BANCO DE ESPAÑA
Eurosistema

PÚBLICO

Dirección General de Supervisión

03.05.2021

Procedimiento de notificación de ciberincidentes relevantes de las entidades de crédito bajo supervisión directa del Banco de España

Departamento de EMS y otras fuera del ámbito del MUS

RESUMEN Este documento contiene las instrucciones necesarias para que las entidades de crédito bajo la supervisión directa del Banco de España notifiquen los ciberincidentes relevantes.

Hoja de Control

Título	Procedimiento de notificación de ciberincidentes relevantes de las entidades de crédito bajo supervisión directa del Banco de España
Autor	Departamento de Funciones Horizontales – Grupo de Riesgo Tecnológico
Versión	1.0
Fecha	03.05.2021

Registro de Cambios

Versión	Fecha	Motivo del cambio

ÍNDICE

1 Introducción

La sofisticación de los ciberataques experimentados por el sistema financiero durante los últimos años ha aumentado significativamente, y el ciberriesgo se ha convertido en una amenaza clave para la estabilidad financiera. La contención del mismo, en concreto, y del riesgo operacional, con carácter general, debe constituir una parte integral del marco de gestión de los riesgos adoptado por las entidades.

Para poder evaluar de manera sistemática los riesgos globales que el sistema bancario español asume, el Banco de España debe conocer los ciberincidentes más significativos acontecidos en el mismo. Por todo ello, y con base en la facultad general del Banco de España para requerir información supervisora (ex. art. 50 Ley 10/2014), se considera necesario que las entidades notifiquen por vía telemática al Banco de España la información sobre los ciberincidentes[1] que les afecten siempre que cumplan con los criterios que se enumeran en el apartado Umbrales de notificación siguiendo los plazos establecidos en el apartado Proceso, plazos y canales de notificación.

2 Objeto

El objeto del presente documento es establecer un marco de referencia y un proceso pautado para la notificación de los ciberincidentes relevantes acontecidos en el sistema financiero español, estableciendo directrices claras sobre qué debe considerarse un ciberincidente relevante y qué información espera recibir Banco de España sobre éstos.

Dicha notificación debe considerarse de forma independiente a cualquier otra obligación que imponga a la entidad la normativa vigente, tal como el Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera (más conocido como PSD2), el Real Decreto 43/2021, de 26 de enero, de seguridad de las redes y sistemas de información (conocido como NIS) o el Reglamento UE 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de estos datos (conocido como GDPR).

3 Ámbito de aplicación

Las entidades deben notificar exclusivamente aquellos eventos categorizados como ciberincidentes según la definición del apartado Definiciones, que abarca tanto eventos internos como externos de naturaleza maliciosa o accidental, empleando la clasificación descrita en el apartado Taxonomía de ciberincidentes y que cumplan con los criterios que se enumeran en el apartado Umbrales de notificación.

Las entidades a las que les resulta de aplicación este procedimiento, también deberán notificar los ciberincidentes relevantes originados fuera del territorio nacional, siempre que afecten a los servicios prestados por la entidad en el territorio español.

Si bien referimos al mencionado procedimiento con el fin de clarificar qué ciberincidentes son objeto de comunicación, qué información se precisa y cuáles son los plazos requeridos,

[1] De acuerdo al apartado Definiciones.

reseñar que el cumplimiento de los requisitos concretados en éste requerirá la implicación de sus proveedores de tecnologías de la información y comunicaciones, en caso de que la actividad haya sido externalizada en todo o en parte.

Con independencia de la posible externalización de funciones en terceros, las notificaciones de los ciberincidentes serán remitidas individualmente por cada entidad, no siendo posible delegar en terceros las obligaciones previstas en este procedimiento. La entidad será plenamente responsable, tanto de cumplir con los requisitos de este procedimiento, como del contenido de la información proporcionada a la autoridad competente.

4 Destinarios

Este procedimiento está dirigido al conjunto de entidades de crédito menos significativas sobre las que Banco de España, en su calidad de autoridad competente, ejerce la supervisión directa de sus actividades.

