NOTAS DE LA SOLUCIÓN

EL REGLAMENTO DE RESILIENCIA OPERATIVA DIGITAL (DORA) Y EL DNS

Cómo aplicar las mejores prácticas del DNS para facilitar el cumplimiento de DORA

INTRODUCCIÓN

El Reglamento de Resiliencia Operativa Digital, conocido como DORA, es una normativa de la Unión Europea (UE) diseñada para reforzar la resiliencia operativa digital de las entidades financieras. Entró en vigor el 17 de enero de 2025 y garantiza que los bancos, las compañías de seguros, las empresas de servicios de inversión y otras entidades financieras puedan resistir, responder y recuperarse de las perturbaciones relacionadas con las tecnologías de la información y la comunicación (TIC), como los ciberataques o los fallos del sistema.

DORA se organiza en nueve capítulos con las correspondientes normas técnicas de regulación. Además de los bancos y otras organizaciones de servicios financieros tradicionales, el Reglamento y sus normas se aplican a otras empresas del sector financiero, como los proveedores de servicios de criptoactivos y los proveedores terceros de servicios de TIC. Según PWC, el cumplimiento obligatorio de DORA se extiende a más de 22 000 entidades[1], ya que la directiva no se limita a las empresas ubicadas en la UE, sino también a cualquier entidad financiera que opere o realice transacciones comerciales dentro de la zona.

El artículo 1 de DORA delinea las diversas normas reglamentarias que se refieren a la seguridad de las redes y los sistemas de información. Entre los temas tratados figuran la gestión del riesgo relacionado con las TIC, la notificación de incidentes, las pruebas de resiliencia operativa digital, la gestión del riesgo relacionado con las TIC derivado de terceros y el intercambio de información e inteligencia sobre ciberamenazas.[2]

A medida que estas normas evolucionen, los requisitos específicos asociados a ellas se irán aclarando para las entidades financieras. Por ejemplo, el *Informe final sobre el proyecto de normas técnicas de regulación que especifican los elementos relacionados con las pruebas de penetración basadas en amenazas*[3] aporta mayor claridad sobre los requisitos de dichas pruebas. El informe explica que los requisitos de DORA serán interoperables con otras iniciativas normativas relacionadas con la seguridad, como el marco Threat Intelligence-Based Ethical Red-Teaming (TIBER-EU) asociado al Banco Central Europeo. Como se indica en el informe, «[el marco TIBER-EU] también puede ayudar a las autoridades competentes y a las entidades financieras a cumplir los requisitos de las pruebas de penetración basadas en amenazas en virtud del Reglamento de Resiliencia Operativa Digital (DORA)».[4] El informe también hace referencia al documento del Banco Central Europeo, *La adopción de TIBER-EU ayudará a cumplir los requisitos de DORA*.[5]

CÓMO EL DNS AYUDA AL CUMPLIMIENTO DE LA NORMATIVA DORA

El Sistema de Nombre de Dominios (DNS) desempeña un papel fundamental en todas las interacciones de red entre dispositivos, aplicaciones, dominios de Internet, bases de datos y recursos en la nube. Cuando se gestiona y se implementa de forma estratégica, el protocolo DNS también sirve como punto proactivo de aplicación de la seguridad de la red, una valiosa fuente de análisis forense digital y un facilitador eficaz para la respuesta rápida ante incidentes. Como tal, el DNS se encuentra en una posición única para ayudar a las entidades financieras a ejecutar una serie de actividades de cumplimiento de la normativa DORA, entre las que se incluyen:

- Gestión del riesgo relacionado con las TIC (Capítulo II)
- Gestión, clasificación y notificación de incidentes relacionados con las TIC (capítulo III)
- Pruebas de resiliencia operativa digital (Capítulo IV)
- Gestión del riesgo relacionado con las TIC derivado de terceros (Capítulo V)
- Acuerdos de intercambio de información (Capítulo VI)

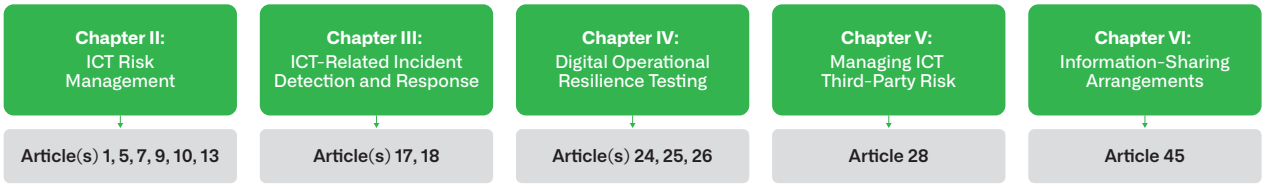

Figura 1. Dónde el DNS contribuye a las actividades de cumplimiento de la normativa DORA

