redes personalizadas de cadena de bloques y la indisponibilidad de los servicios de la cadena de bloques.

7.1.8 Cadena de suministro no fiable

La plataforma de servicio de cadena de bloques emplea componentes de *software* y de *hardware* facilitados por diversos proveedores. La interrupción del suministro de *software* y *hardware* compromete las capacidades de computación, las conexiones y otros recursos de los servicios de cadena de bloques. En estos casos, se pone en riesgo la disponibilidad de los servicios de cadena de bloques. Por ejemplo, el protocolo de consenso de la prueba de trabajo (PoW) se apoya en la competición de capacidades de cálculo entre nodos de la cadena de bloques en línea; por tanto, la

interrupción del suministro de capacidades de computación y conexión puede afectar a los resultados del consenso en redes de cadena de bloques basadas en PoW.

Además, los programas malignos y las vulnerabilidades explotables en el *software* y el *hardware*, así como en las arquitecturas de cadena de bloques de código abierto, pueden provocar generaciones inesperadas de bloques, denegación de servicios, fugas y uso indebido de datos, etc.

7.1.9 Amenazas al entorno físico

Los incendios, las inundaciones y otras catástrofes medioambientales que afecten a las instalaciones fundamentales pueden provocar la indisponibilidad de las mismas y su incapacidad de facilitar servicios de comunicación, computación y otros recursos fundamentales. Por ejemplo, un corte de energía deliberado o accidental puede dar como resultado una partición de los nodos de la cadena de bloques fuera de línea. En este caso, el proceso de consenso queda bajo el control de un menor número de nodos de la cadena de bloques, lo que tiene como consecuencia resultados de consenso incorrectos y un retraso adicional en la generación de bloques.

7.2 Amenazas a la seguridad del BSD

7.2.1 Amenazas a funciones de terceros

El BSD facilita, en calidad de proveedor tercero, componentes básicos de la cadena de bloques, mecanismos de seguridad de la cadena de bloques y funciones de desarrollo de aplicaciones de la cadena de bloques. Entre las amenazas de seguridad asociadas se encuentran las vulnerabilidades inherentes de seguridad de los componentes básicos de la cadena de bloques, los fallos de ejecución de dichas funciones de terceros, las interfaces incompatibles y el control de acceso no seguro a las interfaces.

Además, las conductas maliciosas de los empleados del BSD también pueden causar fugas de información privada, puertas traseras en las funciones de terceros y operaciones inesperadas de las funciones de seguridad.

7.3 Amenazas a la seguridad del BSC

7.3.1 Fugas y pérdidas de claves

Los BSC gestionan claves por su propia cuenta o a través de servicios de terceros. Un almacenamiento inadecuado de claves, la corrupción de los archivos de las claves o los servicios de claves de terceros no fiables pueden provocar fugas o pérdidas de claves que, a su vez, pueden comportar la pérdida de activos del BSC en cuestión, la revelación de información privada y el desorden en las redes personalizadas de cadena de bloques.

7.3.2 Gestión inadecuada de redes personalizadas de cadena de bloques

El BSC establece sus propias redes personalizadas de cadena de bloques y despliega mecanismos de seguridad a partir de las funciones de la cadena de bloques facilitadas por el BSP y el BSD. En este ámbito, las configuraciones inadecuadas de las redes personalizadas de cadena de bloques y de los mecanismos de seguridad constituyen una amenaza para las redes personalizadas de cadena de bloques. Por ejemplo, si un BSC asigna recursos insuficientes de almacenamiento para las operaciones de la red personalizada de cadena de bloques, esta podría presentar fallos en la actualización de los datos de la cadena de bloques, lo que, en última instancia, provoca incoherencias en los libros mayores de datos de la cadena de bloques.

