PROPUESTA

De conformidad con el artículo 116, apartado 6, de la Ley de comunicaciones electrónicas (Boletín Oficial n.º 130/22 y n.º 18/23 – ZDU-1O), la Agencia de Redes y Servicios de Comunicación de la República de Eslovenia, teniendo en cuenta el procedimiento de información de conformidad con la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo, de 9 de septiembre de 2015, por la que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información (DO L 241 de 17.9.2015, p. 1), emite lo siguiente:

LEY GENERAL
sobre requisitos y restricciones de seguridad adicionales

Artículo 1
(Contenido de la Ley general)

La presente Ley general establece lo siguiente:

1. directrices que deberán seguir los operadores de redes de comunicaciones móviles (en lo sucesivo, «operadores») que proporcionen estas redes a entidades críticas que sean gestores de infraestructuras críticas en otros ámbitos de la regulación de las infraestructuras críticas, tal como se especifica en la legislación que rige el ámbito de las infraestructuras críticas (en lo sucesivo, «gestores de infraestructuras críticas»), los proveedores de servicios esenciales determinados por la legislación que rige la seguridad de la información (en lo sucesivo, «proveedores de servicios esenciales»), los organismos de la administración estatal, según lo determine la ley que rige la seguridad de la información (en lo sucesivo, «organismos de administración estatal») o los transportistas de partes clave del sistema de seguridad del país; y
2. elementos críticos de la red y sistemas de información asociados con sus funcionalidades a que se refiere el artículo 116, apartado 6, de la Ley de comunicaciones electrónicas (Boletín Oficial n.º 130/22 y n.º 18/23 – ZDU-1O; (en lo sucesivo, la «Ley»), tal como figura en el anexo, que forma parte integrante de la presente Ley general y se elabora en cooperación con el organismo responsable de la seguridad de la información.

Artículo 2
(Significado de los términos)

(1) Los términos utilizados en la presente Ley general tienen el siguiente significado:

1. «cadena de suministro»: todo el sistema de procesos, personas, organización y distribución involucrados en el diseño, la producción, el almacenamiento, la distribución y el suministro, así como la instalación y el mantenimiento de componentes de elementos críticos de red instalados en la red del operador o en el proveedor de servicios en la nube que presta dichos servicios al operador;

2. «elementos críticos de la red»: aquellos elementos de red, funciones, servicios y sistemas de información de apoyo en forma física, informática o virtualizada en el

operador o en el proveedor de servicios en la nube, que se enumeran en el anexo de la presente Ley general;

3. «entidades críticas»: gestores de infraestructuras críticas en otras áreas de regulación de infraestructuras críticas determinadas de conformidad con la ley que rige el campo de las infraestructuras críticas, proveedores de servicios esenciales según lo determinado por la ley que rige la seguridad de la información, los organismos de administración estatal según lo determine la ley que rige la seguridad de la información y los portadores de partes clave del sistema de seguridad del país.

(2) Otros términos utilizados en la presente Ley general tienen el mismo significado que el establecido en la Ley y en la Ley general de seguridad de redes, servicios y datos.

Artículo 3
(Directrices generales)

(1) Los operadores de la cadena de suministro de componentes de elementos críticos de red y servicios de apoyo de tercer nivel para estos componentes tendrán en cuenta al menos las siguientes directrices a lo largo de todo el ciclo de vida de estos componentes:

1. en el caso de un fabricante o proveedor individual y de un proveedor de servicios de apoyo de tercer nivel debido a las relaciones y los acuerdos con ellos, llevarán a cabo una evaluación del riesgo en términos de suministro y de posibles impactos por parte de terceras personas físicas o jurídicas de Derecho público o privado (en lo sucesivo, «terceros»), compatibilidad con equipos de otros fabricantes, calidad y seguridad de los productos y posibles efectos negativos en el funcionamiento de los servicios y entidades críticas del operador;
2. que la seguridad ya está incorporada y se aplica en el diseño y que los contratos incluyen plazos para la eliminación de las vulnerabilidades percibidas;
3. que las principales características de seguridad (disponibilidad, confidencialidad, integridad y autenticidad) se garantizan a lo largo de todo el ciclo de vida de su uso;
4. que la seguridad y su suministro ininterrumpido están garantizados y se confirma que soportan características de seguridad elevadas de conformidad con las normas reconocidas internacionalmente (3GPP) y las normas técnicas europeas (ETSI);
5. que las directrices a que se refieren los puntos 2 a 4 del presente apartado son verificables en la documentación contractual con el fabricante o con el proveedor;
6. para cada fabricante o proveedor, también se evalúan y se tienen en cuenta los riesgos asociados a los derechos de uso de las tecnologías clave, que son necesarios para la fabricación y el uso del equipo y los riesgos relacionados con el suministro de equipos, piezas de repuesto o servicios de apoyo de tercer nivel;
7. que los componentes utilizados no tienen vulnerabilidades críticas conocidas o explotadas activamente sin resolver;
8. evitar un único fabricante o proveedor, cuando sea técnicamente viable y económicamente sostenible, con el fin de reducir la dependencia y aumentar la resiliencia en caso de vulnerabilidades de componentes críticos, fallo catastrófico de la red o una amenaza para la seguridad de las redes y servicios de entidades críticas por terceras entidades físicas o jurídicas de Derecho público o privado.

(2) Al suministrar equipos, sistemas y servicios de información y comunicación, los operadores cumplirán plenamente las directrices de la Agencia de la Unión Europea para la Ciberseguridad (en lo sucesivo, «ENISA») y las normas vigentes de la Unión Europea relativas a los requisitos básicos de seguridad al adquirir productos y servicios de TIC seguros. La Agencia publicará en su sitio web enlaces a los documentos actuales de ENISA y a la normativa de la UE en el ámbito mencionado y los mantendrá actualizados.

(3) Al suministrar componentes de elementos críticos de red o utilizar servicios en la nube, se dará prioridad a la elección de componentes de aquellos fabricantes o proveedores o servicios de proveedores de servicios en la nube que hayan sido certificados por organismos de evaluación de la conformidad que hayan sido acreditados y, en su caso, autorizados sobre la base del artículo 60, apartado 3, del Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.º 526/2013 (en lo sucesivo, el «Reglamento») para la expedición de certificados europeos de ciberseguridad a cierto nivel de garantía, tal como se determina en el artículo 52 del Reglamento.

(4) A efectos del apartado anterior, el operador revisará un sitio web especial, establecido por ENISA de conformidad con el artículo 55 del Reglamento, destinado a informar al público sobre los esquemas europeos de certificación de la ciberseguridad, los certificados europeos de ciberseguridad y las declaraciones UE de conformidad, incluida la información relativa a los esquemas europeos de certificación de la ciberseguridad que ya no sean válidos o revocados y caducados, y las declaraciones UE de conformidad, así como un repositorio de enlaces a la información sobre ciberseguridad.

Artículo 4
(Evaluación del riesgo)

(1) Al determinar el riesgo del fabricante o el proveedor de componentes y del proveedor de servicios de tercer nivel para los elementos críticos de la red, el operador tendrá en cuenta los siguientes aspectos de riesgo, que evalúa.

