EIOPA-BoS-20/600

Directrices sobre gobernanza y seguridad de las tecnologías de la información y de las comunicaciones

EIOPA – Westhafen Tower, Westhafenplatz 1 - 60327 Fráncfort – Alemania - Tel. + 49 69-951119-20;
Fax + 49 69-951119-19; correo electrónico: info@eiopa.europa.eu sitio web: www.eiopa.europa.eu

Índice

Información general

1. De conformidad con el artículo 16 del Reglamento (UE) n.º 1094/2010, del Parlamento Europeo y del Consejo, de 24 de noviembre de 2010, por el que se crea una Autoridad Europea de Seguros y Pensiones de Jubilación (AESPJ), la AESPJ puede emitir directrices y recomendaciones dirigidas a las autoridades competentes y a entidades financieras con vistas a establecer unas prácticas de supervisión consistentes, eficaces y efectivas y garantizar la aplicación común, uniforme y consistente del Derecho de la Unión.

2. En virtud de lo dispuesto en el apartado 3 de dicho artículo, las autoridades competentes y las entidades financieras harán todo lo posible para cumplir estas Directrices y recomendaciones.

3. La AESPJ detectó la necesidad de desarrollar una orientación específica sobre la gobernanza y la seguridad de las tecnologías de la información y de las comunicaciones (TIC) en relación con los artículos 41 y 44 de la Directiva 2009/138/CE en el contexto del análisis llevado a cabo para responder al Plan de Acción en materia de Tecnología Financiera de la Comisión Europea [COM(2018)0109 final)], el Plan de Convergencia en Materia de Supervisión de la AESPJ 2018-2019[1] y las interacciones siguientes con otras diversas partes interesadas[2].

4. Como se comunicó en el Consejo Conjunto de las Autoridades Europeas de Supervisión a la Comisión Europea, las Directrices de la AESPJ sobre el sistema de gobernanza «*no reflejan adecuadamente la importancia de tener cuidado con la gestión de los riesgos de TIC (incluidos los riesgos de ciberseguridad)*. No existen orientaciones sobre elementos esenciales que generalmente se consideran parte de una seguridad y una gobernanza adecuadas de las TIC».

5. El análisis de la situación (legislativa) actual en la UE respecto del Consejo Conjunto mencionado mostró que la mayoría de los Estados miembros de la UE han establecido normas nacionales en materia de seguridad y gobernanza de las TIC. Aunque los requisitos son similares, el marco regulador sigue fragmentado. Además, un estudio sobre las actuales prácticas de supervisión reveló una amplia variedad de ellas, desde «sin supervisión específica» hasta «supervisión rigurosa» (incluidas las «inspecciones remotas» y las «inspecciones *in situ*»).

6. Por añadidura, la complejidad de las TIC va en aumento, así como la frecuencia de los incidentes asociados a dichas tecnologías (incluidos los ciberincidentes), con el consiguiente impacto negativo de tales incidentes en el funcionamiento operativo de las empresas. Por tal motivo, la gestión de los riesgos de TIC y seguridad es fundamental para que una empresa pueda lograr sus objetivos estratégicos, corporativos, operativos y de reputación.

7. Adicionalmente, en todo el sector de los seguros, incluidos tanto los modelos de negocio tradicionales como los innovadores, la prestación de los servicios de seguros y el funcionamiento operativo normal de las empresas se basa cada vez más en las TIC, por ejemplo la digitalización del sector de los seguros (tecnología aplicada al sector de los seguros, internet de las cosas, etc.), así como la interconexión mediante canales de telecomunicaciones (internet, conexiones móviles e inalámbricas y redes de área amplia). Esto hace que las operaciones de

[1] https://www.eiopa.europa.eu/supervisory-convergence-plans-and-reports_en

[2] El informe publicado por la ~~EIOPA~~AESPJ en respuesta al Plan de Acción en materia de Tecnología Financiera de la Comisión Europea se puede consultar aquí.

las empresas sean vulnerables a los incidentes de seguridad, como los ciber ataques. Por lo tanto, es importante asegurarse de que las empresas estén adecuadamente preparadas para gestionar sus riesgos de TIC y seguridad.

8. Además de reconocer la necesidad de que las empresas estén preparadas para los riesgos cibernéticos[3] y cuenten con un marco de ciberseguridad sólido, las presentes Directrices también abarcan la ciberseguridad dentro del ámbito de las medidas empresariales de seguridad de la información. Aunque en las presentes Directrices se reconoce que la ciberseguridad se debe abordar como parte de la gestión global del riesgo de TIC y seguridad de la empresa, cabe señalar que los ataques cibernéticos presentan ciertas características específicas, que se deben tener en consideración para asegurarse de que las medidas de seguridad de la información mitigan debidamente el riesgo cibernético:

   a) los ataques cibernéticos son a menudo más complicados de gestionar (por ejemplo para su identificación, protección, detección, respuesta y para su completa recuperación) que la mayoría del resto de fuentes de riesgos de TIC y seguridad, siendo por añadidura difícil de determinar el alcance de los daños;

   b) algunos ataques cibernéticos pueden menoscabar la eficacia de las medidas comunes de gestión de riesgos y continuidad del negocio, así como hacer inefectivos los procedimientos de recuperación en caso de catástrofes, ya que podrían propagar programas maliciosos a los sistemas de copia de respaldo a fin de anularlos o corromper los datos almacenados en copia de respaldo;

   c) los proveedores de servicios, los corredores, los agentes y los intermediarios (de seguros) pueden convertirse en vectores de propagación de los ataques cibernéticos. Las amenazas de contagio silenciosas pueden utilizar la interconectividad mediante enlaces de telecomunicaciones de terceros para llegar al sistema de TIC de la empresa. En consecuencia, una empresa interconectada con escasa relevancia individual podría ser vulnerable y una fuente de propagación del riesgo, acarreando así un impacto sistémico. Con arreglo al principio del eslabón más débil, la ciberseguridad no debería ser un factor de preocupación solo para los principales participantes en el mercado o los proveedores de servicios esenciales.