8 Requisitos de seguridad de la cadena de bloques como servicio

8.1 Configuración de seguridad de una red personalizada de cadena de bloques

Se recomienda al BSP que facilite recomendaciones de configuración de una red personalizada de cadena de bloques para cumplir con los requisitos de seguridad del BSC. Además, se recomienda al BSP que formule recomendaciones sobre la aplicación de los mecanismos de seguridad necesarios para las redes personalizadas de cadena de bloques.

a) Se requiere que el BSP especifique el rango recomendado del número total de nodos.

b) Se requiere que el BSP especifique el número mínimo de nodos en línea para evitar el 51% de las amenazas y otras amenazas conocidas a la red de cadena de bloques.

c) Se requiere que el BSP especifique el número mínimo de nodos adyacentes de cada nodo para evitar la partición de la red de cadena de bloques.

d) Se recomienda al BSP que especifique tipos recomendados de nodos, indicando el número y los derechos de cada nodo.

e) Se recomienda al BSP que especifique los recursos mínimos de almacenamiento, la unidad central de procesamiento (CPU) y la unidad de procesamiento gráfico (GPU) de cada tipo de nodo.

f) Se recomienda al BSP que especifique los protocolos de consenso y par a par recomendados en función de las configuraciones de los nodos.

g) Se recomienda al BSP que facilite funciones básicas de seguridad, incluyendo IAM y gestión de claves, para la red personalizada de cadena de bloques.

h) El BSP tiene la opción de facilitar la evaluación de seguridad de las configuraciones personalizadas de redes de cadena de bloques. El BSP facilitará sugerencias y soluciones de seguridad asociadas al BSC.

8.2 Gestión de identidad y acceso

Se recomienda al BSP que facilite funciones de gestión de identidad y acceso para el sistema de BaaS y la red personalizada de cadena de bloques. Las funciones de gestión de identidad y acceso se despliegan no sólo para proteger las identidades, sino también para facilitar la gestión, la autenticación y la autorización de los accesos.

a) Se requiere que el BSP facilite funciones de registro y cancelación del registro de identidad para el sistema de BaaS.

b) Se recomienda al BSP que facilite funciones de registro y cancelación del registro de identidad para la red personalizada de cadena de bloques.

c) Se requiere que el BSP facilite la gestión del acceso a las cuentas para que el sistema de BaaS pueda diferenciar entre BSP, BSC y BSD.

d) Se recomienda al BSP que facilite la gestión del acceso a las cuentas en la red personalizada de cadena de bloques. Toda red personalizada de cadena de bloques deberá tener uno o más actores de clientes con diversos derechos de acceso.

e) Se requiere que el BSP facilite la autenticación del acceso para el sistema de BaaS. Cada identidad podrá acceder únicamente al recurso correspondiente a sus derechos de acceso.

f) Se recomienda al BSP que facilite la autenticación del acceso a la red personalizada de cadena de bloques.

g) El BSP tiene la opción de facilitar funciones más precisas de gestión del acceso, como las funciones de control de acceso basado en roles.

h) El BSP tiene la opción de supervisar la frecuencia de las actividades de acceso desde la IP, la cuenta o los dispositivos de acceso, entre otros elementos. Entre tales actividades de acceso se encuentran el registro, la cancelación del registro y la actualización de claves, entre otras.

8.3 Gestión de claves

Se recomienda al BSP que facilite funciones de gestión de claves para proteger la seguridad de los procesos de generación, almacenamiento, distribución, uso, copia de seguridad, recuperación y revocación de claves.

a) Se requiere que el BSP facilite esquemas integrales de gestión de claves, con la pertinente aclaración de las claves y el procedimiento de gestión.

b) Se requiere que el BSP evalúe la seguridad de los algoritmos de número aleatorio y otros parámetros empleados para generar claves. Los algoritmos de número aleatorio deben satisfacer criterios de aleatoriedad e impredecibilidad.

c) Se recomienda al BSP que preste soporte a funciones de gestión de claves de terceros. Deberá evaluarse y garantizarse la seguridad de las funciones de gestión de claves de terceros antes de facilitarlas al BSC.

d) Se recomienda al BSP que facilite funciones de revocación de claves para las cuentas dadas de baja y sospechosas.

e) Se recomienda al BSP que facilite funciones de recuperación de claves para las claves perdidas. Sólo las cuentas autenticadas podrán acceder a las funciones de recuperación de claves.

f) Se recomienda al BSP que requiera que el BSC actualice las claves periódicamente. Se aplicarán diversos periodos de actualización en función de los niveles de seguridad.

g) Se recomienda al BSC que despliegue una función de gestión de claves en la red personalizada de cadena de bloques.

h) Se requiere que el BSC domine y se atenga a los procedimientos seguros de uso, almacenamiento, recuperación y revocación de claves, de conformidad con la función de gestión de claves desplegada en la red personalizada de cadena de bloques.

i) Se recomienda al BSC que comunique los usos sospechosos de las claves al BSP, tal y como esté predefinido en la función de gestión de claves.

j) El BSP tiene la opción de utilizar un esquema bipartito o multipartito de almacenamiento de las claves principales y secretas.

