BASE DE DATOS DE Norma CEF.-
Referencia: NCL013432

REGLAMENTO DE EJECUCIÓN (UE) 2024/2690, DE LA COMISIÓN, de 17 de octubre, por el que se establecen las disposiciones de aplicación de la Directiva (UE) 2022/2555 en lo que respecta a los requisitos técnicos y metodológicos de las medidas para la gestión de riesgos de ciberseguridad y en el que se detallan los casos en que un incidente se considera significativo con respecto a los proveedores de servicios de DNS, los registros de nombres de dominio de primer nivel, los proveedores de servicios de computación en nube, los proveedores de servicios de centro de datos, los proveedores de redes de distribución de contenidos, los proveedores de servicios gestionados, los proveedores de servicios de seguridad gestionados, los proveedores de mercados en línea, motores de búsqueda en línea y plataformas de servicios de redes sociales, y los proveedores de servicios de confianza.

(DOUE L, de 18 de octubre de 2024)

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Vista la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2), en particular su artículo 21, apartado 5, párrafo primero, y su artículo 23, apartado 11, párrafo segundo,

Considerando lo siguiente:

(1) En lo que se refiere a los proveedores de servicios de DNS, los registros de nombres de dominio de primer nivel, los proveedores de servicios de computación en nube, los proveedores de servicios de centros de datos, los proveedores de redes de distribución de contenidos, los proveedores de servicios gestionados, los proveedores de servicios de seguridad gestionados, los proveedores de mercados en línea, motores de búsqueda en línea y plataformas de servicios de redes sociales, así como los prestadores de servicios de confianza, tal como los contempla el artículo 3 de la Directiva (UE) 2022/2555 (en lo sucesivo, «las entidades pertinentes»), el presente Reglamento tiene por objeto establecer los requisitos técnicos y metodológicos de las medidas previstas en el artículo 21, apartado 2, de la Directiva (UE) 2022/2555 y detallar en qué casos un incidente debe considerarse significativo a tenor del artículo 23, apartado 3, de la Directiva (UE) 2022/2555.

(2) Teniendo en cuenta el carácter transfronterizo de las actividades y a fin de garantizar un marco coherente para los prestadores de servicios de confianza, el presente Reglamento debe, con respecto a los prestadores de servicios de confianza, precisar en qué casos un incidente se considerará significativo y establecer los requisitos técnicos y metodológicos de las medidas para la gestión de riesgos de ciberseguridad.

(3) De conformidad con el artículo 21, apartado 5, párrafo tercero, de la Directiva (UE) 2022/2555, los requisitos técnicos y metodológicos de las medidas para la gestión de riesgos de ciberseguridad previstos en el anexo del presente Reglamento se basan en normas europeas e internacionales, como las normas ISO/IEC 27001, ISO/IEC 27002 y ETSI EN 319401, o en especificaciones técnicas, como CEN/TS 18026: 2024, pertinentes para la seguridad de las redes y los sistemas de información.

(4) En lo que se refiere a la ejecución y la aplicación de los requisitos técnicos y metodológicos de las medidas para la gestión de riesgos de ciberseguridad establecidos en el anexo del presente Reglamento, de acuerdo con el principio de proporcionalidad, ha de tenerse debidamente en cuenta la distinta exposición al riesgo de las entidades pertinentes, en función de su carácter esencial, de los riesgos a los que estén expuestas, de su tamaño y estructura, o de la probabilidad de que se produzcan incidentes y su gravedad, incluidas las repercusiones sociales y económicas, cuando se cumplan los requisitos técnicos y metodológicos de las medidas para la gestión de riesgos que se establecen en el anexo del presente Reglamento.

(5) En consonancia con el principio de proporcionalidad, cuando las entidades pertinentes no puedan aplicar algunos de los requisitos técnicos y metodológicos de las medidas para la gestión de riesgos de ciberseguridad debido a su tamaño, dichas entidades deben poder adoptar otras medidas compensatorias que sean adecuadas para alcanzar los objetivos de dichos requisitos. Por ejemplo, a la hora de designar los roles, responsabilidades y autoridades relativos a la seguridad de los sistemas de redes y de información dentro de la entidad pertinente, las microentidades pueden toparse con dificultades para separar cometidos o áreas de responsabilidad que puedan

entrar en conflicto. Dichas entidades deben poder considerar medidas compensatorias, como, por ejemplo, una supervisión específica por parte de la dirección de la entidad, o un mayor seguimiento y registro.

(6) Las entidades pertinentes deben aplicar determinados requisitos técnicos y metodológicos establecidos en el anexo del presente Reglamento según proceda, cuando proceda o en la medida de lo posible. Cuando una entidad pertinente considere que no procede, que no resulta de aplicación o que no es posible aplicar determinados requisitos técnicos y metodológicos de acuerdo con lo previsto en el anexo del presente Reglamento, dicha entidad pertinente debe documentar de manera comprensible su razonamiento a tal efecto. Las autoridades nacionales competentes podrán, cuando ejerzan la supervisión, tener en cuenta el tiempo necesario para que las entidades pertinentes pongan en marcha los requisitos técnicos y metodológicos de las medidas para la gestión de riesgos de ciberseguridad.

(7) La ENISA o las autoridades nacionales competentes contempladas en la Directiva (UE) 2022/2555 pueden proporcionar orientaciones de apoyo a las entidades pertinentes en la detección, el análisis y la evaluación de riesgos a efectos de poner en práctica los requisitos técnicos y metodológicos relativos al establecimiento y mantenimiento de un marco de gestión de riesgos adecuado. Estas orientaciones pueden consistir, en particular, en evaluaciones de riesgos nacionales y sectoriales, así como en evaluaciones de riesgos específicas relativas a un determinado tipo de entidad. Las orientaciones también pueden facilitar herramientas o plantillas para el desarrollo del marco de gestión de riesgos a escala de las entidades pertinentes. Los marcos, las orientaciones u otros mecanismos previstos por la legislación de los Estados miembros, así como las normas europeas e internacionales correspondientes, también pueden servir de respaldo a las entidades pertinentes para demostrar el cumplimiento del presente Reglamento de ejecución. Además, la ENISA o las autoridades nacionales competentes contempladas en la Directiva (UE) 2022/2555 pueden respaldar a las entidades pertinentes en la búsqueda y puesta en marcha de soluciones adecuadas para tratar los riesgos detectados en las evaluaciones correspondientes. Las orientaciones deben entenderse sin perjuicio de la obligación de las entidades pertinentes de señalar y documentar los riesgos para la seguridad de los sistemas de redes y de información, ni de la obligación de dichas entidades de aplicar los requisitos técnicos y metodológicos de las medidas para la gestión de riesgos de ciberseguridad establecidos en el anexo del presente Reglamento, de conformidad con sus necesidades y recursos.

(8) Las medidas de seguridad de las redes en relación con: i) la transición hacia protocolos de comunicación de la capa de red de última generación, ii) el desarrollo de normas sobre las comunicaciones por correo electrónico modernas, interoperables y aprobadas a escala internacional, y iii) la aplicación de las mejores prácticas sobre seguridad del DNS, la seguridad del enrutamiento de internet y la higiene de enrutamiento conllevan riesgos específicos en lo que se refiere a la designación de las mejores normas disponibles y las técnicas de implantación. A fin de alcanzar lo antes posible un elevado nivel común de ciberseguridad en todas las redes, la Comisión, con la ayuda de la Agencia de la Unión Europea para la Ciberseguridad (ENISA) y, en colaboración con las autoridades competentes, la industria (especialmente la industria de las telecomunicaciones) y otras partes interesadas, debe respaldar el desarrollo de un foro multilateral encargado de determinar las mejores normas y técnicas de implantación disponibles. Estas orientaciones multilaterales deben entenderse sin perjuicio de la obligación de las entidades pertinentes de aplicar los requisitos técnicos y metodológicos de las medidas para la gestión de riesgos que se establecen en el anexo del presente Reglamento.

(9) De conformidad con el artículo 21, apartado 2, letra a), de la Directiva (UE) 2022/2555, además de contar con políticas de análisis de riesgos, las entidades esenciales e importantes deben disponer de políticas de seguridad de los sistemas de información. A tal efecto, las entidades pertinentes deben establecer políticas de seguridad de los sistemas de redes y de información y políticas temáticas (como, por ejemplo, políticas de control de acceso), que han de ser coherentes con las primeras. La política de seguridad de los sistemas de redes y de información debe ser el documento de más alto nivel en el que se establezca el enfoque global de las entidades pertinentes con respecto a la seguridad de sus sistemas de redes y de información y deben aprobarla los órganos de dirección de las entidades pertinentes. Las políticas temáticas debe aprobarlas el nivel de dirección adecuado. La política de seguridad debe establecer indicadores y medidas para supervisar su aplicación y el estado de madurez actual de la seguridad de los sistemas de redes y de información de las entidades pertinentes, en concreto para facilitar el control de la ejecución de las medidas para la gestión de riesgos de ciberseguridad por parte de los órganos de dirección.

(10) En lo que se refiere a los requisitos técnicos y metodológicos establecidos en el anexo del presente Reglamento, el término «usuario» debe englobar a todas las personas físicas y jurídicas que tengan acceso a los sistemas de redes y de información de la entidad.

(11) A fin de detectar y abordar los riesgos que se planteen para la seguridad de los sistemas de redes y de información, las entidades pertinentes deben establecer y mantener un marco de gestión de riesgos adecuado.

Como parte de este marco de gestión de riesgos, las entidades pertinentes deben establecer, poner en marcha y supervisar un plan de tratamiento de los riesgos. Las entidades pertinentes podrán utilizar el plan de tratamiento de los riesgos para detectar y priorizar las opciones y medidas de tratamiento de los riesgos. Las opciones para el tratamiento de los riesgos incluyen, en concreto, evitar, reducir o, en casos excepcionales, aceptar los riesgos. Las alternativas de tratamiento de los riesgos deben tener en cuenta los resultados de la evaluación de riesgos realizada por parte de la entidad pertinente y de conformidad con la política de esta última sobre la seguridad de los sistemas de redes y de información. Para hacer efectivas las opciones de tratamiento de riesgos elegidas, las entidades pertinentes deben adoptar las medidas oportunas de tratamiento de los riesgos.

(12) A fin de detectar sucesos, cuasiincidentes e incidentes, las entidades pertinentes deben supervisar sus sistemas de información y de redes y deben adoptar medidas para evaluar dichos sucesos, cuasiincidentes e incidentes. Estas medidas deben permitir la detección a su debido tiempo de ataques en la red utilizando patrones anómalos del tráfico de entrada o salida y ataques de denegación de servicio.

(13) Se anima a las entidades pertinentes a que, cuando lleven a cabo un análisis de impacto empresarial, este sea exhaustivo y establezca, según proceda, un tiempo de interrupción máximo tolerable, los objetivos de tiempo de recuperación y de punto de recuperación, y los objetivos de prestación de servicios.

(14) A fin de mitigar los riesgos derivados de la cadena de suministro de la entidad pertinente y de su relación con los proveedores, la entidad debe establecer una política de seguridad de la cadena de suministro que rija sus relaciones con los proveedores y prestadores de servicios directos. Además, las entidades deben establecer, en los contratos con los proveedores y los prestadores de servicios directos, cláusulas de seguridad adecuadas que exijan, cuando proceda, medidas para la gestión de los riesgos de ciberseguridad conforme al artículo 21, apartado 2, de la Directiva (UE) 2022/2555, u otras disposiciones legales similares.

(15) Las entidades pertinentes deben realizar pruebas de seguridad regulares, basadas en unas políticas y unos procedimientos específicos, para comprobar que las medidas para la gestión de riesgos de ciberseguridad se están aplicando y están funcionando adecuadamente. Las pruebas de seguridad podrán realizarse en sistemas de redes y de información concretos o en la entidad pertinente en su conjunto, y podrán incluir tests automáticos o manuales, pruebas de penetración, la exploración de vulnerabilidades, pruebas de seguridad de aplicaciones estáticas y dinámicas, pruebas de configuración o auditorías de seguridad. Las entidades pertinentes podrán efectuar las pruebas de seguridad de sus sistemas de redes y de información en el momento de instalarlos, después de mejoras en la infraestructura o de actualizaciones de las aplicaciones o de otras modificaciones que puedan resultar significativas, o tras una operación de mantenimiento. Las conclusiones de las pruebas de seguridad deben servir de referencia a las entidades pertinentes en sus políticas y procedimientos para evaluar la eficacia de las medidas para la gestión de riesgos de ciberseguridad, así como en las revisiones independientes de sus políticas de seguridad de las redes y de la información.

(16) A fin de evitar perturbaciones y daños significativos causados por la explotación de vulnerabilidades no subsanadas en los sistemas de redes y de información, las entidades pertinentes deben establecer y aplicar procedimientos adecuados para la gestión de los parches de seguridad que sean acordes a sus procedimientos de gestión de cambios, gestión de vulnerabilidades, gestión de riesgos u otros procedimientos relevantes. Las entidades pertinentes deben adoptar medidas proporcionales a sus recursos y asegurarse de que los parches de seguridad no introduzcan vulnerabilidades o inestabilidades adicionales. En caso de que se prevea la inaccesibilidad del servicio a causa de la aplicación de parches de seguridad, se anima a las entidades pertinentes a que informen de antemano a sus clientes.

(17) Las entidades pertinentes deben gestionar los riesgos derivados de la adquisición de productos o servicios TIC por parte de sus proveedores o de los prestadores de servicios y deben obtener garantías de que los productos o servicios TIC que van a adquirir alcanzan determinados niveles de protección de la ciberseguridad mediante, por ejemplo, certificados europeos de ciberseguridad o declaraciones de conformidad de la UE para servicios o productos TIC expedidos con arreglo a un régimen europeo de certificación de la ciberseguridad, según lo establecido en el artículo 49 del Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo. Cuando las entidades pertinentes establezcan requisitos de seguridad para aplicarlos a los productos TIC que vayan a adquirir, deben tener en cuenta los requisitos de ciberseguridad clave establecidos en el Reglamento del Parlamento Europeo y del Consejo relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales.

(18) Para protegerse contra las ciberamenazas y apoyar la prevención y contención de las violaciones de la seguridad de los datos, las entidades pertinentes deben aplicar soluciones de seguridad de la red. Las soluciones típicas de seguridad de la red pasan por utilizar cortafuegos para proteger las redes internas de las entidades

pertinentes, limitar la conexión y el acceso a los servicios en los que dicha conexión y dicho acceso sean imprescindibles, utilizar redes privadas virtuales para el acceso remoto y conceder premisos de conexión a los prestadores de servicios previa solicitud de autorización y durante un período de tiempo limitado (por ejemplo, la duración de una operación de mantenimiento).