5 Definiciones

Término	Definición[2]
Cibermedio	Infraestructura para la interconexión e interacción entre personas, procesos, datos y sistemas de información.
Ciberseguridad	Protección de la confidencialidad, integridad y disponibilidad de la información y sistemas de información en el cibermedio.
Ciberevento	Cualquier acontecimiento observable en un sistema de información o en el cibermedio.
Ciberincidente	Ciberevento o conjunto de éstos que comprometen la ciberseguridad o violan las políticas y/o procedimientos de seguridad de la entidad, independientemente de que sean intencionados.
Ciberriesgo	La combinación de la probabilidad de ocurrencia de ciberincidentes y la materialidad de sus consecuencias.

6 Fecha de aplicación

El presente procedimiento será de aplicación a partir del 3 de mayo de 2021.

7 Taxonomía de ciberincidentes

A efectos de notificación, se utilizará una taxonomía para clasificar la naturaleza de los ciberincidentes relevantes compuesta de tres niveles, en la que los dos primeros atienden al origen de la amenaza y el tercero, aplicable a los ciberincidentes intencionados, al vector de ataque utilizado. En función del ciberincidente, la entidad deberá asignar una o varias de

[2] Definiciones basadas en FSB Cyber Lexicon (https://www.fsb.org/wp-content/uploads/P121118-1.pdf).

las siguientes categorías en la plantilla de comunicación, tal y como se describe en el apartado Proceso, plazos y canales de notificación:

1. Ciberincidentes no intencionados

    1.1. Error humano: generados por un usuario en el ejercicio de sus atribuciones de operación, gestión o administración de la plataforma tecnológica, por error y sin ninguna intencionalidad. Por ejemplo, publicación de datos confidenciales o pérdida del servicio en bases de datos productivas o en dispositivos de red por administración errónea.

    1.2. Fallo estructural: problema propio de la infraestructura que compone el cibermedio bajo el ámbito de responsabilidad de la entidad. Por ejemplo, fallos en las instalaciones propias de suministro eléctrico, fuego, fugas de agua o fallo de componentes hardware/software.

    1.3. Desastre natural y eventos externos: problemas asociados al cibermedio en el ámbito no gestionado por la entidad, ya sean debidos a desastres naturales o a eventos en terceros y/o en proveedores de suministros. Por ejemplo, interrupciones en la prestación de proveedores de comunicación, inundaciones o terremotos.

2. Ciberincidentes intencionados

    2.1. Origen en empleados internos o en proveedores de servicio

        a) Uso malicioso de accesos: producidos mediante la utilización de accesos legítimos para fines impropios, como por ejemplo perpetrar fraude, sabotaje de los sistemas o robo de propiedad intelectual.

        b) Circunvalar las medidas de defensa: el empleado o el proveedor utiliza vectores de ataque externo en una posición privilegiada, en la que una o varias medidas de defensa de la organización no son de aplicación. Por ejemplo, utilización de técnicas de ingeniería social aprovechando relaciones de confianza, o análisis de paquetes (sniffing[3]) sobre segmentos de red internos.

    2.2. Origen externo

        a) Malware: uso de software cuyo objetivo es infiltrase o dañar un activo tecnológico. Por ejemplo, virus informáticos, gusanos, troyanos, spyware[4], rootkit[5] o ransomware[6].

[3] Análisis de paquetes (Sniffing): Análisis mediante software del tráfico de una red con la finalidad de capturar información. El tráfico que viaje no cifrado podrá ser capturado y usado para detectar y analizar posibles vulnerabilidades.

[4] Programa espía (spyware): Es un tipo de malware que espía las actividades de un usuario sin su conocimiento o consentimiento. Estas actividades pueden incluir keyloggers, monitorizaciones, recolección de datos, así como robo de datos. Los spyware se pueden difundir como un troyano o mediante explotación de software.

[5] Rootkit: Es un conjunto de software dañino que permite el acceso privilegiado a áreas de una máquina, mientras que al mismo tiempo se oculta su presencia mediante la corrupción del Sistema Operativo u otras aplicaciones. El propósito por tanto de un rootkit es enmascarar eficazmente payloads y permitir su existencia en el sistema.