(2) En la valoración a que se refiere el apartado anterior, el operador evaluará y tendrá en cuenta, como mínimo:

1. la calidad global (incluidos los aspectos de seguridad) y fiabilidad;
2. el nivel de uso de normas e interfaces abiertas que impidan la dependencia y la dependencia de los productos de un determinado fabricante o proveedor, es decir, «dependencia de proveedores» (*vendor lock-in*, por su versión en inglés);
3. el cumplimiento de las normas técnicas internacionales y europeas reconocidas (3GPP, ETSI) y de las normativas de la Unión Europea y de los ajustes de seguridad predeterminados de conformidad con las recomendaciones profesionales (Asociación GSMA);
4. el nivel de compatibilidad con equipos de terceros y funciones de red;
5. la capacidad de proporcionar mejoras y personalizaciones;
6. el proceso de gestión de vulnerabilidades, su divulgación y el proceso actualizado con actualizaciones y correcciones;
7. la disponibilidad y la transparencia de la documentación relativa a:

- las funciones clave y la información sobre la seguridad y otras características del componente y posibles configuraciones; y
- el *software* utilizado, incluido el código fuente abierto (nomenclatura de materiales de los programas informáticos – SBOM, por su versión en inglés);

8. el nivel de dependencia de los servicios de apoyo de tercer nivel en la gestión y el mantenimiento de equipos, si el operador no realiza estos servicios solo con sus empleados;
9. la evaluación preliminar de la conformidad de los equipos o de una entidad que prestaría un servicio de apoyo de tercer nivel por organismos acreditados en la Unión Europea de conformidad con los esquemas europeos de certificación de la ciberseguridad, mediante la cual los organismos acreditados se publican en el *Diario Oficial de la Unión Europea*.

(3) El operador documentará los factores de riesgo y los resultados de la evaluación del riesgo para cada fabricante, proveedor o proveedor de servicios de tercer nivel seleccionados a que se refieren los apartados 2 y 3 del presente artículo y lo actualizará periódicamente.

Artículo 5
(Directrices generales sobre el funcionamiento de los elementos críticos de la red)

(1) Los componentes de los elementos críticos de la red, su funcionamiento y la configuración predeterminada no contendrán características técnicas que puedan afectar negativamente a la seguridad o al funcionamiento de las entidades críticas, entre otras cosas debido al sabotaje, el espionaje, el robo de propiedad intelectual o el terrorismo.

(2) Los elementos críticos de la red se encuentran generalmente en la República de Eslovenia o, teniendo en cuenta todos los riesgos para la seguridad y garantizando un alto nivel de medidas de seguridad, y si la normativa aplicable no especifica otra cosa, en la Unión Europea. El operador informará a la Agencia de Redes y Servicios de Comunicación de la República de Eslovenia (en lo sucesivo, la «Agencia») y al organismo responsable de la seguridad de la información sobre su reubicación prevista, al menos 30 días antes de la reubicación fuera de la Unión Europea.

(3) Los servicios de apoyo de tercer nivel para elementos críticos de la red se prestan generalmente en la República de Eslovenia o, teniendo en cuenta todos los riesgos de seguridad y garantizando un alto nivel de medidas de seguridad, y si la normativa aplicable no especifica otra cosa, en la Unión Europea. El operador notificará a la Agencia y al organismo responsable de la seguridad de la información la reubicación prevista de sus servicios de apoyo de tercer nivel al menos 30 días antes de la reubicación fuera de los países de la Unión Europea.

(4) La ejecución de servicios de apoyo de tercer nivel no pondrá en peligro la seguridad o el funcionamiento de los servicios de las entidades críticas ni la seguridad nacional.

(5) El operador establecerá y aplicará periódicamente el proceso de identificación de los elementos críticos de red. Esto debe llevarse a cabo al menos una vez al año o cuando se adquieran componentes de elementos críticos de la red.

(6) Si un componente individual representa solo parcialmente un elemento crítico de red, se considerará parte de un elemento crítico de red.

(7) El operador mantendrá una lista actualizada de todos los componentes de los elementos críticos de la red, sus funciones, ubicaciones, administradores y gestores, sus proveedores de servicios de apoyo de tercer nivel y sus fabricantes o proveedores. Previa solicitud, la lista se pondrá a disposición de la Agencia y de un organismo responsable de la seguridad de la información.