(19) A fin de proteger sus redes y sistemas de información frente a programas maliciosos o no autorizados, las entidades pertinentes deben aplicar controles para impedir o detectar el uso de programas informáticos no autorizados y deben, cuando proceda, utilizar programas de detección y de respuesta. Las entidades pertinentes también deben considerar la aplicación de medidas para reducir la superficie de ataque, disminuir las vulnerabilidades que puedan ser explotadas por los atacantes, controlar el funcionamiento de las aplicaciones en los dispositivos finales, e introducir filtros de correo electrónico y de aplicación web para reducir la exposición a contenidos malintencionados.

(20) De conformidad con el artículo 21, apartado 2, letra g), de la Directiva (UE) 2022/2555, corresponde a los Estados miembros velar por que las entidades esenciales e importantes apliquen prácticas básicas de ciberhigiene y ofrezcan formación en ciberseguridad. Las prácticas básicas de ciberhigiene pueden incluir principios de confianza cero, actualizaciones de programas, configuración de dispositivos, segmentación de la red, controles de identidad y acceso y sensibilización de los usuarios, organización de formaciones para el personal y una mejor concienciación en torno a las ciberamenazas, el phising o las técnicas de ingeniería social. Las prácticas de ciberhigiene forman parte de los diferentes requisitos metodológicos y técnicos de las medidas para la gestión de riesgos de ciberseguridad establecidos en el anexo del presente Reglamento. En lo que se refiere a las prácticas básicas de ciberhigiene para los usuarios, las entidades pertinentes deben considerar, por ejemplo, una estrategia de escritorios y pantallas despejados, el uso de medios de autenticación multifactorial u otros, el uso seguro del correo electrónico y la navegación web, la protección frente a la suplantación de identidad y la ingeniería social, o unas prácticas seguras de trabajo a distancia.

(21) A fin de evitar el acceso no autorizado a los activos de las entidades pertinentes, estas últimas deben establecer y aplicar políticas temáticas que aborden la cuestión del acceso tanto de personas como de sistemas de redes y de información (como las aplicaciones).

(22) Para evitar que los empleados puedan, por ejemplo, hacer un uso indebido de sus derechos de acceso dentro de la entidad pertinente y provocar daños y perjuicios, estas entidades deben valorar la adopción de medidas adecuadas para la gestión de la seguridad de los empleados y mejorar la concienciación de su personal en torno a estos riesgos. Las entidades pertinentes deben establecer, comunicar y mantener un procedimiento disciplinario para responder a los incumplimientos de las políticas de seguridad de los sistemas de redes y de información de las entidades pertinentes, que podrá estar integrado en otros procedimientos disciplinarios establecidos por estas últimas. La verificación de los antecedentes personales realizada en el caso de los empleados y, cuando proceda, los proveedores o prestadores de servicios directos de las entidades pertinentes debe contribuir al objetivo de la seguridad de los recursos humanos en las entidades pertinentes, y podrá incluir medidas como la comprobación de los antecedentes penales o del desempeño profesional previo de la persona, según se requiera con relación a las funciones de esta persona en la entidad pertinente y de conformidad con la política de esta última en materia de seguridad de los sistemas de redes y de información.

(23) La autenticación multifactorial puede mejorar la ciberseguridad de las entidades, y estas deben tenerla en cuenta, especialmente, cuando los usuarios accedan a los sistemas de redes y de información desde lugares remotos, o cuando tengan acceso a información sensible o a cuentas privilegiadas o de administración del sistema. La autenticación multifactorial puede combinarse con otras técnicas que requieran factores adicionales en circunstancias específicas a partir de unas normas y unos patrones predefinidos; por ejemplo, si el acceso se produce desde una ubicación o un dispositivo inusual, o a una hora poco habitual.

(24) Las entidades pertinentes deben gestionar y proteger los activos que posean un valor para ellos a través de una buena gestión de activos, que a su vez sirva de base para el análisis de riesgos y la continuidad de la actividad. Las entidades pertinentes deben gestionar tanto los activos tangibles como los intangibles, crear un inventario de activos, asociar estos últimos a una categoría de clasificación definida, manejar los activos y hacer un seguimiento de los mismos, y adoptar las medidas necesarias para protegerlos a lo largo de todo su ciclo de vida.

(25) La gestión de activos debe llevar aparejada su clasificación según el tipo, la sensibilidad, el nivel de riesgo y los requisitos de seguridad, y la aplicación de medidas y controles adecuados que aseguren su disponibilidad, integridad, confidencialidad y autenticidad. Cuando clasifiquen los activos según su nivel de riesgo, las entidades pertinentes deben poder aplicar medidas y controles de seguridad adecuados para protegerlos, tales

como el cifrado, el control de acceso (incluido el control del acceso perimetral, físico y lógico), las copias de seguridad, los registros y el seguimiento, la retención y la eliminación. Cuando realicen un análisis de impacto empresarial, las entidades pertinentes podrán determinar la categoría de clasificación en función de las consecuencias de la perturbación de los activos para las entidades. Todo empleado de la entidad que gestione activos debe estar familiarizado con las políticas de manejo de activos y las instrucciones correspondientes.

(26) La granularidad del inventario de activos debe ser adecuada a las necesidades de las entidades pertinentes. Un inventario exhaustivo de activos puede incluir, con relación a cada activo, al menos un identificador único, el propietario del activo, una descripción del activo, su ubicación, su tipo y la clasificación de la información tratada en el mismo, la fecha de la última actualización o parche, la clasificación del activo en la evaluación de riesgos, y el final de la vida útil del activo. Al identificar al propietario de un activo, las entidades pertinentes también deben designar a la persona responsable de proteger dicho activo.

(27) La asignación y organización de los roles, responsabilidades y autoridades en materia de ciberseguridad deben dar lugar a una estructura fiable para la gobernanza de esta última y su puesta en marcha dentro de las entidades pertinentes, y debe velar por una comunicación eficaz en caso de que se produzcan incidentes. Cuando se definan y designen las responsabilidades correspondientes a determinados roles, las entidades pertinentes deben considerar roles del tipo: jefe de seguridad de la información, responsable de la seguridad de la información, encargado de la gestión de incidentes, auditor u otros similares. Las entidades pertinentes podrán asignar roles y responsabilidades a terceros, como los proveedores terceros de servicios TIC.

(28) De conformidad con el artículo 21, apartado 2, de la Directiva (UE) 2022/2555, las medidas para la gestión de riesgos de ciberseguridad se fundamentarán en un enfoque basado en todos los peligros que tenga por objeto proteger los sistemas de redes y de información y el entorno físico de dichos sistemas frente a sucesos como robos, incendios, inundaciones, fallos en las telecomunicaciones o de suministro de electricidad, acceso físico no autorizado o daños a la información que posee la entidad esencial o importante y las instalaciones de procesamiento de información de la entidad, o frente a cualquier tipo de interferencia con dicha información e instalaciones, que puedan poner en peligro la disponibilidad, la autenticidad, la integridad o la confidencialidad de los datos almacenados, transmitidos o tratados, o de los servicios ofrecidos por tales sistemas de redes y de información o accesibles a través de ellos. Por consiguiente, los requisitos técnicos y metodológicos de las medidas para la gestión de riesgos de ciberseguridad deben abordar también la seguridad física y medioambiental de los sistemas de redes y de información mediante la incorporación de medidas para protegerlos frente a fallos de sistema, errores humanos, actos malintencionados o fenómenos naturales. Otros ejemplos de amenazas físicas y medioambientales son los terremotos, las explosiones, el sabotaje, las amenazas internas, los disturbios, los residuos tóxicos y las emisiones medioambientales. La prevención de pérdidas, daños u otros riesgos para los sistemas de redes y de información así como de la interrupción de sus operaciones debido a fallos o problemas en los servicios básicos de apoyo debe contribuir al objetivo de continuidad de las actividades en las entidades pertinentes. Además, la protección frente a las amenazas físicas y medioambientales debe contribuir al mantenimiento de la seguridad de los sistemas de redes y de información en dichas entidades.

(29) Las entidades pertinentes deben diseñar y aplicar medidas de protección contra las amenazas físicas y medioambientales, establecer umbrales mínimos y máximos de control con relación a las mismas y supervisar los parámetros medioambientales. Por ejemplo, deben considerar la posibilidad de instalar sistemas para detectar en una fase temprana la inundación de las zonas en las que se encuentren los sistemas de redes y de información. En cuanto al peligro de incendio, las entidades pertinentes deben considerar la creación de un compartimento contra incendios separado para el centro de datos, el uso de materiales ignífugos y de sensores para controlar la temperatura y la humedad, la conexión del edificio a un sistema de alarma con una notificación automática al servicio contraincendios local, así como sistemas de detección temprana y extinción de incendios. Las entidades pertinentes deben llevar a cabo periódicamente ejercicios e inspecciones de prevención de incendios. Además, para garantizar el suministro eléctrico, las entidades pertinentes deben considerar la protección contra la sobretensión y el correspondiente suministro eléctrico de emergencia, de acuerdo con las normas oportunas. Puesto que el sobrecalentamiento supone un riesgo para la disponibilidad de los sistemas de redes y de información, las entidades pertinentes -en particular los proveedores de servicios de centros de datos- también pueden considerar sistemas de aire acondicionado adecuados, continuos y redundantes.

(30) El presente Reglamento tiene por objeto detallar en mayor medida en qué casos puede considerarse significativo un incidente a efectos del artículo 23, apartado 3, de la Directiva (UE) 2022/2555. Los criterios deben ser tales que las entidades pertinentes sean capaces de determinar si un incidente es significativo a fin de notificarlo de conformidad con la Directiva (UE) 2022/2555. Además, la lista de criterios establecida en el presente Reglamento debe considerarse exhaustiva, sin perjuicio de lo dispuesto en el artículo 5 de la Directiva (UE) 2022/2555. El

presente Reglamento detalla los casos en que un incidente debe considerarse significativo estableciendo casos horizontales y por tipo de entidad.

(31) De conformidad con el artículo 23, apartado 4, de la Directiva (UE) 2022/2555, las entidades pertinentes deben estar obligadas a notificar los incidentes significativos en los plazos previstos en dicha disposición. Estos plazos de notificación se inician en el momento en que la entidad conoce tales incidentes significativos. Por lo tanto, la entidad pertinente debe notificar los incidentes que, de acuerdo con su evaluación inicial, puedan causar alteraciones operativas importantes en los servicios o pérdidas financieras para la entidad, o puedan afectar a otras personas físicas o jurídicas causándoles daños materiales o inmateriales considerables. Así, cuando una entidad pertinente haya detectado un suceso sospechoso, o cuando un tercero -como un particular, un cliente, una entidad, una autoridad, una organización de medios de comunicación u otra fuente- haya puesto en su conocimiento un incidente potencial, la entidad pertinente debe evaluar a su debido tiempo dicho suceso sospecho para determinar si constituye un incidente y, en su caso, su naturaleza y gravedad. Por consiguiente, se considera que la entidad pertinente «tiene conocimiento» del incidente significativo cuando, tras dicha evaluación inicial, la entidad cuente con un grado razonable de certeza de que un incidente significativo ha tenido lugar.

(32) A fin de establecer si un incidente es significativo, las entidades pertinentes deben, cuando proceda, contabilizar el número de usuarios afectados por el mismo, teniendo en cuenta las empresas y clientes finales con los que la entidad pertinente tenga una relación contractual, así como las personas físicas y jurídicas asociadas a los clientes comerciales. Cuando una entidad pertinente no pueda calcular el número de usuarios afectados por el incidente, se tendrá en cuenta su estimación del posible número máximo de usuarios concernidos a efectos del cálculo del número total. La importancia de un incidente que concierna a un servicio de confianza no debe determinarse únicamente en función del número de usuarios, sino también del número de partes usuarias, ya que estas también pueden sufrir repercusiones cuando se produzca un incidente significativo que afecte a un servicio de confianza con relación a fallos operativos o a daños materiales e inmateriales. Por consiguiente, los prestadores de servicios de confianza también deben tener en cuenta, cuando proceda, el número de partes usuarias a la hora de determinar si un incidente es significativo. A tal efecto, las partes usuarias deben entenderse como las personas físicas o jurídicas que dependan de un servicio de confianza.

(33) Las operaciones de mantenimiento que limiten la disponibilidad de los servicios o impliquen su indisponibilidad no deben considerarse incidentes significativos cuando la limitación de la disponibilidad o la indisponibilidad del servicio se produzcan a raíz de una operación de mantenimiento programada. Es más, cuando un servicio esté indisponible debido a una interrupción programada, como las interrupciones o la indisponibilidad que respondan a un acuerdo contractual previo, este hecho no debe considerarse incidente significativo.

(34) La duración de un incidente que repercuta en la disponibilidad de un servicio debe calcularse desde el momento en que el correcto suministro del servicio se vea perturbado hasta el momento en que se recupere. Cuando una entidad pertinente no pueda determinar el momento en que se produjo la interrupción, la duración del incidente debe calcularse desde el momento en que se detectó o desde el momento en que se dejó constancia en el registro de la red o del sistema o en otras fuentes de datos, si esta fecha fuese anterior.

(35) La indisponibilidad total de un servicio debe calcularse desde el momento en que el servicio esté completamente indisponible para los usuarios hasta el momento en que las actividades u operaciones habituales se hayan restablecido al mismo nivel de servicio que se estaba prestando antes del incidente. Cuando una entidad pertinente no pueda determinar el momento en que se inició la indisponibilidad completa de un servicio, esta debe calcularse a partir del momento en que dicha entidad la haya detectado.

(36) A efectos de determinar las pérdidas financieras directas resultantes de un incidente, las entidades pertinentes deben tener en cuenta todas las pérdidas financieras que hayan sufrido como consecuencia del mismo, como los costes de sustitución o reubicación de software, hardware o infraestructura, los costes de personal, incluidos los costes asociados a la sustitución o reubicación del personal, la contratación de personal adicional, la remuneración de las horas extraordinarias y la recuperación de las capacidades perdidas o deterioradas, las tasas por incumplimiento de las obligaciones contractuales, los costes de reparación y compensación a los clientes, las pérdidas por renuncia a ingresos, los costes asociados a la comunicación interna y externa, los costes de asesoramiento, incluidos los costes asociados al asesoramiento jurídico, los servicios forenses y los servicios de reparación, y otros costes asociados al incidente. No obstante, las multas administrativas y los costes necesarios para el funcionamiento cotidiano de la empresa no deben considerarse pérdidas financieras derivadas de un incidente, como los costes de mantenimiento general de la infraestructura, los equipos, el hardware y el software, la actualización de las capacidades del personal, los costes internos o externos para mejorar la actividad después del incidente, incluidas las actualizaciones, las mejoras y las iniciativas relacionadas con la evaluación de riesgos, y las

primas de seguros. Las entidades pertinentes deben calcular los importes de las pérdidas financieras sobre la base de los datos disponibles y, cuando no puedan determinarse los importes reales de las pérdidas financieras, las entidades deben hacer una estimación de dichos importes.