[6] Ransomware: Malware que infecta una máquina, de modo que el usuario es incapaz de acceder a los datos almacenados en el sistema. Normalmente la víctima recibe posteriormente algún tipo de comunicación en la que se le coacciona para que se pague una recompensa que permita acceder al sistema y los archivos bloqueados.

b) Obtención de información: ataques dirigidos a recabar datos que faciliten a su vez ataques con mayor impacto, como por ejemplo identificación de activos y vulnerabilidades, sniffing, ingeniería social[7], phising[8] y spear phising[9].

c) Intrusiones y accesos no autorizados: ataques dirigidos a la explotación de vulnerabilidades de diseño, de operación o de configuración para operar de forma fraudulenta en los sistemas. En esta categoría incluimos todo tipo de inyección de código (SQL[10], Shell, scripting y cross-site scripting[11]), ataques de fuerza bruta, compromisos de cuentas de usuario por derivación de contraseñas (password), accesos por suplantación de identidad (spoofing[12]) y todo uso ilegitimo de credenciales.

d) Compromiso de la información: incidentes específicamente relacionados con el acceso, fuga, modificación o borrado de información, como por ejemplo exfiltración y publicación no autorizada de información sensible.

e) Contenido abusivo y extorsión: campañas para dañar la imagen de la entidad o extorsionar a sus empleados a través del cibermedio. Por ejemplo, publicaciones fraudulentas en redes sociales o chantaje y acoso a través del correo electrónico.

f) Disponibilidad: ataques dirigidos a interrumpir la prestación del servicio de la entidad, con el fin de causar daños o impacto en la reputación, como por ejemplo ataques de denegación y denegación distribuida de servicio, o sabotajes físicos, como corte del cableado o incendios provocados.

g) Otros: casuísticas no incluidas en los apartados anteriores.

Hemos de destacar que las categorías que componen la taxonomía no son excluyentes y, en consecuencia, sobre la plantilla de notificación deberán indicarse todas las clasificaciones aplicables. Por ejemplo, algunos ciberincidentes serán generados por empleados y externos de forma coordinada, cuando un empleado interno circunvale medidas de defensa deberá indicarse adicionalmente el vector de ataque utilizado con origen externo. Asimismo, será frecuente que las distintas fases de un ciberincidente incluyan la obtención de información antes de la intrusión y el compromiso.

[7] Ingeniería social: Se definen así a todas aquellas técnicas que buscan la revelación de información sensible de un objetivo, generalmente mediante el uso de métodos persuasivos y con ausencia de voluntad o conocimiento de la víctima.

[8] Phishing: Consiste en la suplantación de la identidad mediante la que el atacante, de forma masiva, trata de obtener información relevante de usuarios para uso dañino. Para ello se emplean métodos de ingeniería social.

[9] Spear Phishing: Se trata de una variante del Phishing mediante la que el atacante focaliza su actuación sobre un objetivo concreto.

[10] Inyección SQL: Es un tipo de explotación, consistente en la introducción de cadenas mal formadas de SQL, o cadenas que el receptor no espera o controla debidamente; las cuales provocan resultados no esperados en la aplicación o programa objetivo, y por la cual el atacante produce efectos inesperados y para los que no está autorizado en el sistema objetivo.

[11] Cross Site Scripting XSS (Directo o Indirecto): Es un ataque que trata de explotar una vulnerabilidad presente en aplicaciones web, por la cual un atacante inyecta sentencias mal formadas o cadenas que el receptor no espera o controla debidamente.

[12] Spoofing: Empleo de una serie de técnicas de hacking utilizadas de forma maliciosa para suplantar la identidad de una web, entidad o una persona en la Red.

8 Umbrales de notificación

La clasificación de un ciberincidente como relevante y, por tanto, la obligatoriedad de notificación, vendrá determinada por el análisis realizado por la entidad. En su análisis, la entidad evaluará las consecuencias potenciales o materializadas del ciberincidente en sus sistemas de tecnologías de información y comunicación (TIC), personas y procesos, y los efectos adversos que la materialización de la amenaza supone en la continuidad de la prestación de sus servicios.