Artículo 6
(Medidas de seguridad para el suministro de componentes de elementos críticos de red)

(1) El operador será consciente de toda la cadena de suministro y de los riesgos asociados a ella, incluidos los subcontratistas de componentes individuales de elementos críticos de la red, que también incluyen claves de cifrado, UICC/eUICC y otros elementos de seguridad, cuyo uso indebido podría poner en peligro la seguridad de las entidades críticas.

(2) El operador garantizará que los requisitos de seguridad entre el operador y los fabricantes o proveedores de componentes de elementos críticos de red o sus proveedores de servicios de apoyo de tercer nivel se acuerden y documenten contractualmente y exijan a los fabricantes o proveedores que respeten las medidas de seguridad acordadas a lo largo de toda la cadena de suministro.

(3) A fin de evitar la explotación oportuna de las vulnerabilidades por parte de los agentes malintencionados, el operador se asegurará de que el fabricante o proveedor de componentes de un elemento crítico de red se comprometa contractualmente a informar inmediatamente al operador de la vulnerabilidad detectada y de las medidas para reducir los riesgos y asesorar sobre las medidas de protección o reparación que el operador pueda adoptar en respuesta a la amenaza.

(4) Al menos una vez al año, el operador verificará la adecuación de los derechos de acceso sobre elementos críticos de la red o los actualizará sin demora de acuerdo con los cambios en la organización o en el lado de los proveedores de servicios de apoyo de tercer nivel.

(5) El operador evitará su dependencia de un proveedor individual o de un proveedor de servicios de tercer nivel (es decir, «dependencia de proveedores»), cuando sea técnicamente viable y económicamente sostenible, con el objetivo de reducir la dependencia y aumentar la resiliencia en caso de vulnerabilidades de componentes críticos, evitando también contratos a largo plazo con fabricantes o proveedores individuales o proveedores de servicios de apoyo de tercer nivel, o teniendo la opción de cambiarlos con el objetivo de reducir las interrupciones en la prestación de servicios a entidades críticas al nivel más bajo posible.

Artículo 7

(Condiciones contractuales con fabricantes, proveedores o proveedores de servicios de apoyo de tercer nivel)

A fin de garantizar un alto nivel de seguridad, el operador incluirá al menos lo siguiente en nuevas condiciones contractuales con fabricantes, proveedores o proveedores de servicios de apoyo de tercer nivel:

1. una declaración del fabricante o del proveedor de que el componente o sus ajustes predeterminados no tienen puertas traseras indocumentadas ni ningún impacto negativo en el funcionamiento de las entidades críticas;
2. el compromiso del fabricante, del proveedor o del proveedor de servicios de tercer nivel de proteger los datos con los que se familiarice durante la prestación de servicios o el acceso a ellos en relación con la prestación del servicio de acceso;
3. el compromiso del fabricante, del proveedor o del proveedor de servicios de tercer nivel de informar inmediatamente al operador en caso de violación de la protección de la transmisión de datos o del tráfico de datos que afecten o puedan afectar al operador o a las entidades críticas a que se refiere el artículo 1, apartado 1, de la presente Ley general;
4. el compromiso del fabricante, del proveedor o del proveedor de servicios de tercer nivel de notificar inmediatamente al operador cualquier incidente de seguridad y vulnerabilidad que pueda afectar a la seguridad de la red, los servicios asociados o los datos del operador;
5. el compromiso del fabricante, del proveedor o del proveedor de servicios de tercer nivel de cumplir las normas y reglas de seguridad establecidas por el operador y de adoptar las medidas de seguridad adecuadas para garantizar la seguridad de los sistemas y redes de información, así como de los datos del operador o de la entidad crítica;
6. la capacidad del operador para revisar los entornos, los procedimientos, las medidas de seguridad y las herramientas utilizadas por el proveedor de servicios de apoyo de tercer nivel al acceder a la red y los datos del operador en cualquier momento;
7. la responsabilidad del fabricante, del proveedor o del proveedor de servicios de apoyo de tercer nivel por los daños causados por las vulnerabilidades detectadas o el uso indebido de componentes de elementos críticos de la red, su configuración predeterminada o durante la prestación de servicios de apoyo de tercer nivel que el fabricante, el proveedor o el proveedor de apoyo de tercer nivel hayan descuidado o aplicado deliberadamente;
8. la obligación de formar regularmente al personal del fabricante, el proveedor o el proveedor de servicios de apoyo de tercer nivel en el ámbito de los sistemas y las redes de información y seguridad de datos.

