GUÍA PARA LA GESTIÓN DE CRISIS POR CIBERINCIDENTE EN LA CADENA DE SUMINISTRO

APOYO INSTITUCIONAL:

DSN · CCN centro criptológico nacional · CNPIC CENTRO NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURAS Y CIBERSEGURIDAD · incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD · AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

UNA INICIATIVA DE:

isms forum

GUÍA PARA LA GESTIÓN DE CRISIS POR CIBERINCIDENTE EN LA CADENA DE SUMINISTRO

Con la participación de los siguientes profesionales y organizaciones:

Dirección y coordinación

Ángel Pérez
Francisco Lázaro

Capítulo: Buenas Prácticas

Coordinación: Virginia Rodríguez
Colaboradores: Ramón Ortiz
Roger Cabanellas
Rubén Fernández
Vicente Campayo

Capítulo: Protocolo Respuesta a Incidentes

Coordinación: Sergio Padilla
Colaboradores: Eduardo Martín
Juan Ignacio Calvo
María Guillamón
Oscar Sánchez Montaner

Capítulo: Continuidad de Negocio

Coordinación: Cristina Pereira
Colaboradores: Concepción Cordón
Eva Cañete
Josep Estevez
Mª Carmen Moreno-Ventas
Oscar Sánchez Montaner

Capítulo: Ciberseguros

Coordinación: Juan Acosta
Colaboradores: David Moreno
Gustavo Lozano
Idioia Uriarte
Luis Ballesteros

Capítulo: Gestión de Crisis

Coordinación: Albert Girbal
Colaboradores: Elena Matilla
Angel Pérez
Francisco Javier Santos
Elisabet Viladomiu

Capítulo: Cumplimiento

Coordinación: Carlos Alberto Sáiz
Colaboradores: Oscar Sánchez Albarrán
Fabian Vidal

Colaboradores que han participado en las revisiones posteriores

Javier Candau
Alberto Francoso
Marcos Gómez
Alfonso López-Escobar
David Navarrete
Andrés Ruiz
Alberto Sánchez del Monte

Apoyos Institucionales

DSN
CCN
CNPIC
INCIBE
CESICAT

Editor

Daniel García, Director General de ISMS Forum

Diseño y maquetación

Raquel García, Asistente de comunicación de ISMS Forum

isms forum

ÍNDICE

ÍNDICE

ÍNDICE

ÍNDICE

PRÓLOGO

El proceso de digitalización de la economía que se ha desarrollado en los últimos años dará un paso más con la plena incorporación del 5G y la inteligencia artificial. Las oportunidades que estos dos factores, y otras tecnologías habilitadoras, ofrecerán al desarrollo socioeconómico son evidentes, pero los riesgos que desde el punto de vista de la seguridad digital traen consigo no siempre son percibidos con la misma inmediatez, y sobre todo no siempre son gestionados por parte de todos los actores implicados.

En el caso de las empresas, uno de sus principales activos se encuentra en la información que poseen, y por eso resulta de gran interés para los ciberdelincuentes. De ahí que si las empresas protegen su información, protegen su negocio. Esta protección comienza por la concienciación y sensibilización que permita hacer un uso adecuado de la tecnología, protegiendo el negocio y garantizando los derechos de los clientes o usuarios. Las empresas, sin importar su tamaño o su sector, han de aprender a gobernar su seguridad de forma eficiente. Para ello, han de adoptar un enfoque de gestión de riesgos y elaborar un Plan Director de Seguridad. Este Plan contendrá las medidas técnicas y organizativas necesarias para abordar la seguridad de forma consistente con los riesgos detectados y en línea con la estrategia de la empresa.

Pero la prevención no solo viene de la mano de la empresa, también de sus proveedores. En la actividad diaria, las empresas necesitan contratar determinados servicios especializados a proveedores externos para que les den soporte, y en este proceso resulta fundamental que gestionen con seguridad la información que manejan de los clientes, sobre todo si se trata de información sensible como la que se contempla en el Reglamento General de Protección de Datos europeo y otras legislaciones análogas.

Afortunadamente, cada vez más empresas asumen un compromiso con la ciberseguridad y entienden la importancia de estar protegidas ante posibles incidentes. Aun así, es necesario continuar trabajando por proteger la información y los sistemas, y esto supone exigir a los proveedores externos la misma seguridad con la que trabajan las compañías.

Desde INCIBE, como entidad de referencia en ciberseguridad, trabajamos diariamente para que nuestros ciudadanos y nuestras empresas mejoren su seguridad digital en

el día a día. Esta Guía aborda aspectos de indudable interés para la gestión del riesgo en ciberseguridad y la respuesta a incidentes: análisis de buenas prácticas, protocolos de respuesta a incidentes, recomendaciones en materia de continuidad de negocio, ciberseguros, o gestión de crisis desde una perspectiva reputacional. Todos ellos son aspectos que cualquier empresa debe incorporar a su gestión de la información. Por este motivo, desde INCIBE valoramos positivamente la publicación de esta *Guía para la gestión de crisis por ciberincidente en la cadena de suministro* por parte de ISMS Forum, y estamos seguros que contribuirá al desarrollo de la seguridad de la información en España.

Aunque la ciberseguridad 100% no existe, acciones como esta contribuyen sin duda a que nuestras empresas estén más concienciadas y seguras.

ROSA DÍAZ

Directora general del Instituto Nacional de Ciberseguridad (INCIBE)

1. INTRODUCCIÓN

Todos los días ocurren incidentes en el ámbito de la ciberseguridad, incidentes que pueden resultar tremendamente costosos y perjudiciales para las organizaciones.

El abanico de daños es cada vez más amplio y siempre hay, en mayor o menor medida, pérdidas económicas directas e indirectas asociadas a estos incidentes.

Dependiendo de diversos atributos de las organizaciones, tales como la naturaleza del negocio, el tamaño o el grado de externalización, entre otros muchos, podrían existir problemas con la gestión de las terceras partes o proveedores que trabajan con dichas organizaciones.

Las dinámicas actuales de crecimiento y expansión en la mayoría de las empresas hacen necesaria la colaboración de los proveedores y terceros que les prestan servicios y/o realizan funciones y actividades internas, mediante externalización de estas.

La cada vez mayor dependencia de terceros aumenta en las compañías la superficie de exposición frente a un incidente y, por tanto, incrementa el riesgo que deben gestionar las empresas. Riesgo que no gestionan directamente y que normalmente, pasa por confiar en que ese tercero lo gestione adecuadamente.

Esta dependencia y esa actitud, la de no involucrarse en la Gestión del riesgo que generan los proveedores, puede dar lugar a que algún incidente que se produzca en alguno de nuestros proveedores se convierta en un incidente grave para la empresa. Según algunos informes, un 83% de las organizaciones, han sufrido incidentes en alguno de sus proveedores en los últimos 3 años (ver Informe *All together now. Third party governance and risk management*, Deloitte en el anexo 2 - Referencias).

La gestión de la información y los sistemas informáticos no escapa a esta práctica y generalmente todas las organizaciones confían en proveedores directamente para almacenar, procesar o gestionar su información, o bien como fuente de servicios de toda índole, teniendo igualmente y por lo general, un contacto directo con los sistemas de información de nuestra empresa. De este modo, una brecha en un proveedor podría

llegar a afectar a la empresa.

Es por todo ello, por lo que resulta necesario contar con mecanismos de respuesta a incidentes que tengan en cuenta el nivel de dependencia de terceros y, en consecuencia, el riesgo directo e indirecto que ello supone. Si bien todavía en algunos sectores no existe una obligación legal de responder en función del incidente, como sí ocurre ya en otros (como es el caso de operadores de servicios esenciales), sí que nuestra empresa podría sufrir un daño elevado a resultas del impacto directo o indirecto del mismo.

Un proveedor de servicios tendrá mayor o menor protección ante accesos no autorizados y ante cualquier otra amenaza. Lógicamente, esto es algo a considerar a la hora de gestionar los riesgos de terceros en nuestras organizaciones, especialmente para conocer nuestro grado de exposición, así como para prepararnos ante un ciberincidente y responder adecuadamente, aunque el mismo haya tenido su origen en el proveedor. Por otra parte, un proveedor de servicios debería gestionar adecuadamente con sus clientes el riesgo directo e indirecto de un ciberincidente y establecer los mecanismos adecuados de alerta, respuesta y recuperación.

1.1. NECESIDAD Y OBJETIVO

Es por estas cuestiones que, tras un análisis en el seno de ISMS Forum, hemos creído necesario afrontar este trabajo a través de una visión multidisciplinar.

En el equipo de trabajo han participado más de treinta grandes profesionales, todos ellos expertos en varias de las siguientes materias:

- CISO.
- Gestión de incidentes de ciberseguridad.
- Continuidad de Negocio.
- Organización de Empresas.
- Gestión de Crisis.
- Comunicación Empresarial.
- Legal y Cumplimiento.

Al inicio del libro se muestra una relación de profesionales con sus nombres, hay otro grupo de expertos que han preferido colaborar de forma anónima. A todos ellos: nuestro agradecimiento.

Este trabajo nace con el objetivo de ofrecer un conjunto de recomendaciones y buenas prácticas sobre cómo las empresas deben abordar una estrategia de prevención, protección y respuesta a incidentes de ciberseguridad, con origen en un proveedor, los cuales puedan llegar a suponer una amenaza grave para la propia empresa.

Asimismo, este trabajo complementa al ya publicado por ISMS Forum bajo el título ***Protocolo de actuación frente a incidente en proveedor***, de forma que el primero aporta recomendaciones y guías de acción rápida frente a un incidente y este lo complementa desde una perspectiva más estratégica.

El documento se estructura en varios apartados:

- Una reflexión sobre cómo clasificar proveedores en función del riesgo y qué aspectos debemos contemplar en cada caso y en cada fase del ciclo de vida de relación de prestación del servicio.
- Una guía sobre cómo desplegar un Plan de Respuesta a ciberincidentes que contemple las distintas fases de este (situación previa, identificación, etc.).
- Aspectos que deben ser contemplados desde una perspectiva de Continuidad de Negocio.
- Cómo debemos relacionarnos con los órganos de gestión de crisis de la empresa y cómo afrontar un plan de comunicación en este ámbito, incluyendo un decálogo de buenas prácticas.
- Qué cláusulas y coberturas conviene incluir en un ciberseguro.
- En qué responsabilidades podemos incurrir desde un punto de vista de Cumplimiento.

En resumen: en este trabajo consideramos diversos aspectos relevantes, aunque ya le anticipamos que la prevención es fundamental para evitar, o cuanto menos minimizar, el impacto en su empresa frente a estos incidentes.

1.2. ¿ESTA ES UNA GUÍA EXHAUSTIVA DE CIBERINCIDENTES?

Esta sección se dirige específicamente, y por eso nos permitimos tutearte en el lenguaje, a los profesionales de la seguridad de la información.

Durante la elaboración y revisión de la guía, de forma colectiva y muy colaborativa, detectamos que podríamos haber escrito más información, citar más controles o incluso dependiendo de la trayectoria profesional y experiencias de cada uno de los participantes, haber "situado" un control, concepto o idea en un párrafo más arriba, más abajo o en un apartado diferente. Es por ello, que antes de acometer la lectura, queremos expresar:

- Este trabajo es el resultado del "mínimo común múltiplo" del conocimiento, en esta materia, de los profesionales que han participado en su elaboración, revisión y edición. Todos nos sentimos satisfechos del trabajo.
- Hay capítulos que se tratan más extensamente en otras guías, como por ejemplo el capítulo dedicado a la Gestión de incidentes.
- Hay normas y marcos de referencia que identifican un conjunto mayor de controles de seguridad.
- En cada uno de los capítulos, hemos **focalizado el contenido** en los incidentes de la cadena de suministro que, por afectación, directa o indirecta, pueden generarnos incidentes de seguridad y/o situaciones de crisis.

Por eso, a veces echarás en falta algún control de seguridad, pero debes situarte mentalmente en el objetivo que nos hemos propuesto y por el que estás leyendo estas líneas.

Explicado este contexto, la respuesta a la pregunta con la que se abre esta sección, es: **No, esta no es una guía exhaustiva de ciberincidentes, si no una guía especializada, para la Gestión de crisis por ciberincidentes en la cadena de suministro.**

2. BUENAS PRÁCTICAS EN GESTIÓN PROACTIVA DE PROVEEDORES

El control y validación de proveedores se puede convertir en una tarea que consuma muchos recursos y, además, puede incluso suponer un riesgo para el negocio al cargar con requerimientos excesivos en algunos servicios, provocando su encarecimiento.

Esto, unido al hecho de que cada cliente solicita requerimientos diferentes, hace muy complejo al proveedor que puedan ser asumidos para cada uno de sus clientes.

Debemos tratar de ponernos en la piel de nuestros proveedores cuando tratan de gestionar adecuadamente (y de una manera homogénea) la protección de sus activos y la respuesta antes los incidentes… ¿Cómo gestionaríamos tener que cumplir con 200 políticas distintas?

En este capítulo tratamos de establecer algunas líneas base que puedan ser aplicadas por el mercado para asegurar la implantación de medidas de prevención, detección, respuesta y recuperación adecuadas. Es por ello muy recomendable estandarizar, como mínimo a nivel sectorial, un conjunto de requerimientos comunes para futuras contrataciones.

Este capítulo debe considerarse en conjunto con el capítulo de Continuidad de Negocio para asegurar que nuestros proveedores no solo son seguros, sino que también disponemos de mecanismos para garantizar la capacidad de nuestra empresa de continuar con sus operaciones.

2.1. GESTIÓN DE PROVEEDORES BASADA EN EL RIESGO

Dado el elevado número de proveedores que nos prestan servicio es necesario establecer una gestión basada en el riesgo, de modo que sea posible focalizar los esfuerzos en aquellos proveedores que tengan una afectación significativa en nuestra seguridad y/o la continuidad de la actividad de nuestra organización.

Cada empresa deberá tener su propia clasificación de proveedores. Para ello debe hacer un ejercicio introspectivo previo para conocer cuáles son los servicios esenciales

para su negocio, y qué actividades dentro de las mismas le son proporcionadas por terceros. Así podrá realizar esta gestión basada en el riesgo, con la finalidad de focalizar adecuadamente y no exigir medidas de seguridad de manera indiscriminada y/o excesivas a los proveedores que, consecuentemente, lo repercutirían en los costes de los contratos y dispersaría el foco de atención.