Las entidades notificarán los ciberincidentes que pueden afectar a los sistemas TIC empleados para la prestación de sus servicios conforme al cumplimiento de, al menos, uno de los siguientes criterios, aun cuando no hayan tenido un efecto adverso real:

1. El ciberincidente puede causar un daño de reputación material: de aplicación si ha tenido cobertura en medios de comunicación significativos o repercusión en redes sociales. En el caso de que existan dudas sobre la importancia del medio, la gravedad de la repercusión en redes sociales o la noticia no afecte explícitamente a la entidad, debe ponderarse el impacto de reputación de la situación específica.

   Adicionalmente, debe considerarse como relevante cualquier incidente con impacto directo sobre la confianza del cliente, incluso si aún no ha trascendido a medios o redes sociales, como puede ser la indisponibilidad de sistemas de pagos o banca personal.

2. El ciberincidente ha supuesto la destrucción, robo o revelación de información confidencial o sensible: umbral satisfecho cuando la información afectada pueda tener algún impacto sobre la operación futura de la entidad, como pueden ser los datos de clientes (sean o no personas físicas), estrategias de negocio o de inversión, incluso si no se cumple el criterio asociado al daño de reputación (criterio 1) por no haberse publicado en medios o por haberse revelado sólo a un conjunto limitado de personas.

3. El ciberincidente ha requerido un escalado de emergencia a un comité u órgano de gestión de la entidad: se considerará relevante cuando haya sido preciso trasladarlo a cualquier comité u órgano de gestión, a fin de facilitar la toma de decisiones ejecutivas u operativas en las fases de respuesta y recuperación ante un ciberincidente, al margen del proceso de reporte y cuadros de mando habituales.

   Dado que la nomenclatura de los cargos y puestos asociados a la gestión de la ciberseguridad y, en general, a las tecnologías de información y comunicación, difieren entre las distintas entidades, este criterio será de aplicación con independencia del cargo que presida o participe en el órgano de gestión, y será suficiente siempre y cuando el comité tenga capacidad operativa y atribuciones para pronunciarse sobre el ciberincidente.

4. El ciberincidente ha supuesto o es probable que suponga el incumplimiento de obligaciones legales o regulatorias, tales como (pero no limitadas a):

   - Exceder plazos en la entrega de reportes fiscales o regulatorios.
   - Incapacidad de cumplir obligaciones con clientes (ejecución de transacciones financieras, transferencias, etc.).

- Incapacidad de observar las medidas para la prevención de blanqueo de capitales y financiación al terrorismo.

5. El ciberincidente ha supuesto la activación de los planes de continuidad de negocio o de contingencia tecnológica: deberá considerarse relevante en el caso de recurrir a alguno de los procedimientos descritos en los planes de continuidad. Así mismo, el criterio será de aplicación en el caso de precisarse de los procedimientos de contingencia tecnológica, independientemente de la existencia o activación de un escenario específico para ciberincidentes.

   En el caso de ser necesario escalar la situación a comités de crisis, se considerará satisfecho tanto el presente criterio como el asociado al escalado a órganos de gestión (criterio 3).

6. El ciberincidente ha sido comunicado al Centro de Respuesta ante Incidentes (CERT/CSIRT) nacional o autonómico, o bien a las Fuerzas y Cuerpos de Seguridad del Estado.

7. Otras entidades o infraestructuras relevantes podrían verse potencialmente afectadas: si el riesgo de afección sistémica es material, el ciberincidente debe considerarse relevante, incluso habiendo sido contenido satisfactoriamente por la entidad. Por ejemplo, si la causa raíz del ciberincidente es una vulnerabilidad común en un producto ampliamente distribuido.

Incluso si ninguno de estos criterios se cumple, la entidad tiene la potestad de clasificar el ciberincidente como relevante con base en criterios internos o particulares. Si la valoración no concluye claramente que el ciberincidente deba clasificarse como relevante, se recomienda hacerlo y proceder con la notificación.

En el caso de detectarse varios ciberincidentes relevantes relacionados, queda a criterio experto de la entidad la decisión de incluirlos en una única notificación o gestionarlos como acontecimientos independientes.