8.4 Protección de la privacidad

Se recomienda al BSP que facilite protección para la recogida, el acceso y otras operaciones relacionadas con la información de identificación personal (IIP).

a) Se requiere que el BSP se atenga a la legislación, las normativas y las políticas nacionales y locales en relación con la protección de la privacidad, como los aspectos de recogida y almacenamiento de IIP.

b) Se requiere que el BSP facilite la desidentificación de la IIP mostrada.

c) Se requiere que el BSP ponga en marcha medidas de seguridad para garantizar que la IIP en la cadena pueda borrarse por completo cuando el BSC así lo requiera, por ejemplo, utilizando tecnologías de cadena de bloque basadas en un algoritmo chameleon hash, o que la IIP se pueda almacenar fuera de la cadena.

d) Se recomienda al BSP que invite a organizaciones profesionales a realizar auditorías sobre las operaciones sensibles relacionadas con la IIP.

8.5 Seguridad de los motores criptográficos

Se recomienda al BSP que garantice la seguridad de los motores criptográficos utilizados en las redes personalizadas de cadena de bloques.

a) Se requiere que el BSP soporte los criptoalgoritmos convencionales cuya seguridad haya sido verificada públicamente.

b) Se requiere que el BSP invite a organizaciones profesionales para auditar la seguridad de los motores criptográficos.

c) Se recomienda al BSP que soporte los motores criptográficos facilitados por el BSD. Se recomienda al BSD que facilite los resultados de la evaluación de seguridad de los motores criptográficos.

8.6 Seguridad de la conexión par a par

Se recomienda al BSP que garantice que las conexiones par a par sean resistentes a los nodos no fiables o maliciosos.

a) Se requiere que el BSP facilite esquemas de autenticación para gestionar el acceso a las redes par a par.

b) Se requiere que el BSP emplee tecnologías criptográficas para establecer canales seguros de transmisión entre nodos distribuidos.

c) Se requiere que el BSP soporte protocolos par a par con fiabilidad y escalabilidad. La fiabilidad indica que los nodos desconectados mantienen la coherencia con otros nodos tras la reconexión. La escalabilidad indica que los protocolos soportan la adición o la supresión dinámica o estática de nodos con un funcionamiento normal de las redes de cadena de bloques.

d) Se requiere que el BSP soporte protocolos par a par en cualquier nodo que tenga más de un vecino.

e) Se recomienda al BSP que soporte protocolos par a par de modo que la desconexión de un nodo cualquiera no suponga particiones de red.

f) Se recomienda al BSP que facilite una topología en tiempo real de la red par a par.

g) Se recomienda al BSP que emita una alerta si la red par a par afronta particiones o nodos perniciosos.

8.7 Seguridad del mecanismo de consenso

Se recomienda al BSP que garantice que el diseño y las operaciones del mecanismo de consenso son seguros.

a) Se requiere que el BSP facilite algoritmos de consenso cuya seguridad haya sido probada o evaluada públicamente.

b) Se requiere que el BSP preste asistencia al BSC para aplicar algoritmos de consenso facilitados por el BSD.

c) Se requiere que el BSP facilite una evaluación de la seguridad de los algoritmos de consenso al BSC. La evaluación de seguridad debe incluir el número umbral de nodos de consenso, la frecuencia recomendada de consenso y otros elementos.

d) Se requiere que el BSP garantice que los nodos de consenso se autentiquen antes de unirse al consenso.

e) Se requiere que el BSP supervise el proceso de consenso y evalúe el periodo de consenso, el nodo de consenso y el resultado del consenso.

f) Se recomienda al BSP que emita alertas y facilite soluciones cuando se estime que el proceso de consenso supervisado es anormal.