Artículo 8
(Reglas relativas al acceso y uso de los elementos críticos de red)

(1) Cuando acceda física o lógicamente a los componentes de los elementos críticos de la red, a su configuración y a los datos del operador almacenados, tratados o modificados en ellos, el operador garantizará que:

1. el acceso está estrictamente limitado a las personas previamente autorizadas;
2. todos los trabajos sobre elementos críticos de red llevados a cabo *in situ* o a través del acceso remoto son controlados por el operador;

3. se lleva a cabo una autenticación multifactor para los usuarios a los que se asignan los mayores privilegios de derechos para acceder a componentes individuales de elementos críticos de red, su configuración o los datos almacenados o tratados allí;
4. cada persona autorizada a la que se concede el acceso tiene una cuenta de usuario y una contraseña únicas;
5. solo se utilizan contraseñas que se modifican de forma regular o inmediata en caso de que se detecte un uso indebido, de al menos quince caracteres y que incluyan letras mayúsculas y minúsculas, números y caracteres especiales, si el *software* lo permite;
6. el concepto de tolerancia o confianza cero se aplica en la medida de lo posible en el acceso;
7. la seguridad de la conexión de comunicación del usuario autorizado a los componentes individuales está protegida por el uso de cifrado, teniendo en cuenta los últimos avances tecnológicos y las mejores buenas prácticas industriales en el ámbito de la seguridad de la información, o los recomendados por las instituciones establecidas en el ámbito de la seguridad de la información;
8. se lleva a cabo un registro indeleble de los accesos y los intentos de acceso, que se mantiene durante al menos seis meses, incluida una copia de seguridad, pero también puede ser durante un período más largo, cuando el análisis de la gestión de riesgos y la evaluación del nivel aceptable de riesgos demuestren que los riesgos deben gestionarse adecuadamente manteniendo los registros durante un período más largo;
9. el registro y el seguimiento de todas las intervenciones de *software* en los componentes se realiza siempre que sea posible, incluidos los cambios de configuración. Los registros, incluida una copia de seguridad de estos datos, se conservarán durante el tiempo indicado en el punto anterior;
10. el acceso a los componentes individuales y a los datos almacenados o tratados en ellos está limitado en el tiempo y abierto solo mientras dure el trabajo necesario.

(2) En el caso de que el personal o los empleados de un proveedor de servicios de apoyo de tercer nivel accedan a componentes individuales de elementos críticos de red, deberán:

1. utilizar únicamente una estación de trabajo dedicada intermedia segura, es decir, un «servidor de salto» (*jump server*, por su versión en inglés), que estará sujeta a controles de seguridad periódicos;
2. instalar en una estación de trabajo dedicada solo las herramientas, componentes y servicios activos absolutamente necesarios para acceder a otros recursos en la red que son absolutamente necesarios y deben actualizarse con los últimos parches de seguridad;
3. utilizar operaciones y claves criptográficas seguras en una estación de trabajo dedicada, que debe estar ubicada en la red del operador y que está bajo su control exclusivo;
4. cada acceso es aprobado y activado por el operador manualmente y solo mientras dure el acceso;
5. todos los accesos y actividades son controlados y registrados físicamente por el operador;
6. utilizar una autenticación de dos factores y contraseñas de al menos quince caracteres y que incluyan letras mayúsculas y minúsculas, números y caracteres especiales, que se modificarán en función de los riesgos evaluados.