Los procesos de clasificación de los proveedores, tienen como principal objetivo la agrupación y clasificación de los proveedores en función del riesgo que supone para la propia compañía el hecho de que cualquiera de estos sufra un incidente de seguridad que pueda tener impacto, tanto en el cumplimiento de los acuerdos de niveles Operativos (OLAs en inglés), en la seguridad de la información de la organización, como en las operaciones de la compañía.

En el siguiente apartado establecemos un ejemplo básico de clasificación, en cuatro niveles, acompañado de las recomendaciones también básicas, pero específicas del tema que estamos tratando, que podríamos considerar por cada uno de los niveles.

Este capítulo no está orientado al cumplimiento (no pretende ser una relación exhaustiva de cláusulas y considerandos) sino a las medidas organizativas y técnicas a implantar que por nuestra experiencia tienen un impacto real en la seguridad. Por lo tanto, de cara a la definición de un programa completo de seguridad, será necesario consultar otras fuentes y buenas prácticas.

2.1.1. Recomendaciones para clasificar a los proveedores

Las medidas solicitadas a un proveedor pueden tener un alto impacto financiero si no son adecuadas y proporcionales.

RIESGO	DESCRIPCIÓN	EJEMPLOS
MUY ALTO	Proveedores que por su importancia pueden poner en riesgo la continuidad de un servicio crítico, la confidencialidad de un nivel significativo de datos y/o estén sujetos a regulaciones específicas	- Proveedores que accedan a información muy confidencial o que, en igual medida, se dependa para garantizar la disponibilidad o la integridad. - Proveedores con un gran número de datos de la empresa en sus instalaciones. - Proveedores clasificados como críticos. - Servicios esenciales para la organización. - Necesarios para la prestación de Servicios Esenciales, designados por el Estado. Proveedores sujetos a regulación específica: PCI-DSS, infraestructura crítica, etc.

RIESGO	DESCRIPCIÓN	EJEMPLOS
ALTO	Proveedores con un impacto significativo en las operaciones y aquellos que por su nivel de conectividad tecnológica pueden afectar a operaciones de la propia empresa en el caso de que se produzca un incidente en los mismos por su riesgo de propagación.	- Proveedores con datos de la empresa en sus instalaciones. - Proveedores conectados a nuestras instalaciones. - Proveedores que acceden a nuestras instalaciones con sus dispositivos. - En algunos casos (nómina, marketing/publicidad, por ejemplo), podemos tener proveedores No Tecnológicos, que si tengan cierta criticidad para nuestra empresa.
MEDIO	Proveedores con acceso a datos en nuestras instalaciones y con nuestros dispositivos.	- Proveedores de servicios no críticos para determinados servicios o departamentos, no incluidos en las descripciones anteriores.
BAJO	Proveedores No Tecnológicos .	- Limpieza. - Tratamiento de residuos. - Hostelería. - Control de acceso a instalaciones.

A esta clasificación, basada en el servicio que prestan, y/o a la información que manejan y/o al grado de dependencia de su prestación, habría que ponderarla con otros dos factores:

- Las capacidades en materia de Seguridad de la Información/ Ciberseguridad del proveedor (tratado tanto en el apartado Análisis de Riesgo y marco de control de proveedores, como en el apartado correspondiente a la Fase 0 del Plan de Respuesta a Incidentes de Proveedores).
- Nuestras propias capacidades en esta misma materia.

2.1.2 Buenas prácticas en cada fase

A continuación, se presenta una enumeración de aquellos aspectos que consideramos diferenciales a la hora de gestionar el riesgo de los proveedores en función de la fase en la que se encuentre el servicio.

Estas medidas son incrementales, es decir, un proveedor de riesgo muy alto deberá cumplir con los puntos indicados para los proveedores de nivel alto, medio y bajo que no estén ya recogidos con un grado de exigencia superior, y así sucesivamente.

Los controles propuestos deben ser tomados por las organizaciones como una referencia, siendo evaluada la necesidad de estos y su ubicación en función del nivel de riesgo

(que puede derivarse de un incidente en el proveedor).

A las medidas generales propuestas se deben de añadir las medidas propuestas en los escenarios de riesgo identificados más adelante. En todos los niveles de riesgo es necesario guardar métricas de seguimiento e impacto, KPIs y KGIs que permitan medir la eficacia y la eficiencia de los controles y que permitan mejorar los procedimientos de gestión de incidentes.

2.1.2.1 Acciones previas a la contratación

Deberíamos fijarnos como objetivo que los requerimientos que se indicarán a continuación (sean estos, similares, o cualquier otro que la empresa quiera exigir), no solo deberían requerirse como obligaciones, sino conforme a como se detallen o como valoremos su eficacia, deberían formar parte de la valoración de las ofertas de cualquier servicio que tratará con información, sistemas o redes de nuestra empresa.

RIESGO	ACCIONES A REALIZAR
MUY ALTO	- Nombrar un responsable de seguridad del proveedor para el proyecto/producto o servicio que proporcione a la empresa. - Incluir dentro de los parámetros de valoración de la propuesta, la valoración de la seguridad. - Solicitar un análisis de riesgos realizado por el proveedor con el alcance del proyecto/producto o servicio que proporcione a la empresa. Esta información, habitualmente no querrá ser entregada por el aspirante a proveer el servicio, en la fase previa a la contratación, pero al menos servirá para que incorpore técnica y económicamente los controles de seguridad a su oferta. - Solicitar certificado de cumplimiento (en lugar de *self assesment*) con el ámbito de validación adecuado (que realmente cubra nuestro servicio) según la regulación aplicable (ISO 27001, ENS, PCI-DSS, ISO 22301). - Para los servicios Cloud se les puede exigir una certificación de conformidad del ENS y la demostración de un perfil de cumplimiento. - Valorar la posibilidad de pedir resultados recientes de auditoría realizados, por un tercero independiente, al proveedor. - Incluir el requerimiento que en el caso de que sea contratado será auditado (no aplica en Cloud porque no se dejan) o requerir una auditoría específica al proveedor (a realizar periódicamente) de modo que sea posible desistir del contrato de no pasarla. - Establecer la posibilidad de realizar pruebas de seguridad dentro del ámbito del servicio - Valorar la necesidad de exigir al proveedor habilitaciones de seguridad, de empresa o personales del equipo que trabaja hacia el cliente. - Establecer la necesidad de que el proveedor disponga de un servicio de CSIRT 24x7, así como planes de respuesta ante incidentes que cubran adecuadamente el servicio proporcionado.

RIESGO	ACCIONES A REALIZAR
ALTO	- Establecer la necesidad de realizar ejercicios de *red-team* comunes. - Identificar la necesidad y desplegar en su caso, la monitorización y la trazabilidad de los trabajos contratados. - Incluir la necesidad de disponer y ejecutar un plan de concienciación en privacidad y seguridad y exigir evidencias de ello, a lo largo del contrato. - Incluir Acuerdos de Nivel de Servicio (ANS) alineados con KPIs de seguridad. Periodicidad de reporte. - Establecer penalizaciones por incumplimientos de los ANS. - Establecer requerimientos de devolución del servicio. - Valorar la disponibilidad de un ciberseguro, asociado al contrato o de forma global, siempre que la naturaleza de los servicios prestados incluyan bien el tratamiento de información de la organización sensible o de datos de clientes, bien que dichos servicios puedan tener un impacto considerable en la prestación de servicios de la propia organización o bien que exista la posibilidad de propagación de un incidente de seguridad a la red de la propia organización. - Nombrar un responsable de seguridad - Establecer la necesidad de que el proveedor disponga de un servicio de CSIRT 24x7, así como planes de respuesta ante incidentes que cubran adecuadamente el servicio proporcionado. - Requerir que el proveedor realice un análisis de riesgos, con el alcance del proyecto/producto o servicio que vaya a proporcionar a la empresa. Esta información, habitualmente no querrá ser entregada por el aspirante a proveer el servicio, pero servirá para que incorpore técnica y económicamente los controles de seguridad a su oferta. - Para los servicios Cloud se les puede exigir una certificación de conformidad del ENS y la demostración de un perfil de cumplimiento. - Exigir una autoevaluación del cumplimiento de las medidas de seguridad específicas (*Self assesment*) basado en el marco normativo de seguridad del cliente. - Establecer ANS concretos para los principales riesgos y, en concreto, para que tengan que gestionar las vulnerabilidades. - Indicar que será necesario que el proveedor nos informe del CERT de referencia, así como que establezca mecanismos para la compartición de información de indicadores de compromiso con la mayor diligencia y agilidad posible. - Establecer la posibilidad de realizar pruebas de seguridad a sus instalaciones, así como la obligación de colaboración por parte del proveedor. - Valorar la posibilidad de pedir resultados recientes de auditoría realizados, por un tercero independiente, al proveedor. - Incluir la necesidad de disponer y ejecutar un plan de concienciación en privacidad y seguridad. - Penalizaciones por incumplimiento de los ANS. -Establecer requerimientos de devolución del servicio.

RIESGO	ACCIONES A REALIZAR
MEDIO	- Nombramiento de responsable de seguridad. - Incluir medidas generales de seguridad a cumplir enfocadas al uso de la tecnología + confidencialidad + medidas físicas. - Incluir medidas de concienciación en privacidad y seguridad. - Contemplar requerimientos de formación y concienciación para los usuarios.
BAJO	- Incluir medidas generales de seguridad a cumplir enfocadas a la confidencialidad y medidas físicas. - Contemplar la obligación de notificación de cualquier cambio en el personal del proveedor adscrito al servicio. - Revisar los requisitos legales de la contratación y en su caso gestionar la documentación correspondiente (Contrato de Encargado de Tratamiento, HSEM, etc.). - Incluir medidas de concienciación básicas en materia de privacidad y seguridad.

2.1.2.2. Puesta en marcha del servicio

Adicionalmente a las obligaciones anteriores que se materializan en esta fase, se recomienda realizar las siguientes acciones en el momento de la firma del contrato y de manera previa al inicio operativo del servicio:

RIESGO	ACCIONES A REALIZAR
MUY ALTO	- Identificar los escenarios de ataque posibles y establecer planes de respuesta. - Establecer capacidades para el aislamiento selectivo del proveedor (de modo que, si nos proporciona varios servicios, sea posible aislarlos y reconectarlos progresivamente). - Verificar la implantación de las medidas de seguridad adecuadas. - Requerir la entrega del análisis de riesgos realizado por el proveedor. Este análisis debe ser revisado por la empresa, exigiendo su modificación si corresponde o complementándolo en el "lado" de la empresa. - Asegurar la adecuada monitorización de seguridad. - Requerir que el personal reciba información adecuada sobre los procedimientos de respuesta en nuestra empresa. - Generar un marco común de Gestión para los incidentes del proveedor con afectación a la empresa. - Identificar los contactos 24x7 del proveedor y acordar un formato común de reporte. Deberá quedar claro para nuestro equipo de respuesta ante incidentes el rol de cada uno de los posibles contactos inventariados. - Realización de auditorías de cumplimiento con carácter anual/bianual contra el estándar que se determine.

ALTO	- Identificar los contactos 24x7 del proveedor y acordar un formato común de reporte. Deberá de quedar claro para nuestro equipo de respuesta ante incidentes el rol de cada uno de los posibles contactos inventariados. - Requerir que el personal reciba información adecuada sobre los procedimientos de respuesta en nuestra empresa.
MEDIO	- Requerir que el personal reciba información adecuada sobre los procedimientos de respuesta en nuestra empresa.
BAJO	- N/A

2.1.2.3. Durante la ejecución del contrato

Adicionalmente a las obligaciones anteriores que se materializan en esta fase, habría que considerar las siguientes acciones, que deberían ser realizadas de manera periódica a lo largo del contrato:

RIESGO	ACCIONES A REALIZAR
MUY ALTO	- Incluir al proveedor en nuestros procesos de gestión de vulnerabilidades o contemplar la solicitud de información periódica sobre la gestión realizada.
ALTO	- Realizar escenarios de prueba (*red-team*) inclusivos que no consideren la existencia de límites entre las empresas. - Solicitar periódicamente información sobre auditorías de intrusión y gestión de vulnerabilidades realizadas por el proveedor.
MEDIO	- Revisar y validar periódicamente usuarios y accesos. - Llevar a cabo acciones de monitorización y seguimiento de los puntos clave del contrato para garantizar la calidad del servicio prestado por el proveedor.
BAJO	- N/A

2.1.2.4. Devolución del servicio

Adicionalmente, a las que a continuación se aconsejan, es importante que previamente (al comienzo del servicio) el proveedor firme unas cláusulas de confidencialidad en las que figure que el deber de confidencialidad no finaliza con la terminación del servicio.

RIESGO	ACCIONES A REALIZAR
MUY ALTO	- Establecer internamente tiempos requeridos para realizar adecuadamente la devolución del servicio. - Establecer período de solapamiento de proveedor saliente con proveedor entrante para garantizar la transferencia del servicio.
ALTO	- Emitir, por parte del proveedor, una carta certificando la eliminación de toda la información de la empresa.
MEDIO	- Eliminar todos los Permisos de Acceso del Proveedor. - Solicitar la devolución o borrado de la información sensible de nuestra empresa en los - Sistemas de Información del Proveedor. - Certificar la entrega de todos los activos de la empresa por parte del proveedor.
BAJO	- Emisión por parte del proveedor de una carta certificando la eliminación de toda la información de la empresa.

2.2. ESCENARIOS DE RIESGO

2.2.1. Proveedores estratégicos o críticos

2.2.1.1. Situación de riesgo actual

El acceso externo por parte de proveedores que son considerados estratégicos o críticos vamos a considerarlo como un único escenario de riesgo.

Se considerarán también dentro de esta clasificación aquellos proveedores que realicen labores técnicas con accesos privilegiados.

Estos proveedores estratégicos o críticos en la mayoría de los casos requieren accesos privilegiados ya sean a nuestros sistemas de Tecnología de Información, o a aplicaciones críticas con datos sensibles o procesos críticos.

Se trata para estos proveedores de establecer mecanismos de acceso en el que, además del control de accesos y de la gestión de identidades, tengamos un nivel de confianza cero en dichos proveedores.

Tendremos que analizar cómo gestionar y gobernar las identidades privilegiadas otorgadas a este tipo de proveedores.