(37) Las entidades pertinentes también están obligadas a notificar aquellos incidentes que hayan causado o puedan causar la muerte de personas físicas o daños considerables a la salud de estas, ya que estos incidentes son casos especialmente graves que causan daños materiales o inmateriales importantes. Por ejemplo, un incidente que afecte a una entidad pertinente podría provocar la indisponibilidad de servicios sanitarios o de emergencia, o la pérdida de confidencialidad o integridad de los datos con repercusiones para la salud de las personas físicas. Con el fin de determinar si un incidente ha causado o puede causar daños considerables a la salud de una persona física, las entidades pertinentes deben tener en cuenta si el incidente ha causado o puede causar lesiones graves u otros problemas de salud. A tal efecto, no debe exigirse a las entidades pertinentes que recopilen información adicional a la que no tengan acceso.

(38) En concreto, debe considerarse que existe una disponibilidad limitada cuando un servicio prestado por una entidad pertinente sea considerablemente más lento que el tiempo medio de respuesta, o cuando no todas las funciones de un servicio estén disponibles. Cuando sea posible, deben utilizarse criterios objetivos basados en los tiempos medios de respuesta de los servicios prestados por las entidades pertinentes para evaluar los retrasos en el tiempo de respuesta. Una función de un servicio puede ser, por ejemplo, una función de chat o de búsqueda de imágenes.

(39) La obtención de acceso, el acceso presuntamente malicioso y el acceso no autorizado a los sistemas de redes y de información de una entidad pertinente deben considerarse incidentes significativos cuando dicho acceso pueda causar graves perturbaciones operativas. Por ejemplo, cuando un agente de ciberamenazas se sitúe anticipadamente en los sistemas de redes y de información con el objetivo de causar la perturbación de los servicios en el futuro, el incidente debe considerarse significativo.

(40) Los incidentes recurrentes que aparentemente estén relacionados por la misma causa subyacente y que, individualmente, no cumplan los criterios para considerarlos incidente significativo deben considerarse como tal colectivamente, siempre y cuando cumplan de manera colectiva el criterio de pérdida financiera y se hayan producido al menos dos veces en un plazo de seis meses. Tales incidentes recurrentes pueden ser muestra de deficiencias y puntos débiles importantes en los procedimientos de gestión de los riesgos de ciberseguridad de la entidad pertinente, así como de su nivel de madurez en materia de ciberseguridad. Además, estos incidentes pueden causar importantes pérdidas financieras para la entidad pertinente.

(41) La Comisión ha intercambiado asesoramiento y cooperado con el Grupo de Cooperación y la ENISA sobre el proyecto de acto de ejecución, de conformidad con el artículo 21, apartado 5, y el artículo 23, apartado 11, de la Directiva (UE) 2022/2555.

(42) El Supervisor Europeo de Protección de Datos, al que se consultó de conformidad con el artículo 42, apartado 1, del Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, emitió su dictamen el 1 de septiembre de 2024.

(43) Las medidas previstas en el presente Reglamento se ajustan al dictamen del Comité establecido de acuerdo con el artículo 39, de la Directiva (UE) 2022/2555.

HA ADOPTADO EL PRESENTE REGLAMENTO:

Artículo 1. *Objeto.*

En lo que se refiere a los proveedores de servicios de DNS, los registros de nombres de dominio de primer nivel, los proveedores de servicios de computación en nube, los proveedores de servicios de centros de datos, los proveedores de redes de distribución de contenidos, los proveedores de servicios gestionados, los proveedores de servicios de seguridad gestionados, así como los proveedores de mercados en línea, de motores de búsqueda en línea y de plataformas de servicios de redes sociales, y los prestadores de servicios de confianza (en adelante, las entidades pertinentes), el presente Reglamento establece los requisitos técnicos y metodológicos de las medidas previstas en el artículo 21, apartado 2, de la Directiva (UE) 2022/2555 y detalla en qué casos un incidente se considerará significativo a tenor del artículo 23, apartado 3, de la Directiva (UE) 2022/2555.

Artículo 2. *Requisitos técnicos y metodológicos.*

1. Con relación a las entidades pertinentes, los requisitos técnicos y metodológicos de las medidas para la gestión de riesgos de ciberseguridad a que se refiere el artículo 21, apartado 2, letras a) a j), de la Directiva (UE) 2022/2555 se establecen en el anexo del presente Reglamento.

2. Las entidades pertinentes garantizarán un nivel de seguridad de los sistemas de redes y de información adecuado a los riesgos que se planteen al llevar a la práctica y aplicar los requisitos técnicos y metodológicos de las medidas para la gestión de riesgos de ciberseguridad establecidos en el anexo del presente Reglamento. Para ello, tendrán debidamente en cuenta su grado de exposición a los riesgos, su tamaño y la probabilidad de que se produzcan incidentes y su gravedad, especialmente sus repercusiones sociales y económicas, a la hora de cumplir los requisitos técnicos y metodológicos de las medidas para la gestión de riesgos de ciberseguridad establecidos en el anexo del presente Reglamento.

Cuando el anexo del presente Reglamento establezca que los requisitos técnicos y metodológicos de las medidas de gestión de riesgos de ciberseguridad se aplicarán «según proceda», «cuando proceda» o «en la medida de lo posible», y la entidad pertinente considere que no procede, que no resulta de aplicación o que no es posible aplicar determinados requisitos técnicos y metodológicos, la entidad redactará de manera comprensible su razonamiento a tal efecto.

Artículo 3. *Incidentes significativos.*

1. Un incidente se considerará significativo a efectos del artículo 23, apartado 3, de la Directiva (UE) 2022/2555 con respecto a las entidades pertinentes cuando se cumplan uno o varios de los siguientes criterios:

a) que el incidente haya causado o pueda causar a la entidad pertinente pérdidas financieras directas superiores a 500 000 EUR o al 5% de su volumen de negocios total anual en el ejercicio financiero anterior, si esta cifra es inferior;

b) que el incidente haya causado o pueda causar la exfiltración de secretos comerciales a tenor del artículo 2, apartado 1, de la Directiva (UE) 2016/943, de la entidad pertinente;

c) que el incidente haya causado o pueda causar la muerte de una persona física;

d) que el incidente haya causado o pueda causar daños considerables a la salud de una persona física;

e) que se haya producido efectivamente el acceso presuntamente malicioso y no autorizado a los sistemas de redes y de información, lo que puede causar graves perturbaciones operativas;

f) que el incidente cumpla los criterios establecidos en el artículo 4;

g) que el incidente cumpla uno o varios de los criterios establecidos en los artículos 5 a 14.

2. Las interrupciones programadas del servicio y las consecuencias previstas de las operaciones de mantenimiento programadas llevadas a cabo por las entidades pertinentes o en su nombre no se considerarán incidentes significativos.

3. Al calcular el número de usuarios afectados por un incidente a efectos del artículo 7 y los artículos 9 a 14, las entidades pertinentes tendrán en cuenta todo lo siguiente:

a) el número de clientes que tengan un contrato con la entidad pertinente que les permita acceder a las redes y sistemas de información de dicha entidad o a los servicios ofrecidos por dichas redes y sistemas de información, o que sean accesibles a través de ellos;

b) el número de personas físicas y jurídicas asociadas a clientes empresariales que utilicen las redes y los sistemas o servicios de información de las entidades ofrecidos por dichas redes y sistemas de información o que sean accesibles a través de ellos.

Artículo 4. *Incidentes recurrentes.*

Los incidentes que, individualmente, no se consideren incidentes significativos en el sentido del artículo 3, se considerarán conjuntamente un incidente significativo cuando cumplan todos los criterios siguientes:

a) que se hayan producido al menos dos veces en un plazo de seis meses;

b) que tengan la misma causa fundamental aparente;

c) que cumplan colectivamente los criterios establecidos en el artículo 3, apartado 1, letra a).

Artículo 5. *Incidentes significativos con respecto a los proveedores de servicios del sistema de nombres de dominio.*

Por lo que respecta a los proveedores de servicios del sistema de nombres de dominio (DNS, por sus siglas en inglés), un incidente se considerará significativo con arreglo al artículo 3, apartado 1, letra g), cuando cumpla uno o varios de los siguientes criterios:

a) que un servicio de resolución de nombres de dominio recursivo o autoritativo esté completamente indisponible durante más de treinta minutos;
b) que, durante más de una hora, el tiempo medio de respuesta de un servicio de resolución de nombres de dominio recursivo o autoritativo a las solicitudes de DNS sea superior a diez segundos;
c) que la integridad, confidencialidad o autenticidad de los datos almacenados, transmitidos o tratados en relación con la prestación del servicio de resolución autoritativa de nombres de dominio se vean comprometidas, excepto en los casos en que los datos de menos de 1 000 nombres de dominio gestionados por el proveedor de servicios DNS, que representen como máximo el 1% de los nombres de dominio gestionados por el proveedor de servicios DNS, no sean correctos debido a fallos de configuración.

Artículo 6. *Incidentes significativos con respecto a los registros de nombres de dominio de primer nivel.*

Por lo que respecta a los registros de nombres de dominio de primer nivel, un incidente se considerará significativo con arreglo al artículo 3, apartado 1, letra g), cuando cumpla uno o varios de los criterios siguientes:

a) que un servicio autoritativo de resolución de nombres de dominio esté totalmente indisponible;
b) que, durante más de una hora, el tiempo medio de respuesta de un servicio autoritativo de resolución de nombres de dominio a las solicitudes de DNS sea superior a diez segundos;
c) que la integridad, confidencialidad o autenticidad de los datos almacenados, transmitidos o tratados en relación con el funcionamiento técnico del dominio de primer nivel se vean comprometidas.

Artículo 7. *Incidentes significativos con respecto a los proveedores de servicios de computación en nube.*

Por lo que respecta a los proveedores de servicios de computación en nube, un incidente se considerará significativo con arreglo al artículo 3, apartado 1, letra g), cuando cumpla uno o varios de los siguientes criterios:

a) que un servicio de computación en nube esté totalmente indisponible durante más de treinta minutos;
b) que la disponibilidad del servicio de computación en nube de un proveedor esté limitada en el caso de más del 5% de los usuarios de servicios de computación en nube de la Unión, o de más de un millón de usuarios de servicios de computación en nube en la Unión, si esta cifra es menor, durante más de una hora;
c) que la integridad, confidencialidad o autenticidad de los datos almacenados, transmitidos o tratados en relación con la prestación de un servicio de computación en nube se vean comprometidas como consecuencia de una acción presuntamente malintencionada;
d) que la integridad, confidencialidad o autenticidad de los datos almacenados, transmitidos o tratados en relación con la prestación del servicio de computación en la nube se vean comprometidas y ello afecte a más del 5% de los usuarios de dicho servicio de computación en la nube de la Unión, o a más de un millón de sus usuarios en la Unión, si esta cifra es menor.

Artículo 8. *Incidentes significativos con respecto a los proveedores de servicios de centros de datos.*

Por lo que respecta a los proveedores de servicios de centros de datos, un incidente se considerará significativo con arreglo al artículo 3, apartado 1, letra g), cuando cumpla uno o varios de los siguientes criterios:

a) que el servicio del centro de datos gestionado por el proveedor esté totalmente indisponible;
b) que la disponibilidad de un servicio de un centro de datos gestionado por el proveedor esté limitada durante más de una hora;
c) que la integridad, confidencialidad o autenticidad de los datos almacenados, transmitidos o tratados en relación con la prestación de un servicio de centro de datos se vean comprometidas como consecuencia de una acción presuntamente malintencionada;
d) que el acceso físico a un centro de datos gestionado por el proveedor esté en riesgo.

Artículo 9. *Incidentes significativos con respecto a los proveedores de redes de distribución de contenidos.*

Por lo que respecta a los proveedores de redes de distribución de contenidos, un incidente se considerará significativo con arreglo al artículo 3, apartado 1, letra g), cuando cumpla uno o varios de los siguientes criterios:

a) que una red de distribución de contenidos esté totalmente indisponibles durante más de treinta minutos;
b) que la disponibilidad de una red de distribución de contenidos esté limitada en el caso de más del 5% de los usuarios de la red de distribución de contenidos en la Unión, o de más de un millón de usuarios de la red de distribución de contenidos en la Unión, si esta cifra es menor, durante más de una hora;
c) que la integridad, confidencialidad o autenticidad de los datos almacenados, transmitidos o tratados en relación con el suministro de la red de distribución de contenidos se vean comprometidas como consecuencia de una acción presuntamente malintencionada;
d) que la integridad, confidencialidad o autenticidad de los datos almacenados, transmitidos o tratados en relación con el suministro de la red de distribución de contenidos se vean comprometidas y ello afecte a más del 5% de los usuarios de la red de distribución de contenidos en la Unión, o a más de un millón de usuarios de la red de distribución de contenidos en la Unión, si esta cifra es menor.

Artículo 10. *Incidentes significativos con respecto a los proveedores de servicios gestionados y los proveedores de servicios de seguridad gestionados.*

Por lo que respecta a los proveedores de servicios gestionados y los proveedores de servicios de seguridad gestionados, un incidente se considerará significativo con arreglo al artículo 3, apartado 1, letra g), cuando cumpla uno o varios de los criterios siguientes:

a) que un servicio gestionado o un servicio de seguridad gestionado esté completamente indisponible durante más de treinta minutos;
b) que la disponibilidad de un servicio gestionado o de un servicio de seguridad gestionado esté limitada en el caso de más del 5% de los usuarios de este servicio en la Unión, o de más de un millón de sus usuarios en la Unión, si esta cifra es menor, durante más de una hora;
c) que la integridad, confidencialidad o autenticidad de los datos almacenados, transmitidos o tratados en relación con la prestación de un servicio gestionado o de un servicio de seguridad gestionado se vean comprometidas como consecuencia de una acción presuntamente malintencionada;
d) que la integridad, confidencialidad o autenticidad de los datos almacenados, transmitidos o tratados en relación con la prestación de un servicio gestionado o de un servicio de seguridad gestionado se vean comprometidas y ello afecte a más del 5% de los usuarios del servicio gestionado o del servicio de seguridad gestionado en la Unión, o a más de un millón de usuarios de estos servicios en la Unión, si esta cifra es menor.