Cabe señalar que, además de ajustarse a los principios específicos de DORA, la eficacia del DNS es tal que muchas organizaciones se beneficiarían de incorporar sus capacidades para cumplir la mayor parte de la normativa. Dado que el DNS ya está integrado en las redes de las organizaciones, ofrece una forma más práctica y eficiente de mejorar la resiliencia operativa digital y la seguridad que la adopción de tecnologías y controles completamente nuevos. A la hora de considerar en qué puede contribuir el DNS a las actividades de DORA, las entidades deben aplicar el principio de proporcionalidad del artículo 4 del reglamento.

Las recomendaciones que figuran a continuación se organizan por capítulos pertinentes de las directrices de DORA, junto con anotaciones sobre los artículos específicos del reglamento con los que se alinean.

GESTIÓN DEL RIESGO RELACIONADO CON LAS TIC

Muchas entidades financieras consideran que el DNS es «solo una parte de la infraestructura de la red», pero es esencial para la resiliencia operativa digital que DORA tiene como objetivo mejorar. Una perturbación del DNS es catastrófica, ya que afecta a casi todas las aplicaciones y servicios de una entidad financiera. Por esta razón, las entidades que cumplen con DORA deben incorporar la disponibilidad del servicio DNS en la planificación de la gestión del riesgo relacionado con las TIC al mismo nivel que otros sistemas básicos.[6] Parte de ese esfuerzo implica utilizar las mejores prácticas del sector en la implementación y gestión de la infraestructura del DNS interna.

Además, dado que las entidades financieras interactúan regularmente con entidades externas y usuarios externos, se debe prestar la misma atención a la ciberhigiene en torno al DNS externo. A efectos de cumplimiento, las organizaciones deben garantizar que los dominios del DNS públicos (autoritativos) sigan siendo resilientes y seguros. Los agentes de amenazas se dirigen activamente a los dominios autoritativos mal configurados debido a la laxitud de las políticas y los procesos de seguridad. La gestión del DNS externo también puede implicar a proveedores terceros de servicios de TIC, a los que también se aplican las normativas, por lo que los responsables del cumplimiento de DORA deben tener en cuenta la gestión y mitigación del riesgo relacionado con las TIC derivado de terceros de los servicios del DNS asociados a estas partes.

Recomendaciones:

- Implemente arquitecturas de DNS resilientes, diseñadas para soportar la continuidad del servicio y dimensionadas para la capacidad máxima, junto con políticas y procedimientos coherentes para mantener la infraestructura del DNS y la disponibilidad y seguridad del servicio. (Artículos 7, 9)
- Asegúrese de que una parte de la organización sea responsable de gestionar los nombres de dominio externos, actuando como un registrador/registro interno, para evitar que partes dispares de la organización registren y gestionen dominios a través de múltiples proveedores. (Artículo 5)
- Implemente servicios de DNS de protección para bloquear y registrar el tráfico del DNS malicioso, evitar que el DNS se utilice para la exfiltración de datos, identificar el tráfico anómalo y proporcionar datos para el análisis forense y la respuesta a incidentes. (Artículos 9, 10, 13)

GESTIÓN, CLASIFICACIÓN Y REPORTE DE INCIDENTES RELACIONADOS CON LAS TIC

Los profesionales de la seguridad utilizan el DNS durante la respuesta a incidentes para identificar y bloquear nuevas comunicaciones maliciosas y ayudar a clasificar y determinar el alcance de cualquier compromiso. Todas las comunicaciones de red comienzan con una consulta al DNS, lo que hace que los registros, que contienen datos de consultas y respuestas, junto con los registros de DHCP y la información de los activos, sean esenciales para la gestión de incidentes relacionados con las TIC. Por ejemplo, el acceso inmediato a los registros de los dispositivos de una red que pueden haberse comunicado con un host malicioso ayuda a los equipos de seguridad a identificar la magnitud y la clasificación de cualquier incidente. Del mismo modo, los registros DHCP identifican qué direcciones IP se han asociado a un activo determinado. Dado que la mayoría de los registros de seguridad identifican los dispositivos basándose en direcciones IP transitorias en lugar de fijas, las organizaciones que deseen garantizar una correlación precisa y coherente de los eventos y las amenazas deben asegurarse de que los datos y el contexto relevantes a nivel de dispositivo puedan compartirse con las herramientas de operaciones de seguridad.