2.2.1.2. Recomendaciones específicas

- Asegurar que se realizan pruebas de seguridad que abarquen:
  - Controles de acceso lógicos exclusivamente a los recursos necesarios.
  - Controles de acceso físico exclusivamente a los recursos autorizados.
  - Acceso a la red corporativa (acceso remoto y local).
- Implantar el Doble factor de autentificación.
- Para el alcance de los trabajos, el proveedor debe mantener un inventario completo de sus equipos (servidores y equipos finales) y disponer de políticas de gestión de vulnerabilidades y securización de los mismos.
- Virtualización y aislamiento de sesiones de usuario. Implantación de solución PAM (Privileged Access Management).
- Inventariar los activos a los que van a tener acceso el proveedor.
- Establecer mecanismos de prevención frente a pérdidas o fugas de información.
- Establecer mecanismos de notificación y gestión de incidentes.
- Establecer mecanismo reforzados de acceso remoto (entre los que se encuentran el ya citado Doble factor de autenticación).

2.2.2. Proveedores de desarrollo de Software

2.2.2.1. Situación de riesgo actual

Cada vez son más las vulnerabilidades existentes en librerías de código comúnmente utilizadas. Además, en algunos casos los proveedores proporcionan soluciones completas (basadas en distinto software base) que pueden complicar significativamente la gestión de las vulnerabilidades.

Esta gestión de vulnerabilidades incluye en muchos casos la realización de cambios en el software, por lo que su mantenimiento ya no es un tema funcional, sino de seguridad y se requieren por lo tanto recursos para realizar cambios urgentes en las aplicaciones. También es posible que estos proveedores tengan que acceder a los entornos de prue-

bas y en muchos casos también a los entornos de producción.

Por último, otro aspecto para tener en cuenta es la propiedad intelectual de los desarrollos realizados.

2.2.2.2. Recomendaciones específicas

- Asegurar que se realizan pruebas de seguridad que cubran:
  - Control de accesos exclusivamente a los recursos necesarios.
  - Acceso (local y remoto) a la red corporativa.
  - Auditoria, Registros, Monitorización cambios código fuente realizados por el proveedor
  - Buenas prácticas aplicables.
- Definir accesos diferenciados por tipos de entorno: Desarrollo, Pruebas y Producción.
- Asegurar que se dispone de una metodología de desarrollo seguro y que, en consecuencia, se realiza análisis de código (auditoría de calidad y de seguridad) bien de manera interna o por un tercero autorizado, con pruebas de seguridad en el marco de la homologación del software antes de su puesta en producción, con escaneo de vulnerabilidades y un *pen test* (esta última prueba es especialmente recomendable si el software estará abierto a internet).
- Inventariar los activos a los que van a tener acceso el proveedor.
- Establecer un listado de software base permitido. Identificar de manera especial el uso de Gestores de Contenido (CMS).
- Establecer ANS para la resolución de vulnerabilidades.
- Establecer mecanismos de prevención de perdida de información, en este caso el código.

2.2.3. Proveedores menores que utilizan ordenadores propios de la empresa

2.2.3.1. Situación de riesgo actual

En este escenario de riesgo, consideramos que los riesgos inherentes a los proveedores se quedan minimizados al utilizar equipos propios (de la empresa que los contrata) que estarán debidamente securizados siguiendo la política de seguridad propia de cada empresa.

Adicionalmente, se debe reforzar el control de accesos y la gestión de identidades para asegurar que dichos proveedores solo tienen acceso a los activos necesarios.

Para poder simplificar las categorías de riesgo establecidas se consideran dentro de esta clasificación aquellos proveedores que se conecten desde el exterior a través de una solución de Virtualización del puesto de trabajo proporcionada por la empresa. Esta solución deberá de incluir una autenticación reforzada.

2.2.3.2. Recomendaciones específicas

- Aceptación por parte del usuario de las políticas internas y de confidencialidad. Debe quedar una trazabilidad adecuada de la misma.
- Asegurar que se realizan pruebas de seguridad que abarquen:
  - Control de accesos exclusivamente a los activos necesarios
  - Auditoría de los accesos realizados.
- Inventariar los recursos a los que cada proveedor debe de tener acceso.
- Gestión de vulnerabilidades de aplicaciones no corporativas específicas.
- Establecer trazabilidad de la información accedida.
- Establecer mecanismos de prevención frente a pérdidas o fugas de información.

2.2.4. Proveedores menores que utilizan sus propios ordenadores (activos ajenos a la empresa contratante)

2.2.4.1. Situación de riesgo actual

En este escenario riesgo, vamos a depender mucho del servicio que preste el proveedor y de los tipos de conexión que utilicen para realizar dicho servicio.

En la medida que sea posible, es preciso que las conexiones se realicen a través de máquinas/aplicaciones virtuales, de tal forma que evitemos la conexión directa entre los equipos del proveedor y nuestra red.

En el caso que haya conexión directa entre la red corporativa y los equipos del proveedor, hay que fijar el foco en establecer una política de cumplimiento de seguridad de los equipos del proveedor lo más similar posible a la aplicada en nuestros propios equipos, e intentar forzar su implementación de forma que no permitamos la conexión directa a nuestra red si no cumple dicha política.

Una vez que nos aseguremos que los equipos de los proveedores tienen una configuración correcta, lo siguiente es garantizar que dichos equipos solo tienen acceso a los activos necesarios para el servicio a realizar.

2.2.4.2. Recomendaciones específicas

- Asegurar que se realizan pruebas de seguridad que garanticen la validación del cumplimiento de nuestros requerimientos:
  - Configuración de los equipos.
  - Herramientas de protección adecuadas.
  - Controles de accesos lógicos exclusivamente a los recursos necesarios.
  - Controles de acceso físico exclusivamente a los recursos autorizados Acceso a la red corporativa (según nuestros requerimientos de segmentación y de acceso remoto).
- Inventariar los activos a los que van a tener acceso el proveedor.
- Establecer mecanismos de prevención frente a pérdida o fuga de información.
- Recomendable evitar acceso directo de equipos de proveedor a la red interna, usando técnicas de virtualización.
- En el caso de utilizar VPNs, asegurar mediante filtros del tipo *host checker* que los equipos que se conectan cumplen con un mínimo de controles de seguridad (disponer de antimalware, etc..).

3. PLAN DE RESPUESTA A INCIDENTES EN PROVEEDORES

En el supuesto caso, que un proveedor que nos ofrece un servicio se vea implicado en un ciberataque, debemos considerar algunos aspectos clave:

- La Comunicación del incidente, a nosotros, por parte del proveedor.
- Gestión interna del incidente. ¿Activación del comité de crisis?
- Primeros minutos: ¿tenemos elementos de monitorización que nos aporten información de valor para este caso?, la puesta en marcha de medidas de contención, erradicación y/o mitigación.
- Registro de actividades del incidente (bitácora de todo lo que se hace) y preservación e investigación de evidencias.
- Gestión del incidente con el proveedor afectado. Comunicación CISOs, establecimiento de canal de comunicación adecuado (quién, cuándo, cómo, etc.) y Coordinación de respuestas.
- Gobernanza interna del incidente. Protección de la información antes y después del incidente.
- Métricas de seguimiento e impacto.
- Monitorización específica, para la detección de incidentes posteriores al inicialmente detectado; incluyendo, la extensión del problema a nuestros servicios, sistemas y redes.
- Estrategia y comunicación del incidente.
- Notificación a reguladores/ autoridades de control y/o CERTs de los mismos. Notificación, si procede (por sufrir daños propios) a las Fuerzas y Cuerpos de Seguridad del Estado.
- Involucración del Departamento Jurídico.
- Posible intervención y reclamación a Seguros.
- Lecciones identificadas y aprendidas (serán aprendidas cuando no se repitan). Revisar internamente el registro de actividades y ver dónde se ha fallado y qué se puede mejorar. En una segunda iteración, involucrar al proveedor para mejorar el procedimiento.

- Posincidente: derechos a auditoría de riesgos y seguridad, así como inspecciones *on-site*.

Estos aspectos deben ser tenidos en cuenta en el caso que un ciberincidente afecte a un proveedor de nuestra empresa. En estos casos y a diferencia de un incidente directo a nuestra empresa, es crucial mantener una comunicación efectiva con los responsables del proveedor de gestionar y mitigar el ciberincidente. En los primeros minutos es vital contener/mitigar el daño, no es momento de discusiones, sino de colaboraciones. Las discusiones sobre responsabilidades se deben mantener una vez el incidente está controlado.

Adicionalmente, debemos ordenar las ideas ante dicha eventualidad. Esto significa que debemos ser cuidadosos, así como llevar a cabo, de forma ordenada, las comprobaciones y acciones necesarias para intentar mitigar el impacto.

Lógicamente, dependerá mucho de la tipología del incidente, de su severidad y del tipo de relación que mantenemos con nuestro proveedor, el que se deba actuar de un modo u otro y que se deban seguir los pasos arriba descritos de una forma parcial o total.

Los objetivos de un Protocolo de respuesta a incidentes en proveedores deben ser:

- **Establecer los mecanismos metodológicos y organizativos, así como las responsabilidades**, necesarios para llevar a cabo una adecuada gestión de ciberincidentes con dichos proveedores.
- Identificar la documentación con relación al proveedor, identificando personas, servicios y activos.
- **Determinar las acciones generales necesarias** durante la respuesta a ciberincidentes desde un punto de vista táctico, favoreciendo la coordinación y agilidad en la toma de decisiones.
- **Clasificar y categorizar** los ciberincidentes, evaluando, clasificando e identificando las siguientes acciones a realizar, en aras de disminuir el posible impacto.
- **Identificar todas las partes interesadas y establecer los canales de comunicación** necesarios con respecto a los ciberincidentes.
- Establecer el procedimiento para **determinar el nivel de criticidad**, el impacto.
- En virtud de estos últimos, el **proceso de escalado** (interno y externo) de los ciberincidentes. Determinar si deben ser notificadas las Fuerzas y cuerpos de seguridad del Estado.

- **Identificar los actores principales** que intervendrán en la ejecución de cada fase de gestión de los incidentes, sus capacidades y sus responsabilidades.
- **Mitigar los riesgos** a los que podemos estar expuestos, respondiendo a ciberincidentes de manera efectiva y eficiente.
- Establecer la documentación necesaria para dar por cerrado el incidente y poder **reabrir la operativa habitual**.

Cada empresa debería de ser capaz de encajar este protocolo en sus mecanismos de gestión de ciberincidentes o similar, de modo que este sea un posible punto de entrada en la Detección de un ciberincidente o, alternativamente, poder establecer los mecanismos adecuados para atender y gestionar un ciberincidente en un proveedor.

Es evidente que hay tres factores muy importantes a la hora de gestionar un ciberincidente en un proveedor: la relación con el proveedor, las características técnicas del servicio y la naturaleza del ciberincidente. Por ello, se intenta aquí protocolizar de forma general, dando pautas que cada empresa deberá tener en cuenta y adaptar.

Se deben tener en cuenta cuatro fases fundamentales:

Fase 0: Evaluación del riesgo de ciberseguridad de un proveedor (matriz de evaluación de proveedores).

Fase 1: Preparación y prevención ante ciberincidentes en proveedores

Fase 2: Detección, investigación y análisis, contención, erradicación y recuperación

Fase 3: Post Incidente y lecciones aprendidas.

La lectura de este capítulo se complementa con el documento ***Protocolo de actuación frente a incidente en proveedor***, de ISMS Forum 2020 (Ref 2).

3.1. FASE 0: EVALUACIÓN DEL RIESGO DE CIBERSEGURIDAD DE UN PROVEEDOR

En esta fase corresponde realizar una evaluación del nivel de riesgo de ciberseguridad de un proveedor. En el Anexo 1 hallará una propuesta de cuestionario de autoevaluación por parte del proveedor.

3.2. FASE 1: PREPARACIÓN Y PREVENCIÓN ANTE CIBERINCIDENTES EN PROVEEDORES

Esta fase se refiere al conjunto de medidas y estado de preparación estable que permita una reacción lo más ágil posible ante un ciberincidente.

Dichas medidas deberán de estar acompañadas de un responsable que debe hacerlas cumplir. Las acciones a considerar siempre serán acordes al nivel de madurez y capacidades de nuestra empresa, siendo también necesaria una adecuada priorización. A continuación, se indican las principales a considerar:

- Inventario de Proveedores vinculados a nuestra empresa.
- Niveles de Riesgo de Ciberseguridad.
- Controles de Riesgos de Ciberseguridad según riesgo evaluado y gestionado.
- Análisis de criticidad de Proveedores para nuestra empresa.
- Mapa de Riesgos de proveedores para nuestra empresa (relación contractual, servicios que prestan, forma de conexión, uso de equipamiento interno/externo…).
- Monitorización de Proveedores (herramientas y gestión), que permitan conocer el rating de nuestros proveedores y su nivel de exposición.
- Supervisión, esto es, todos los servicios de terceros deben pasar por un proceso de supervisión para detectar vulnerabilidades o cambios en los servicios que puedan suponer un impacto en seguridad.
- Identificación de los criterios de evaluación y notificación de los incidentes.
- Pueden -y en los casos legamente establecidos, deben- tomarse como referencias las guías y procedimientos:
  - *Guía Nacional de Notificación y gestión de Ciberincidentes*[1].
  - *CCN-STIC-817 – Gestión de ciberincidentes*[2].
- Cláusulas de notificación de ciberincidentes categorizados como relevantes (Medio/Alto/Crítico) por el proveedor, con un ANS determinado en los Contratos (nuevos y revisar los ya vigentes) y con una definición de cuáles van a ser los criterios y requisitos para considerar un incidente bajo control, con las consecuentes responsabilidades para el proveedor en caso de ha-

[1] Guía Nacional de Notificación y gestión de Ciberincidentes.
[2] CCN-STIC-817 – Gestión de ciberincidentes.

ber proporcionado información incorrecta o no completa, o haber dado por erradicado un problema en su lado, sin que realmente lo estuviera.