Artículo 11. *Incidentes significativos con respecto a los proveedores de mercados en línea.*

Por lo que respecta a los prestadores de mercados en línea, un incidente se considerará significativo con arreglo al artículo 3, apartado 1, letra g), cuando cumpla uno o varios de los siguientes criterios:

a) que un mercado en línea esté completamente indisponible para más del 5% de los usuarios de un mercado en línea de la Unión, o para más de un millón de sus usuarios en la Unión, si esta cifra es menor;
b) que más del 5% de los usuarios de un mercado en línea de la Unión, o más de un millón de usuarios, si esta cifra es menor, se vean afectados por la disponibilidad limitada de dicho mercado en línea;
c) que la integridad, confidencialidad o autenticidad de los datos almacenados, transmitidos o tratados en relación con el suministro de un mercado en línea se vean comprometidas como consecuencia de una acción presuntamente malintencionada;
d) que la integridad, confidencialidad o autenticidad de los datos almacenados, transmitidos o tratados en relación con el suministro de un mercado en línea se vean comprometidas y ello afecte a más del 5% de los usuarios del mercado en línea en la Unión, o a más de un millón de usuarios del mercado en línea en la Unión, si esta cifra es menor.

Artículo 12. *Incidentes significativos con respecto a los proveedores de motores de búsqueda en línea.*

Por lo que respecta a los proveedores de motores de búsqueda en línea, un incidente se considerará significativo con arreglo al artículo 3, apartado 1, letra g), cuando cumpla uno o varios de los siguientes criterios:

a) que un motor de búsqueda en línea esté completamente indisponible para más del 5% de los usuarios del motor de búsqueda en línea de la Unión, o para más de un millón de sus usuarios en la Unión, si esta cifra es menor;

b) que más del 5% de los usuarios de los servicios del motor de búsqueda en línea de la Unión, o más de un millón de usuarios, si esta cifra es menor, se vean afectados por la disponibilidad limitada de dicho motor de búsqueda en línea;

c) que la integridad, confidencialidad o autenticidad de los datos almacenados, transmitidos o tratados en relación con el suministro de un motor de búsqueda en línea se vean comprometidas como consecuencia de una acción presuntamente malintencionada;

d) que la integridad, confidencialidad o autenticidad de los datos almacenados, transmitidos o tratados en relación con el suministro de un motor de búsqueda en línea se vean comprometidas y ello afecte a más del 5% de los usuarios del motor de búsqueda en línea en la Unión, o a más de un millón de usuarios de los servicios del motor de búsqueda en línea en la Unión, si esta cifra es menor.

Artículo 13. *Incidentes significativos con respecto a los proveedores de plataformas de servicios de redes sociales.*

Por lo que respecta a los proveedores de plataformas de servicios de redes sociales, un incidente se considerará significativo con arreglo al artículo 3, apartado 1, letra g), cuando cumpla uno o varios de los siguientes criterios:

a) que una plataforma de servicios de redes sociales esté completamente indisponible para más del 5% de los usuarios de la plataforma de servicios de redes sociales en la Unión, o para más de un millón de sus usuarios en la Unión, si esta cifra es menor;

b) que más del 5% de los usuarios de una plataforma de servicios de redes sociales de la Unión, o más de 1 millón de usuarios de la plataforma de servicios de redes sociales en la Unión, si esta cifra es menor, se vean afectados por la disponibilidad limitada de dicha plataforma de servicios de redes sociales;

c) que la integridad, confidencialidad o autenticidad de los datos almacenados, transmitidos o tratados en relación con la prestación de una plataforma de servicios de redes sociales se vean comprometidas como consecuencia de una acción presuntamente malintencionada;

d) que la integridad, confidencialidad o autenticidad de los datos almacenados, transmitidos o tratados relacionados con la prestación de la plataforma de servicios de redes sociales se vean comprometidas y ello afecte a más del 5% de los usuarios de la plataforma de servicios de redes sociales en la Unión, o a más de un millón de sus usuarios en la Unión, si esta cifra es menor.

Artículo 14. *Incidentes* significativos con respecto a los prestadores de servicios de confianza.

Por lo que respecta a los prestadores de servicios de confianza, un incidente se considerará significativo con arreglo al artículo 3, apartado 1, letra g), cuando cumpla uno o varios de los siguientes criterios:

a) que un servicio de confianza esté completamente indisponible durante más de veinte minutos;

b) que un servicio de confianza esté indisponible para los usuarios o las partes usuarias durante más de una hora calculada sobre la base de una semana natural;

c) que más del 1% de los usuarios o partes usuarias en la Unión, o más de 200 000 usuarios o partes usuarias en la Unión, si esta cifra es menor, se vean afectados por la disponibilidad limitada de un servicio de confianza;

d) que el acceso físico a una zona en las que estén situados los sistemas de redes y de información y en la que el acceso esté restringido al personal acreditado del prestador de servicios de confianza o la protección de dicho acceso físico se vea comprometido;

e) que la integridad, confidencialidad o autenticidad de los datos almacenados, transmitidos o tratados en relación con la prestación de un servicio de confianza se vean comprometidas y ello afecte a más del 0,1% de los usuarios o partes usuarias, o a más de cien usuarios o partes usuarias del servicio de confianza en la Unión, si esta cifra es menor.

Artículo 15. *Derogación.*

Queda derogado el Reglamento de Ejecución (UE) 2018/151 de la Comisión.

Artículo 16. *Entrada en vigor y aplicación*.

El presente Reglamento entrará en vigor a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*.

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

Hecho en Bruselas, el 17 de octubre de 2024.

Por la Comisión
La Presidenta
Ursula VON DER LEYEN

ANEXO

Requisitos técnicos y metodológicos contemplados en el artículo 2 del presente Reglamento

1. **Política sobre la seguridad de los sistemas de redes y de información [artículo 21, apartado 2, letra a), de la Directiva (UE) 2022/2555]**

1.1. *Política sobre la seguridad de las redes y sistemas de información*

1.1.1. A efectos del artículo 21, apartado 2, letra a), de la Directiva (UE) 2022/2555, la política de seguridad de los sistemas de redes y de información:

a) determinará el enfoque de las entidades pertinentes para gestionar la seguridad de sus sistemas de redes y de información;
b) se adecuará a la estrategia y los objetivos operativos de las entidades pertinentes y los completará;
c) establecerá los objetivos de seguridad de las redes y de la información;
d) se comprometerá a mejorar constantemente la seguridad de los sistemas de redes y de información;
e) se comprometerá a facilitar los recursos oportunos para su aplicación, incluidos el personal, los recursos financieros, los procedimientos, las herramientas y las tecnologías que se necesiten;
f) será comunicada a los empleados y partes externas que proceda, que deberán aprobarla;
g) presentará los roles y responsabilidades con arreglo al punto 1.2;
h) detallará la documentación que debe conservarse y la duración del período de conservación;
i) enumerará las políticas específicas;
j) fijará indicadores y medidas para supervisar su aplicación y el estado actual del nivel de madurez de la seguridad de las redes y de la información de las entidades pertinentes;
k) indicará la fecha de la aprobación formal por parte de los órganos de dirección de las entidades pertinentes [en adelante, «órgano(s) de dirección»].

1.1.2. El órgano de dirección revisará y, cuando proceda, actualizará la política de seguridad de los sistemas de redes y de información al menos una vez al año, así como cuando se produzcan incidentes significativos o cambios significativos en las operaciones o los riesgos. Los resultados de las revisiones quedarán documentados.

1.2. *Roles, responsabilidades y autoridades*

1.2.1. Como parte de la política de seguridad de los sistemas de redes y de información a que hace referencia el punto 1.1, las entidades pertinentes determinarán las responsabilidades y autoridades en materia de seguridad de los sistemas de redes y de información y las asignarán a distintos roles, las repartirán en función de las necesidades de la entidad y se las comunicarán a los órganos de dirección.
1.2.2. Las entidades pertinentes exigirán a todo el personal y a terceros que apliquen la seguridad de los sistemas de redes y de información de conformidad con la política de seguridad de las redes y la información y las políticas específicas existentes, así como con los procedimientos de las entidades pertinentes.
1.2.3. Al menos una persona informará directamente a los órganos de dirección sobre cuestiones de seguridad de los sistemas de redes y de información.
1.2.4. En función del tamaño de las entidades pertinentes, la seguridad de las redes y los sistemas de información corresponderá a roles o funciones específicos que se desempeñarán además de los roles existentes.
1.2.5. Aquellos cargos o áreas de responsabilidad que entren en conflicto se separarán, cuando proceda.
1.2.6. Los órganos de dirección revisarán y, cuando proceda, actualizarán los roles, responsabilidades y autoridades a intervalos planificados, así como cuando se produzcan incidentes significativos o cambios significativos en las operaciones o los riesgos.

2. **Política de gestión de riesgos [artículo 21, apartado 2, letra a), de la Directiva (UE) 2022/2555]**

2.1. *Marco de la gestión de riesgos*

2.1.1. A efectos del artículo 21, apartado 2, letra a), de la Directiva (UE) 2022/2555, las entidades pertinentes establecerán y mantendrán un marco de la gestión de riesgos adecuado para detectar y abordar los riesgos que se planteen para la seguridad de los sistemas de redes y de información. Las entidades pertinentes realizarán evaluaciones de riesgos cuyos resultados documentarán y, a partir de estos últimos, establecerán un plan de tratamiento de riesgos, que aplicarán y supervisarán. Siempre que las entidades pertinentes garanticen una información adecuada a los órganos de dirección, estos últimos o, cuando proceda, las personas que sean responsables y tengan autoridad para gestionar los riesgos, aprobarán los resultados de la evaluación de riesgos y los riesgos residuales.

2.1.2. A los efectos del punto 2.1.1, las entidades pertinentes establecerán procedimientos para detectar, analizar, evaluar y tratar los riesgos («proceso de gestión de riesgos de ciberseguridad»). El proceso de gestión de riesgos de ciberseguridad formará parte del proceso de gestión de riesgos general de la entidad pertinente, según proceda. Como parte del proceso de gestión de riesgos de ciberseguridad, las entidades pertinentes:

a) seguirán una metodología de gestión de riesgos;
b) establecerán un nivel de tolerancia al riesgo conforme con la propensión al riesgo de la entidad;
c) establecerán y mantendrán criterios de riesgo pertinentes;
d) de conformidad con un enfoque que abarque todos los riesgos, determinarán y registrarán todos los riesgos existentes para la seguridad de los sistemas de redes y de información, en especial con relación a terceros o a aquellos riesgos que puedan generar alteraciones en la disponibilidad, integridad, autenticidad y confidencialidad de los sistemas de redes y de información, incluida la detección de puntos únicos de fallo;
e) analizarán los riesgos que se planteen para la seguridad de los sistemas de redes y de información, especialmente la amenaza, la probabilidad, el impacto y el nivel de riesgo, teniendo en cuenta la inteligencia sobre ciberamenazas y las vulnerabilidades;
f) evaluarán los riesgos detectados a partir de los criterios de riesgo;
g) determinarán y priorizarán las opciones y medidas adecuadas de tratamiento de riesgos;
h) supervisarán constantemente la aplicación de las medidas de tratamiento de riesgos;
i) determinarán quién es responsable de la aplicación de las medidas de tratamiento de riesgos y cuándo deben aplicarse estas;
j) informarán de manera comprensible de las medidas de tratamiento de riesgos elegidas en un plan de tratamiento de riesgos y de las razones que justifiquen la aceptación de los riesgos residuales.

2.1.3. Cuando detecten y prioricen las opciones y medidas adecuadas para el tratamiento de los riesgos, las entidades pertinentes tendrán en cuenta los resultados de la evaluación de riesgos, los resultados del procedimiento para evaluar la eficacia de las medidas para la gestión de riesgos de ciberseguridad, el coste de su aplicación en relación con los beneficios previstos, la clasificación de activos contemplada en el punto 12.1 y el análisis de impacto operativo a que se refiere el punto 4.1.3.

2.1.4. Las entidades pertinentes revisarán y, cuando proceda, actualizarán los resultados de la evaluación de riesgos y el plan de tratamiento de riesgos a intervalos planificados y como mínimo anualmente, así como cuando se produzcan incidentes significativos o cambios significativos en las operaciones o los riegos.

2.2. *Control del cumplimiento*

2.2.1. Las entidades pertinentes revisarán periódicamente el cumplimiento de sus políticas en materia de seguridad de los sistemas de redes y de información, políticas específicas, reglas y normas. Los órganos de dirección serán informados, mediante informes periódicos, del estado de seguridad de las redes y la información a partir de las revisiones del cumplimiento.

2.2.2. Las entidades pertinentes pondrán en marcha un sistema eficaz de notificación del cumplimiento que será adecuado a sus estructuras, sus entornos operativos y su panorama de amenazas. El sistema de notificación del cumplimiento podrá ofrecer a los órganos de dirección una visión informada del estado en que se encuentre la gestión de riesgos de las entidades pertinentes.

2.2.3. Las entidades pertinentes realizarán el control del cumplimiento a intervalos planificados, así como cuando se produzcan incidentes significativos o cambios significativos en las operaciones o los riesgos.

2.3. *Revisión independiente de la seguridad de la información y las redes*

2.3.1. Las entidades pertinentes revisarán de forma independiente su enfoque de gestión de la seguridad de los sistemas de redes y de información y su aplicación, incluidas las personas, los procesos y las tecnologías.

2.3.2. Las entidades pertinentes desarrollarán y mantendrán procedimientos para llevar a cabo revisiones independientes que serán ejecutados por personas con las debidas competencias en materia de auditoría. Cuando miembros del personal de la entidad pertinente realicen una revisión independiente, las personas encargadas de la misma no podrán ejercer poder jerárquico sobre el personal de la zona objeto de la revisión. Si el tamaño de la entidad pertinente no permite esta separación del poder jerárquico, la entidad pondrá en marcha medidas alternativas para garantizar la imparcialidad de las revisiones.

2.3.3. Los resultados de las revisiones independientes, especialmente los resultados del control del cumplimiento de conformidad con el punto 2.2 y del control y la medición con arreglo al punto 7, se notificarán a los órganos de control. De acuerdo con los criterios de aceptación del riesgo de las entidades pertinentes, se adoptarán medidas correctoras o se aceptará el riesgo residual.

2.3.4. Las revisiones independientes tendrán lugar a intervalos planificados, así como cuando se produzcan incidentes significativos o cambios significativos en las operaciones o los riesgos.

3. **Gestión de incidentes [artículo 21, apartado 2, letra b), de la Directiva (UE) 2022/2555]**

3.1. *Política de gestión de incidentes*

3.1.1. A los efectos del artículo 21, apartado 2, letra b), de la Directiva (UE) 2022/2555, las entidades pertinentes elaborarán y pondrán en marcha una política de gestión de incidentes por la que se establezcan los roles, responsabilidades y procedimientos para la detección, el análisis, la contención y la gestión de los incidentes, así como la posterior recuperación, documentación y notificación de los mismos a su debido tiempo.