9. El objetivo de las presentes Directrices es:

   a) aportar aclaraciones y transparencia a los participantes en el mercado sobre las capacidades mínimas previstas de ciberseguridad y seguridad de la información, es decir, la referencia en materia de seguridad;

   b) evitar posibles arbitrajes regulatorios;

   c) fomentar la convergencia en la supervisión con relación a las expectativas y los procesos aplicables respecto de la seguridad y la gobernanza de las TIC como factor clave para una gestión adecuada del riesgo de TIC y seguridad.

[3] Para una definición de riesgo cibernético, consulte el ciberléxico del Consejo de Estabilidad Financiera, 12 de noviembre de 2018, https://www.fsb.org/wp-content/uploads/P121118-1.pdf

Directrices sobre gobernanza y seguridad de las tecnologías de la información y de las comunicaciones

Introducción

1. De conformidad con el artículo 16 del Reglamento (UE) n.º 1094/2010[4], la AESPJ emite estas Directrices dirigidas a las autoridades de supervisión para aportar una orientación sobre cómo las empresas de seguros y reaseguros (en conjunto, las «empresas») deben aplicar los requisitos de gobernanza previstos en la Directiva 2009/138/CE[5] («Directiva Solvencia II») y en el Reglamento Delegado de la Comisión (UE) n.º 2015/35[6] («Reglamento Delegado») en el contexto de la seguridad y la gobernanza de las tecnologías de la información y de las comunicaciones («TIC»). A tal efecto, las presentes Directrices se basan en las disposiciones en materia de gobernanza a que se refieren los artículos 41, 44, 46, 47, 132 y 246 de la Directiva Solvencia II y los artículos 258 a 260, 266, 268 a 271 y 274 del Reglamento Delegado. Por añadidura, las presentes Directrices se fundamentan asimismo en la orientación brindada por las Directrices de la AESPJ sobre el sistema de gobernanza (EIOPA-BoS-14/253)[7] y por las Directrices de la AESPJ sobre la externalización a proveedores de servicios en la nube (EIOPA-BoS-19/270)[8].
2. Las Directrices se aplican tanto a empresas individuales como, *mutatis mutandis*, a nivel de grupo[9].
3. Al cumplir o supervisar el cumplimiento de las presentes Directrices, las autoridades competentes deberán tener en cuenta el principio de proporcionalidad[10], que ha de garantizar que el sistema de gobernanza, incluidas las medidas relacionadas con la seguridad y la gobernanza de las TIC, es proporcionado a la naturaleza, la escala y la complejidad de los correspondientes riesgos a los que se enfrentan o se pueden enfrentar las empresas.
4. Las presentes Directrices se deben leer junto a y sin perjuicio de la Directiva de Solvencia II, el Reglamento Delegado, las Directrices de la AESPJ sobre el sistema de gobernanza y las Directrices de la AESPJ sobre la externalización a proveedores de servicios en la nube. Estas Directrices pretenden ser neutrales desde los puntos de vista tecnológico y metodológico.

Definiciones

5. Si no se definen en las presentes Directrices, los términos tendrán el significado que se les atribuye en la Directiva Solvencia II.
6. A los efectos de las presentes Directrices, se entenderá por:

---

[4] Reglamento (UE) n.º 1094/2010 del Parlamento Europeo y del Consejo, de 24 de noviembre de 2010, por el que se crea una Autoridad Europea de Supervisión (Autoridad Europea de Seguros y Pensiones de Jubilación), se modifica la Decisión n.º 716/2009/CE y se deroga la Decisión n.º 2009/79/CE de la Comisión (DO L 331 de 15.12.2010, p. 48).

[5] Directiva 2009/138/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, sobre el seguro de vida, el acceso a la actividad de seguro y de reaseguro y su ejercicio (Solvencia II), DO L 335 de 17.12.2019, p. 1.

[6] Reglamento Delegado (UE) 2015/35 de la Comisión, de 10 de octubre de 2014, por el que se completa la Directiva 2009/138/CE del Parlamento Europeo y del Consejo sobre el acceso a la actividad de seguro y de reaseguro y su ejercicio (Solvencia II), DO L 12, 17.1.2015, p. 1.

[7] https://www.eiopa.europa.eu/content/guidelines-system-governance_en?source=search

[8] https://www.eiopa.europa.eu/sites/default/files/publications/eiopa_guidelines/guidelines_on_outsourcing_to_cloud_service_providers_cor_es_0.pdf

[9] Artículo 212, apartado 1, de la Directiva 2009/138/CE.

[10] Artículo 29, apartado 3, de la Directiva 2009/138/CE.

Propietario del activo	Persona física o jurídica con la responsabilidad y la autoridad sobre un activo de información y de TIC.
Disponibilidad	Propiedad de ser accesible y utilizable previa petición (conveniencia) por una persona jurídica autorizada.
Confidencialidad	Propiedad de que la información no se ponga a disposición o se divulgue a terceros, entidades, procesos o sistemas no autorizados.
Ataque cibernético	Cualquier tipo de intrusión informática que conlleve un intento ofensivo o malicioso de destruir, revelar, modificar, desactivar, robar, obtener un acceso no autorizado o hacer un uso no autorizado de un activo de información dirigida contra sistemas de TIC.
Ciberseguridad	Preservación de la confidencialidad, la integridad y la disponibilidad de la información o los sistemas de información a través del medio cibernético.
Activo de TIC	Activo de *software* o *hardware* que se encuentra en el entorno empresarial.
Proyectos de TIC	Cualquier proyecto, o parte del mismo, en el que se modifiquen, reemplacen o implementen sistemas y servicios de TIC.
Riesgo de TIC y seguridad	Como subcomponente del riesgo operativo, el riesgo de pérdida debido a la violación de la confidencialidad, al fallo de la integridad de los sistemas y los datos, a la inadecuación o indisponibilidad de los sistemas y los datos o a la incapacidad de cambiar las TIC en un plazo y costes razonables, cuando cambian las necesidades del entorno o del negocio (es decir, la agilidad). Esto incluye los riesgos cibernéticos, así como los riesgos de seguridad de la información resultantes de procesos internos que fallen o no sean adecuados o de acontecimientos externos, incluidos los ataques cibernéticos o una seguridad física no adecuada.
Seguridad de la información	Preservación de la confidencialidad, la integridad y la disponibilidad de la información o los sistemas de información. Además, también pueden verse implicadas otras propiedades, como la autenticidad, la responsabilidad, el consentimiento y la fiabilidad.