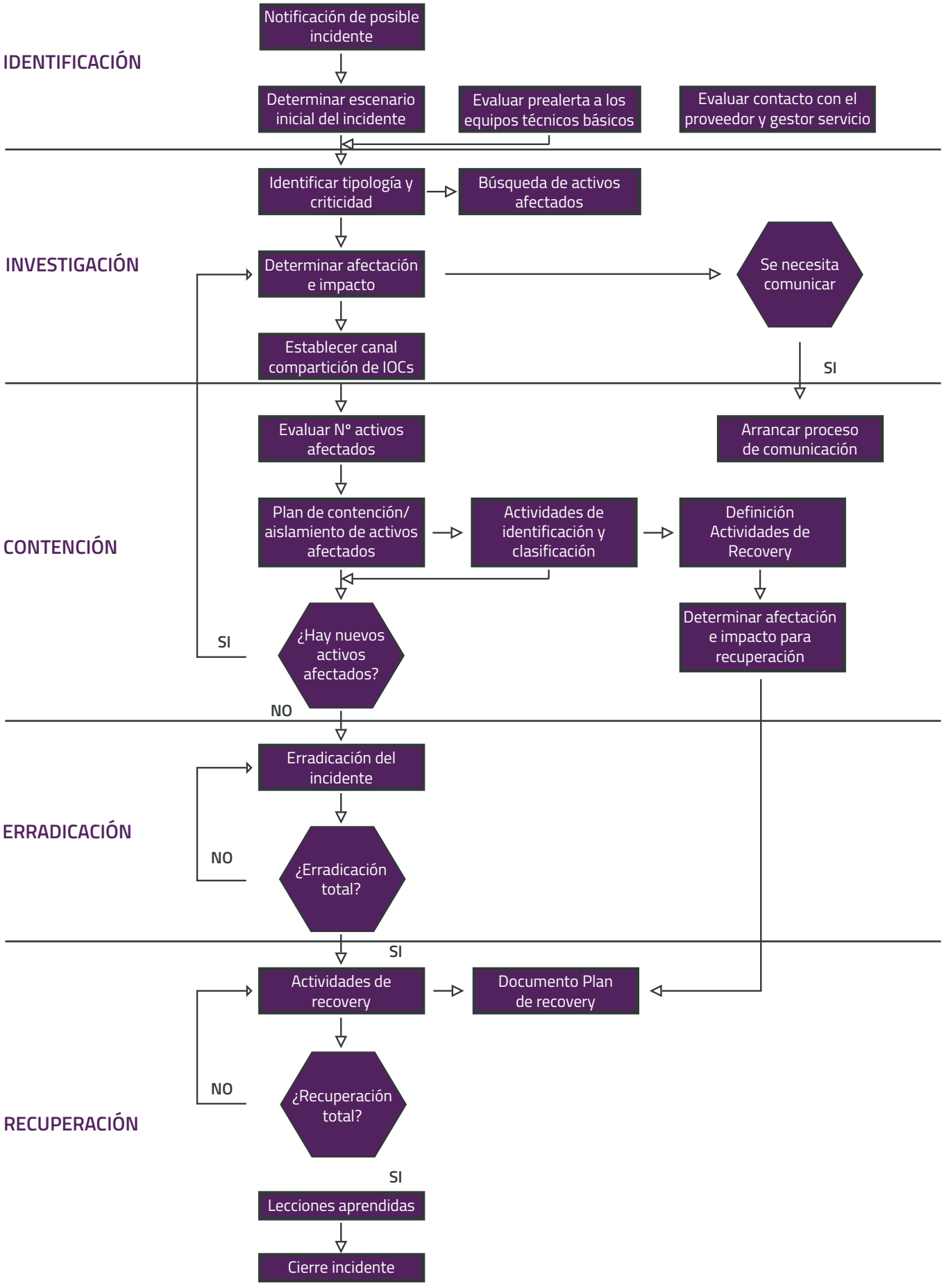
- Cláusula de derecho de auditoría (directa o indirecta) de riesgos y seguridad sobre el proveedor, así como inspecciones *on site* al mismo, y obligación del proveedor a facilitar y colaborar en estas auditorías.
- Cláusula de Confidencialidad de la información que maneje de nuestra empresa.
- Establecimiento de un Anejo al Contrato, con acuerdo de gestión de ciberincidentes, donde se establezcan las responsabilidades, mecanismos de comunicación y de gestión en caso de ciberincidente en el proveedor.
- Se deben poder tratar las vulnerabilidades críticas y las amenazas potenciales como un incidente, si el que contrata el servicio lo considera necesario.

3.3. FASE 2: GESTIÓN DEL INCIDENTE: IDENTIFICACIÓN O DETECCIÓN, INVESTIGACIÓN Y ANÁLISIS, CONTENCIÓN, ERRADICACIÓN Y RECUPERACIÓN

La gestión de un ciberincidente podemos considerar que se inicia una vez detectado el mismo (identificación o detección), continuando, en primer lugar, con la investigación o análisis previo (esta actividad desde este momento será vertical y omnipresente durante el resto de las etapas). Durante las etapas de contención y erradicación, una vez que ya se comienza a tener un relativo grado de conocimiento del ciberincidente, es habitual la realización de un nuevo análisis, lo que conlleva volver a fases anteriores tantas veces como sea necesario para erradicar el ciberincidente al completo y pasar, ya sí, a la fase de recuperación.

A continuación, se muestra un diagrama con las etapas esquematizadas del proceso:

03 / Plan de respuesta a incidentes en proveedores



3.3.1. Etapa 2.1. Identificación o detección

Esta etapa es crucial e implica el descubrimiento de la existencia de un ciberincidente en el proveedor, confirmado por él mismo o por terceros.

Lo habitual y deseable es que el proveedor sea quien informe a la empresa de la existencia de un ciberincidente relevante. En ocasiones, presuponiendo el cumplimiento del ANS existente (ver Fase 1), es posible que la empresa sea consciente del ciberincidente en el proveedor por otras vías (CERTs, otras organizaciones y Servicios de Monitorización, contactos del sector o incluso medios de comunicación…), en cuyo caso, la empresa podrá contactar con el proveedor afectado. En función del origen y fiabilidad de la información, la actuación por parte de la empresa será más preventiva o reactiva. Lo más importante es conocer lo antes posible la existencia de un ciberincidente.

En esta fase, se debe, además, identificar el tipo de incidente a gestionar (malware, fuga de información, etc.) para poder determinar los equipos técnicos a involucrar en la prealerta.

Las acciones para realizar en esta fase son:

- Análisis preliminar de la información comunicada por el proveedor y/o detectada para determinar escenario inicial del incidente.
- Evaluar el interés de contactar con las áreas técnicas involucradas para activar estado de prealerta y asegurar que será posible realizar una respuesta ágil.
- En el caso de que el incidente haya sido identificado a través de una vía diferente al proveedor, contacto con el proveedor, así como con el responsable del servicio definido dentro de nuestra empresa.

3.3.2. Etapa 2.2. Investigación y análisis

Esta fase da comienzo una vez determinado que el ciberincidente en el proveedor afecta o podría, potencialmente, afectar a los sistemas y/o a la información de nuestra empresa.

Se contrasta la información con la que contamos para determinar si, efectivamente, debemos gestionar el ciberincidente en la empresa; darlo de alta en nuestro sistema de gestión de ciberincidentes y analizarlo en profundidad viendo si se queda en un falso positivo o, si por el contrario, pasa a ser un ciberincidente a gestionar (traslación del ci-

berincidente en un tercero, categorizado como tal, a ciberincidente propio).

A la información inicialmente aportada por el proveedor, podemos pedir evidencias e indicadores de compromiso, si bien el resultado de esta petición dependerá de las cláusulas que hayamos firmado en el contrato, del nivel de transparencia que le hayan fijado sus órganos directivos, el grado real de conocimiento sobre lo que le está pasando y de la presión y capacidad de atender a la urgencia en su propio negocio.

Teniendo en cuenta lo anterior, la organización debería solicitar los siguientes documentos, en especial aquellos que aparentemente no hayan tenido impacto:

- Carta de descargo en el que el proveedor reconozca la ocurrencia del incidente de seguridad y la afectación o no sobre nuestra organización.
- Informe de incidente, en el que se explique las causas, impacto propio y potencial impacto sobre nuestra organización con un adecuado nivel de detalle.

Si se descarta el falso positivo, la empresa deberá:

- Identificar la tipología del ciberincidente siguiendo la taxonomía de la empresa (sin perjuicio de la que el proveedor haya asignado).
- Establecer la criticidad del ciberincidente siguiendo los criterios de la empresa (sin perjuicio de la que el proveedor haya asignado).
- Escalado y notificaciones internas y externas, acordes a los criterios definidos en cada empresa.
- Valorar el notificar/activar, si se tiene, el ciberseguro.
- Determinar el canal de comunicación apropiado con el proveedor, estableciendo tiempos de comunicación mínimos, intercambio de información tanto técnica (IOCs,) como de gestión y de comunicación externa, si fuera relevante, de forma coordinada
- Recopilación, documentación y salvaguarda de evidencias lo antes posible.

3.3.2.1. Notificaciones internas

Deberán existir unos criterios de notificación interna y externa a los que atenerse en caso de ciberincidente.

- En el caso de las notificaciones internas, deberán definirse unos mecanismos de escalado y notificación, donde claramente se identifiquen los roles y responsabilidades dentro de la empresa (CISO, CIO, CEO, CRO, Comités…).

- Cuando hablamos de notificaciones "internas" en el caso de Grupos de empresas deberíamos incluir a otras empresas de nuestro Grupo que puedan verse afectadas. En este tipo de comunicaciones, es importante establecer un clima de transparencia y confianza entre empresas del Grupo y en ningún caso tratar de ocultar información por cuestiones de imagen interna.

- Esta cuestión; la transparencia, junto con el debido equilibrio entre la no exposición de información innecesaria o a personas no autorizadas, junto con la debida prudencia, hacen que si bien conceptualmente, es fácil referirnos a ella, sin embargo, es realmente complejo y es algo a trabajar durante años en la cultura empresarial.

3.3.2.2. Notificaciones externas

En el caso de las notificaciones externas, hay de diferente naturaleza:

- Notificaciones a organizaciones que puedan ayudar a nuestra empresa, en el caso de que exista sospecha de que un ciberincidente en un proveedor podría afectar a nuestra empresa. Es conveniente mantener un listado actualizado de a quién podríamos recurrir (INCIBE-CERT, CCN-CERT, otros proveedores de referencia en nuestra empresa, contactos, etc.).

- Notificaciones a reguladores y/o stakeholders: en función de la naturaleza del incidente, cada empresa debe identificar a quién notificar, qué información proporcionar, los plazos para notificar y los contactos relevantes para hacerlo. Para ello, se debe contar con una tabla donde estén identificados previamente todos estos aspectos.

- Denuncia ante las Fuerzas y Cuerpos de Seguridad del Estado, si procede.

En este punto nos parece interesante volver a citar para su consulta la *Guía Nacional de Notificación de Incidentes*.

3.3.3. Etapa 2.3. Contención

El objetivo principal es limitar el impacto del ciberincidente en nuestra empresa. Eso no siempre será posible si, por ejemplo, se trata de información que un proveedor ha perdido o que se ha visto expuesta. Pero sí lo será en el caso de que un ciberincidente como un malware pudiera acabar afectando a nuestros sistemas, para lo cual será muy

relevante evitar la propagación.

Debe primar la contención rápida y efectiva, estableciéndose también las oportunas medidas que permitan un análisis forense para determinar lo ocurrido y obtener, posteriormente, lecciones aprendidas. En función de la tipología del incidente (ver Etapa 2.2), será recomendable tomar evidencias antes incluso de realizar ciertas acciones de contención.

Es recomendable tener un modelo de actuación para la contención basado, por ejemplo, en preguntas que debemos hacernos y que, en función de las respuestas a las mismas, realicemos unas acciones u otras.

Las medidas de contención se pueden categorizar en dos, por el impacto que tienen sobre las operaciones de negocio de nuestra empresa:

- Medidas que no afectan a la operativa normal: incluirá actividades que pueden ser realizadas de forma preventiva lo antes posible y que mitigan el riesgo de forma casi transparente.

- Medidas que sí afectan a la operativa normal: se deben valorar las actividades a realizar, reconocer a qué partes del negocio impactaría y cómo. En este momento se debe involucrar a las áreas de negocio afectadas y establecer con ellos un plan de seguimiento del impacto interno.

En ambos casos, es muy importante también comenzar a definir un plan, incluyendo el horizonte temporal de aplicación de dichas medidas. Siempre ha de contarse con el feedback del proveedor que es quien, en última instancia, debe confirmar que la situación está bajo control en sus dominios. Sin esa confirmación, no podríamos asegurar en último término la correcta contención en nuestra empresa.

Además, se debe recordar que es posible que el incidente siga evolucionando, por lo que es necesario dedicar un equipo de trabajo a la búsqueda de nuevos indicadores de ataque y a su clasificación. Este equipo deberá trabajar de manera coordinada con el equipo de contención validando las diferentes hipótesis de ataque que se realicen.

Es necesario también implantar una adecuada monitorización y supervisión para verificar que los controles que se están llevando a cabo son eficaces.

Por último, es más que recomendable activar un equipo de recuperación lo antes posible, recurriendo a los medios con los que cuente cada empresa y que, a partir de la

información disponible, active los mejores planes de vuelta a la normalidad y coordine, en caso necesario, las acciones derivadas del plan de continuidad de negocio (ver Etapa de Recuperación). Es por ello también importante informar y alertar a los departamentos de negocio afectados y a los potenciales afectados en función de las medidas que la empresa decida tomar, de la posibilidad de la puesta en marcha de algún/os plan/es.

3.3.4. Etapa 2.4. Erradicación

En esta etapa, el objetivo principal es la eliminación del ciberincidente de nuestros sistemas, hasta donde sea posible y conozcamos, o bien garantizar que se está realizando en los sistemas donde nuestra información esté almacenada.

La naturaleza de esta etapa conlleva una serie de actividades que se ejecutan en algunos casos de forma inmediata (desconexiones, controles de acceso, revisiones…) y en otros, con posterioridad (infraestructuras no críticas, gestión de parches y vulnerabilidades, restructuraciones y cambios en infraestructuras…).

Deben establecerse de forma clara, entre ambas partes, cuáles van a ser los criterios y requisitos que determinen que el incidente estará efectivamente erradicado para poder proceder a la recuperación de la normalidad (ver Fase 1).

Similar a la Etapa 2.3, siempre ha de contarse con el feedback del proveedor que es quien, en última instancia, debe confirmar que la situación está bajo control en sus dominios. Sin esa confirmación, no podríamos asegurar en último término la correcta erradicación en nuestra empresa.

3.3.5. Etapa 2.5. Recuperación

Restaurar los sistemas a su funcionamiento normal, en el caso de que los sistemas de nuestra empresa hayan sido afectados, y/o restaurar los accesos a la información, en el caso de que esta residiera fuera de nuestros sistemas, es el objetivo de esta etapa. Adicionalmente, se reforzarán las medidas para evitar que un nuevo caso aún no detectado o futuro, pongan en riesgo nuevamente la información y/o los sistemas de la empresa.