8.8 Seguridad del contrato inteligente

Se recomienda al BSP que facilite la gestión del ciclo de vida completo para los contratos inteligentes, incluyendo su creación, su implantación, su actualización, su lanzamiento, su ejecución y su supresión.

a) Se requiere que el BSP facilite especificaciones de códigos, requisitos lógicos y otras orientaciones normativas relativas a los contratos inteligentes.

b) Se recomienda al BSP que facilite un entorno aislado fiable, como un banco de pruebas o "sandbox", para la ejecución de los contratos inteligentes.

c) Se requiere que el BSP facilite una gestión de accesos apropiada para los contratos inteligentes, a fin de restringir las operaciones maliciosas o evitar que los contratos inteligentes erróneos infecten a otros contratos.

d) Se requiere que el BSP soporte mecanismos de respuesta de seguridad de emergencia para los contratos inteligentes.

e) Se requiere que el BSP limite la complejidad de los contratos inteligentes en términos de consumo de recursos y tiempo de ejecución.

f) Se recomienda al BSP que supervise y controle el consumo excesivo de recursos de la cadena de bloques por parte de los contratos inteligentes.

g) Se recomienda al BSP que soporte la terminación de contratos inteligentes cuando estos excedan la restricción de recursos.

h) Se recomienda al BSP que facilite soluciones técnicas para prevenir los ataques de denegación de servicio distribuida (DDoS) en relación con el contrato inteligente.

i) Se recomienda al BSP que prevea la provisión, por parte del BSD, de funciones para detectar automáticamente las vulnerabilidades de seguridad del código fuente y el código de byte del contrato inteligente.

j) Se recomienda al BSP que prevea la supervisión, por parte del BSD, de las actividades de los contratos inteligentes, a fin de detectar alertas tempranas de conductas anómalas de los mismos.

8.9 Supervisión de recursos

Se recomienda al BSP que supervise el consumo de recursos en la BaaS y emita una alerta cuando el estado de los recursos sea anómalo.

a) Se recomienda al BSC que permita al BSP que supervise el consumo de recursos de los nodos en las redes personalizadas de cadena de bloques en términos de almacenamiento, computación, CPU, conexiones de red, estado en línea y duración en línea, entre otros.

b) Se recomienda al BSP que emita una alerta de escasez de recursos para el BSC cuando los nodos de la red personalizada de cadena de bloques afronten una escasez de recursos. El BSP facilitará al BSC soluciones para subsanar la escasez de recursos.

c) Se recomienda al BSC que permita al BSP que supervise el estado de red de las redes personalizadas de cadena de bloques en términos de velocidad de generación de bloques, generadores de bloques y tamaño de los bloques, entre otros.

d) Se recomienda al BSP que facilite una alerta de intrusión al BSC cuando se detecte que el estado de la red es anómalo. El BSP facilitará al BSC el análisis correspondiente de la situación anómala, la información correspondiente sobre los nodos anómalos y las soluciones recomendadas.

8.10 Sistema de detección de intrusiones

Se recomienda al BSP que facilite y actualice mecanismos para evitar los códigos maliciosos y otras intrusiones.

a) Se requiere que el BSP facilite normas de seguridad para los contratos inteligentes y una biblioteca de vulnerabilidades. El BSP facilitará interfaces de acceso en formato común para la detección de vulnerabilidades.

b) Se requiere que el BSP instale *software* contra los programas malignos o configure *software* con las funciones pertinentes para detectar y eliminar los programas malignos.

c) Se recomienda al BSP que facilite medidas de prevención contra el código malicioso en cada nodo de la cadena de bloques y elimine el código malicioso antes de acceder a la red de cadena de bloques.

d) Se recomienda al BSP que facilite normativas sobre los mecanismos de prevención del código malicioso, incluyendo la actualización periódica de la librería de códigos maliciosos y la comprobación periódica y la eliminación de todo código malicioso.

e) Se recomienda al BSP que prevea la evaluación periódica, por parte del BSD, de la eficacia de las medidas técnicas contra los ataques de código malicioso.

8.11 Auditoría de seguridad

Se recomienda al BSP que prevea la ejecución, por parte de uno o más BSD, de una auditoría de seguridad de la infraestructura de la cadena de bloques, del código fuente y de otras funciones básicas.

a) Se recomienda al BSP que seleccione uno o más BSD para que realicen evaluaciones de seguridad y auditorías del *software* básico de la cadena de bloques, la red y otros entornos operativos previos al servicio en línea de la cadena de bloques, a fin de asegurarse de que los riesgos de seguridad a nivel de infraestructura sean controlables.

b) Se recomienda al BSP que prevea la ejecución, por parte de al menos un BSD, de una auditoría de seguridad del código fuente, que se centre principalmente en los riesgos y los problemas de calidad a nivel del código fuente.

c) Se recomienda al BSD que facilite al BSP un informe de la auditoría del código fuente con una enumeración de los elementos de cumplimiento e infracción y sugerencias de revisión del código fuente.

d) Se recomienda al BSP que prevea la evaluación, por parte del BSD, de las funciones de IAM, a fin de garantizar que no haya riesgos como los de fuga de claves privadas o de información de los usuarios.