(3) Antes de que el operador transfiera el servicio de gestión, mantenimiento o actualización de los elementos críticos de red o de sus componentes individuales a un tercero, verificará y garantizará que tiene al menos los mismos o mejores mecanismos de seguridad y procesos de gestión de la seguridad en comparación con sus mecanismos y procesos. Informará inmediatamente a la entidad crítica de que se trate, a la Agencia y al organismo responsable de la seguridad de la información sobre la intención de la transferencia.

(4) El operador verificará el estado real de los procesos de seguridad antes del inicio de la prestación del servicio y, posteriormente, al menos una vez al año. El operador mantendrá registros de las revisiones y controles internos de la prestación de servicios de apoyo a terceros y los conservará durante la prestación de los servicios y durante un año después de su terminación, pero no más de cinco años.

DISPOSICIÓN TRANSITORIA Y FINAL

Artículo 9
(Disposiciones transitorias)

(1) El operador notificará a la Agencia y al organismo responsable de la seguridad de la información las ubicaciones existentes de elementos críticos de red en un plazo de 30 días a partir de la entrada en vigor de la presente Ley general.

(2) El operador notificará a la Agencia y al organismo responsable de la seguridad de la información las ubicaciones existentes de los servicios de apoyo de tercer nivel para los elementos críticos de red en un plazo de 30 días a partir de la entrada en vigor de la presente Ley general.

(3) La Agencia publicará por primera vez los documentos a que se refiere el artículo 3, apartado 2, de la presente Ley general a partir de la fecha de su entrada en vigor.

Artículo 10
(Entrada en vigor)

La presente Ley general entrará en vigor el trigésimo día después de su publicación en el Boletín Oficial de la República de Eslovenia, mediante la cual los operadores podrán utilizar el equipo y mantener la prestación de servicios de apoyo de tercer nivel hasta la expiración de los plazos especificados en el artículo 312, apartados 2 y 3, de la Ley.

N.º . _____ mag. Marko Mišmaš

Liubliana, a _____ director

EVA 2023-3150-0034

PROPUESTA

PROPUESTA

Anexo

Lista de elementos críticos de red y sistemas de información asociados:

Elementos críticos de red	**Funcionalidades de la red y de los sistemas de información**
Mecanismos de gestión y encriptación de abonados	- Gestión de sesiones (voz y datos), - autenticación de usuarios y equipos con la red, - gestión y almacenamiento de claves para la autorización de abonados y componentes de red (UICC/eUICC, certificados digitales/HSM), - funciones de autenticación segura, protección de la integridad de la comunicación (encriptación) y almacenamiento de claves de usuario, componentes de red y de gestión, - gestión de los derechos de acceso.
Interconexión	- Características de alojamiento e interfaces a otras redes y servicios.
Servicios de red gestionados	- Registro y autorización de servicios de red, - almacenamiento y tratamiento de datos de comunicación, ubicación y tráfico, - exposición de la red y las funciones de red y a aplicaciones y servicios externos.
Gestión y orquestación de funciones de red virtualizadas (NFV) y orquestación de redes (MANO), incluida la infraestructura de virtualización	- Funciones de gestión de orquestación y configuración de NFV independientemente del tipo de implementación (VM, contenedor, microservicios), - funciones de virtualización para la implementación y uso de NFV, - función de selección de fragmentación de red (*Network Slice Selection Function*, NSSF).
Red de acceso por radio	- Estaciones base que soportan tecnología 5G o superior.
Sistemas de gestión y otros sistemas de apoyo	- Supervisar el funcionamiento y la gestión de la red de comunicaciones móviles, incluida la parte de acceso (RAN/O-RAN), - sistemas para detectar eventos de seguridad, anomalías, amenazas y su gestión (funciones de seguridad incluyendo SIEM/SOAR).
Interceptación legal	- Funciones de acceso a los contenidos de comunicación y a los datos sobre el tráfico de usuarios por parte de la autoridad competente.