Así mismo, es necesario reseñar que el análisis de relevancia debe enfocarse como un proceso continuo, que se debe efectuar durante todo el ciclo de vida del ciberincidente, de modo que un evento considerado inicialmente como no relevante, en función de su evolución, puede derivar en el cumplimiento de umbrales de notificación.

9 Proceso, plazos y canales de notificación

El proceso de notificación consta de tres fases, incrementales en cuanto al contenido, y estructurados en torno a la plantilla en formato Excel (archivo .xlsx) descrita en el Anejo I.

Los plazos de notificación están referidos respecto al momento en el que el ciberincidente es clasificado como relevante, es decir, a partir de que alguno de los criterios definidos en el apartado Umbrales de notificación del presente documento se satisfaga.

El acceso al procedimiento de notificación de ciberincidentes relevantes está disponible en el trámite 'Notificación de ciberincidentes relevantes de entidades de crédito bajo la supervisión directa del Banco de España' dentro de la Oficina Virtual del Banco de España.

En cuanto al canal de comunicación, Banco de España pone a disposición de las entidades el servicio electrónico 'NCR – Notificación de ciberincidentes relevantes de entidades de crédito bajo la supervisión directa del Banco de España'. Para remitir las comunicaciones, las entidades tendrán que adherirse a dicho servicio siguiendo las instrucciones publicadas. Una vez autorizadas, el envío se realizará a través del portal ITW[13] del Banco de España. Tras cada envío, la entidad podrá verificar el resultado del procesamiento a través del portal ITQ[14].

Por cada envío, la entidad enviará exclusivamente la plantilla Excel debidamente cumplimentada a través del servicio NCR. La plantilla de notificación debe renombrarse utilizando la siguiente codificación: "EEEEAAAAMMDDNN", donde:

- EEEE es el código de la entidad tal y como aparece en el Registro de Entidades del Banco de España
- AAAAMMDD hace referencia a la fecha de la primera notificación.
- NN será un número secuencial para identificar las diferentes notificaciones que podrían producirse en una misma entidad y fecha.

Es muy importante que se respete la nomenclatura de los archivos para que los informes puedan ser procesados.

En los casos en los que se solicite información adicional sobre el ciberincidente, la entidad deberá enviar un correo al buzón de correo electrónico (Ciberincidentes@bde.es) con la información solicitada. Para garantizar la seguridad de las comunicaciones, la entidad deberá cifrar el correo utilizando la clave pública del certificado que se podrá descargar en la sección "Otra información de interés" y firmarlo digitalmente. En aquellos casos en que no fuese posible la descarga por el procedimiento anterior, se enviará desde el buzón de correo electrónico un mensaje firmado utilizando su certificado PKIBDE.

9.1 Primera comunicación

La entidad debe completar al menos los campos destacados en rojo en la plantilla de notificación, marcando el indicador de "Primera comunicación" sobre la misma.

Se trata de datos generales, orientados a proporcionar una descripción global del ciberincidente e identificar el contacto dentro de la entidad para posteriores comunicaciones.

El plazo para su entrega es de dos horas.

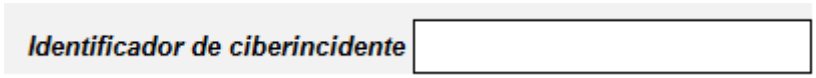
[13] https://aps.bde.es/itw_www
[14] https://aps.bde.es/itq_www

*Nota: **con carácter excepcional**, y debido a que, durante el horizonte temporal definido para esta primera comunicación, la entidad puede estar sufriendo los efectos del ciberincidente, se permite cursar esta primera notificación, y únicamente ésta, verbalmente a través de las líneas telefónicas habilitadas al efecto, siempre que no sea posible enviar la plantilla telemáticamente mediante el canal habilitado. No obstante, si se opta por esta vía, la plantilla de primera comunicación deberá enviarse igualmente tan pronto como sea posible, para facilitar la trazabilidad y asignación de identificador único de ciberincidente.*

9.2 Informe preliminar

La entidad debe completar al menos los campos destacados en azul en la plantilla de notificación, marcando el indicador de "Informe preliminar" sobre la misma.