Servicios de TIC	Servicios prestados mediante sistemas y proveedores de servicios de TIC a uno o más usuarios internos o externos.
Sistemas de TIC	Conjunto de aplicaciones, servicios, activos de tecnología de la información, activos de TIC u otros componentes de manejo de la información, que incluye el entorno operativo.
Activo de información	Recopilación de información, tangible o intangible, que merece la pena proteger.
Integridad	Propiedad de precisión y completitud.
Incidente operativo o de seguridad	Situación particular o serie de situaciones relacionadas no planificadas que tengan o puedan tener un impacto negativo en la integridad, la disponibilidad y la confidencialidad de los sistemas y servicios de TIC.
Proveedor de servicios	Un tercero que realiza un proceso, servicio o actividad, o partes de los mismos, con arreglo a un acuerdo de externalización.
Prueba de intrusión dirigida sobre amenaza (threat-led penetration testing en inglés)	Un intento controlado de comprometer la resistencia cibernética de una entidad simulando las tácticas, técnicas y procedimientos de los autores de las amenazas de la vida real. Se basa en inteligencia de amenazas dirigida y se centra en las personas, los procesos y la tecnología de una entidad, con un conocimiento previo y un impacto mínimos en las operaciones.
Vulnerabilidad	Una deficiencia, una susceptibilidad o un defecto de un activo o control que una o varias amenazas pueden aprovechar.

7. Las presentes Directrices serán de aplicación a partir del 1 de julio de 2021.

Directriz 1 – Proporcionalidad

8. Las empresas deberán aplicar las presentes Directrices de una manera proporcionada a la naturaleza, la escala y la complejidad de los riesgos inherentes a sus actividades.

Directriz 2 – TIC dentro del sistema de gobernanza

9. El órgano de administración, de dirección o supervisión de la empresa (en lo sucesivo, "OADS") deberá velar por que el sistema de gobernanza de las empresas,

en especial el sistema de gestión de riesgos y control interno, gestione adecuadamente sus riesgos de TIC y seguridad.

10. El OADS garantizará que la cifra de personal de las empresas y sus capacidades sean adecuadas para apoyar sus necesidades operativas de TIC y sus procesos de gestión de riesgos de TIC y seguridad de manera continuada y velará por la aplicación de su estrategia de TIC. Por añadidura, el personal deberá recibir de manera periódica la formación oportuna sobre riesgos de TIC y seguridad, incluida la seguridad de la información, según lo expuesto en la Directriz 13.

11. El OADS garantizará que los recursos asignados son adecuados para cumplir los requisitos anteriores.

Directriz 3 – Estrategia de TIC

12. El OADS tendrá la responsabilidad general de establecer y aprobar la estrategia de TIC escrita de las empresas en el marco de su estrategia empresarial general y en consonancia con esta, así como de supervisar su comunicación y aplicación.

13. En la estrategia de TIC se deberá definir, como mínimo:

    a) cómo deben evolucionar las TIC de las empresas para apoyar y aplicar con eficacia su estrategia empresarial, incluida la evolución de la estructura organizativa, los modelos de negocio, el sistema de TIC y las principales dependencias con proveedores de servicios;

    b) la evolución de la arquitectura de TIC, incluidas las dependencias con proveedores de servicios; y

    c) unos objetivos de seguridad de la información claros, centrados en los sistemas y los servicios, el personal y los procesos de TIC.

14. Las empresas deberán garantizar que la estrategia de TIC se aplica, adopta y comunica a todo el personal y los proveedores de servicios pertinentes, según sea aplicable y relevante, de manera oportuna.

15. Las empresas también establecerán un proceso para realizar un seguimiento y medir la eficacia de la aplicación de la estrategia de TIC. Dicho proceso debe ser objeto de revisiones y actualizaciones de manera periódica.

Directriz 4 – Riesgos de TIC y seguridad en el ámbito del sistema de gestión de riesgos

16. El OADS tiene la responsabilidad general de establecer un sistema efectivo para gestionar los riesgos de TIC y seguridad como parte del sistema global de gestión de riesgos de la empresa. Esto incluye la determinación de la tolerancia a tales riesgos, de conformidad con la estrategia sobre riesgos de la empresa, así como un informe periódico escrito sobre el resultado del proceso de gestión de riesgos dirigido al OADS.

17. Como parte de su sistema global de gestión de riesgos, las empresas deberán considerar al menos lo siguiente en relación con los riesgos de TIC y seguridad (al definir los requisitos de protección de TIC, según se describen más adelante):

    a) las empresas deberán establecer y actualizar periódicamente un mapa de sus procesos y actividades comerciales, así como de sus cargos, funciones y activos de negocio (p. ej., activos de información y activos de TIC) a fin de identificar su importancia y sus interdependencias con los riesgos de TIC y seguridad;

b) las empresas deberán identificar y medir todos los riesgos de TIC y seguridad pertinentes a los que están expuestas y clasificar los procesos y actividades de negocio, así como las funciones, los roles y los activos de negocio identificados (p. ej., los activos de información y los activos de TIC) según su importancia. Las empresas deberán valorar asimismo los requisitos de protección de, al menos, la confidencialidad, la integridad y la disponibilidad de dichos procesos y actividades de negocio, así como de las funciones, los roles y los activos de negocio (p. ej., los activos de información y los activos de TIC). Se deberá identificar a los propietarios de los activos, responsables de su clasificación;

c) los métodos utilizados para determinar la importancia, así como el nivel de protección necesario, en especial con respecto a los objetivos de protección de la integridad, la disponibilidad y la confidencialidad, deberán garantizar que los requisitos de protección resultantes son consistentes y exhaustivos;

d) la medición de los riesgos de TIC y seguridad se deberá llevar a cabo con arreglo a los criterios definidos al respecto, teniendo en consideración la importancia de los procesos y actividades de negocio y de las funciones, los roles y los activos de negocio (p. ej., los activos de información y los activos de TIC), el alcance de las vulnerabilidades conocidas y los incidentes que afectaron a la empresa en el pasado;

e) la evaluación de los riesgos de TIC y seguridad se deberá realizar y documentar periódicamente. Dicha evaluación se deberá acometer igualmente antes de cualquier modificación importante de la infraestructura, los procesos o los procedimientos que afectan a los procesos y actividades de negocio y a las funciones, los roles y los activos de negocio (p. ej., los activos de información y los activos de TIC);

f) con arreglo a su evaluación de riesgos, las empresas deberán como mínimo definir y aplicar medidas para gestionar los riesgos de TIC y seguridad identificados y proteger los activos en materia de información de conformidad con su clasificación. Esto deberá incluir la definición de medidas para gestionar los riesgos residuales restantes.