Recomendaciones:

- Registre continuamente los datos de las consultas y respuestas DNS, la actividad de concesión del DHCP y los datos de los activos para facilitar la correlación precisa de los eventos y proporcionar contexto para el análisis forense como parte de la gestión de incidentes relacionados con las TIC. (Artículos 17.3 y 18.1)
- Implemente los servicios DNS de protección como un punto de control para bloquear el tráfico DNS malicioso. Este punto de control debe incluir inteligencia de amenazas relacionada con los indicadores utilizados en el servicio DNS de Protección, de modo que el contexto asociado con cualquier tráfico bloqueado pueda compartirse con las herramientas del ecosistema de seguridad para ayudar en la evaluación. (Artículo 17)

PRUEBAS DE RESILIENCIA OPERATIVA DIGITAL

El cumplimiento de la norma de resiliencia operativa digital DORA requiere pruebas adicionales de continuidad del negocio y recuperación ante desastres (artículo 24), así como pruebas de vulnerabilidad y penetración dentro de un marco de autoridad competente (artículos 25 y 26). Al igual que con las consideraciones de riesgo, quienes supervisan el cumplimiento de DORA deben tener en cuenta el papel fundamental que desempeña el DNS en la disponibilidad de la red. Por ejemplo, las organizaciones pueden aprovechar el DNS para proporcionar continuidad del negocio mediante el balanceo de la carga de los servidores globales. En lo que respecta a la recuperación ante desastres, una perturbación del DNS debido a un ciberataque, una configuración incorrecta o un desastre natural puede provocar la interrupción de las operaciones comerciales. Por lo tanto, es obligatorio que las entidades financieras fortalezcan el DNS y los servicios de red esenciales asociados, como el DHCP, para cumplir los requisitos de resiliencia operativa digital.

Recomendaciones:

- Revise la arquitectura y los servicios de DNS internos y externos para «identificar debilidades, deficiencias y brechas en la resiliencia operativa digital, y aplicar rápidamente medidas correctivas». Normas técnicas como NIST 800-81 pueden ser útiles en este sentido. (Artículo 24(1))
- Al desarrollar un programa integral de pruebas de resiliencia operativa digital, asegúrense de que abarque específicamente los servicios, la infraestructura y los protocolos del DNS. La restauración de los servicios del DNS es un requisito previo esencial para la recuperación de las aplicaciones y servicios de una organización, y el propio DNS puede facilitar la continuidad del servicio y la recuperación ante desastres. (Artículo 24.1)
- Dada la dependencia de una red del DNS, asegúrese de que los procedimientos de prueba específicos para los servicios y la infraestructura de DNS formen parte del plan general de pruebas de resiliencia operativa digital. (Artículo 24.2)
- Al probar la resiliencia operativa digital y trabajar con proveedores externos de pruebas de penetración basadas en amenazas (TLPT), asegúrese de que se llevan a cabo pruebas específicas relacionadas con el DNS para verificar la disponibilidad y la seguridad. (Artículos 25, 26)
- Áreas clave que deben incluirse:
    - » Verifique que la resiliencia del DNS funciona según lo previsto, especialmente que existen múltiples rutas redundantes para la resolución de nombres.
    - » Asegúrese de que el tráfico del DNS saliente de las redes y sistemas de información de una organización se enruta a través de resolutores del DNS controlados (que deben registrar los datos de las consultas y las respuestas).
    - » Consulte los nombres de dominio asociados a la actividad maliciosa actual.
    - » Compruebe si es posible extraer datos a través de consultas DNS e infiltrar malware a través de respuestas del DNS.
    - » Implemente procedimientos y herramientas automatizadas que tengan en cuenta la ciberhigiene del DNS, como garantizar que se rectifiquen los nombres de dominios tipo "dangling" y la delegación incorrecta de subdominios.

GESTIÓN DEL RIESGO RELACIONADO CON LAS TIC DERIVADO DE TERCEROS

Los servicios del DNS, como el DNS externo, entran en el ámbito de aplicación de DORA porque pueden ser gestionados por proveedores terceros de servicios de TIC. Además, también pueden gestionar subdominios del DNS que les han sido delegados para servicios específicos.