3.1.2. La política prevista en el punto 3.1.1 será coherente con el plan de continuidad de las actividades y de recuperación en caso de catástrofe a que hace referencia el punto 4.1. La política incluirá:

a) un sistema de clasificación de incidentes que sea coherente con la evaluación y clasificación de sucesos realizada de conformidad con el punto 3.4.1;

b) planes de comunicación eficaces, especialmente en lo relativo a la activación de los niveles sucesivos de intervención y la presentación de informes;

c) la asignación, a los empleados competentes, de roles para detectar y gestionar adecuadamente los incidentes;

d) los documentos que han de utilizarse durante el proceso para detectar y gestionar los incidentes, como, por ejemplo, manuales de respuesta a incidentes, cuadros de activación por niveles, listas de contactos y plantillas.

3.1.3. Los roles, responsabilidades y procedimientos establecidos en la política se probarán, revisarán y, cuando proceda, se actualizarán a intervalos planificados, así como cuando se produzcan incidentes significativos o cambios significativos en las operaciones o los riesgos.

3.2. *Supervisión y registro*

3.2.1. Las entidades pertinentes establecerán procedimientos y utilizarán herramientas para supervisar y registrar las actividades en sus sistemas de redes y de información a fin de detectar sucesos que puedan considerarse incidentes y dar una respuesta consecuente para mitigar su impacto.

3.2.2. En la medida de lo posible, la supervisión se automatizará y se llevará a cabo bien de forma continua bien a intervalos periódicos, en función de las capacidades operativas. Las entidades pertinentes pondrán en marcha sus actividades de seguimiento de manera que se minimicen los falsos positivos y falsos negativos.

3.2.3. A partir de los procedimientos contemplados en el punto 3.2.1, las entidades pertinentes mantendrán, completarán y revisarán sus registros. Las entidades pertinentes establecerán una lista de los activos que deban registrarse teniendo en cuenta los resultados de la evaluación de riesgos efectuada conforme al punto 2.1. Cuando proceda, los registros incluirán información sobre:

a) el tráfico de entrada y salida de la red;

b) la creación, modificación o supresión de usuarios de los sistemas de redes y de información de las entidades pertinentes y la ampliación de los permisos;

c) el acceso a los sistemas y aplicaciones;

d) los sucesos relacionados con la autenticación;

e) todo acceso privilegiado a los sistemas y aplicaciones, así como las actividades realizadas por las cuentas de administración;

f) el acceso a los archivos críticos de configuración y a las copias de seguridad y todo cambio en los mismos;

g) los registros de sucesos y los registros de las herramientas de seguridad, como antivirus, sistemas de detección de intrusiones o cortafuegos;

h) el uso de los recursos del sistema, así como su rendimiento;
i) el acceso físico a las instalaciones;
j) el acceso a los equipos y dispositivos de red y su utilización;
k) la activación, detención e interrupción de los distintos registros;
l) los sucesos medioambientales.

3.2.4. Se revisará periódicamente la existencia de tendencias inusuales o indeseadas en los registros. Cuando proceda, las entidades pertinentes establecerán valores adecuados para los umbrales de alerta. Cuando se superen los valores establecidos para los umbrales de alerta, saltará una alarma que será, en su caso, automática. Las entidades pertinentes se asegurarán de que, en las situaciones de alerta, se adopte a su debido tiempo una respuesta cualificada y adecuada.

3.2.5. Las entidades pertinentes mantendrán registros, de los que harán copias de seguridad, durante un período predefinido, y los protegerán contra el acceso o los cambios no autorizados.

3.2.6. En la medida de lo posible, las entidades pertinentes velarán por que todos los sistemas dispongan de fuentes de información temporal sincronizadas para permitir la vinculación de registros entre sistemas de cara a la evaluación de sucesos. Las entidades pertinentes establecerán y mantendrán una lista de todos los activos que se registren y velarán por que los sistemas de seguimiento y registro sean redundantes. La disponibilidad de los sistemas de supervisión y registro se controlará con independencia de los sistemas que estén supervisando.

3.2.7. Tanto los procedimientos como la lista de activos que se registren se revisarán y, cuando proceda, se actualizarán a intervalos regulares y después de incidentes significativos.

3.3. *Notificación de sucesos*

3.3.1. Las entidades pertinentes pondrán en marcha un mecanismo sencillo que permita a sus empleados, proveedores y clientes notificar los sucesos sospechosos.

3.3.2. Las entidades pertinentes informarán, cuando proceda, del mecanismo de notificación de sucesos a sus proveedores y clientes, y formarán periódicamente a sus empleados en el uso del mismo.

3.4. *Evaluación y clasificación de sucesos*

3.4.1. Las entidades pertinentes evaluarán los sucesos sospechosos para determinar si constituyen incidentes y, en su caso, esclarecer su naturaleza y gravedad.

3.4.2. A los efectos del punto 3.4.1, las entidades pertinentes realizarán las acciones siguientes:

a) una evaluación basada en criterios predefinidos fijados de antemano y en una clasificación que establezca las prioridades de contención y erradicación de incidentes;
b) la evaluación trimestral de la existencia de incidentes recurrentes tal como contempla el artículo 4 del presente Reglamento;
c) la revisión de los registros adecuados a efectos de la evaluación y clasificación de los sucesos;
d) la puesta en marcha de un procedimiento para vincular los registros y el análisis;
e) y la reevaluación y reclasificación de los sucesos cuando se disponga de nueva información o tras analizar la información disponible previamente.

3.5. *Respuesta ante incidentes*

3.5.1. Las entidades pertinentes responderán a los incidentes a su debido tiempo y de conformidad con procedimientos documentados.

3.5.2. Los procedimientos de respuesta ante los incidentes incluirán las siguientes fases:

a) contención del incidente, para evitar las consecuencias de que se propague;
b) erradicación, para evitar que el incidente continúe o reaparezca;
c) recuperación tras el incidente, cuando se requiera.

3.5.3. Las entidades pertinentes establecerán procedimientos y planes de comunicación:

a) con los equipos de respuesta ante incidentes de seguridad informática (CSIRT) o, cuando proceda, las autoridades competentes, en materia de notificación de incidentes;
b) para la comunicación entre los miembros del personal de la entidad pertinente, y para la comunicación con las partes interesadas ajenas a la entidad.

3.5.4. Las entidades pertinentes registrarán tanto las actividades de respuesta ante incidentes de conformidad con los procedimientos contemplados en el punto 3.2.1 como las pruebas correspondientes.

3.5.5. Las entidades pertinentes probarán a intervalos planificados sus procedimientos de respuesta ante los incidentes.

3.6. *Revisiones posteriores al incidente*

3.6.1. Cuando proceda, y una vez se hayan recuperado del incidente, las entidades pertinentes llevarán a cabo revisiones posteriores al mismo. Las revisiones posteriores al incidente identificarán, cuando se pueda, la causa subyacente y se traducirán en conclusiones documentadas para reducir la ocurrencia y las consecuencias de futuros incidentes.

3.6.2. Las entidades pertinentes velarán por que las revisiones posteriores a los incidentes contribuyan a mejorar su enfoque en materia de seguridad de las redes y de la información, de medidas de tratamiento de riesgos y de procedimientos de gestión, detección y respuesta ante incidentes.

3.6.3. Las entidades pertinentes comprobarán a intervalos planificados si los incidentes condujeron a revisiones posteriores al incidente.

4. **Continuidad de las actividades y gestión de las crisis [artículo 21, apartado 2, letra c), de la Directiva (UE) 2022/2555]**

4.1. *Plan de continuidad de las actividades y de recuperación en caso de catástrofe*

4.1.1. A efectos del artículo 21, apartado 2, letra c), de la Directiva (UE) 2022/2555, las entidades pertinentes establecerán y mantendrán un plan de continuidad de las actividades y de recuperación en caso de catástrofe que pondrán en marcha si se producen incidentes.

4.1.2. Las operaciones de las entidades pertinentes se restablecerán de acuerdo con el plan de continuidad de las actividades y de recuperación en caso de catástrofe. El plan se basará en los resultados de la evaluación de riesgos realizada con arreglo al punto 2.1 e incluirá, según proceda, lo siguiente:

a) objetivos, ámbito de aplicación y público destinatario;
b) roles y responsabilidades;
c) contactos clave y canales de comunicación (internos y externos);
d) condiciones de activación y desactivación del plan;
e) orden de recuperación de las operaciones;
f) planes de recuperación de operaciones específicas, incluidos los objetivos de recuperación;
g) recursos necesarios, incluidas las copias de seguridad y las redundancias;
h) restablecimiento y reanudación de las actividades a partir de medidas temporales.

4.1.3. Las entidades pertinentes realizarán un análisis de impacto operativo para evaluar el posible impacto de las perturbaciones graves en sus operaciones y establecerán, a partir de los resultados de dicho análisis, requisitos de continuidad para los sistemas de redes y de información.

4.1.4. El plan de continuidad de las actividades y el plan de recuperación en caso de catástrofe se probarán, revisarán y, cuando proceda, se actualizarán a intervalos planificados o tras incidentes significativos o cambios significativos en las operaciones o los riesgos. Las entidades pertinentes velarán por que dichos planes engloben las conclusiones extraídas en las pruebas.

4.2. *Gestión de las copias de seguridad y las redundancias*

4.2.1. Las entidades pertinentes mantendrán copias de seguridad de los datos y pondrán a disposición recursos suficientes, como instalaciones, sistemas de redes y de información y personal, para velar por un nivel de redundancia adecuado.

4.2.2. A partir de los resultados de la evaluación de riesgos realizada según el punto 2.1 y el plan de continuidad de las actividades, las entidades pertinentes establecerán planes de copia de seguridad que incluirán lo siguiente:

a) plazos de recuperación;

b) garantías de que las copias de seguridad sean completas y precisas, especialmente los datos de configuración y la información almacenada en el entorno de proveedores de servicios de computación en nube;

c) almacenamiento de copias de seguridad (en línea o fuera de línea) en uno o varios lugares seguros, que no estén en la misma red que el sistema y que estén a una distancia suficiente para escapar de cualquier daño provocado por una catástrofe en el emplazamiento principal;
d) controles adecuados de acceso lógico y físico a las copias de seguridad, de conformidad con el nivel de clasificación de activos;
e) recuperación de datos de las copias de seguridad;
f) plazos de conservación sustentados en los requisitos operativos y reglamentarios.

4.2.3. Las entidades pertinentes verificarán regularmente la integridad de las copias de seguridad.
4.2.4. A partir de los resultados de la evaluación de riesgos realizada con arreglo al punto 2.1 y el plan de continuidad de las actividades, las entidades pertinentes garantizarán una disponibilidad suficiente de los recursos mediante, como mínimo, la redundancia parcial de lo siguiente:

a) los sistemas de redes y de información;
b) los activos, incluidos las instalaciones, los equipos y los suministros;
c) el personal con la responsabilidad, la autoridad y las competencias necesarias;
d) los canales de comunicación adecuados.

4.2.5. Cuando proceda, las entidades pertinentes velarán por que la supervisión y el ajuste de los recursos, incluidas las instalaciones, los sistemas y el personal, estén debidamente fundados en los requisitos de copias de seguridad y redundancia.
4.2.6. Las entidades pertinentes llevarán a cabo pruebas periódicas de la recuperación de copias de seguridad y las redundancias para asegurarse de que, en condiciones de recuperación, es posible depender de ellas y que engloban las copias, los procesos y los conocimientos necesarios para llevar a cabo una recuperación eficaz. Las entidades pertinentes documentarán los resultados de las pruebas y, cuando sea necesario, adoptarán medidas correctoras.

4.3. *Gestión de crisis*

4.3.1. Las entidades pertinentes pondrán en marcha procesos de gestión de crisis.
4.3.2. Las entidades pertinentes velarán por que los procesos de gestión de crisis aborden al menos los siguientes elementos:

a) los roles y responsabilidades del personal y, cuando proceda, los proveedores y los prestadores de servicios, especificando la asignación de roles en situaciones de crisis y los pasos específicos que deben seguirse;
b) los medios de comunicación adecuados entre las entidades pertinentes y las autoridades competentes;
c) la aplicación de medidas adecuadas para garantizar el mantenimiento de la seguridad de los sistemas de redes y de información en situaciones de crisis.

A efectos de la letra b), el flujo de información entre las entidades pertinentes y las autoridades competentes incluirá comunicaciones obligatorias, como informes de incidentes y los plazos correspondientes, así como comunicaciones facultativas.

4.3.3. Las entidades pertinentes pondrán en marcha procesos para gestionar y usar la información recibida de los CSIRT o, cuando proceda, las autoridades competentes, en relación con incidentes, vulnerabilidades, amenazas o posibles medidas de mitigación.
4.3.4. Las entidades pertinentes comprobarán, revisarán y, cuando proceda, actualizarán los planes de gestión de la crisis de forma periódica o después de incidentes significativos o cambios significativos en las operaciones o los riesgos.

5. **Seguridad de las cadenas de suministro [artículo 21, apartado 2, letra d), de la Directiva (UE) 2022/2555]**

5.1. *Política de seguridad de las cadenas de suministros*

5.1.1. A efectos del artículo 21, apartado 2, letra d), de la Directiva (UE) 2022/2555, las entidades pertinentes establecerán, pondrán en marcha y aplicarán una política de seguridad de las cadenas de suministros que rija las relaciones con sus proveedores y prestadores de servicios directos con el fin de mitigar los riesgos detectados para la seguridad de los sistemas de redes y de información. En la política de seguridad de las cadenas de suministros,

las entidades pertinentes determinarán su papel en la cadena de suministro y se lo comunicarán a sus proveedores y prestadores de servicios directos.

5.1.2. Como parte de la política de la cadena de suministro contemplada en el punto 5.1.1, las entidades pertinentes establecerán criterios para seleccionar y contratar a los proveedores y prestadores de servicios. Dichos criterios incluirán lo siguiente:

a) las prácticas de ciberseguridad de sus proveedores y prestadores de servicios, incluidos sus procedimientos de desarrollo seguro;

b) la capacidad de los proveedores y prestadores de servicios para cumplir las especificaciones de ciberseguridad establecidas por las entidades pertinentes;

c) la calidad general y la resiliencia de los productos y servicios TIC y las medidas para la gestión de riesgos de ciberseguridad integradas en ellos, incluidos los riesgos y el nivel de clasificación de los productos y servicios TIC;

d) la capacidad de las entidades pertinentes de diversificar las fuentes de suministro y limitar la dependencia de un proveedor, cuando proceda.

5.1.3. Cuando establezcan su política de seguridad de la cadena de suministro, las entidades pertinentes tendrán en cuenta los resultados de las evaluaciones coordinadas de riesgos para la seguridad de las cadenas de suministro críticas realizadas de conformidad con el artículo 22, apartado 1, de la Directiva (UE) 2022/2555, según proceda.