18. Los resultados del proceso de gestión de riesgos de TIC y seguridad deberán ser aprobados por el OADS e incluidos en el proceso de gestión de los riesgos operativos en el ámbito de la gestión global de riesgos de la empresa.

Directriz 5 – Auditoría

19. La gobernanza, los sistemas y los procesos de las empresas para sus riesgos de TIC y seguridad deberán ser auditados de manera periódica y en consonancia con su correspondiente plan de auditoría[11] por unos auditores dotados de unos conocimientos, unas competencias y una experiencia suficientes en riesgos de TIC y seguridad, a fin de garantizar de manera independiente su eficacia al OADS. La frecuencia y el objeto de estas auditorías deberán ser adecuados a los riesgos de TIC y seguridad pertinentes.

Directriz 6 – Política y medidas de seguridad de la información

20. Las empresas deberán instaurar una política escrita de seguridad de la información aprobada por el OADS en la que se deberán definir los principios de alto nivel y las

[11] Artículo 271 del Reglamento Delegado.

normas para proteger la confidencialidad, la integridad y la disponibilidad de la información de las empresas a fin de respaldar la aplicación de la estrategia de TIC.

21. La política deberá incluir una descripción de las principales funciones y responsabilidades para la gestión de la seguridad de la información y en ella se habrán de establecer los requisitos del personal, los procesos y la tecnología en relación con la seguridad de la información, poniendo de manifiesto que el personal de todos niveles tiene responsabilidades a la hora de garantizar dicha seguridad en las empresas.

22. La política se deberá comunicar en el seno de la empresa y deberá ser de aplicación a todo el personal. Cuando sea aplicable y pertinente, la política de seguridad de la información o partes de la misma se deberán comunicar y aplicar también a los proveedores de servicios.

23. Con arreglo a la política, las empresas deberán establecer e instaurar procedimientos y medidas de seguridad de la información más específicas para, entre otras cosas, mitigar los riesgos de TIC y seguridad a los que estén expuestas. Entre dichos procedimientos y medidas de seguridad de la información se deberán incluir todos los procesos descritos en las presentes Directrices, en su caso.

Directriz 7 – Función de seguridad de la información

24. Las empresas deberán establecer, dentro de su sistema de gobernanza y de acuerdo con el principio de proporcionalidad, una función de seguridad de la información, asignando las correspondientes responsabilidades a una persona específica. La empresa garantizará la independencia y objetividad de la función de seguridad de la información separándola de forma adecuada de los procesos de desarrollo y operaciones de TIC. La función dependerá del OADS.

25. Los cometidos de la función de seguridad de la información serán normalmente:

    a) apoyar al OADS a definir y mantener la política de seguridad de la información para las empresas y controlar su implantación;

    b) informar y aconsejar al OADS periódicamente y en momentos puntuales sobre la situación de seguridad de la información y su evolución;

    c) supervisar y revisar la aplicación de las medidas de seguridad de la información;

    d) asegurarse de que al utilizar proveedores de servicios se cumplen los requisitos de seguridad de la información;

    e) asegurarse de que todos los empleados y proveedores de servicios que acceden a la información y los sistemas son adecuadamente informados de la política de seguridad de la información, por ejemplo mediante sesiones de formación y sensibilización al respecto;

    f) coordinar el análisis de los incidentes operativos o de seguridad y comunicar los más relevantes al OADS.

Directriz 8 – Seguridad lógica

26. Las empresas deberán definir, documentar e instaurar procedimientos para el control del acceso lógico o la seguridad lógica (gestión de la identidad y los accesos) en consonancia con los requisitos de protección establecidos en la Directriz 4. Dichos procedimientos se deberán instaurar, aplicar, supervisar y revisar periódicamente y, además, habrán de incluir controles para la supervisión de irregularidades. Estos

procedimientos deberán, como mínimo, aplicar los siguientes elementos, en los que el término «usuario» también incluye a los usuarios técnicos:

a) necesidad de conocer, privilegio mínimo y separación de funciones: las empresas deberán gestionar los derechos de acceso, incluido el acceso remoto a los activos de información y sus sistemas de apoyo según el principio de «necesidad de conocer». A los usuarios se les deben conceder los derechos de acceso mínimos que sean estrictamente necesarios para ejercer sus funciones (principio del «privilegio mínimo»), a fin de evitar el acceso no justificado a datos o la asignación de combinaciones de derechos de acceso que puedan ser utilizados para eludir controles (principio de «separación de funciones»);

b) responsabilidad del usuario: las empresas deberán limitar, en la medida de lo posible, el uso de cuentas de usuario genéricas y compartidas y asegurarse de poder identificar y rastrear en todo momento a los usuarios hasta una persona física responsable o una tarea autorizada respecto de las acciones llevadas a cabo en los sistemas de TIC;

c) derechos de acceso privilegiado: las empresas deberán aplicar controles sólidos sobre el acceso privilegiado a los sistemas mediante la limitación estricta y la supervisión rigurosa de las cuentas con derechos de acceso elevado a los sistemas (por ejemplo, cuentas de administración);

d) acceso remoto: con el fin de garantizar una comunicación segura y reducir el riesgo, el acceso administrativo remoto a sistemas de TIC esenciales solo se concederá según el principio de «necesidad de conocer» y en caso de que se usen soluciones de autenticación muy seguras;

e) registro de las actividades del usuario: las actividades de los usuarios se deberán registrar y supervisar de una manera proporcionada al riesgo, incluyendo como mínimo las actividades de los usuarios privilegiados. Los registros de acceso se protegerán para evitar modificaciones o supresiones no autorizadas y se conservarán durante un periodo definido por la criticidad de las funciones empresariales, los procesos de apoyo y los activos de información identificados, sin perjuicio de los requisitos de conservación estipulados en la legislación nacional y de la Unión Europea. Las empresas usarán dicha información para facilitar la identificación y la investigación de actividades irregulares que se hayan detectado en la prestación de los servicios;