Recomendaciones:

- Revise los acuerdos con cualquier tercero que gestione servicios o infraestructuras DNS, como dominios externos, para asegurarse de que se ajustan a las normativas y políticas de su organización y proporcionen los mismos niveles de resiliencia y seguridad operativa. (Artículo 28)

ACUERDOS DE INTERCAMBIO DE INFORMACIÓN

Las entidades financieras comparten regularmente indicadores de compromiso (IoCs) y tácticas, técnicas y procedimientos (TTP) con comunidades de servicios financieros de confianza, incluidas las protecciones adecuadas para salvaguardar la información confidencial. Dentro de estos grupos de confianza, las entidades financieras pueden utilizar los registros de consultas y respuestas DNS, así como la información de los dominios maliciosos bloqueados, como parte de la información que comparten.

Recomendaciones:

- Prepárese para compartir información mediante la implementación de una política para proporcionar IoC relacionados con el DNS. Acordar previamente los formatos de datos con un grupo de intercambio sería de gran ayuda desde el punto de vista operativo, especialmente cuando los indicadores se incorporen a herramientas operativas, como un sistema de gestión de eventos e información de seguridad (SIEM). En particular, la información sobre actividades maliciosas capturada y compartida a través de los servicios de DNS protector suele ayudar a otras entidades financieras a mejorar la defensa de la red. (Artículo 45)

SIMPLIFIQUE EL CUMPLIMIENTO DE DORA CON INFOBLOX

Para cumplir más fácilmente con DORA, las entidades financieras deben alinear sus servicios de DNS con los principios de DORA, centrándose en la resiliencia operativa digital y la seguridad para gestionar eficazmente el riesgo relacionado con las TIC. Esta alineación incluye la mejora de las protecciones contra amenazas como el phishing y la exfiltración de datos, y la adhesión a marcos como TIBER-EU y MITRE ATT&CK para la inteligencia sobre amenazas. Infoblox ofrece soluciones diseñadas para mitigar estos riesgos y ayudar a cumplir las normativas de gestión del riesgo relacionado con las TIC.

Además, la sólida infraestructura DNS y las soluciones de seguridad de Infoblox están especialmente diseñadas para ayudar a las entidades financieras a cumplir los principios de DORA. Al centrarse en servicios de DNS seguros y resilientes, Infoblox ayuda a las entidades sujetas a DORA a mitigar los riesgos asociados a las comunicaciones del DNS no gestionadas, como el phishing, el comando y control de malware (C2) y la exfiltración de datos. Aprovechando marcos líderes en el sector, como MITRE ATT&CK, Infoblox proporciona inteligencia procesable y mitigaciones personalizadas que se ajustan a los requisitos de gestión del riesgo relacionado con las TIC. Además, la experiencia de Infoblox en la integración de las directrices de ENISA y NIST garantiza que las entidades financieras cumplan sus obligaciones de disponibilidad y seguridad mientras navegan eficazmente por complejos entornos normativos.

1. How the digital operational resilience act helps your continuity, PwC.
2. DORA Capítulo 1 Disposiciones Generales, Artículo 1(1) Objeto
3. Final Report on draft RTS specifying elements related to threat led penetration tests (reference JC 2024 29), Autoridad Europea de Valores y Mercados (AEVM), 7 de julio de 2024.
4. What is TIBER-EU?, Banco Central Europeo.
5. Adopting TIBER-EU will help fulfil DORA requirements, Banco Central Europeo, septiembre de 2024.
6. Reglamento DORA: «función esencial o importante»: una función cuya perturbación afectaría significativamente al rendimiento financiero de una entidad financiera o a la solidez o continuidad de sus servicios y actividades o cuya interrupción o ejecución defectuosa o fallida afectaría significativamente al cumplimiento continuado de una entidad financiera con las condiciones y obligaciones de su autorización, o con sus demás obligaciones con arreglo al Derecho aplicable en materia de servicios financieros».

infoblox.

Infoblox une redes y seguridad para ofrecer un rendimiento y una protección inigualables. Con la confianza de empresas Fortune 100 e innovadores emergentes, proporcionamos visibilidad y control en tiempo real sobre quién y qué se conecta a su red, para que su organización funcione más rápido y detenga antes las amenazas.

Sede corporativa
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054 (EE. UU.)

+1.408.986.4000
www.infoblox.com/es

Versión: 20250625v1