5.1.4. A partir de la política de seguridad de las cadenas de suministro y teniendo en cuenta los resultados de la evaluación de riesgos realizada de conformidad con el punto 2.1 del presente anexo, las entidades pertinentes se asegurarán de que sus contratos con los proveedores y prestadores de servicios especifiquen, cuando proceda mediante acuerdos de nivel de servicio, los siguientes elementos, según se requiera:

a) los requisitos de ciberseguridad correspondientes a los proveedores y prestadores de servicios, incluidos los requisitos relativos a la seguridad en la adquisición de productos y servicios TIC establecidos en el punto 6.1;

b) los requisitos relativos a la sensibilización, las capacidades y la formación y, cuando proceda, los certificados requeridos de los empleados de los proveedores o prestadores de servicios;

c) los requisitos relativos a los controles de los antecedentes personales de los empleados de los proveedores y prestadores de servicios;

d) la obligación de los proveedores y prestadores de servicios de informar, sin demora indebida, a las entidades pertinentes de aquellos incidentes que presenten un riesgo para la seguridad de los sistemas de redes y de información de dichas entidades;

e) el derecho de auditoría o el derecho a recibir informes de auditoría;

f) la obligación de los proveedores y prestadores de servicios de hacerse cargo de las vulnerabilidades que presenten un riesgo para la seguridad de los sistemas de redes y de información de las entidades pertinentes;

g) los requisitos relativos a la subcontratación y, cuando las entidades pertinentes permitan esta última, los requisitos de ciberseguridad de los subcontratistas de conformidad con los requisitos de seguridad contemplados en la letra a);

h) las obligaciones de los proveedores y prestadores de servicios al finalizar el contrato, tales como la recuperación y eliminación de información que hayan obtenido en el ejercicio de sus funciones.

5.1.5. Las entidades pertinentes tendrán en cuenta los elementos a que se refieren los puntos 5.1.2 y 5.1.3 como parte del proceso de selección de nuevos proveedores o prestadores de servicios, y como parte del proceso de contratación a que se refiere el punto 6.1.

5.1.6. Las entidades pertinentes revisarán la política de seguridad de la cadena de suministro y supervisarán, evaluarán y, cuando proceda, tomarán medidas acordes con los cambios en las prácticas de ciberseguridad de los proveedores y prestadores de servicios, a intervalos planificados o cuando se produzcan cambios significativos en las operaciones o en los riesgos, o acontezcan incidentes significativos relativos a la prestación de servicios TIC o que tengan repercusiones en la seguridad del producto TIC de los proveedores y prestadores de servicios.

5.1.7. A los efectos del punto 5.1.6, las entidades pertinentes:

a) supervisarán periódicamente los informes relativos a la aplicación de los acuerdos de nivel de servicio, cuando proceda;

b) revisarán los incidentes relacionados con los productos y servicios TIC de los proveedores y prestadores de servicios;

c) evaluarán la necesidad de revisiones no programadas y recopilarán las conclusiones de manera comprensible;

d) analizarán los riesgos que planteen los cambios relativos a los productos y servicios TIC de los proveedores y prestadores de servicios y, cuando proceda, adoptarán medidas de mitigación a su debido tiempo.

5.2. *Directorio de proveedores y prestadores de servicios*

Las entidades pertinentes mantendrán y actualizarán un registro de sus proveedores y prestadores de servicios directos, en el que incluirán:

a) los puntos de contacto correspondientes a cada proveedor o prestador de servicios directo;
b) una lista de productos TIC, servicios TIC y procesos TIC proporcionados por el proveedor o prestador de servicios directo a las entidades pertinentes.

6. **Seguridad en la adquisición, el desarrollo y el mantenimiento de sistemas de redes y de información [artículo 21, apartado 2, letra e), de la Directiva (UE) 2022/2555]**

6.1. *Seguridad en la adquisición de servicios TIC o productos TIC*

6.1.1. A los efectos del artículo 21, apartado 2, letra e), de la Directiva (UE) 2022/2555, las entidades pertinentes establecerán y pondrán en marcha procedimientos para gestionar los riesgos derivados de la adquisición de servicios o productos TIC para componentes que sean críticos para la seguridad de los sistemas de redes y de información de las entidades pertinentes, de acuerdo con la evaluación de riesgos realizada con arreglo al punto 2.1, de los proveedores o prestadores de servicios a lo largo de su vida útil.
6.1.2. A los efectos del punto 6.1.1, los procedimientos contemplados en el mismo incluirán:

a) requisitos de seguridad aplicables a los servicios o productos TIC que vayan a adquirirse;
b) requisitos relativos a las actualizaciones de seguridad a lo largo de toda la vida útil de los productos o servicios TIC o a su sustitución tras el final del período de soporte;
c) información que describa los componentes de hardware y software utilizados en los servicios y productos TIC;
d) información que describa las funciones de ciberseguridad de los servicios o productos TIC puestas en marcha o la configuración necesaria para su funcionamiento seguro;
e) garantías de que los servicios o productos TIC cumplen los requisitos de seguridad con arreglo a la letra a);
f) métodos para validar el cumplimiento de los requisitos de seguridad declarados por parte de los servicios o productos de TIC suministrados, y documentación de los resultados de la validación.

6.1.3. Las entidades pertinentes revisarán y, cuando proceda, actualizarán los procedimientos a intervalos planificados, así como cuando se produzcan incidentes significativos.

6.2. *Ciclo de vida del desarrollo seguro*

6.2.1. Antes de desarrollar un sistema de redes y de información, incluidos los programas informáticos, las entidades pertinentes establecerán normas para el desarrollo seguro del mismo, y las aplicarán al desarrollar estos sistemas de redes y de información internamente o cuando externalicen dicho desarrollo. Las normas englobarán todas las fases de desarrollo, como las especificaciones, el diseño, la creación, la implantación y las pruebas.
6.2.2. A los efectos del punto 6.2.1, las entidades pertinentes:

a) llevarán a cabo análisis de los requisitos de seguridad en las fases de especificación y diseño de cualquier proyecto de desarrollo o adquisición emprendido por ellas mismas o en su nombre;
b) aplicarán los principios para diseñar sistemas seguros y principios de codificación seguros a toda actividad de desarrollo de sistemas de información, tales como la promoción de la ciberseguridad desde el diseño o las arquitecturas de confianza cero;
c) establecerán requisitos de seguridad en relación con los entornos de desarrollo;
d) establecerán y aplicarán procesos de pruebas de seguridad en el ciclo de vida del desarrollo;
e) seleccionarán, protegerán y gestionarán adecuadamente los datos de las pruebas de seguridad;
f) sanearán y anonimizarán los datos de las pruebas con arreglo a la evaluación de riesgos realizada de conformidad con el punto 2.1.

6.2.3. En cuanto a la externalización del desarrollo de sistemas de redes y de información, las entidades pertinentes también aplicarán las políticas y procedimientos a que se refieren los puntos 5 y 6.1.

6.2.4. Las entidades pertinentes revisarán y, cuando proceda, actualizarán las normas de desarrollo seguro a intervalos planificados.

6.3. *Gestión de configuraciones*

6.3.1. Las entidades pertinentes adoptarán las medidas adecuadas para establecer, documentar, poner en marcha y supervisar las configuraciones, incluidas las configuraciones de seguridad del hardware de los equipos y programas informáticos, los servicios y las redes.

6.3.2. A los efectos del punto 6.3.1, las entidades pertinentes:

a) crearán un entorno seguro en las configuraciones de sus equipos y programas informáticos, servicios y redes y lo mantendrán;

b) establecerán y pondrán en marcha procesos y herramientas para dar cumplimiento a las configuraciones seguras establecidas para los equipos y programas informáticos, servicios y redes, para los sistemas de nueva instalación y los sistemas en funcionamiento a lo largo de todo su ciclo de vida.

6.3.3. Las entidades pertinentes revisarán y, cuando proceda, actualizarán las configuraciones a intervalos planificados, así como cuando se produzcan incidentes significativos o cambios significativos en las operaciones o los riesgos.

6.4. *Gestión de cambios, reparaciones y mantenimiento*

6.4.1. Las entidades pertinentes aplicarán procedimientos de gestión de cambios para controlar aquellos que se produzcan en los sistemas de redes y de información. Los procedimientos serán, según proceda, coherentes con las políticas generales de las entidades pertinentes relativas a la gestión de cambios.

6.4.2. Los procedimientos contemplados en el punto 6.4.1 se aplicarán en el caso de lanzamientos, modificaciones y cambios de emergencia de cualquier equipo o programa informático en funcionamiento o de cambios en la configuración. Los procedimientos garantizarán que dichos cambios se documenten y, a partir de la evaluación de riesgos realizada de acuerdo con el punto 2.1, se prueben y evalúen teniendo en cuenta el impacto potencial antes de su aplicación.

6.4.3. En caso de que los procedimientos habituales de gestión de cambios no puedan seguirse debido a una emergencia, las entidades pertinentes documentarán el resultado del cambio y explicarán por qué no pudieron seguirse dichos procedimientos.

6.4.4. Las entidades pertinentes revisarán y, cuando proceda, actualizarán los procedimientos a intervalos planificados, así como cuando se produzcan incidentes significativos o cambios significativos en las operaciones o los riesgos.

6.5. *Pruebas de seguridad*

6.5.1. Las entidades pertinentes establecerán, pondrán en marcha y aplicarán orientaciones y procedimientos para las pruebas de seguridad.

6.5.2. Las entidades pertinentes:

a) establecerán, a partir de la evaluación de riesgos realizada de acuerdo con el punto 2.1, la necesidad, el alcance, la frecuencia y el tipo de pruebas de seguridad;

b) realizarán pruebas de seguridad de acuerdo con una metodología de prueba documentada, que englobe los elementos señalados como relevantes para el funcionamiento seguro en un análisis de riesgos;

c) documentarán el tipo, el alcance, la fecha y los resultados de las pruebas, incluidas la evaluación del carácter esencial y las medidas de mitigación correspondientes a cada hallazgo;

d) aplicarán medidas de mitigación en caso de que se produzcan hallazgos críticos.

6.5.3. Las entidades pertinentes revisarán y, cuando proceda, actualizarán las políticas de pruebas de seguridad a intervalos planificados.

6.6. *Gestión de parches de seguridad*

6.6.1. Las entidades pertinentes detallarán y aplicarán procedimientos coherentes con los procedimientos de gestión de cambios a que se refiere el punto 6.4.1, de gestión de vulnerabilidades, de gestión del riesgo y otros procedimientos de gestión pertinentes para garantizar que:

a) los parches de seguridad se apliquen en un plazo razonable desde el momento en que estén disponibles;
b) los parches de seguridad se sometan a ensayo antes de ponerlos en marcha en los sistemas de producción;
c) los parches de seguridad procedan de fuentes de confianza y se compruebe su integridad;
d) se adopten medidas adicionales y se acepten los riesgos residuales en aquellos casos en que no haya un parche disponible o no pueda aplicarse conforme al punto 6.6.2.

6.6.2. Como excepción al punto 6.6.1, letra a), las entidades pertinentes podrán optar por no aplicar parches de seguridad cuando las desventajas de aplicarlos superen los beneficios de ciberseguridad. Las entidades pertinentes documentarán y justificarán debidamente los motivos de tal decisión.

6.7. *Seguridad de las redes*

6.7.1. Las entidades pertinentes adoptarán medidas adecuadas para proteger sus sistemas de redes y de información de las ciberamenazas.
6.7.2. A los efectos del punto 6.7.1, las entidades pertinentes:

a) documentarán la arquitectura de la red de manera comprensible y actualizada;
b) establecerán y aplicarán controles para proteger los dominios de red internos de las entidades pertinentes frente al acceso no autorizado;
c) configurarán los controles para impedir el acceso y las comunicaciones de la red que no sean necesarios para el funcionamiento de las entidades pertinentes;
d) establecerán y aplicarán controles del acceso remoto a los sistemas de redes y de información, incluido el acceso por parte de los proveedores de servicios;
e) no utilizarán los sistemas empleados para gestionar la aplicación de la política de seguridad para otros fines;
f) prohibirán de manera explícita o desactivarán las conexiones y servicios que no sean necesarios;
g) cuando proceda, únicamente permitirán el acceso a los sistemas de redes y de información de las entidades pertinentes a los dispositivos autorizados por estas últimas;
h) permitirán la conexión de los proveedores de servicios previa solicitud de autorización únicamente y durante un período de tiempo limitado, como la duración de una operación de mantenimiento;
i) establecerán la comunicación entre distintos sistemas únicamente a través de canales de confianza que estén aislados mediante separación lógica, criptográfica o física de otros canales de comunicación, y facilitarán la identificación segura de su punto final y la protección de sus datos frente a la modificación o la revelación;
j) adoptarán un plan de ejecución para realizar la transición hacia protocolos de comunicación de la capa de red de última generación de manera segura, adecuada y gradual, y establecerán medidas para acelerar dicha transición;
k) adoptarán un plan de ejecución relativo a la implantación de normas sobre las comunicaciones por correo electrónico modernas, interoperables y aprobadas a escala internacional para proteger las comunicaciones por correo electrónico y mitigar las vulnerabilidades vinculadas a las amenazas relativas a este último, y establecerán medidas para acelerar dicha implantación;
l) aplicarán las mejores prácticas sobre seguridad del sistema de nombres de dominio, la seguridad del enrutamiento de internet y la higiene del enrutamiento del tráfico con origen en la red o destinado a ella.

6.7.3. Las entidades pertinentes revisarán y, cuando proceda, actualizarán estas medidas a intervalos planificados o cuando se produzcan incidentes significativos o cambios significativos en las operaciones o los riesgos.

6.8. *Segmentación de la red*

6.8.1. Las entidades pertinentes segmentarán los sistemas en redes o zonas de acuerdo con los resultados de la evaluación de riesgos a que se refiere el punto 2.1. Segmentarán sus sistemas y redes de los sistemas y redes de terceros.
6.8.2. A tal efecto, las entidades pertinentes:

a) considerarán la relación funcional, lógica y física, incluida la ubicación, entre sistemas y servicios fiables;
b) concederán acceso a una red o zona sobre la base de una evaluación de sus requisitos de seguridad;
c) mantendrán los sistemas que resulten críticos para el funcionamiento de la entidad pertinente o para la protección en zonas seguras;

d) implantarán una zona desmilitarizada dentro de sus redes de comunicación para ofrecer una comunicación segura desde o hacia sus redes;
e) restringirán el acceso y las comunicaciones entre zonas y dentro de ellas a lo necesario para el funcionamiento de las entidades pertinentes o la seguridad;
f) separarán la red específica para la administración de los sistemas de redes y de información de la red operativa de las entidades pertinentes;
g) segregarán los canales de administración de la red del resto de tráfico de la red;
h) separarán los sistemas de producción de los servicios de las entidades pertinentes de los sistemas utilizados para el desarrollo y las pruebas, incluidas las copias de seguridad.