f) gestión de los accesos: los derechos de acceso se deberán conceder, suprimir y modificar de una manera oportuna, de acuerdo con rutinas predefinidas de aprobación en las que participe el propietario del activo de información oportuno. En caso de que el acceso ya no resulte necesario, los derechos de acceso se deberán revocar inmediatamente;

g) evaluación de los accesos: los derechos de acceso deberán revisarse periódicamente para garantizar que los usuarios no poseen privilegios excesivos y que los derechos de acceso se retiran o suprimen cuando ya no son necesarios;

h) la concesión, la modificación y la revocación de los derechos de acceso se deberán documentar de manera que se facilite su comprensión y análisis; y

i) métodos de autenticación: las empresas deberán aplicar métodos de autenticación suficientemente sólidos para garantizar de forma adecuada y eficaz el cumplimiento de las políticas y los procedimientos de control de

acceso. Los métodos de autenticación deberán ser adecuados a la criticidad de los sistemas de TIC, la información o el proceso a los que se accede. Estos deberán incluir, como mínimo, contraseñas fuertes o métodos de autenticación más seguros (como la autenticación de dos factores), en función del riesgo pertinente.

27. El acceso electrónico por parte de las aplicaciones a los datos y sistemas de TIC deberá limitarse al mínimo imprescindible para prestar el servicio correspondiente.

Directriz 9 – Seguridad física

28. Las medidas de seguridad física de las empresas (p. ej., protección contra interrupciones del suministro eléctrico, incendios, inundaciones y accesos físicos no autorizados) se deberán definir, documentar y aplicar para proteger sus instalaciones, centros de datos y áreas sensibles contra el acceso no autorizado y los peligros ambientales.

29. El acceso físico a los sistemas de TIC se permitirá únicamente a las personas autorizadas. La autorización se asignará conforme a las tareas y responsabilidades de la persona y se deberá limitar a aquellas personas que cuenten con la formación adecuada y a las que se supervise de manera oportuna. El acceso físico deberá revisarse con regularidad para garantizar que los derechos de acceso no necesarios se revocan o suprimen inmediatamente.

30. Las medidas adecuadas para proteger de peligros ambientales deberán ser acordes a la importancia de los edificios y la criticidad de las operaciones o sistemas de TIC ubicados en ellos.

Directriz 10 – Seguridad de las operaciones de TIC

31. Las empresas deberán instaurar procedimientos para garantizar la confidencialidad, la integridad y la disponibilidad de los sistemas y servicios de TIC a fin de minimizar en consecuencia el impacto de los problemas de seguridad en la prestación de servicios de TIC. Estos procedimientos deberán incluir en su caso las siguientes medidas:

    a) identificación de vulnerabilidades potenciales, que deberán evaluarse y corregirse garantizando que los sistemas de TIC están actualizados, incluido el *software* proporcionado por las empresas a sus usuarios internos y externos, desarrollando parches de seguridad críticos, incluyendo actualizaciones de las definiciones de los antivirus o aplicando controles de compensación;

    b) implementación de referencias de configuración seguras para todos los componentes esenciales, como sistemas operativos, bases de datos, rúters o conmutadores;

    c) implementación de segmentación de red, sistemas de prevención de pérdida de datos y cifrado del tráfico de red (de conformidad con la clasificación de los activos de información);

    d) implementación de protección de los terminales, incluidos los servidores, las estaciones de trabajo y los dispositivos móviles. Las empresas deberán evaluar si un terminal reúne los estándares de seguridad definidos por ellas antes de concederle acceso a la red corporativa;

    e) garantizar que hay instaurados mecanismos de control de la integridad para comprobar la integridad de los sistemas de TIC;

f) cifrado de datos en reposo y en tránsito (de conformidad con la clasificación de los activos de información).

Directriz 11 – Supervisión de la seguridad

32. Las empresas deberán establecer e instaurar procedimientos y procesos para supervisar continuamente las actividades que inciden en la seguridad de su información. La supervisión abarcará al menos:

    a) los factores internos y externos, incluidas las funciones administrativas comerciales y de TIC;

    b) las transacciones de los proveedores de servicios, otras entidades y los usuarios internos; y

    c) las amenazas potenciales internas y externas.

33. En función de la supervisión, las empresas deberán aplicar unas capacidades apropiadas y efectivas para detectar, comunicar y responder a actividades irregulares y amenazas, como intrusiones físicas o lógicas, violaciones de la confidencialidad, la integridad y la disponibilidad de los activos de información, programas perjudiciales y vulnerabilidades conocidas en general de los equipos y programas informáticos.

34. Los informes de supervisión de la seguridad deberán ayudar a las empresas a comprender la naturaleza de los incidentes operativos o de seguridad, identificar tendencias y apoyar sus investigaciones internas, a fin de poder tomar las decisiones oportunas.

Directriz 12 – Revisiones, evaluaciones y pruebas de la seguridad de la información

35. Las empresas deberán realizar diversas revisiones, evaluaciones y pruebas de la seguridad de la información para garantizar la identificación eficaz de las vulnerabilidades en sus sistemas y servicios de TIC. Por ejemplo, las empresas podrán realizar análisis de deficiencias respecto de los estándares de seguridad de la información, revisiones del cumplimiento, auditorías internas y externas de los sistemas de información o revisiones de la seguridad física.

36. Las empresas deberán establecer y aplicar un marco de pruebas de la seguridad de la información que valide la solidez y la eficacia de sus medidas al respecto y garantizar que este marco considera las amenazas y vulnerabilidades identificadas mediante el seguimiento de amenazas y el proceso de evaluación de riesgos de TIC y seguridad.

37. Las pruebas se deberán llevar a cabo de una manera segura y protegida por profesionales independientes con el conocimiento, las capacidades y la experiencia suficientes en la realización de pruebas de medidas de seguridad de la información.

38. Las empresas deberán llevar a cabo pruebas de manera periódica. El alcance, la frecuencia y el método de las pruebas (como las pruebas de penetración, incluidas las pruebas de intrusión dirigida sobre amenaza (threat-led penetration testing)) deberán ser acordes al nivel de riesgo detectado. Las pruebas de los sistemas de TIC esenciales y los análisis de vulnerabilidades se deberán llevar a cabo anualmente.