Actividades o acciones típicas serán: la verificación del funcionamiento normal o mínimo de nuestros sistemas y/o del acceso a nuestra información, realizar los ajustes necesarios en nuestras redes y el perímetro de estas, y restauraciones desde copias de seguridad disponibles, cuando sea posible.

Cabe revisar si es necesario para recuperar esa situación normal hacer uso del plan de continuidad de negocio (en caso de no haberlo activado antes), revisar los RTO, RPO, MTD, etc.

También se han de terminar de revisar las cláusulas y términos legales con el proveedor para clarificar que está todo correcto y no cabe penalización o acciones legales, revisión de cumplimientos de los ANS/SLA, etc.

Dada la complejidad, sofisticación y estrategia de algunos tipos de ciberataques, deberemos afinar la monitorización y la detección, para identificar anomalías y comportamientos que pudieran indicar una presencia latente, que pasara de una situación durmiente asintomática a otra de reinicio de actividad maliciosa.

Una vez estemos en disposición de operar con normalidad y tengamos la confirmación del proveedor de que también ellos están libres de incidencias y operan con normalidad, queda un último paso antes de proceder al cierre definitivo del incidente. Se trata de comenzar con el proceso de "lecciones aprendidas". En cualquier caso, también es posible que hubiera circunstancias que aconsejaran esperar antes de cerrar, formalmente, el incidente.

En lo relativo al proceso de lecciones aprendidas, que aquí comienza y que podrá finalizar incluso tras el cierre del incidente, lo más importante es:

- Si se ha actuado con determinación y de forma correcta en la gestión del ciberincidente.
- Si estaban claras las responsabilidades y roles dentro de nuestra empresa,

así como con el proveedor.

- Como empresa, también debemos valorar si los procedimientos de continuidad, escalado y gestión de crisis se han realizado correctamente y aprovechar este punto para incluir mejoras y/o actualizaciones.

- También es importante plantearnos como empresa si prevemos que sea necesario o aconsejable realizar alguna auditoría de seguridad o riesgos al proveedor o, en su defecto, exigirle evidencias de aquellos cambios que, debido a la naturaleza del ciberincidente, fuera necesario acometer, tanto técnicos como procedimentales o de gestión.

El cierre del incidente incluye las notificaciones oportunas, tanto internas, como externas (proveedor y organismos relevantes, incluso medios de comunicación, si fuera el caso), y también incluye el correcto registro del incidente, en una base de datos de conocimiento o similar, que permita poder disponer de información en un futuro.

3.4. FASE 3: POST INCIDENTE Y LECCIONES IDENTIFICADAS/ APRENDIDAS

Serán lecciones identificadas mientras no aseguremos que, en base a nuestro aprendizaje y mejora de mecanismos de respuesta, consigamos que, frente a un nuevo incidente similar, podamos reducir la probabilidad o impacto de este. Si lo conseguimos serán **lecciones aprendidas**.

Es importante:

- Evaluar la información que hemos ido obteniendo y registrando a lo largo del ciclo de vida del incidente, de forma que podamos también identificar si tenemos toda información relevante, se han recogido todas las actuaciones llevadas a cabo, si se han obtenido todas las evidencias necesarias, y el estado de estas.

- Es sustancial almacenar esa información (trazabilidad), tanto técnica como de gestión (escalado y notificación), para garantizar que se ha gestionado el ciberincidente de forma adecuada, qué es lo que ha funcionado y qué no, incluso para presentar a un tercero al que estemos obligados las acciones tomadas y así evitar o reducir el riesgo de sanciones. También, para contar con esta información a futuro y continuar identificando lecciones aprendidas, a todos los niveles.

- Revisar y evaluar cómo de útiles han sido nuestros procedimientos, con qué

grado de cumplimiento los hemos seguido, cómo de eficaces y eficientes han sido nuestros trabajos, las cláusulas y controles de seguridad, identificando mejoras y proyectos específicos y acotados, también de mejora.

- Dependiendo de la naturaleza del incidente y de su afectación conviene revisar nuestro SGSI y actualizarlo debidamente: cuadros de mando (aquí conviene ver si debemos añadir algún indicador adicional o hacer un seguimiento más exhaustivo de algún indicador ya existente durante los meses posteriores al incidente), registro de riesgos, cuerpo normativo, planes de continuidad (esto ya expone en el documento), plan de formaciones/concienciación, procedimientos existentes (no necesariamente relacionados con continuidad), auditorías, clausulados a firmar por terceras partes.

- También dependiendo de la naturaleza del incidente y de su potencial impacto en el futuro, deberemos incorporarlo a futuras simulaciones y ciberejercicios a desarrollar, ya sea solo con los actores propios de la compañía o con el concurso de proveedores.

Adicionalmente, es el momento de revisar si el proveedor ha cumplido con lo que por contrato se le puede exigir. Esto es:

- Si ha actuado con diligencia, si ha informado del incidente dentro de los límites establecidos en el ANS, si ha respetado los acuerdos de confidencialidad previstos, y si los mecanismos de comunicación han seguido los cauces previstos.

Finalmente, la empresa también debe valorar la necesidad de involucrar en cualquier momento, incluso en fases anteriores, al Departamento Jurídico o similar o al departamento de proveedores/compras a modo de asesoría y para poder contrastar qué es exigible al proveedor.

4. CONTINUIDAD DE NEGOCIO

4.1. IDENTIFICACIÓN DE LOS PROVEEDORES TOP CRÍTICOS EN EL ÁMBITO CÍBER

Desde el punto de vista de continuidad de negocio es importante tener identificados a los proveedores en función del nivel de riesgo que representan en materia de ciberseguridad y/o seguridad de la información (en adelante cíber, por simplificar).

Un buen punto de partida para esta identificación es el BIA (Análisis de Impacto de Negocio), metodología que nos ayuda a identificar la dependencia de los procesos de la empresa con los servicios prestados por proveedores, o un inventario específico que recoja el listado de proveedores de la empresa con la relación de los servicios que nos prestan. Esto implica que un mismo proveedor estará registrado en nuestro inventario tantas veces como servicios nos preste, por lo que este inventario debe ser actualizado cada vez que se produzca un cambio en el servicio prestado o se externalice un nuevo servicio. Dicho inventario debe, como mínimo, mostrar la siguiente información para cada servicio:

- Nombre del proveedor.
- Servicio que presta.
- Descripción del servicio.
- Necesidades que requiere el proveedor para prestar este servicio. Recursos que le tendremos que proporcionar al proveedor.
- Fecha de inicio y fin del servicio.
- Responsable de seguridad del proveedor para este servicio.
- Resto de contactos necesarios según los procedimientos de comunicación existente.
- Valor del riesgo por una indisponibilidad del servicio o del proveedor.

- Valor de riesgo de seguridad del proveedor.
- Ubicación de las instalaciones del proveedor.
- Ubicación de los CPD (Centros de Procesamiento de Datos) del proveedor.
- Contactos 24x7h para emergencias (incluyendo contactos de backup).
- Acuerdos de Nivel de Servicio, RTOs, RPOs del servicio.
- Penalizaciones.
- Enlace a la gestión documental a nuestro histórico de incidentes de este proveedor.

Información de nuestra empresa:

- Responsable del servicio que contrata el proveedor.
- Datos de contacto.
- Canal y modo de comunicación con el proveedor.

Una vez obtenidos estos datos mínimos, el siguiente paso es identificar aquellos que podrían suponer un riesgo ciber para la empresa, para lo que se puede partir de un formulario autoevaluación (que se adjunta como Anexo 1 y se desarrolla en el punto de Análisis de Riesgos y Marco de Control de Proveedores) del que poder extraer una primera versión del impacto, considerando al menos:

- Pérdidas económicas directas.
- Indisponibilidad de los procesos productivos o de entrega de servicio.
- Sanciones reglamentarias.
- Responsabilidades penales y/o civiles.
- Penalizaciones contractuales.
- Daño reputacional.

De los proveedores identificados, que además sean susceptibles de sufrir un incidente cíber con consecuencias significativas para el negocio, se debería realizar un análisis de riesgo más profundo e identificar los posibles escenarios de impacto para el negocio

en el área de ciberseguridad y/o seguridad de la información (ver Sección siguiente de Análisis de Riesgos).

4.1.1. Proveedores “pasivos”

Igualmente se debe tener planificada la posible sustitución del servicio prestado por un proveedor crítico, por otro que pudiera suministrar al menos unos mínimos previamente establecidos. Con este proveedor “suplente” o pasivo, se deben aplicar los mismos protocolos que con el/los proveedor/es que sustituye y, sobre todo, las condiciones de prestación de servicio en la que se debe quedar perfectamente identificadas todos los detalles de activación de puesta en servicio.

Sin lugar a duda, estos proveedores pasivos deben estar integrados en todos los planes de Continuidad de negocio como estrategias de recuperación, pruebas periódicas, etc.

Somos conscientes que esta medida en la práctica es difícil de llevar a cabo para las entidades que se rigen por la contratación pública, debido a los condicionantes, plazos y procesos administrativos que les son de aplicación.

4.2. ANÁLISIS DE RIESGO Y MARCO DE CONTROL DE PROVEEDORES

La Continuidad de los servicios prestados por un proveedor debe enmarcarse en un proceso de gestión y control de terceros trasversal a la empresa. Cada compañía debe analizar los riesgos que supone la externalización de sus servicios y gestionarlos adecuadamente para minimizar su impacto potencial.

En algunos sectores, como el financiero, existen regulaciones específicas en este sentido, pero aquellos que no estén obligados por ninguna regulación, deberían igualmente desarrollar procedimientos que les permita gestionar el ciclo de vida completo de la externalización y gestión de terceros.

Se describen a continuación algunas acciones que se considera necesario integrar dentro del proceso de gestión de terceros para minimizar los riesgos de indisponibilidad del servicio por un incidente cíber de nuestro proveedor.

4.2.1. Evaluación y análisis de valor de riesgo

La prestación de un servicio por un tercero o proveedor incorpora nuevas amenazas a

nuestro entorno que deberán ser analizadas desde todos los ámbitos de riesgo, en función de sus correspondientes impactos. En esta sección nos centramos en la evaluación y análisis del riesgo de la no disponibilidad del servicio que nos presta un proveedor, o la indisponibilidad del propio proveedor para prestarlo/s, debido fundamentalmente a que el proveedor está siendo víctima de un incidente de seguridad o la pérdida de confidencialidad de la información (exfiltración de información, por ejemplo), o de la integridad de la información o los servicios. No obstante, se recomienda valorar los riesgos para cada servicio ya que un mismo proveedor puede estar prestando servicios críticos y servicios muy poco críticos o fácilmente asumibles por la propia empresa

.

A la hora de realizar este análisis, es aconsejable recurrir a la metodología de riesgos existente en cada empresa. Esto nos permite dar homogeneidad al proceso y asignar unos valores de riesgo con los que están familiarizadas otras áreas que requieren de esta información para realizar su trabajo. En todo caso, se puede utilizar la que mejor nos encaje en el momento de establecer el proceso.

A modo de ejemplo, se propone analizar los riesgos en base al cálculo de probabilidad por impacto utilizando valores cualitativos tanto del impacto como de la probabilidad, adoptando los siguientes rangos:

- **Impacto:** muy alto, alto, medio o bajo.
- **Probabilidad:** alta, media o baja.

Centrándonos en la amenaza objeto de esta sección:

- El proveedor está sufriendo un incidente cíber.

El **impacto** de esta amenaza se establece del siguiente modo:

- **Muy alto:** el servicio prestado por el proveedor es muy crítico para nuestra empresa, la plataforma para la prestación del servicio está ubicada en las instalaciones del proveedor. Por ejemplo, se pueden clasificar como muy alto los servicios de proveedores que pueden afectar a:
  - Los rendimientos financieros.
  - La solvencia.
  - La continuidad de la actividad.

- **Alto:** el servicio es muy crítico para nuestra empresa, pero la plataforma está en nuestro CPD.
- **Medio:** el servicio tiene una criticidad media y está ubicado en las instalaciones del proveedor o en nuestro CPD.
- **Bajo:** el servicio es poco crítico, tanto si está en nuestras instalaciones como en las del proveedor.

El valor de la probabilidad se puede asignar en base al nivel de seguridad demostrable por el proveedor y a los reportes de ciberataques medidos en el último año de modo general y sectorial. De este modo, podríamos tener los siguientes valores de **probabilidad**:

- **Alta:** proveedores que cuentan con escasas medidas de seguridad o tienen un nivel de madurez bajo respecto de la seguridad. El número de ataques reportados a nivel mundial, regional o sectorial durante el último año es alto.
- **Media:** tiene ciertos controles y acreditan cierta madurez de seguridad basada en riesgos y cuentan con una mínima estructura de ciberseguridad. Existe un número importante de ataques a nivel mundial y regional.
- **Baja:** el proveedor cuenta con un nivel de madurez alto y demostrable respecto a la seguridad. Existe un número bajo de incidentes reportados o apenas afecta al sector en el que se mueve el proveedor.

Como resultado del análisis se obtendrá un mapa de calor del riesgo que nos indicará qué acciones mitigantes tendremos que tomar.

Incluimos una tabla a modo de ejemplo:

RIESGO		INDISPONIBILIDAD DE UN SERVICIO DEBIDO A UN INCIDENTE CÍBER EN UN PROVEEDOR			
		IMPACTO			
		MUY ALTO	ALTO	MEDIO	BAJO
PROBABILIDAD	ALTA				
	MEDIO				
	BAJA				

Las acciones y controles a realizar dependerán de la zona en el mapa de calor en el que se ubiquen los servicios o proveedores analizados.

Deberemos dejar constancia del riesgo residual que permanece tras la gestión del riesgo.

Los valores de riesgo tanto de indisponibilidad como de seguridad asociados a cada proveedor/servicio, deberán calcularse en el momento correspondiente. Estos valores deberán revisarse periódicamente, especialmente cuando se produzca un cambio en el servicio o en el proveedor.

4.2.2. Cuestionario para la evaluación del riesgo

La información necesaria para la realización del análisis se puede obtener mediante el desarrollo del cuestionario indicado en el **Anexo 1** y se deberá integrar con nuestro inventario de servicios y proveedores. El cuestionario debe ser rellenado en la fase de inicio por el Responsable del Servicio o similar de la empresa.