6.8.3. Las entidades pertinentes revisarán y, cuando proceda, actualizarán la segmentación de la red a intervalos planificados, así como cuando se produzcan incidentes significativos o cambios significativos en las operaciones o los riesgos.

6.9. *Protección frente a los programas informáticos maliciosos y no autorizados*

6.9.1. Las entidades pertinentes protegerán sus sistemas de redes y de información frente a los programas informáticos maliciosos y no autorizados.
6.9.2. Para ello, las entidades pertinentes aplicarán, en particular, medidas para detectar o impedir el uso de programas informáticos maliciosos o no autorizados. Las entidades pertinentes velarán, cuando proceda, por que sus sistemas de redes y de información estén equipados con programas informáticos de detección y respuesta, que se actualicen periódicamente de conformidad con la evaluación de riesgos realizada con arreglo al punto 2.1 y los acuerdos contractuales con los proveedores.

6.10. *Gestión y divulgación de las vulnerabilidades*

6.10.1. Las entidades pertinentes recibirán información sobre las vulnerabilidades de sus sistemas de redes y de información, evaluarán su exposición a dichas vulnerabilidades y adoptarán las medidas necesarias para gestionarlas.
6.10.2. A los efectos del punto 6.10.1, las entidades pertinentes:

a) supervisarán la información sobre vulnerabilidades a través de los canales adecuados, tales como los anuncios de los CSIRT, las autoridades competentes o la información facilitada por los proveedores o prestadores de servicios;
b) realizarán, según proceda, exploraciones de vulnerabilidad y registrarán pruebas de los resultados de las mismas, a intervalos planificados;
c) abordarán, sin demora indebida, las vulnerabilidades que las entidades pertinentes consideren críticas para sus operaciones;
d) asegurarán que su gestión de vulnerabilidades sea compatible con sus procedimientos de gestión de cambios, gestión de parches de seguridad, gestión de riesgos y gestión de incidentes;
e) establecerán un procedimiento de divulgación de las vulnerabilidades de conformidad con la política coordinada de divulgación de las vulnerabilidades nacional aplicable.

6.10.3. Cuando esté justificado por el posible impacto de la vulnerabilidad, las entidades pertinentes crearán y llevarán a la práctica un plan para mitigarla. En otros casos, las entidades pertinentes documentarán y justificarán el motivo por el que la vulnerabilidad no requiere reparación.
6.10.4. Las entidades pertinentes revisarán y, cuando proceda, actualizarán a intervalos planificados los canales que utilizan para supervisar la información relativa a las vulnerabilidades.

7. **Orientaciones y procedimientos para evaluar la eficacia de las medidas de gestión de riesgos de ciberseguridad [artículo 21, apartado 2, letra f), de la Directiva (UE) 2022/2555]**

7.1. A los efectos del artículo 21, apartado 2, letra f), de la Directiva (UE) 2022/2555, las entidades pertinentes establecerán, llevarán a la práctica y aplicarán orientaciones y procedimientos para evaluar si las medidas para la gestión de riesgos de ciberseguridad que hayan adoptado se ejecutan y mantienen de manera efectiva.
7.2. Las orientaciones y procedimientos a que hace referencia el punto 7.1 tendrán en cuenta los resultados de la evaluación de riesgos conforme al punto 2.1 y los incidentes significativos ocurridos en el pasado. Las entidades pertinentes determinarán:

a) qué medidas para la gestión de riesgos de ciberseguridad deben supervisarse y medirse, incluidos los procedimientos y controles;
b) los métodos de supervisión, medición, análisis y evaluación, según corresponda, para asegurar resultados válidos;
c) cuándo deben realizarse la supervisión y la medición;
d) quiénes son los responsables de supervisar y medir la eficacia de las medidas para la gestión de riesgos de ciberseguridad;
e) cuándo se deben analizar y evaluar los resultados de la supervisión y la medición;
f) quiénes deben analizar y evaluar estos resultados.

7.3. Las entidades pertinentes revisarán y, cuando proceda, actualizarán las orientaciones y los procedimientos a intervalos planificados, así como cuando se produzcan incidentes significativos o cambios significativos en las operaciones o los riesgos.

8. **Formación en seguridad y prácticas básicas de ciberhigiene [artículo 21, apartado 2, letra g), de la Directiva (UE) 2022/2555]**

8.1. *Mejora de la sensibilización y prácticas básicas de ciberhigiene*

8.1.1. A los efectos del artículo 21, apartado 2, letra g), de la Directiva (UE) 2022/2555, las entidades pertinentes se asegurarán de que sus empleados, incluidos los miembros de los órganos de dirección, así como sus proveedores y prestadores de servicios directos sean conscientes de los riesgos, estén informados de la importancia de la ciberseguridad y apliquen prácticas de ciberhigiene.
8.1.2. A los efectos del punto 8.1.1, las entidades pertinentes ofrecerán a sus empleados, incluidos los miembros de los órganos de dirección, así como a sus proveedores y prestadores de servicios directos, según proceda de conformidad con el punto 5.1.4, un programa de mejora de la sensibilización que:

a) se programará a lo largo del tiempo, de forma que se repitan las actividades e incluya a los nuevos empleados;
b) se establecerá en consonancia con la política de seguridad de las redes y la información, las políticas específicas y los procedimientos pertinentes en materia de seguridad de las redes y de la información;
c) englobará las ciberamenazas relevantes, las medidas para la gestión de riesgos de ciberseguridad en vigor, los puntos de contacto y los recursos para obtener información adicional y asesoramiento sobre aspectos de ciberseguridad, así como las prácticas de ciberhigiene para los usuarios.

8.1.3. El programa de mejora de la sensibilización se probará en términos de eficacia, según proceda. El programa de mejora de la sensibilización se actualizará y se ofrecerá a intervalos planificados teniendo en cuenta los cambios en las prácticas de ciberhigiene y el panorama actual de amenazas y de riesgos para las entidades pertinentes.

8.2. *Formación en seguridad*

8.2.1. Las entidades pertinentes indicarán cuáles son los empleados cuyos roles exigen capacidades y conocimientos especializados de seguridad y velarán por que reciban formación periódica sobre la seguridad de los sistemas de redes y de información.
8.2.2. Las entidades pertinentes establecerán, pondrán en marcha y ejecutarán un programa de formación en consonancia con la política de seguridad de las redes y de la información, las políticas específicas y otros procedimientos pertinentes en materia de seguridad de las redes y de la información que determine las necesidades de formación de ciertos roles y puestos de acuerdo con criterios concretos.
8.2.3. La formación contemplada en el punto 8.2.1 se adecuará a las funciones laborales de los empleados y se evaluará su eficacia. La formación tendrá en cuenta las medidas de seguridad en vigor y englobará lo siguiente:

a) instrucciones relativas a la configuración y el funcionamiento seguros de los sistemas de redes y de información, incluidos los dispositivos móviles;
b) información sobre ciberamenazas conocidas;
c) formación relativa al comportamiento frente a sucesos relevantes para la seguridad.

8.2.4. Las entidades pertinentes llevarán a cabo la formación para los miembros del personal que se trasladen a nuevos puestos o roles que requieran capacidades y conocimientos especializados en seguridad.

8.2.5. El programa se actualizará y desarrollará de manera periódica teniendo en cuenta las normas y reglas aplicables, los roles asignados, las responsabilidades, así como las ciberamenazas conocidas y los avances tecnológicos.

9. **Criptografía [artículo 21, apartado 2, letra h), de la Directiva (UE) 2022/2555]**

9.1. A los efectos del artículo 21, apartado 2, letra h), de la Directiva (UE) 2022/2555, las entidades pertinentes establecerán, llevarán a la práctica y aplicarán orientaciones y procedimientos relativos a la criptografía, con el objetivo de asegurar un uso adecuado y eficaz de la misma para proteger la confidencialidad, autenticidad e integridad de la información en consonancia con la clasificación de activos de las entidades pertinentes y los resultados de la evaluación de riesgos realizada de conformidad con el punto 2.1.

9.2. Las orientaciones y procedimientos a que hace referencia el punto 9.1 establecerán:

a) de acuerdo con la clasificación de activos de las entidades pertinentes, el tipo, la firmeza y la calidad de las medidas criptográficas necesarias para proteger los activos de dichas entidades, incluidos los datos en reposo y los datos en tránsito;

b) teniendo en cuenta la letra a), los protocolos o las familias de protocolos que deben adoptarse, así como los algoritmos criptográficos, la solidez del cifrado, las soluciones criptográficas y las prácticas de uso que deben aprobarse y exigirse para su uso en las entidades, siguiendo, cuando proceda, un enfoque de agilidad criptográfica;

c) el enfoque de las entidades pertinentes sobre la gestión de claves, que incluya, cuando proceda, métodos para lo siguiente:

i) generar distintas claves para sistemas y aplicaciones criptográficos;

ii) expedir y obtener certificados de clave pública;

iii) distribuir claves a las entidades en cuestión, incluida información sobre cómo activar las claves cuando se reciban;

iv) almacenar claves, incluida información sobre cómo acceden a ellas los usuarios autorizados;

v) cambiar o actualizar las claves, incluida información sobre cuándo y cómo modificarlas;

vi) gestionar las claves en riesgo;

vii) anular claves, incluida información sobre cómo retirarlas o desactivarlas;

viii) recuperar las claves perdidas o corrompidas;

ix) hacer copias de seguridad y crear archivos de las claves;

x) destruir claves;

xi) hacer un registro y auditar las actividades relativas a la gestión de claves.

xii) fijar las fechas de activación y desactivación de las claves asegurándose de que estas solo pueden utilizarse durante el período de tiempo especificado de acuerdo con las normas de gestión de claves de la organización.

9.3. Las entidades pertinentes revisarán y, cuando proceda, actualizarán las orientaciones y los procedimientos a intervalos planificados teniendo en cuenta los últimos avances en criptografía.

10. **Seguridad de los recursos humanos [artículo 21, apartado 2, letra i), de la Directiva (UE) 2022/2555]**

10.1. *Seguridad de los recursos humanos*

10.1.1. A los efectos del artículo 21, apartado 2, letra i), de la Directiva (UE) 2022/2555, las entidades pertinentes se asegurarán de que sus empleados y sus proveedores y prestadores de servicios directos, cuando proceda, entiendan sus responsabilidades en materia de seguridad y se comprometan a ellas, según convenga con relación a los servicios ofrecidos y el puesto de trabajo y en consonancia con la política de seguridad de los sistemas de redes y de información de la entidad pertinente.

10.1.2. El requisito contemplado en el punto 10.1.1 incluirá lo siguiente:

a) mecanismos para garantizar que todos los empleados, proveedores y prestadores de servicios directos, cuando proceda, entiendan y respeten las prácticas estándar de ciberhigiene aplicadas por las entidades pertinentes de acuerdo con el punto 8.1;

b) mecanismos para garantizar que todos los usuarios que dispongan de acceso de administración o privilegiado conozcan sus roles, responsabilidades y autoridades y actúen de conformidad con ellos;

c) mecanismos para garantizar que los miembros de los órganos de dirección conozcan sus roles, responsabilidades y autoridades y actúen de conformidad con ellos en lo que se refiere a la seguridad de los sistemas de redes y de información;
d) mecanismos para contratar personal cualificado para los roles correspondientes, como por ejemplo, los controles de referencia, los procedimientos de evaluación, la validación de certificaciones o las pruebas escritas.

10.1.3. Las entidades pertinentes revisarán la asignación de personal a roles específicos, tal como se recoge en el punto 1.2, así como su atribución de recursos humanos a este respecto, a intervalos planificados y al menos una vez al año. Las entidades actualizarán la asignación cuando sea necesario.

10.2. *Comprobación de antecedentes*

10.2.1. Las entidades pertinentes se asegurarán, en la medida posible, de comprobar los antecedentes personales de sus empleados y, cuando proceda, de sus proveedores y prestadores de servicios directos, de conformidad con el apartado 5.1.4, cuando resulte necesario para sus roles, responsabilidades y autoridades.
10.2.2. A los efectos del punto 10.2.1, las entidades pertinentes:

a) aplicarán criterios que establezcan qué roles, responsabilidades y autoridades deben ejercer exclusivamente aquellas personas cuyos antecedentes hayan sido comprobados;
b) se asegurarán de que estas comprobaciones contempladas en el punto 10.2.1 se lleven a cabo antes de que estas personas empiecen a ejercer dichos roles, responsabilidades y autoridades, que tendrán en cuenta las disposiciones legales, normativas y éticas aplicables en proporción a los requisitos operativos, la clasificación de activos contemplada en el apartado 12.1 y los sistemas de redes y de información a los que va a accederse, así como los riesgos percibidos.

10.2.3. Las entidades pertinentes revisarán la política a intervalos planificados y la actualizarán según proceda.

10.3. *Terminación o cambio de los procedimientos de contratación*

10.3.1. Las entidades pertinentes se asegurarán de que la seguridad de los sistemas de redes y de información y las tareas que sigan siendo válidas tras la terminación o el cambio de empleo de sus empleados se definan y ejecuten contractualmente.
10.3.2. A los efectos del punto 10.3.1, las entidades pertinentes recogerán en las condiciones de empleo, contrato o acuerdo de cada persona, las responsabilidades y funciones que siguen teniendo validez una vez finalizado el empleo o contrato, como por ejemplo las cláusulas de confidencialidad.

10.4. *Procedimiento disciplinario*

10.4.1. Las entidades pertinentes establecerán, comunicarán y mantendrán un procedimiento disciplinario para gestionar los incumplimientos de las políticas de seguridad de los sistemas de redes y de información. El proceso tendrá en cuenta los requisitos legales, estatutarios, contractuales y empresariales pertinentes.
10.4.2. Las entidades pertinentes revisarán y, cuando proceda, actualizarán los procedimientos disciplinarios a intervalos planificados o cuando resulte necesario debido a cambios jurídicos o cambios significativos en las operaciones o los riesgos.

11. **Control de accesos [artículo 21, apartado 2, letras i) y j), de la Directiva (UE) 2022/2555]**

11.1. *Política de control de accesos*

11.1.1. A los efectos del artículo 21, apartado 2, letra i), de la Directiva (UE) 2022/2555, las entidades pertinentes establecerán, documentarán y pondrán en marcha políticas de control de acceso lógico y físico relativas al acceso a sus sistemas de redes y de información; basándose en requisitos empresariales y en requisitos de seguridad de los sistemas de redes y de información.
11.1.2. La política a que hace referencia el punto 11.1.1 se encargará de lo siguiente:

a) el acceso de personas, como el personal, los visitantes y las entidades externas, como los proveedores y prestadores de servicios;
b) el acceso por parte de los sistemas de redes y de información;
c) garantizar que solo se autorice el acceso a usuarios que hayan sido debidamente autenticados.