39. Las empresas deberán garantizar que se realizan pruebas de las medidas de seguridad en el caso de cambios en la infraestructura, los procesos o procedimientos; también si se realizan cambios derivados de importantes incidentes

operativos o de seguridad o debido al lanzamiento de aplicaciones esenciales nuevas o modificadas de forma significativa. Las empresas controlarán y evaluarán los resultados de las pruebas de seguridad y actualizarán sus medidas de seguridad en consecuencia sin demoras injustificadas en el caso de los sistemas de TIC esenciales.

Directriz 13 – Formación y sensibilización sobre seguridad de la información

40. Las empresas deberán instaurar programas de formación sobre seguridad de la información para todo el personal, incluido el OADS, a fin de garantizar que reciben la formación necesaria para cumplir con sus obligaciones y responsabilidades y reducir los errores humanos, los robos, el fraude, los usos indebidos y las pérdidas. Las empresas deberán asegurarse de que el programa de formación se imparte a todo el personal de manera periódica.

41. Las empresas deberán instaurar y aplicar programas periódicos de sensibilización sobre seguridad de la información para enseñar a su personal, incluido el OADS, sobre cómo tratar los riesgos en la materia.

Directriz 14 – Gestión de las operaciones de TIC

42. Las empresas deberán gestionar sus operaciones de TIC con arreglo a su estrategia al respecto. En los documentos correspondientes se deberá definir cómo operan, supervisan y controlan las empresas los sistemas y los servicios de TIC, incluida la documentación de los procesos, los procedimientos y las operaciones esenciales.

43. Las empresas deberán aplicar procedimientos de seguimiento y registro de las operaciones de TIC esenciales con el objetivo de detectar, analizar y corregir los errores.

44. Las empresas deberán mantener un inventario actualizado de sus activos de TIC. El inventario de activos de TIC habrá de ser lo suficientemente detallado para permitir una identificación inmediata de un activo de TIC, su ubicación, clasificación de seguridad y propiedad.

45. Las empresas deberán realizar un seguimiento y gestionar el ciclo de vida de los activos de TIC para garantizar que continúan cumpliendo y respaldando las necesidades del negocio y de la gestión de riesgos. Las empresas deberán supervisar que sus proveedores y desarrolladores internos dan soporte a sus activos de TIC y que todos los parches y actualizaciones relevantes se aplican sobre la base de un proceso documentado. Deberán evaluarse y mitigarse los riesgos derivados de activos de TIC obsoletos o sin soporte. Los activos de TIC fuera de servicio deberán procesarse y eliminarse de una manera segura.

46. Las empresas deberán implementar procesos de planificación y seguimiento de la capacidad y el rendimiento para prevenir, detectar y dar respuesta a problemas importantes de rendimiento de los sistemas de TIC y a la escasez de capacidad de TIC de manera oportuna.

47. Las empresas deberán definir e implementar procedimientos de copia de seguridad y restauración de datos y sistemas de TIC para garantizar que puedan recuperarse si es preciso. El alcance y la frecuencia de las copias de seguridad deberán establecerse conforme a los requisitos de restauración de la empresa y la criticidad de los datos y los sistemas de TIC y valorarse según la evaluación de riesgos realizada. Deberán llevarse a cabo pruebas de los procedimientos de copia de seguridad y restauración de forma periódica.

48. Las empresas deberán asegurarse de que las copias de seguridad de los datos y el sistema de TIC se almacenan en uno o varios lugares diferentes del emplazamiento principal, seguros y lo suficientemente alejados de este para no estar expuestos a los mismos riesgos.

Directriz 15 – Gestión de incidentes y problemas de TIC

49. Las empresas deberán establecer y aplicar un proceso de gestión de incidentes y problemas para realizar un seguimiento y registrar los incidentes operativos o de seguridad y permitirles continuar o restablecer sus funciones y procesos esenciales si se producen interrupciones.

50. Las empresas determinarán los criterios y umbrales adecuados para clasificar un suceso como incidente operativo o de seguridad, así como los indicadores de alerta rápida que deben servir como aviso para permitir realizar una detección temprana de dichos incidentes.

51. Para minimizar el efecto de acontecimientos adversos y permitir una recuperación oportuna, las empresas deberán establecer procesos y estructuras organizativas apropiadas que garanticen un control, tratamiento y seguimiento integrado y coherente de los incidentes operativos y de seguridad para asegurarse de que se identifican y tratan las causas subyacentes y se toman acciones o medidas correctoras para evitar que se repita el incidente. El proceso de gestión de incidentes y problemas deberá establecer al menos:

    a) los procedimientos para identificar, seguir, registrar, categorizar y clasificar los incidentes según una prioridad definida por la empresa y basada en la criticidad para la misma y en acuerdos de servicio;

    b) las funciones y responsabilidades en el caso de distintos escenarios de incidentes (por ejemplo, errores, funcionamiento defectuoso, ciberataques, etc.);

    c) un procedimiento de gestión de problemas para identificar, analizar y resolver las causas subyacentes de uno o varios incidentes; las empresas deberán analizar los incidentes operativos o de seguridad que han sido identificados o han sucedido dentro o fuera de la organización y habrán de considerar las principales lecciones aprendidas de estos análisis y actualizar en consecuencia las medidas de seguridad;

    d) unos planes de comunicación interna eficaces, incluidos los procedimientos de elevación a otro nivel y notificación, que también abarquen las reclamaciones de los clientes relacionadas con la seguridad, para garantizar que:

        i. los incidentes con un efecto adverso potencialmente elevado sobre sistemas y servicios de TIC esenciales se notifican a la alta dirección pertinente;

        ii. se informa al OADS de manera *ad hoc* en el caso de incidentes significativos y, al menos, del efecto, la reacción y los controles adicionales que deben definirse en razón de los incidentes;

    e) procedimientos de respuesta para mitigar el impacto relacionado con los incidentes y garantizar que el servicio esté operativo y sea seguro de manera oportuna;

    f) planes específicos de comunicación externa para funciones y procesos esenciales de la empresa con el objetivo de:

i. colaborar con las partes interesadas pertinentes para responder con eficacia y recuperarse del incidente;

ii. ofrecer información a tiempo, incluidos los informes sobre los incidentes, a las partes externas [por ejemplo, clientes, otros participantes del mercado, las autoridades (de supervisión) pertinentes, etc. según corresponda y de conformidad con la normativa aplicable].