Dado que la responsabilidad de un incidente recae sobre la empresa en primera instancia, es el Responsable del Servicio de la empresa quien debe encargarse de que se realice dicho análisis descrito en el cuestionario del Anexo 1, siempre con el concurso del proveedor y apoyo del personal experto en continuidad de negocio de la empresa.

Es importante que se realice en las fases iniciales ya que es posible que se identifiquen acciones mitigantes del riesgo que deben adoptarse para la viabilidad de este.

A continuación, se indica, a modo de ejemplo, otras preguntas complementarias a dicho anexo para realizar el mapa de calor anteriormente descrito y para focalizar la modalidad de servicio prestado:

- **¿Es un servicio crítico para nuestra empresa?**

  a. La respuesta a esta pregunta debe venir del BIA correspondiente a este servicio.

- **¿Dónde estará ubicada la plataforma necesaria para la prestación del servicio?**

  a. En las instalaciones del proveedor.
  b. En nuestro CPD.
  c. Cloud.

- **¿Quién opera?**
  - **a.** El proveedor.
  - **b.** Equipos propios.
- **En caso de que sea el proveedor el que opera la plataforma. ¿Contamos con personal entrenado para asumir el servicio en caso necesario?**
- **Los Acuerdos de Nivel de Servicio (ANS), Objetivos de Punto de Recuperación (OPRs) y Objetivos de Tiempo de Recuperación (OTRs) que garantiza el proveedor ¿son inferiores a los necesarios por la empresa trasladados en el BIA?**

El cuestionario se debe trasladar al proveedor a través del Responsable del Servicio.

Este cuestionario puede variar en función de la metodología de riesgos adoptada en la empresa y de las descripciones de los impactos y probabilidades establecidos. A cada respuesta se debe asignar, de acuerdo con su relevancia, un valor/peso que permita calcular el nivel de madurez y seguridad del proveedor y que se utilizará para calcular la probabilidad en combinación con la información de ciberataques en el entorno indicado que se maneje. Cada empresa debe establecer, en todo caso, los criterios de evaluación que mejor se ajusten a su perfil de riesgo y metodologías existentes, así como su cultura y madurez respecto de la seguridad y continuidad

Además, el cuestionario debe idearse como una herramienta que proporcione los controles a aplicar según los resultados del análisis de riesgos efectuado. La finalidad es establecer controles para cada una de las fases del servicio:

- **Contratación:** controles en fases iniciales que nos ayuden a establecer el marco de trabajo minimizando los riesgos.
- **Prestación el servicio:** aquellos focalizados en garantizar la disponibilidad del servicio acordada con el proveedor durante las negociaciones.
- **Terminación:** controles que nos permitan tener la capacidad de continuar con el servicio si así lo requerimos, bien con otro proveedor o bien internalizando los propios servicios, así como la terminación segura del contrato con el proveedor saliente, si fuera el caso.

Para el caso que nos ocupa los controles relevantes y en los que se centra la siguiente sección, son aquellos cuya finalidad es garantizar los tiempos de respuesta establecidos en nuestros BIAs para el servicio analizado (OTRs y OPRs).

4.2.3. Controles recomendados y supervisión

En el cuestionario del **Anexo 1** se indican controles enfocados a reforzar un mejor contexto de seguridad del proveedor para aplicar, en función del riesgo obtenido, en las fases iniciales, de manera que se pueda acordar con el proveedor una mejora de las medidas de seguridad orientada sobre todo a las siguientes áreas:

- El proveedor realiza auditorías (externas o internas) de forma periódica.
- El resultado de estas es favorable, no teniendo incumplimientos críticos.
- Cuenta con un Cuerpo Normativo de Seguridad de la Información y con un Cuerpo Normativo de Continuidad de Negocio.
- Dispone de una política y un procedimiento de gestión de riesgos.
- Dispone de una política y un procedimiento de gestión de incidentes.
- Dispone de una política y un procedimiento de gestión de vulnerabilidades.
- Existe un Responsable de Seguridad de la Información nombrado con dedicación completa.
- Realiza pruebas de recuperación de sistemas al menos una vez al año.
- Cuenta con personal entrenado y equipo de gestión de crisis.
- Tiene implementadas y probadas estrategias de continuidad.
- Incluye en las pruebas de recuperación los servicios que nos presta que han sido objeto de análisis por nuestra parte.
- Efectúa simulacros de incidentes de seguridad al menos una vez al año.
- Cuenta con ciberejercicios para concienciar a los empleados (por ejemplo, envío de *phishing* u otras acciones de ingeniería social a empleados).
- Realiza pruebas de recuperación de sistemas con periodicidad mínima anual, y está dispuesto a compartir con nuestra empresa el resultado de estas.
- Se definen en el contrato y para el servicio en cuestión, ANS de recuperación y penalización.

4.2.3.1. Supervisión de medidas y controles

Durante la fase de ejecución del servicio es importante asegurar su monitorización, con el objetivo de controlar los riesgos identificados y verificar que estos no varían. Para ello será necesario realizar reevaluaciones del riesgo periódicas, así como de los controles aplicados.

Para todo se pueden establecer indicadores y métricas que permitan medir estos controles con la periodicidad que se establezca en base a los riesgos identificados. Los indicadores y los umbrales de medición deben ser acordados con el proveedor del servicio, para que ambas partes se sientan confortables. Estos deberán, asimismo, estar ajustados al servicio específico para el que se pretende realizar la supervisión.

Otro control será el seguimiento de la ejecución de pruebas para el entrenamiento de seguridad y continuidad, siendo muy positiva la participación de la empresa cliente o contratante cuando esto se haya acordado y aceptado previamente. En caso contrario, se deberá solicitar el resultado de la ejecución de estos con la periodicidad acordada.

En esta fase, y en el caso de no haberlo realizado previamente, se podrá aprovechar para mejorar la interrelación con el proveedor, reforzando los datos de contacto y mecanismos de comunicación entre ambas partes, en el caso de afección por incidente. Es de gran utilidad, haber definido personas de contacto a distintos niveles (estratégico, táctico y operativo) tanto titulares como suplentes, o buzones de correo cuya atención sea asegurada 24x7.

Con aquellos proveedores de mayor riesgo, se podrá plantear simulacros *table-top*, o ejercicios de mesa que permitan validar los mecanismos de comunicación definidos, así como protocolos de respuesta por ambas partes, donde se asegure que el proveedor tiene contemplada a nuestra empresa dentro de sus mecanismos de notificación de incidentes.

4.3. MECANISMOS DE RESPUESTA ÁGIL A LA CONTINGENCIA EN CASO DE CIBERINCIDENTE DEL PROVEEDOR

En las secciones previas se ha expuesto qué acciones preventivas debe acometer una empresa para mitigar el riesgo de afectación de un incidente de ciberseguridad y/o seguridad de la información en un proveedor. Asimismo, se han descrito las acciones reactivas para dar respuesta al incidente en sí. Pero no menos importante es asumir que, en el momento que ocurra el incidente, la empresa sufrirá con gran probabilidad algún tipo de impacto en la continuidad de su negocio.

Dado que el objetivo principal de una empresa es asegurar el mínimo daño reputacional, operativo, financiero y legal ante un incidente, ésta deberá contar con mecanismos de respuesta ágil (también llamados planes de continuidad de negocio) definidos a priori para estos escenarios que permitan asegurar la continuidad de sus operativas y proce-

sos de negocio críticos.

Recopilando lo visto hasta ahora, podríamos decir que, una vez confirmado el incidente, la empresa debería de estar adoptando medidas a tres niveles:

- Respuesta al Incidente (Capítulo 3).
- Activación de los Planes de Gestión de Crisis (Capítulo 5).
- Activación de los planes de continuidad de negocio necesarios para garantizar la recuperación de los procesos de negocio críticos afectados.

En este bloque nos centraremos en el tercer punto, que además es uno de los incluidos en el ámbito de gestión de crisis y /o continuidad de negocio.

4.3.1. Escenarios de afectación a nuestra empresa

¿Qué afectación podemos tener, por tanto, cuando uno de nuestros proveedores sufre un incidente cíber y qué planes deberíamos de activar en cada caso?

La realidad es que podemos tener dos tipos de afectación:

1. Incidente cíber en nuestra propia empresa, por propagación del incidente sufrido por el proveedor. Alcance de afectación potencialmente global a nuestra empresa.
2. Incidente exclusivo de continuidad de negocio asociado a la disrupción del servicio prestado por parte del proveedor. Alcance de afectación a priori más acotado.

A continuación, se describen los mecanismos de respuesta específicos a contemplar en cada uno de estos dos casos, siguiendo con la descripción de pautas para su activación y seguimiento.

4.3.1.1. Caso A) Propagación del incidente ciber a nuestra empresa

En el caso de que ese incidente se haya extendido a nuestra empresa, a causa de la interacción existente con nuestro proveedor, estaríamos ante un escenario de contingencia que afecta a nuestra empresa y ello conllevaría aplicar todos los procedimientos y planes de respuesta internos que tengamos definidos para este escenario. Podemos asumir que, ante este hecho, el peor escenario podría significar una afectación "glo-

bal" a nuestra empresa (imaginemos toda nuestra red corporativa o equipos de usuario afectados) y, en consecuencia, a la mayor parte de los procesos de negocio. Por ello, la empresa debe de contar a priori con los planes de respuesta definidos para este tipo de contingencia, y en particular:

- Haber identificado cuáles son los procesos más críticos para la empresa (por ejemplo, con el apoyo del BIA) y tenerlos ordenados por prioridad en la que deberán de ser recuperados.
- Conocer los recursos mínimos necesarios para poner en marcha esos procesos (personas, equipamiento, sistemas, proveedores, etc.).
- Tener definidos los planes de contingencia alternativos para poner en marcha esos procesos, ante ausencia de los medios habituales (por ejemplo, activando protocolos manuales, contando con el apoyo de terceros que puedan asumir esas operativas temporalmente en nuestro lugar, habiendo definido ubicaciones y sistemas alternativos desde los que ejecutar esos procesos, etc.)
- Realizar simulacros y pruebas de los planes de respuesta con una periodicidad al menos anual para los procesos críticos de la empresa.

4.3.1.2. Caso B) Afectación acotada al servicio proporcionado por el proveedor

En este caso, la afectación en la empresa está directamente relacionada con el servicio que nos presta el proveedor y la criticidad asignada al mismo a través del formulario adjunto en el Anexo 1, por lo que la clave para garantizar una respuesta ágil es haber considerado este escenario de contingencia con anterioridad, trabajando en lo siguiente:

- Tener bien identificados los servicios que dicho proveedor nos presta en la empresa con su criticidad asociada y las áreas afectadas (por ejemplo: mediante el BIA y el inventario de proveedores, como se indicó en la Sección Identificación de proveedores Top Críticos en ámbito cíber).
- Disponer de una monitorización e indicadores de los servicios críticos prestados por el proveedor de cara a poder acotar los tiempos de reacción.
- Haber solicitado al proveedor afectado la definición de planes de continuidad para el escenario en cuestión, de manera que él mismo nos pueda garantizar la continuidad de sus servicios mínimos con mecanismos alternativos (explicado en el Apartado Análisis de Riesgos y Marco de Control del Proveedor)

- Haber desarrollado estrategias de continuidad ante la disrupción del servicio de ese proveedor y para los servicios que hayamos identificado de mayor criticidad (por ejemplo: haber diversificado a priori los servicios con otro proveedor que pueda asumir parte de la carga temporalmente, llevando parte del esfuerzo con recursos internos, contratar apoyo externo expertos que puedan asumir ese servicio etc., descritos como "proveedor suplente" en el apartado primero del presente capítulo).

4.3.2. Activación de los planes de contingencia definidos

En el momento de la contingencia, los Comités de Gestión de Crisis evaluarán la conveniencia de activar total o parcialmente los planes existentes o, en el caso de no estar definidos, aquellos que deben ponerse en marcha. La ventaja de haber desarrollado estos planes "en frío", es la agilidad en los tiempos de respuesta y el no pensar "en caliente" en momentos de caos, estrés y nerviosismo, lo cual conlleva a asumir mayores riesgos al aumentar la probabilidad de olvidar aspectos relevantes.

Tan importante es contar con los planes definidos como con los mecanismos de coordinación de activación de dichos planes, esto es:

- Haber definido un responsable de activarlos, que podría residir en el Comité de Crisis (la activación de planes puede conllevar autorización de recursos adicionales, movilización de personas y otros cambios relevantes, por lo que es importante que su activación sea ratificada por un Órgano Competente).

- Haber formado previamente a todo el personal y áreas involucradas, así como haber realizado simulacros para garantizar su correcto funcionamiento.

- Haber definido mecanismos de comunicación y aviso de todas las áreas afectadas, de manera que se garantice una localización temprana en caso de ser necesario (en estas situaciones nuestros medios habituales de comunicación pueden no estar disponibles; correo electrónico, teléfonos corporativos, móviles, etc.) por lo que puede ser conveniente valorar la adopción de herramientas de notificación específicas para situaciones de crisis, que sean independientes de nuestra infraestructura corporativa.

- Haber definido un responsable de hacer el seguimiento de su activación, para reportar el estado al Comité de Crisis.

- Haber trabajado de forma periódica (a ser posible anualmente) todos estos planes y contar con listados actualizados de responsables e interlocutores tanto de nuestra empresa como del proveedor.

Es importante saber que los equipos de respuesta a la contingencia no tienen por qué responder a la estructura organizativa de la empresa en situación de normalidad. Los roles y funciones son diferentes, dado que no estamos ante la operativa habitual de la empresa, sino ante una situación de "mínimos y supervivencia". Por ello, es clave que estos roles hayan sido definidos, revisados y validados con anterioridad y que las empresas cuenten con programas de formación periódica en materia de continuidad de negocio que les permitan estar preparadas para estos eventos.

4.3.3. Seguimiento de los planes de continuidad activados

Durante el tiempo que dure la contingencia se deberá realizar un seguimiento periódico de la ejecución de los planes por parte del Comité de Crisis, ya que el impacto del incidente suele variar con el tiempo y habrá que hacer una reevaluación de la criticidad de los procesos. Será el Comité quien valore la conveniencia de adoptar cualquier otra medida que se estime oportuna en base a la evolución de la situación o a la casuística específica a la que pueda estar expuesta la empresa en un momento en particular (por ejemplo: fin de mes, final de año, día de una relevancia específica, etc.).