Destacar que el campo fecha de notificación debe actualizarse respecto a la primera comunicación, y que debe emplearse el mismo identificador de ciberincidente de la primera notificación para mantener el seguimiento.



En este caso, la notificación incluirá datos detallados, tanto de la naturaleza del ciberincidente, como de su impacto.

Siempre y cuando no se produzcan modificaciones significativas sobre la información reportada anteriormente, el plazo para su entrega es de 10 días hábiles. Mientras el ciberincidente no sea resuelto y no acontezcan novedades materiales, deberá actualizarse el informe preliminar al menos cada 10 días hábiles mediante nuevas notificaciones, siguiendo el mismo formato.

En el caso de registrarse modificaciones esenciales en la información disponible del ciberincidente, independientemente de que afecten a la causa raíz, vector de ataque, vulnerabilidad explotada o impacto en la entidad, éstas deberán notificarse inmediatamente en un informe preliminar específico, sea o no posible completar todos los campos requeridos en el mismo. A efectos de reporte se considerará un informe preliminar al uso, y por tanto deberá actualizarse en 10 días hábiles si no acontece novedad y mientras el incidente no sea resuelto.

9.3 Informe final

La entidad debe completar al menos los campos destacados en verde en la plantilla de notificación, marcando el indicador de "Informe final" sobre la misma.

De nuevo, deberá actualizarse el campo fecha de notificación y emplearse el mismo identificador de ciberincidente.

El informe completo incluye, además de todo lo referido en apartados anteriores, información sobre la investigación y resolución del incidente.

La obligación de entrega del presente informe nace una vez se considere el ciberincidente resuelto, en un plazo no superior a 10 días hábiles desde ese momento. En consecuencia, se enviará un único informe final, salvo que la entidad detecte a posteriori modificaciones materiales en los impactos notificados, en cuyo caso se procederá a una actualización del mismo. En el caso de resolver el incidente antes del plazo máximo de envío del informe preliminar (10 días hábiles), puede optarse por enviar el informe final sin necesidad de elaborar un informe preliminar previo, si bien será necesario completar los campos tanto del informe preliminar como del final sobre la plantilla.

9.4 Reclasificaciones

Tras la primera comunicación, se contempla que el ciberincidente pueda ser reclasificado por dos motivos:

- El ciberincidente no es relevante: mediante un análisis detallado, se comprueba que el criterio que generó su clasificación como relevante, finalmente, no se satisface. Puede ser de aplicación a los criterios de potencial impacto de reputación (criterio 1) o posible incumplimiento regulatorio (criterio 4).
- La actividad fue clasificada como ciberincidente erróneamente: bien porque se trate de un incidente que no guarde relación con el cibermedio, bien porque se haya considerado ciberincidente una actividad lícita. Por ejemplo, un análisis de vulnerabilidades interno puede considerarse erróneamente como un ataque de obtención de información.

En el caso de que acontezca alguna de estas situaciones, deberá cumplimentarse la plantilla con el suficiente detalle, incluyendo el análisis del evento de manera que permita comprender la peligrosidad e impacto del mismo y la justificación por la que se determina la reclasificación. Se deberá marcar sobre la plantilla el indicador específico.

Evento reclasificado como no ciberincidente	☐
Ciberincidente reclasificado como no relevante	☐

Anejo I: Plantilla de notificación

Las entidades deben usar para la notificación de ciberincidentes relevantes la última versión de la 'Plantilla NCR' que se encuentra en el apartado 'Tramitación'. Dicha plantilla está diseñada para recoger conjuntos incrementales de información, a medida que la entidad disponga de la misma, tal y como se describe en el apartado Proceso, plazos y canales de notificación.

Todos los campos de la plantilla son de reporte obligatorio, y en el específico caso de no aplicar alguno de ellos, debe indicarse la razón sobre el mismo. A continuación, se ofrece una guía descriptiva de la información que se espera recibir en ellos.