Directriz 16 – Gestión de proyectos de TIC

52. Las empresas deberán instaurar una metodología de proyectos de TIC (incluidas las consideraciones de requisitos de seguridad independientes) con un proceso de gobernanza y un liderazgo de aplicación de los proyectos adecuados para apoyar efectivamente la instauración de la estrategia de TIC mediante los proyectos en la materia.

53. Las empresas deberán realizar un seguimiento apropiado y mitigar los riesgos derivados de la cartera de proyectos de TIC, considerando también los riesgos que puedan resultar de las interdependencias entre proyectos distintos y de las dependencias de varios proyectos de los mismos recursos o conocimientos técnicos.

Directriz 17 – Adquisición y desarrollo de sistemas de TIC

54. Las empresas deberán desarrollar e instaurar un proceso que regule la adquisición, el desarrollo y el mantenimiento de sistemas de TIC a fin de asegurarse de que la confidencialidad, la integridad y la disponibilidad de los datos tratados se protegen exhaustivamente y de que se cumplen los requisitos de protección definidos. Este proceso deberá diseñarse según un enfoque basado en el riesgo.

55. Las empresas deberán garantizar que antes de que tengan lugar las actividades de adquisición o desarrollo de los sistemas se hayan definido claramente los requisitos funcionales y de diversa índole (incluido los requisitos de seguridad de la información) y los objetivos técnicos.

56. Las empresas deberán garantizar que hay medidas instauradas para impedir la modificación accidental o la manipulación intencional de los sistemas de TIC durante su desarrollo.

57. Las empresas deberán contar con una metodología para las pruebas y la aprobación de los sistemas y servicios de TIC y las medidas de seguridad de la información.

58. Las empresas deberán probar adecuadamente los sistemas y los servicios de TIC y las medidas de seguridad de la información para identificar posibles debilidades, violaciones e incidentes de seguridad.

59. Las empresas habrán de garantizar la separación de los entornos de producción de los de desarrollo, realización de pruebas y otros entornos ajenos a la producción.

60. Las empresas deberán aplicar medidas para proteger la integridad del código fuente (si se encuentra disponible) de los sistemas de TIC. También deberán documentar el desarrollo, la aplicación, la operación o la configuración de los sistemas de TIC de manera exhaustiva para reducir cualquier dependencia innecesaria de expertos en la materia.

61. Los procesos de las empresas para la adquisición y el desarrollo de sistemas de TIC también deberán aplicarse a los sistemas de TIC desarrollados o gestionados por los usuarios finales de una función de negocio externa a la organización de TIC (p. ej., aplicaciones gestionadas por la empresa o aplicaciones de computación para usuarios finales) según un enfoque basado en el riesgo. Las empresas deberán

mantener un registro de las aplicaciones que apoyan funciones o procesos comerciales esenciales.

Directriz 18 – Gestión de cambios de TIC

62. Las empresas deberán establecer y aplicar un proceso de gestión de cambios de TIC para garantizar que todos los cambios en los sistemas de TIC se registren, evalúen, prueben, aprueben, autoricen y apliquen de forma controlada. Los cambios de TIC durante situaciones de urgencia o emergencia deberán ser rastreables y notificarse al propietario del activo pertinente para su análisis *a posteriori*.

63. Las empresas deberán determinar si los cambios en el entorno operativo existente inciden en las medidas de seguridad presentes o si es necesaria la adopción de medidas adicionales para mitigar los riesgos que conllevan. Estos cambios deberán ser conformes con el proceso formal de gestión de cambios de las empresas.

Directriz 19 – Gestión de la continuidad del negocio

64. En el ámbito de la política global de continuidad del negocio de las empresas, el OADS tendrá la responsabilidad general de establecer y aprobar su política de continuidad de TIC. La política de continuidad de TIC deberá comunicarse adecuadamente en el seno de las empresas y aplicarse a todo el personal pertinente y, en su caso, a los proveedores de servicios.

Directriz 20 – Análisis de impacto en el negocio

65. En el marcado de una sólida gestión de la continuidad del negocio, las empresas deberán llevar a cabo un análisis de impacto en el negocio para evaluar su exposición a perturbaciones en el negocio graves y su posible repercusión, cuantitativa y cualitativa, utilizando datos internos o externos y análisis de escenarios. En el análisis de impacto en el negocio se deberá considerar asimismo la importancia de los procesos y actividades comerciales y de las funciones, los roles y los activos de negocio identificados y clasificados (p. ej., los activos de información y los activos de TIC), así como sus interdependencias, de conformidad con la Directriz 4.

66. Las empresas deberán garantizar que sus sistemas y servicios de TIC están diseñados y se hallan en consonancia con su análisis de impacto en el negocio, por ejemplo, mediante la redundancia de ciertos componentes esenciales para evitar interrupciones causadas por acontecimientos que impacten en dichos componentes.

Directriz 21 – Planificación de la continuidad del negocio

67. En los planes globales de continuidad del negocio de las empresas se deberán considerar los riesgos materiales que podrían afectar negativamente a los sistemas y los servicios de TIC. En los planes se deberán apoyar los objetivos que hay que proteger y, si es necesario, restablecer la confidencialidad, la integridad y la disponibilidad de los procesos y las actividades del negocio de las empresas, así como de las funciones, los roles y los activos de negocio (p. ej., los activos de información y los activos de TIC). Las empresas deberán coordinarse con las partes interesadas relevantes internas y externas, según corresponda, durante el establecimiento de estos planes.

68. Las empresas deberán instaurar planes de continuidad del negocio para asegurarse de que pueden reaccionar adecuadamente a posibles escenarios de fallos en un tiempo objetivo de recuperación (RTO, el tiempo máximo dentro del cual un sistema o un proceso se deberán restablecer tras un incidente) y un punto objetivo de

recuperación (RPO el máximo período temporal durante el cual se pueden perder datos en caso de un incidente bajo un nivel de servicio predefinido).

69. En sus planes de continuidad del negocio, las empresas deberán considerar un abanico de diferentes escenarios, incluidos aquellos extremos pero posibles y las situaciones de ataques cibernéticos, y evaluar su posible impacto. Sobre la base de estos escenarios, las empresas deberán describir cómo se garantizan la continuidad de los sistemas y servicios de TIC, así como la seguridad de su información.