8.12 Gestión de funciones de terceros

Se recomienda al BSP que garantice que las funciones de terceros funcionen de forma segura, tal y como estén predefinidas.

a) Se requiere que el BSP aclare los requisitos funcionales y de seguridad de los terceros proveedores.

b) Se requiere que el BSP suscriba acuerdos de cooperación con terceros proveedores de servicios en materia de componentes de servicios y aclare sus obligaciones y responsabilidades.

c) Se recomienda al BSP que supervise o audite los servicios de proveedores terceros y los evalúe con arreglo al acuerdo suscrito.

8.13 Seguridad de la cadena de suministro

Se recomienda al BSP que garantice que su cadena de suministro sea resistente contra los proveedores maliciosos y los cambios de proveedores.

a) Se requiere que el BSP desarrolle políticas y procedimientos de gestión de seguridad de la cadena de suministro, incluyendo criterios de gestión de la seguridad de los participantes en la misma.

b) Se requiere que el BSP evalúe de forma rutinaria la vulnerabilidad de la cadena de suministro en su infraestructura y el uso del código fuente abierto en el sistema.

c) Se recomienda al BSP que informe al BSC sobre los riesgos de la cadena de suministro en el sistema de la cadena de bloques como servicio.

d) Se requiere que el BSP confirme la diversidad de sus proveedores de *software* y *hardware* imprescindible.

Cuadro 1 – Requisitos de seguridad de la BaaS

Amenazas de seguridad		Requisitos de seguridad												
		Configuración de seguridad	**IAM**	**Gestión de claves**	**Protección de la privacidad**	**Seguridad de los motores criptográficos**	**Seguridad de la conexión P2P**	**Seguridad del mecanismo de consenso**	**Seguridad del contrato inteligente**	**Supervisión de recursos**	**Sistema de detección de intrusiones**	**Auditoría de seguridad**	**Gestión de funciones de terceros**	**Seguridad de la cadena de suministro**
BSP	7.1.1	✓	✓	✓	✓				✓			✓	✓	✓
	7.1.2					✓	✓	✓	✓		✓	✓	✓	✓
	7.1.3	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	7.1.4							✓	✓	✓	✓			
	7.1.5										✓	✓	✓	✓
	7.1.6		✓	✓										
	7.1.7		✓										✓	
	7.1.8											✓	✓	✓
	7.1.9												✓	
BSD	7.2.1			✓	✓	✓	✓	✓		✓	✓		✓	
BSC	7.3.1		✓	✓										
	7.3.2	✓								✓			✓	

Bibliografía

[b-UIT-T X.1400] Recomendación UIT-T X.1400 (2020), *Términos y definiciones sobre la tecnología de libro mayor distribuido.*

[b-UIT-T Y.3500] Recomendación UIT-T Y.3500 (2014) | ISO/CEI 17788:2014, *Tecnología de la información – Computación en la nube – Descripción general y vocabulario.*

[b-UIT-T Y.3530] Recomendación UIT-T Y.3530 (2020), *Computación en la nube – Requisitos funcionales de las cadenas de bloques como servicio.*

[b-ISO 22739] ISO 22739:2020, *Blockchain and distributed ledger technologies – Vocabulary.*
<https://www.iso.org/standard/73771.html>

[b-ISO/CIE 27000] ISO/CIE 27000:2018(en), *Information technology – Security techniques – Information security management systems – Overview and vocabulary.*
<https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en>

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios de tarificación y contabilidad y cuestiones económicas y políticas de las telecomunicaciones/TIC internacionales
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Medio ambiente y TIC, cambio climático, ciberdesechos, eficiencia energética, construcción, instalación y protección de los cables y demás elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de la transmisión telefónica, instalaciones telefónicas y redes de líneas locales
Serie Q	Conmutación y señalización, y mediciones y pruebas asociadas
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	**Redes de datos, comunicaciones de sistemas abiertos y seguridad**
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet, redes de próxima generación, Internet de las cosas y ciudades inteligentes
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Publicado en Suiza
Ginebra, 2023