1. Campos generales, que se deben completar en todas las notificaciones enviadas:
   - Campo "Primera comunicación", "Informe preliminar" o "Informe final": deberá optarse por una de las tres tipologías de notificación, en función de la fase del proceso en la que se encuentren.
   - Identificador de ciberincidente: corresponderá al nombre del fichero de la primera notificación. Este identificador, al igual que el nombre del fichero, se mantendrá igual en todos los envíos.
   - Fecha/hora de detección: momento en el que el ciberincidente fue detectado por la entidad o cualquiera de sus proveedores.
   - Fecha de clasificación como relevante: momento en el que el ciberincidente pasó a considerarse como relevante, es decir, se estimó que cumplía con alguno de los requerimientos consignados en el apartado Umbrales de notificación.
   - Fecha de notificación: fecha efectiva del envío de la presente plantilla.
   - Campos "Ciberincidente reclasificado como no relevante" y "Evento reclasificado como no ciberincidente": dedicados a reflejar las casuísticas expuestas en el apartado Reclasificaciones del presente documento.
2. En el caso de la primera comunicación:
   - Nombre de la entidad afectada: nombre exacto de la entidad que ha sufrido el ciberincidente.
   - Número de identificación único de la entidad: o NRBE, Número de Registro de Entidades del Banco de España.
   - Entidad cabecera del grupo, si aplica: nombre y en su caso NRBE, Número de Registro de Entidades del Banco de España.
   - País/países afectados por el incidente: lista de países en los que la entidad afectada ha registrado impacto o estima que puede registrarlo, por causa del ciberincidente.
   - Campos "Persona de contacto principal" y "Persona de contacto alternativa": deben incluirse los nombres, direcciones de correo electrónico y teléfonos de las personas encargadas, dentro de la entidad afectada, de recibir las posibles solicitudes de información y comunicaciones de Banco de España.
   - Descripción corta del incidente: campo de texto libre en el que se espera que la entidad afectada describa, de forma somera y general, el ciberincidente acontecido, sus estimaciones sobre el origen, el vector de

ataque utilizado, la vulnerabilidad explotada y su posible impacto, tanto para la propia entidad como para el resto del sector financiero.

3. Informe preliminar:
   - El incidente fue detectado por: agente que detectó, en primer término, la ocurrencia del ciberincidente, ya sea este una unidad organizativa de la entidad, un cliente, un proveedor o el mismo atacante.
   - Fecha y hora de comienzo del incidente: hace referencia al momento a partir del cual se considera que el ciberincidente comenzó, o la entidad se vio afectada por el mismo. Por definición, será anterior a la fecha de detección facilitada en los campos de carácter general.
   - Estado del ciberincidente: fase en la que se encuentra el mismo en el momento de notificación del informe preliminar. Las categorizaciones están basadas en la guía "CCN-STIC 817 – Gestión de ciberincidentes" del Centro Criptológico Nacional[15].
   - Fecha y hora en la que el incidente fue solventado o en la que se espera que lo esté: en el caso de enviarse el informe preliminar antes del fin del ciberincidente, se espera que en este campo se incluya una estimación, que se complementará con el campo homónimo del informe final.
   - Descripción detallada del incidente: campo de texto libre en el que se espera que la entidad afectada describa, de forma detallada y ampliando la información de la primera comunicación, el ciberincidente acontecido, su impacto y las medidas puestas en marcha para su mitigación.
   - Afección directa del ciberincidente o a través de un proveedor: deberá indicarse si el ciberincidente aconteció directamente sobre el medio de la entidad o, como parte de la cadena de causas, si la entidad se vio afectada debido a uno o varios de sus proveedores de servicio.
   - Categoría del incidente: deberá indicarse la clasificación que la entidad le ha otorgado, con base en el esquema descrito en el apartado Taxonomía de ciberincidentes del presente documento.
   - Razón de reporte: en estos 8 campos se incluyen las posibles causas que han llevado a considerar el ciberincidente como relevante. Responden a las definiciones incluidas en el apartado Umbrales de notificación del presente documento. Para cada una de ellas, se solicita un detalle adicional, al margen de su aplicabilidad, en un campo de texto libre. Destacar que no son excluyentes, e independientemente de que alguno de los criterios sea de aplicación, deberán analizarse todos ellos y completar el pertinente campo del reporte.
   - Edificio(s) afectado(s), si aplica: deben indicarse las localizaciones de la compañía que se han visto afectadas por el evento.
   - Campos "Canales comerciales afectados", "Líneas de negocio afectadas", "Sistemas y componentes afectados" y "Aplicaciones afectadas": dedicados, a distintos niveles de abstracción, a plasmar el impacto que el ciberincidente ha tenido sobre la entidad. Es necesario indicar, sobre las listas propuestas, aquellas categorías que son de aplicación. Tal y como ocurre con la taxonomía del ciberincidente, serán frecuentes las selecciones de múltiples valores o, lo que es lo mismo, que