Los planes se mantendrán activos mientras continúe declarada la situación de contingencia y crisis en la empresa y debería ser ámbito de responsabilidad de Comité de Crisis declarar la vuelta a la normalidad y desactivación de todos los planes de continuidad.

4.3.4. Vuelta a la normalidad

Una vez se declare la vuelta a la normalidad, es recomendable recopilar las lecciones aprendidas en la activación de los planes e incorporarlas a las conclusiones globales del incidente/crisis de manera que se definan los planes de acción que correspondan y se garantice la mejora continua de la empresa, con la consiguiente actualización de dichos planes.

5. GESTIÓN DE CRISIS

Con frecuencia las organizaciones deben afrontar situaciones de especial gravedad, denominadas **crisis**. En este capítulo se apuntan algunos aspectos que es conveniente sean contemplados para su gestión, haciendo foco principal en aquellos casos de origen cíber por incidente en proveedor.

Una crisis refiere a aquellas situaciones de especial gravedad que requieren una respuesta integral, coordinada y ejecutiva de alto nivel, y que pueden llegar a comprometer, no solo el funcionamiento de la empresa, sino incluso sus objetivos estratégicos, llegando en el peor escenario posible a comprometer el propio futuro de la empresa.

La gestión de una crisis cuyo origen sea un incidente de ciberseguridad, como se verá en este capítulo, no es un tema exclusivo del equipo de ciberseguridad o de seguridad de la información, sino que conlleva la implicación de toda la empresa. Por ello, este capítulo va dirigido tanto al responsable de seguridad de la información como al conjunto del equipo directivo: CEO, responsable de comunicación, responsable de operaciones, responsable jurídico, responsable comercial, responsable de atención al cliente, responsable de recursos humanos, responsable de sistemas, etc.

La resolución de la crisis, por tanto, debe gestionarse en dos planos; uno más operativo, desde el que se debe contener y resolver el incidente por el equipo de respuesta ante incidentes de la empresa, y otro más de coordinación organizativa y reputacional, en el que el equipo directivo resuelva la situación de especial gravedad y facilite el proceso de toma de decisiones. En este documento nos referiremos al gobierno de la crisis para englobar los dos planos de resolución de la crisis:

- En el plano operativo se deberá lidiar con los aspectos propios de seguridad tecnológica (identificación, contención, erradicación y vuelta a la normalidad tras el incidente).
- En el plano de coordinación, con los aspectos de obligaciones (regulatorias y contractuales con clientes y proveedores) y de continuidad del negocio.

Deben también afrontarse dos ejes de actuación adicionales a los de operación y cumplimiento que, progresivamente, han adquirido mayor relevancia debido a la gravedad de los incidentes:

- **Aspectos reputacionales:** Cuando el incidente afecte a la imagen de marca de la empresa y pueda llegar a condicionar su propia existencia.
- **Aspectos de "management":** Cuando el equipo directivo y resto de mánagers deban incrementar sus habilidades de gestión, tales como anticipación, liderazgo y creatividad, para afrontar estas situaciones de especial gravedad, donde se debe trabajar bajo presión y en situación de estrés, debiendo tomar decisiones de diversa índole.

En el contexto de esta Guía se consideran los escenarios más probables de crisis de ciberseguridad:

- Se ha propagado el ciberincidente desde el proveedor a los sistemas de información y comunicaciones de la compañía, y por tanto la empresa está afectada. En este caso, se deberá gestionar la crisis interna propia de un incidente de alto impacto en la empresa, junto con la gestión del bloqueo de los accesos del proveedor que nos ha infectado.
- Un proveedor está sufriendo un incidente y, dada su gravedad, requiere acción inmediata por parte de la empresa para reducir la probabilidad de infección. Esto significa aplicar, entre otras medidas: el bloqueo de las comunicaciones, restringir los accesos logísticos y físicos del personal del proveedor, etc. Todo ello puede afectar al correcto funcionamiento de los procesos de negocio de la empresa, dado que si estos son prestados por el proveedor se dejarían de prestar, suponiendo para la empresa una pérdida no solo económica sino reputacional.
- Un proveedor ha sufrido una fuga de información de la compañía y, dado el nivel de criticidad de esta, requiere una respuesta ejecutiva coordinada.

A lo largo de este capítulo se exponen brevemente los conceptos clave en la gestión de una crisis: las fases en las que se desarrolla una crisis; sus órganos de gobierno más habituales en compañías de mediano y gran tamaño; los tipos de stakeholders que pueden estar implicados y posiblemente afectados, y las bases de un plan de gestión de la comunicación en crisis.

Se concluye el capítulo con la enumeración de un decálogo de buenas prácticas para abordar una situación de crisis.

5.1. CUÁNDO UN INCIDENTE DE CIBERSEGURIDAD SE CONVIERTE EN CRISIS

Tal como se pudo ver en el capítulo de Plan de Respuesta a Incidentes, durante la fase de Investigación del incidente se determina la afectación e impacto de este.

El equipo de respuesta a incidentes es, en primera instancia, el responsable de evaluar la gravedad de este y, si procede, proponer la declaración de Crisis y activación de mecanismos específicos.

Es bastante habitual aplicar un sistema de evaluación de peligrosidad e impacto para llegar a determinar la gravedad del incidente. Las guías *CCN-STIC 817 del Esquema Nacional de Seguridad*, y la *Guía Nacional de Notificación y Gestión de Ciberincidentes* (Anexo 2 – Referencias), proporcionan instrucciones para determinar la peligrosidad e impacto de un incidente.

En la presente tabla se muestra el ejemplo aportado por una organización asociada a ISMS Forum, que establece una clasificación de 4 Niveles de gravedad de un incidente basados en la interpretación de los niveles de peligrosidad e impacto, siendo:

Nivel 1: Incidente poco grave, se suele gestionar por el equipo aplicando procedimientos estandarizados de respuesta.

Nivel 2: Incidente de gravedad media, requiere la intervención de un equipo especializado de respuesta para investigar, contener y erradicar la amenaza.

Nivel 3: Incidente grave, puede llegar a afectar de forma grave a procesos o reputación de la compañía y requiere involucrar a los primeros niveles de gestión de crisis de la compañía.

Nivel 4: Incidente crítico, requiere una coordinación ejecutiva de máximo nivel.

NIVEL DE IMPACTO		NIVEL DE PELIGROSIDAD				
		BAJO	MEDIO	ALTO	MUY ALTO	CRÍTICO
	Algunos Ejemplos	Spam Escaneo de Redes	Discurso de odio/ Ingeniería Social	Phishing/ Pornografía Infantil	Distribución de malware/ Sabotaje	APT
Sin impacto		Nivel 1	Nivel 1	Nivel 1	Nivel 2	Nivel 2
BAJO	Costo < 5K€ Afecta algún sistema	Nivel 1	Nivel 1	Nivel 2	Nivel 2	Nivel 2
MEDIO	Costo < 5K€-250K€ +20% de sistemas	Nivel 2	Nivel 2	Nivel 2	Nivel 2	Nivel 2
ALTO	Costo < 5K€-1M€ +50% de sistemas	Nivel 2	Nivel 2	Nivel 3	Nivel 3	Nivel 3
MUY ALTO	Costo 1M€-10M€ +75% de sistemas	Nivel 3	Nivel 3	Nivel 3	Nivel 4	Nivel 4
CRÍTICO	Costo > 10M€ +90% de sistemas	Nivel 3	Nivel 3	Nivel 3	Nivel 4	Nivel 4

Ejemplo tabla de decisión nivel de gravedad de incidente en una empresa

A título ejemplo, y con una visión de riesgo para el país, los CERTs pueden adoptar esquemas similares para determinar la gravedad del incidente.

NIVEL DE PELIGROSIDAD REAL DEL INCIDENTE

L5 - NIVEL CRÍTICO

Amenazas Persistentes Avanzadas (APT).

L4 - MUY ALTO

Distribución de malware, configuración de malware, robo, sabotaje, interrupciones.

L3 - ALTO

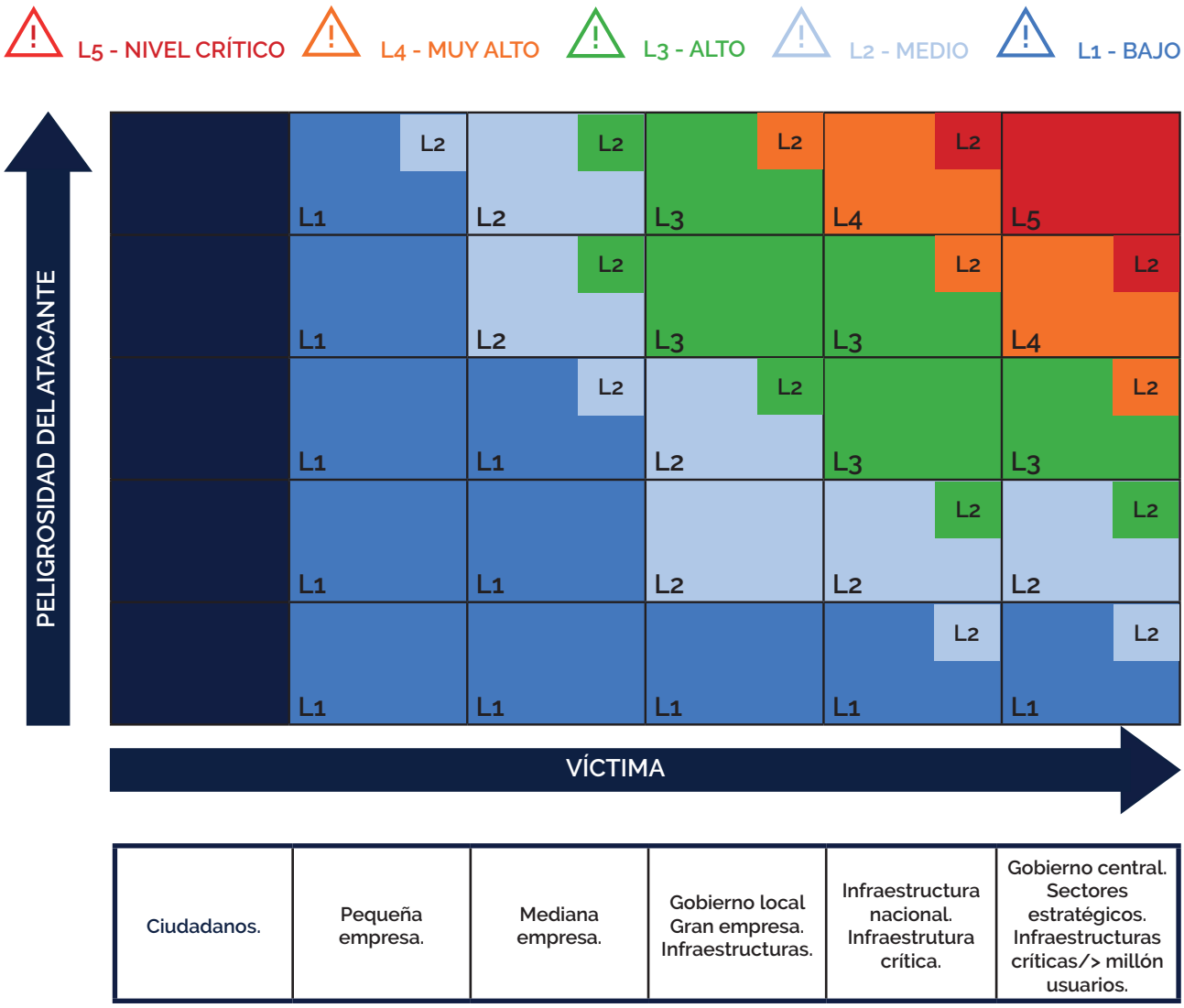
Pornografía infantil/contenido sexual o violento inadecuado, sistema infectado, servidor C&C, compromiso de aplicaciones, compromiso de cuentas con privilegios, ataque desconocido, DoS, DDoS, acceso no autorizado a información, modificación no autorizada de información, pérdida de datos, *phishing*.

L2 - MEDIO

Discurso de odio, ingeniería social, explotación de vulnerabilidades conocidas, intento de acceso con vulneración de credenciales, compromiso de cuentas sin privilegios, desconfiguración, uso no autorizado de recursos, derechos de autor, suplantación, criptografía débil, amplificador DDoS, servicios con acceso potencial no deseado, revelación de información, sistema vulnerable.

L1 - BAJO

Spam, escaneo de redes (*scanning*), análisis de paquetes (*sniffing*), otros.



Fuente: CCN-CERT

5.2. GOBIERNO DE CRISIS DE CIBERSEGURIDAD EN LA CADENA DE SUMINISTRO

5.2.1. Órganos de gestión de la crisis

Ante una situación de crisis, se precisa una respuesta coordinada y adaptativa al contexto cambiante, siendo por ello necesario que se definan correctamente los equipos de gestión de esta.

Sin entrar en la estructura de organizaciones complejas o de ámbito internacional, que requieren un diseño más específico, una buena práctica es **definir dos o tres niveles de gestión** en función de la complejidad de la empresa. Presentados en orden de menor a

mayor nivel de responsabilidad, son los siguientes:

1. ***Bronze Team:*** su responsabilidad se ciñe al ámbito operativo y sus funciones principales son:

   - Gestionar los incidentes a los que se enfrenta el negocio sin que necesariamente deriven en una situación de crisis.
   - Reportar el incidente al ámbito superior de forma inmediata cuando concurran circunstancias predefinidas.
   - Realizar el análisis y valoración de amenazas y riesgos.
   - Asegurar que se atienden las obligaciones de cumplimiento de la compañía.

2. ***Silver Team:*** su responsabilidad tiene un aspecto táctico. Este equipo complementa al anterior desempeñando las siguientes funciones:

   - Asegurar que el *Bronze Team* al frente de la emergencia cuenta con los recursos necesarios y, si no es así, asegurar su capacidad operativa.
   - En el caso de que el incidente sea tan inesperado que no haya un *Bronze Team* identificado, su misión es la de identificar qué personas son las más adecuadas para afrontarlo y constituir el equipo operativo.
   - Realizar el análisis de situación, con especial dedicación al impacto causado (servicios, imagen institucional, económico y financiero, etc.), así como:
     - Identificar su posible evolución y extensión. Es frecuente que el *Bronze Team* esté focalizado en aspectos específicos del incidente y tenga dificultad para entender la complejidad y evolución previsible del mismo desde una perspectiva de negocio.
   - Velar por el mantenimiento de la capacidad de respuesta del *Bronze Team* durante el tiempo. El incidente puede prolongarse en el tiempo y debe hacerse frente al desgaste físico y psíquico que se producen.
   - Enviar prealertas al *Golden Team* en función de la gravedad del episodio y, si es preciso, solicitar que se decrete situación de crisis.
   - Identificar los stakeholders afectados, identificar las carencias de comunicación existentes y actuar en consecuencia.
   - Definir los aspectos clave del Plan de Comunicación y validar los contenidos de los principales comunicados. En este sentido es importante que la compañía disponga de un Plan de Comunicación establecido y un responsable de comunicación y/o un equipo asignado para llevar a

cabo su aplicación.

