

Procedimiento de notificación a la CNMV de Incidentes graves relacionados con las TIC y notificación voluntaria de las ciberamenazas importantes

09 de diciembre de 2024

Introducción

Las entidades financieras, para cumplir con sus obligaciones del artículo 19 del Reglamento (UE) 2022/2554 (de resiliencia operativa digital o DORA), deberán notificar los incidentes graves relacionados con las TIC siguiendo el contenido y los plazos que se especifican en los RTS e ITS¹ a su autoridad competente.

La CNMV está implementando un sistema de recepción de dichas notificaciones a través de su Sede Electrónica por medio de certificado de persona jurídica.

Procedimiento de notificación

El procedimiento para notificar tanto los incidentes graves como las ciberamenazas importantes a la CNMV, de manera transitoria, es el que se describe a continuación:

1. La entidad debe descargar la siguiente plantilla, en formato Excel, con la información a rellenar:

https://cnmv.es/DocPortal/Ciberseguridad/Plantilla_DORA_IR.xlsx

2. La entidad enviará un correo electrónico al buzón de ciberseguridad de la CNMV para informar de su intención de enviar una notificación. Dicho correo tendrá en cuenta los siguientes requisitos:

Para: ciberseguridad@cnmv.es

Asunto: DORA, notificación de incidente grave/ciberamenaza importante.

Cuerpo del mensaje:

- Nombre e Identificador de Entidad Legal (código LEI) de la entidad financiera afectada (o el de varias, si se trata de un reporte agregado).
 - Código de referencia del incidente asignado por la entidad financiera.
3. La CNMV dará de alta a la entidad en su sistema de intercambio. La entidad recibirá un correo electrónico, a la dirección que se usó en el paso anterior, para darse de alta en dicho sistema de intercambio.

¹ [Reglamento Delegado \(UE\) 2024/1772 de la Comisión sobre los criterios para la clasificación de los incidentes relacionados con las TIC y RTS e ITS sobre el contenido, formato y plazos para notificar incidentes graves relacionados con las TIC y ciberamenazas importantes.](#)

4. Una vez que acceda a este sistema de intercambio podrá enviar la notificación a la CNMV adjuntando la plantilla con la información a enviar, junto con otra información adicional que quiera aportar.
5. La CNMV le responderá con un acuse de recibo de dicha notificación.

Observaciones adicionales

Si la entidad que comunica incidentes a la CNMV no es la entidad financiera afectada por el incidente², la entidad financiera debe de notificarlo previamente³ al buzón de ciberseguridad@cnmv.es (informando del nombre de la entidad que va a notificar, los datos de contacto y el código de identificación de dicha entidad). Y de manera similar, cuando dicha entidad deje de notificar los incidentes en nombre de la entidad financiera, la entidad financiera deberá notificarlo a la CNMV del mismo modo.

Si la entidad ya ha notificado un incidente previamente y sigue dada de alta en el sistema de intercambio de la CNMV, no resultará necesaria la realización del paso número 3.

Sólo se debe enviar a la CNMV incidentes de entidades financieras en las que la CNMV es la autoridad competente de conformidad con lo dispuesto en DORA en el Artículo 46 de DORA.

El contenido de la plantilla, en formato Excel, podrá ser rellenado en el idioma español o inglés, salvo los campos seleccionables.

Si la entidad financiera no es capaz de enviar alguna de las notificaciones con el contenido y en el plazo indicado en los RTS e ITS, de acuerdo con el apartado 3 del artículo 5 del borrador final de los RTS, deberá informar a la CNMV, sin demora indebida, pero no después del plazo especificado para la notificación. Para ello, informe por correo electrónico al buzón de ciberseguridad: ciberseguridad@cnmv.es, justificando las razones del retraso.

Si tiene alguna duda, envíe su consulta al buzón de ciberseguridad de la CNMV: ciberseguridad@cnmv.es (no se debe enviar información de carácter confidencial por este canal).

Sin perjuicio del reporte a la CNMV, el INCIBE-CERT puede ofrecerle soporte técnico para la resolución de incidentes:

<https://www.incibe.es/incibe-cert/incidentes/respuesta-incidentes>

² Apartado 5 del artículo 19 de DORA.

³ Artículo 6 del borrador final del ITS sobre la notificación de incidentes graves relacionados con las TIC.