[15] Guía de Seguridad de las TIC CCN-STIC 817. (https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html)

más de un canal, línea de negocio, sistema o aplicación se haya visto afectado. En cada campo se incluye, adicionalmente, una opción de texto libre para detallar, si fuera necesario, valores que no figuren en la plantilla.

- Personal afectado: en el caso de que parte del personal de la entidad se haya visto impactado, por ejemplo, no pudiendo realizar sus funciones habituales, debe consignarse en este campo. La información aquí contenida debe ser consistente con la reportada en los campos de impacto anteriormente descritos.
- Contención, erradicación y recuperación: se espera una descripción detallada de las acciones y medidas puestas en marcha para responder y recuperarse ante el ciberincidente.
- Modificación del entorno de control: en el caso de que, con carácter temporal, haya sido preciso deshabilitar alguno de los controles que constituyen el entorno habitual, debe describirse en el presente campo.

4. Informe final:

- Fecha y hora en la que el incidente fue solventado: campo que actualiza la información del homónimo incluido en el informe preliminar, con la fecha y hora efectiva de cierre del ciberincidente frente a la estimación del anterior. En el caso de que el ciberincidente se solventara antes del envío del informe preliminar, ambos campos contendrán el mismo valor.
- Reporte final: campo de texto libre en el que se espera que la entidad actualice y amplíe la información aportada en la descripción del informe preliminar, incluyendo datos relativos a las acciones de remediación finalmente tomadas, las lecciones aprendidas tras el acontecimiento y, en general, cualquier otra información relevante asociada a la actividad post-incidente.
- Modificación del entorno de control: en el caso de que fuera necesario deshabilitar alguno de los controles que constituyen el entorno habitual, debe indicarse en el presente campo si se ha reestablecido, rediseñado o mejorado.
- Causa raíz / Vulnerabilidad expuesta: campo de texto libre para indicar, tras el pertinente análisis interno, cuál fue la causa que originó el ciberincidente, así como las vulnerabilidades que fueron explotadas durante el mismo. En cuanto a causa raíz, ejemplos comunes son la inadecuada gestión de actualizaciones y parches de seguridad, la inadecuada gestión de usuarios o una segmentación de red insuficiente. En lo relativo a vulnerabilidades expuestas, se aconseja, siempre que sea posible, utilizar identificadores CVE (Common Vulnerabilities and Exposures) en lugar de descriptivos.
- Futuras medidas preventivas: si bien pueden haberse descrito en el reporte final, este campo direcciona específicamente las medidas concretas, puestas en marcha o futuras, para mitigar ocurrencias o explotaciones de la vulnerabilidad indicada en el campo “Causa raíz / Vulnerabilidad expuesta”.
- Impacto económico: campo habilitado para incluir los costes financieros tanto directos como indirectos derivados del ciberincidente, ya sean cifras consolidadas o estimaciones.
- Ciberseguro: complementando el campo de impacto económico, deberá consignarse si se dispone de alguna póliza de seguro que cubra total o

parcialmente el ciberincidente y, en el caso de que así sea, qué importe se recuperará tras su ejecución.

- Comunicación con otras entidades: se espera que se indique si se han establecido, por iniciativa propia, canales de comunicación con otras entidades de cara a coordinar las acciones de contención, erradicación y recuperación, o para anticipar posibles afecciones en el sector.
- Acciones legales contra la entidad: deberá indicarse si se han emprendido acciones legales contra la entidad o si es previsible que se inicien, independientemente de cual sea el origen de las mismas.