11.1.3. Las entidades pertinentes revisarán y, cuando proceda, actualizarán las políticas a intervalos planificados o cuando se produzcan incidentes significativos o cambios significativos en las operaciones o los riesgos.

11.2. *Gestión de derechos de acceso*

11.2.1. Las entidades pertinentes ofrecerán, modificarán, retirarán y documentarán los derechos de acceso a los sistemas de redes y de información de conformidad con la política de control de accesos prevista en el punto 11.1.

11.2.2. Las entidades pertinentes:

a) concederán y retirarán los derechos de acceso sobre la base de los principios de necesidad de conocer, el mínimo privilegio y separación de competencias;

b) velarán por que los derechos de acceso se modifiquen en consecuencia tras la terminación o el cambio de empleo;

c) velarán por que las personas pertinentes autoricen el acceso a los sistemas de redes y de información;

d) velarán por que los derechos de acceso se encarguen debidamente del acceso de terceros, como visitantes o proveedores y prestadores de servicios, especialmente limitando los derechos de acceso en su alcance y duración;

e) mantendrán un registro de los derechos de acceso concedidos;

f) realizarán un registro de la gestión de los derechos de acceso.

11.2.3. Las entidades pertinentes revisarán los derechos de acceso a intervalos planificados y los modificarán según los cambios organizativos. Las entidades pertinentes documentarán los resultados de la revisión e incluirán los cambios necesarios de los derechos de acceso.

11.3. *Cuentas privilegiadas y cuentas de administración del sistema*

11.3.1. Las entidades pertinentes dispondrán de orientaciones para la gestión de cuentas privilegiadas y cuentas de administración del sistema como parte de la política de control de acceso contemplada en el punto 11.1.

11.3.2. La política a que hace referencia el punto 11.3.1 se encargará de lo siguiente:

a) establecer procedimientos sólidos de identificación y autenticación, como la autenticación de múltiples factores, y procedimientos de autorización para cuentas privilegiadas y cuentas de administración del sistema;

b) crear cuentas específicas que vayan a utilizarse exclusivamente para operaciones de administración del sistema, tales como la instalación, la configuración, la gestión o el mantenimiento;

c) personalizar y restringir en la mayor medida posible los privilegios de la administración del sistema;

d) prever que las cuentas de administración del sistema solo se utilicen para conectarse a los sistemas de administración correspondientes.

11.3.3. Las entidades pertinentes revisarán los derechos de acceso de las cuentas privilegiadas y las cuentas de administración del sistema a intervalos planificados, los modificarán teniendo en cuenta los cambios organizativos y documentarán los resultados de la revisión, incluidos los cambios necesarios en los derechos de acceso.

11.4. *Sistemas de administración*

11.4.1. Las entidades pertinentes restringirán el uso de los sistemas de administración del sistema de conformidad con la política de control de accesos prevista en el punto 11.1.

11.4.2. A tal efecto, las entidades pertinentes:

a) utilizarán únicamente sistemas de administración del sistema a efectos de administración del mismo y no para otras operaciones;

b) separar lógicamente estos sistemas de los programas de aplicación que no se utilicen con fines de administración del sistema;

c) protegerán el acceso a los sistemas de administración del sistema mediante la autenticación y el cifrado.

11.5. *Identificación*

11.5.1. Las entidades pertinentes gestionarán todo el ciclo de vida de las identidades de los sistemas de redes y de información y sus usuarios.

11.5.2. A tal efecto, las entidades pertinentes:

a) crearán identidades únicas para los sistemas de redes y de información y sus usuarios;
b) asociarán la identidad de los usuarios a una sola persona;
c) se encargarán de la supervisión de las identidades de los sistemas de redes y de información;
d) realizarán un registro de la gestión de las identidades.

11.5.3. las entidades pertinentes solo autorizarán las identidades asignadas a múltiples personas, como las identidades compartidas, cuando sean necesarias por razones empresariales u operativas y estén sujetas a un proceso de aprobación y documentación explícito. Las entidades pertinentes tendrán en cuenta las identidades asignadas a múltiples personas en el marco de gestión de riesgos de ciberseguridad contemplado en el punto 2.1.

11.5.4. Las entidades pertinentes revisarán periódicamente las identidades correspondientes a los sistemas de redes y de información y sus usuarios y, cuando ya no sean necesarias, las desactivarán inmediatamente.

11.6. *Autenticación*

11.6.1. Las entidades pertinentes pondrán en marcha tecnologías y procedimientos de autenticación seguros basados en las restricciones de acceso y en la política de control de acceso.

11.6.2. A tal efecto, las entidades pertinentes:

a) garantizarán que la solidez de la autenticación sea adecuada para a la clasificación del activo al que se va a acceder;
b) controlar la asignación a los usuarios y la gestión de información de autenticación secreta mediante un proceso que garantice la confidencialidad de la información, incluido el asesoramiento al personal sobre el tratamiento adecuado de la información de autenticación;
c) exigir el cambio de credenciales de autenticación al principio, a intervalos predefinidos y cuando se sospeche que las credenciales corren algún peligro;
d) exigir el restablecimiento de las credenciales y el bloqueo de los usuarios tras un número predefinido de intentos de conexión infructuosos;
e) cerrar las sesiones inactivas tras un período de inactividad predefinido; y
f) exigir credenciales separadas para obtener un acceso privilegiado o acceder a cuentas de administración.

11.6.3. En la medida de lo posible, las entidades pertinentes utilizarán los métodos de autenticación más avanzados, de conformidad con el riesgo evaluado asociado y la clasificación del activo al que se vaya a acceder, así como información de autenticación exclusiva.

11.6.4. Las entidades pertinentes revisarán los procedimientos y las tecnologías de autenticación a intervalos planificados.

11.7. *Autenticación de múltiples factores*

11.7.1. Las entidades pertinentes velarán por que los usuarios sean autenticados mediante múltiples factores de autenticación o mecanismos de autenticación continua para acceder a los sistemas de redes y de información la entidad, cuando proceda, de conformidad con la clasificación del activo al que se va a acceder.

11.7.2. Las entidades pertinentes se asegurarán de que la solidez de la autenticación sea adecuada a la clasificación del activo al que se va a acceder.

12. **Gestión de activos [artículo 21, apartado 2, letra i), de la Directiva (UE) 2022/2555]**

12.1. *Clasificación de activos*

12.1.1. A los efectos del artículo 21, apartado 2, letra i), de la Directiva (UE) 2022/2555, las entidades pertinentes establecerán los niveles de clasificación de todos los activos, incluida la información, que formen parte del ámbito de sus sistemas de redes y de información con relación al nivel de protección requerido.

12.1.2. A los efectos del punto 12.1.1, las entidades pertinentes:

a) establecerán un sistema de niveles de clasificación de los activos;

b) asociarán todos los activos con un nivel de clasificación, basado en los requisitos de confidencialidad, integridad, autenticidad y disponibilidad, para indicar la protección requerida en función de su sensibilidad, criticidad, riesgo y valor empresarial;

c) amoldarán los requisitos de disponibilidad de los activos a los objetivos de entrega y recuperación establecidos en sus planes de continuidad de las actividades y de recuperación en caso de catástrofe.

12.1.3. Las entidades pertinentes realizarán revisiones periódicas de los niveles de clasificación de los activos y los actualizarán, según proceda.

12.2. *Gestión de activos*

12.2.1. Las entidades pertinentes establecerán, pondrán en marcha y aplicarán una política para la correcta gestión de los activos, incluida la información, acorde con su política de seguridad de las redes y de la información y la pondrán en conocimiento de todo aquel que utilice o gestione los activos.

12.2.2. Dicha política:

a) hará referencia a toda la vida útil de los activos, especialmente su adquisición, uso, almacenamiento, transporte y eliminación;

b) establecerá normas para su uso seguro, su almacenamiento seguro, su transporte seguro y la supresión y destrucción irreversibles de los activos;

c) preverá que la transferencia se lleve a cabo de manera segura, de conformidad con el tipo de activo que transfiera.

12.2.3. Las entidades pertinentes revisarán y, cuando proceda, actualizarán la política a intervalos planificados o cuando se produzcan incidentes significativos o cambios significativos en las operaciones o los riesgos.

12.3. *Política de soportes extraíbles*

12.3.1. Las entidades pertinentes establecerán, pondrán en marcha y aplicarán una política relativa a la gestión de soportes de almacenamiento extraíbles y la pondrán en conocimiento de sus empleados y de terceros que manipulen soportes de almacenamiento extraíbles en las instalaciones de las entidades pertinentes o en otros lugares en los que los soportes extraíbles estén conectados a los sistemas de redes y de información de la entidad.

12.3.2. Dicha política:

a) preverá una prohibición técnica para la conexión de soportes extraíbles salvo que existan razones internas para su uso;

b) preverá la deshabilitación de la reproducción automática desde dichos soportes y la detección de códigos maliciosos en los mismos antes de que se utilicen en los sistemas de las entidades pertinentes;

c) preverá medidas para controlar y proteger los soportes de almacenamiento extraíbles que contengan datos durante el tránsito y el almacenamiento;

d) según proceda, preverá medidas para la utilización de técnicas criptográficas para proteger los datos contenidos en los soportes de almacenamiento extraíbles.

12.3.3. Las entidades pertinentes revisarán y, cuando proceda, actualizarán la política a intervalos planificados o cuando se produzcan incidentes significativos o cambios significativos en las operaciones o los riesgos.

12.4. *Inventario de activos*

12.4.1. Las entidades pertinentes crearán y mantendrán un inventario completo, preciso, actualizado y coherente de sus activos. Registrarán los cambios en las entradas del inventario de manera que puedan rastrearse.

12.4.2. La granularidad del inventario de los activos se situará en un nivel adecuado a las necesidades de las entidades pertinentes. El inventario incluirá lo siguiente:

a) la lista de operaciones y servicios y su descripción;

b) la lista de sistemas de redes y de información y otros activos asociados que sirvan de apoyo a las operaciones y servicios de las entidades pertinentes.

12.4.3. Las entidades pertinentes revisarán y actualizarán periódicamente el inventario y sus activos y registrarán el historial de cambios.

12.5. *Depósito, devolución o supresión de activos al término de la relación laboral*

Las entidades pertinentes crearán, pondrán en marcha y aplicarán procedimientos para que los activos bajo custodia del personal sean depositados, devueltos o suprimidos al término de la relación laboral, y documentarán el depósito, la devolución y la supresión de dichos activos. Cuando no sea posible el depósito, la devolución o la supresión de activos, las entidades pertinentes se asegurarán de que dichos activos ya no puedan acceder a los sistemas de redes y de información de la entidad de conformidad con el punto 12.2.2.

13. **Seguridad medioambiental y física [artículo 21, apartado 2, letras c), e) e i), de la Directiva (UE) 2022/2555]**

13.1. *Servicios públicos*

13.1.1. A los efectos del artículo 21, apartado 2, letra c), de la Directiva (UE) 2022/2555, las entidades pertinentes evitarán las pérdidas, los daños o riesgos de los sistemas de redes y de información o la interrupción de sus operaciones debido al fallo y la interrupción de los servicios públicos.

13.1.2. A tal efecto, cuando proceda, las entidades pertinentes:

a) protegerán las instalaciones de los fallos eléctricos y de otras alteraciones causadas por fallos en servicios públicos como la electricidad, las telecomunicaciones, el suministro de agua, el gas, las aguas residuales, la ventilación o el aire acondicionado;

b) considerarán la utilización de redundancias en los servicios de utilidad pública;

c) protegerán los servicios públicos de electricidad y telecomunicaciones, que transportan datos u ofrecen sistemas de redes y de información, frente a la interceptación y los daños;

d) supervisarán los servicios públicos contemplados en la letra c) e informarán al personal interno o externo competente de los sucesos que tengan lugar más allá de los umbrales mínimo y máximo de control a que se refiere el punto 13.2.2, letra b), que afecten a los servicios de utilidad pública;

e) concluirán contratos para el suministro de emergencia con los servicios correspondientes, tales como el combustible para el suministro eléctrico de emergencia;

f) Garantizarán la eficacia continua, supervisarán, mantendrán y probarán el suministro de los sistemas de redes y de información necesarios para el funcionamiento del servicio ofrecido, especialmente la electricidad, el control de la temperatura y la humedad, las telecomunicaciones y la conexión a Internet.

13.1.3. Las entidades pertinentes comprobarán, revisarán y, cuando proceda, actualizarán las medidas de protección de forma periódica o después de incidentes significativos o cambios significativos en las operaciones o los riesgos.

13.2. *Protección contra las amenazas físicas y medioambientales*

13.2.1. A los efectos del artículo 21, apartado 2, letra e), de la Directiva (UE) 2022/2555, las entidades pertinentes evitarán o reducirán las consecuencias de los sucesos que tengan lugar a causa de amenazas físicas y medioambientales, como las catástrofes naturales y otras amenazas intencionadas o inintencionadas, a partir de los resultados de la evaluación de riesgos realizada de conformidad con el punto 2.1.

13.2.2. A tal efecto, cuando proceda, las entidades pertinentes:

a) diseñarán y pondrán en marcha medidas de protección contra las amenazas físicas y medioambientales;

b) determinarán umbrales mínimos y máximos de control de las amenazas físicas y medioambientales;

c) supervisarán los parámetros medioambientales e informarán al personal interno o externo competente de los sucesos que tengan lugar más allá de los umbrales mínimo y máximo de control a que se refiere la letra b).

13.2.3. Las entidades pertinentes comprobarán, revisarán y, cuando proceda, actualizarán las medidas de protección de forma periódica o después de incidentes significativos o cambios significativos en las operaciones o los riesgos.

13.3. *Control de acceso perimetral y físico*

13.3.1. A los efectos del artículo 21, apartado 2, letra i), de la Directiva (UE) 2022/2555, las entidades pertinentes evitarán y controlarán el acceso físico no autorizado, los daños y las interferencias a sus sistemas de redes y de información.

13.3.2. A tal efecto, las entidades pertinentes:

a) sobre la base de la evaluación de riesgos realizada con arreglo al punto 2.1, establecerán y utilizarán perímetros de seguridad para proteger las zonas en las que se ubican los sistemas de redes y de información;

b) protegerán las zonas a que se refiere la letra a) mediante controles de entrada y puntos de acceso adecuados;

c) diseñarán e implantarán la seguridad física de las oficinas, las salas y las instalaciones;

d) supervisarán de manera continuada sus instalaciones en lo que se refiere al acceso físico no autorizado.

13.3.3. Las entidades pertinentes comprobarán, revisarán y, cuando proceda, actualizarán las medidas de control del acceso físico de forma periódica o después de incidentes significativos o cambios significativos en las operaciones o los riesgos.