Directriz 22 – Planes de respuesta y recuperación

70. Sobre la base del análisis de impacto en el negocio y escenarios recomendables, las empresas deberán elaborar planes de respuesta y recuperación. Estos planes deberán especificar qué condiciones pueden requerir su activación y qué acciones habrán de adoptarse para garantizar la integridad, disponibilidad, continuidad y la recuperación de, al menos, los sistemas, servicios y datos esenciales de las empresas. Los planes de respuesta y recuperación deberán tener como objetivo cumplir los objetivos de recuperación de las operaciones de las empresas.

71. Los planes de respuesta y recuperación deberán considerar opciones de recuperación tanto a corto plazo como, en su caso, a largo plazo. Como mínimo, los planes deberán:

    a) centrarse en la recuperación de las operaciones de importantes servicios de TIC, funciones de negocio, procesos auxiliares y activos de información y sus interdependencias a fin de evitar efectos adversos en el funcionamiento de la empresa;

    b) estar documentados y puestos a disposición de las unidades de negocio y de apoyo y ser fácilmente accesibles en caso de emergencia, incluida una definición clara de las funciones y las responsabilidades; y

    c) estar continuamente actualizados conforme a la experiencia adquirida durante los incidentes, las pruebas, los nuevos riesgos y amenazas identificados y los cambios en los objetivos y prioridades de recuperación.

72. Los planes también deberán considerar opciones alternativas cuando no sea posible la recuperación a corto plazo debido a los costes, los riesgos, la logística o circunstancias imprevistas.

73. Dentro de los planes de respuesta y recuperación, las empresas deberán considerar y aplicar medidas de continuidad para mitigar los incumplimientos de los proveedores de servicios, que son de una importancia clave para la continuidad de sus servicios de TIC (en consonancia con las disposiciones de las Directrices de la AESPJ sobre el sistema de gobernanza y de las Directrices de la AESPJ sobre la externalización a proveedores de servicios en la nube).

Directriz 23 – Pruebas de los planes

74. Las empresas deberán someter a pruebas sus planes de continuidad del negocio y asegurarse de que la operación de sus procesos y actividades de negocio críticos y de sus funciones, roles y activos de negocio esenciales (p. ej., los activos de información), así como de sus activos de TIC y sus interdependencias (incluidos los proporcionados por proveedores de servicios) se prueban periódicamente en función de su perfil de riesgo.

75. Los planes de continuidad del negocio deberán actualizarse periódicamente sobre la base de los resultados de las pruebas, conocimiento sobre amenazas actuales y las

lecciones aprendidas de sucesos anteriores. Se deberán incluir asimismo todos los cambios pertinentes en los objetivos de recuperación (incluido el tiempo objetivo de recuperación y el punto objetivo de recuperación) y/o los cambios en los procesos y las actividades de negocio y las funciones, los roles y los activos de negocio (p. ej., los activos de información y los activos de TIC).

76. Las pruebas de los planes de continuidad del negocio deberán demostrar que son capaces de mantener la viabilidad del negocio hasta el restablecimiento de las operaciones esenciales a un nivel de servicio o conforme a una tolerancia a impactos predefinidos.

77. Los resultados de las pruebas deberán documentarse y las deficiencias identificadas como resultado de las pruebas habrán de analizarse, tratarse y notificarse al OADS.

Directriz 24 – Comunicaciones de crisis

78. En el caso de que ocurra una interrupción o una emergencia y durante la implantación de los planes de continuidad del negocio, las empresas garantizarán que disponen de medidas eficaces de comunicación de crisis que permitan que todas las partes implicadas, incluidas las autoridades de supervisión pertinentes, cuando así lo requiera la normativa nacional, así como los proveedores de servicios pertinentes, sean informados de manera oportuna y adecuada.

Directriz 25 – Externalización de los servicios y los sistemas de TIC

79. Sin perjuicio de las Directrices de la AESPJ sobre la externalización a proveedores de servicios en la nube, las empresas deberán asegurarse de que, si se externalizan servicios y sistemas de TIC, se cumplen los requisitos pertinentes para el servicio o el sistema en cuestión.

80. En caso de externalización de funciones importantes o esenciales, las empresas deberán velar por que las obligaciones contractuales del proveedor de servicios (p. ej., contrato, acuerdos de nivel de servicio, disposiciones de rescisión en los contratos pertinentes) incluyan como mínimo:

    a) unos objetivos y unas mediciones de seguridad de la información apropiados y proporcionados, incluidas determinadas condiciones, como unos requisitos mínimos de seguridad de la información, especificaciones del ciclo de vida de los datos de las empresas, derechos de auditoría y acceso y cualesquiera requisitos relativos a la localización de los centros de datos y el cifrado de los mismos, la seguridad de la red y los procesos de supervisión de la seguridad;

    b) acuerdos de nivel de servicio, a fin de asegurar la continuidad de los servicios y los sistemas de TIC y los objetivos de rendimiento en circunstancias normales, así como los dispuestos en planes de contingencia en el supuesto de una interrupción del servicio; y

    c) procedimientos de gestión de incidentes de seguridad y operativos, incluidos el escalado de nivel y las notificaciones.

81. Las empresas deberán controlar y obtener garantías del nivel de cumplimiento de los objetivos de seguridad, las medidas y los objetivos de rendimiento por parte de los proveedores de servicios.

Normas sobre el cumplimiento y el deber de información

82. El presente documento contiene las Directrices emitidas en virtud del artículo 16 del Reglamento (UE) n.º 1094/2010. En virtud de lo dispuesto en el apartado 3 de dicho artículo, las autoridades competentes y las empresas harán todo lo posible para respetar las directrices y recomendaciones.

83. Las autoridades competentes que cumplan o tengan la intención de cumplir estas Directrices deberán incorporarlas debidamente a su marco regulador o supervisor.

84. Las autoridades competentes deberán confirmar a la AESP si cumplen o tienen la intención de cumplir estas Directrices, junto con los motivos de incumplimiento, en el plazo de dos meses tras la publicación de las versiones traducidas.

85. A falta de respuesta antes del plazo señalado, se considerará que las autoridades competentes no cumplen y se informará sobre ellas en consecuencia.

Disposición final sobre revisiones

86. Las presentes Directrices serán objeto de revisión por parte de la AESPJ.