- Reportar el desarrollo del incidente al *Golden Team* con la frecuencia y nivel de detalle que se haya definido.
- Preparar y apoyar a la toma de decisiones del *Golden Team*.
- En organizaciones extensas o complejas, es habitual que el *Silver Team* tenga un ámbito geográfico o funcional (por ejemlo: una línea de negocio específica).

3. ***Golden Team:*** aplica al máximo nivel de responsabilidad de la empresa y sus funciones principales se pueden resumir en:

   - Asumir el liderazgo de la crisis en sus casos más extremos y pilotar las medidas necesarias para la recuperación.
   - Definir aspectos clave como el posicionamiento de la empresa, dotaciones de recursos extraordinarios, etc.
   - Desplegar los contactos institucionales al mayor nivel posible.
   - Asegurarse de que se están respetando las prioridades de la empresa, haciendo foco en aspectos clave como la seguridad de las personas, el cumplimiento y los valores de esta.
   - Establecer las directrices para alinear los mensajes de comunicación pública.
   - Designar portavoces según lo establecido en el Plan de Comunicación.
   - Identificar los nuevos frentes que se abren de la crisis cuando esta evoluciona y asegurarse se dedican los recursos necesarios para hacerle frente.

Es a su vez importante determinar cómo van a interactuar los distintos equipos, es frecuente que el Jefe del equipo de respuesta a incidentes (líder del *Bronze Team*), forme parte del *Silver Team* e, incluso, llegue a estar presente en algunas reuniones del *Golden Team*.

En organizaciones de tamaño medio es habitual que se fusione el *Silver Team* con el *Golden Team*.

Dado que una situación de crisis pone a la empresa en jaque, es más conveniente plantearse la constitución de equipos de respuesta formados por expertos con capacidad de resolución, en lugar de equipos formados por aspectos de jerarquía formal existente. Con frecuencia los prejuicios culturales de la empresa pueden impedir una gestión ágil del episodio.

Asimismo, también es buena práctica designar un rol de Coordinador del Comité de Crisis, con una doble visión:

- En situación de normalidad, asegurarse que se revisan los análisis de riesgos, protocolos y se realizan las acciones de capacitación y formación necesarias.
- Ante episodios graves, constituirse en un facilitador del equipo directivo, velando por que, en la medida de lo posible, se sigan las pautas metodológicas predefinidas, con el objetivo de minimizar la toma de decisiones reactivas e improvisadas en el conjunto de la empresa, decisiones que con frecuencia suelen tener consecuencias no deseadas por falta de perspectiva.

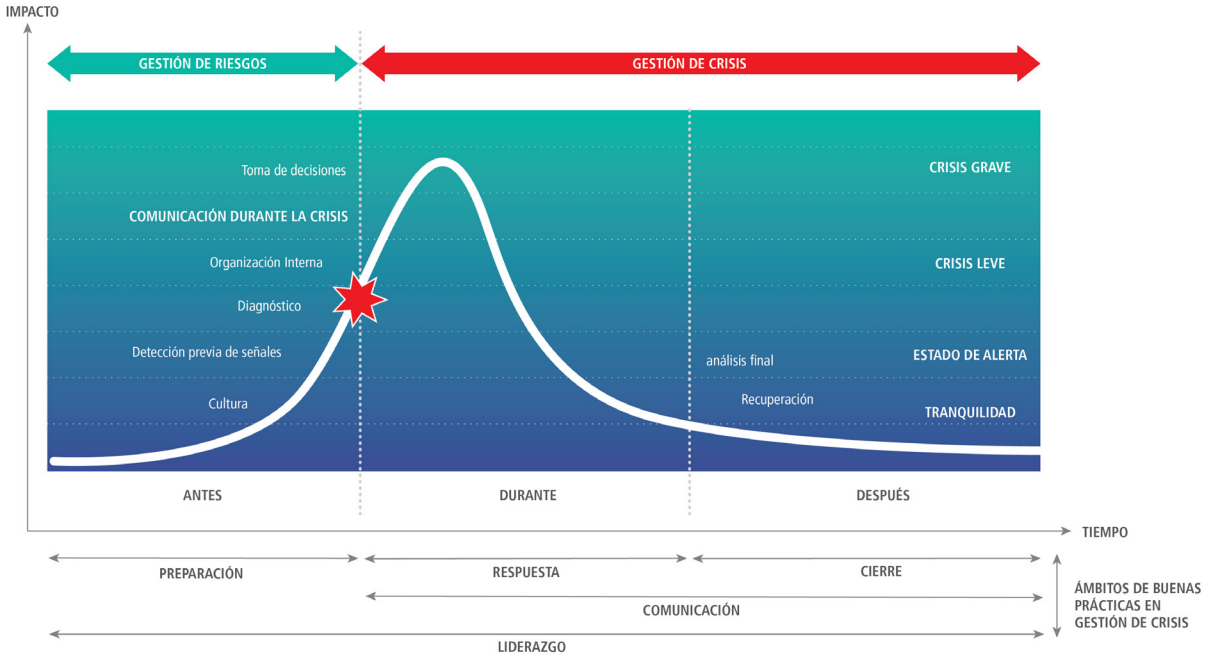
5.3. FASES DE UNA CRISIS

El ciclo de vida de las crisis puede representarse en las siguientes fases:

1. Situación previa o de normalidad.
2. Identificación y notificación del incidente.
3. Declaración de situación de crisis.
4. Gestión de la crisis.
5. Final de la crisis: vuelta a la normalidad.
6. Gestión post crisis.

El **siguiente esquema** sintetiza la secuencia del ciclo de una crisis con dos ejes, tiempo e impacto sobre la compañía, sobre el cual se destacan los ámbitos de buenas prácticas en la gestión de crisis: la preparación, la respuesta, el cierre y, de forma continua, la comunicación y el liderazgo, que se desarrollarán a lo largo de este capítulo.

Fases de una crisis y ámbitos de las buenas prácticas.



Fuente: Institut Cerdà

5.3.1.1. Situación previa: normalidad

En esta fase ha de trabajarse en tareas preventivas y de detección, por lo que es conveniente que se dediquen los esfuerzos a definir todo el material metodológico que debe guiar la gestión de un episodio.

Algunos de estos trabajos pueden ser:

- Identificar riesgos más probables, evaluar impacto potencial (*BIAs- Business Impact Analysis*) y establecer planes de respuesta asociados (estrategias de continuidad) orientados a, si es posible, eliminar, transferir o mitigar dichos riesgos. También cabe destacar la necesidad de hacer revisiones periódicas del nivel de impacto de los riesgos identificados y hacer pruebas de verificación.

- Identificar actores clave en situación de crisis, nombrar las personas responsables y sus sustitutos en caso de ausencia, incluyendo los medios necesarios para llevar a cabo las reuniones del comité (presenciales, virtuales), así como alternativas para que, en el caso de que los medios primarios no funcionen, haya otras opciones para celebrar el Comité de Crisis.

- Describir, de forma sintética, las funciones clave que estos actores deben desempeñar (roles y responsabilidades) y dar formación a titulares y susti-

tutos. Dentro de esta formación debe incluirse simulacros o *role-play* que prueben la capacitación real del Comité de Crisis.

- Identificar umbrales de gravedad de incidentes (evolución de incidente a desastre/crisis).
- Establecer canales de comunicación y gestión de la crisis, así como medidas de contingencia si estos no están disponibles.
- Definir un Plan de Comunicación en situación de crisis.
- Realizar acciones de concienciación, sensibilización y formación a todos los niveles.

Asimismo, es conveniente -una vez se haya definido todo el bloque metodológico- realizar simulacros periódicos, con el objetivo de reducir la incertidumbre en situaciones graves y llevar a cabo un proceso de mejora continua, revisando al menos anualmente toda la documentación y siempre que haya algún cambio relevante.

Es también conveniente realizar seguimiento de situaciones de crisis sobrevenidas a otras organizaciones para intentar detectar qué aspectos de gestión son aplicables en el contexto propio.

5.3.1.2. Fase 2. Identificación y notificación del incidente

En el capítulo del Plan de respuesta a incidentes ya se explica cómo tratar la identificación y detección de incidente.

Un aspecto importante en gestión de crisis estriba en saber catalogar el nivel de gravedad del incidente y saberlo escalar al nivel de responsabilidad que corresponde. Para ello es preciso tener correctamente definidos los umbrales de gravedad por tipología, así como los grupos de notificación a quienes debe reportarse.

Es más habitual de lo que parece ver los siguientes errores en los primeros estadios de crisis:

- Diagnóstico inicial incorrecto o insuficiente.
- La dificultad y soledad en la evaluación de la gravedad de un incidente.
- Adoptar una postura de "yo lo arreglo" por voluntarismo y buena voluntad, provocando que estalle por falta de aviso previo.

Si no se dispone de un esquema de clasificación de la gravedad de un incidente de ciberseguridad, se puede recurrir a la reciente *Guía Nacional de Notificación y Gestión de Ciberincidentes* elaborada por el Centro Criptológico Nacional (CCN-CERT), el Instituto Nacional de Ciberseguridad de España (INCIBE-CERT), Mando Conjunto de Ciberdefensa (MCCD) y el Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC), y aprobada por el Consejo Nacional de Ciberseguridad (Anexo 2, Referencias).

Es recomendable disponer de un sistema de *reporting* (que se habrá realizado dentro de las acciones preventivas) para informar desde las capas más operativas a la alta dirección, de cualquier incidente con cierto impacto (potencial o real), de forma que se asegure que el equipo directivo es conocedor de hechos significativos y, por tanto, puede activar medidas adicionales a las ya realizadas por la capa operativa.

Debe entenderse que la gravedad de un incidente puede variar durante el tiempo. Es por ello conveniente mantener una revisión periódica del nivel de gravedad y, si es preciso, cambiar el nivel de reporte.

5.3.1.3. Fase 3. Declaración de situación de crisis

La decisión de que un incidente deviene en un desastre que provoca una situación de crisis no debe ser una responsabilidad directa del equipo operativo, dado que requiere analizar su impacto y sus consecuencias extralimitándose de las competencias operativas.

Una buena práctica es incluir un equipo intermedio, de nivel directivo (por ejemplo, algunos miembros ad-hoc del *Silver Team*), al que se reporta el incidente y su clasificación técnica para que, desde una mayor distancia operativa y con mayor visión global, evalúe y reevalúe la gravedad del episodio y recomiende si aplica la declaración de situación de crisis.

La alta dirección de la empresa (a través del Comité de Crisis del que se haya dotado) suele ser la responsable de decretar que un incidente ha devenido en situación de crisis. En ese momento deben desencadenarse, entre otros, los siguientes bloques:

- Activación de los titulares o suplentes del grupo permanente del Comité de Crisis.
- Evaluación de si se requieren actores adicionales en función del episodio.
- Convocatoria urgente de primera reunión.
- Activación de aspectos logísticos necesarios.

- Activación del Plan de Continuidad, si procede.
- Activación del Plan de Comunicación.

Es conveniente realizar una primera reunión rápida de diagnóstico inicial para intentar comprender el alcance del episodio, así como su posible evolución. Este encuentro puede ser presencial o virtual. Se recomienda disponer de medios probados con antelación, para prever posibles fallos en la comunicación. Si se ha previsto celebrar el Comité de forma virtual y las redes de comunicaciones están afectadas, se deberá tener previsto un plan alternativo para que sus miembros puedan reunirse.

Asimismo, es recomendable que exista un *checklist* de aspectos a considerar en las reuniones del Comité de Crisis, pues estas estarán supeditadas por un contexto de urgencia e incertidumbre que requiere la supervisión de que se contemplan todos los aspectos. En este sentido, para el correcto desarrollo de esta reunión, la figura del Coordinador del Comité de Crisis cobra especial relevancia.

5.3.1.4. Fase 4. Gestión de la crisis

Una vez se haya realizado la primera reunión de diagnóstico, muy probablemente se entrará en una dinámica de reuniones frecuentes de coordinación para:

- Monitorizar la evolución de la crisis y de los frentes abiertos.
- Identificar si se abren nuevos frentes (reputacionales, operativos, legales, comerciales, etc.).
- Definir nuevas líneas de actuación de alto nivel si así se considera preciso y aprobación de estas. Es necesario recordar que puede darse el caso de requerir la adquisición de un bien o u servicio o material que implique un coste extraordinario y que deberá aprobarse previamente por el Comité.
- Informar a los stakeholders. En este punto es importante realizar una revisión de los stakeholders, de sus expectativas y de la estrategia a seguir con cada uno, especialmente si hubiese requisitos de información a cumplir en tiempo y forma.

Es una muy buena práctica tener preestablecida la frecuencia, formato y contenidos tipo de reporting de los equipos operativos. Debe comprenderse que el reclamo de información hacia los equipos operativos suele apabullar a los técnicos, colapsa su tiempo y genera distracciones no deseadas.

Por otra parte, el tener predefinido el formato, contenido y frecuencia de envío de r*eporting* que debe hacer el equipo operativo aporta confianza a las partes y reduce el estrés.

5.3.1.5. Fase 5. Final de crisis: vuelta a la normalidad

Es el Comité de Crisis quien debe decretar la finalización de dicha situación. Siendo conscientes de que, con toda probabilidad, existirán frentes abiertos que requerirán un tiempo prolongado hasta su resolución.

Se puede considerar que el episodio va bajando progresivamente de intensidad hasta que los frentes restantes solo necesitan una dedicación operativa discreta.

Cuando se decreta el final de crisis, deben necesariamente desencadenarse acciones de cierre de la misma, bien sea a nivel de comunicación, responsabilidades sobrevenidas, o de lecciones identificadas que pasarán a ser aprendidas cuando no se vuelvan a repetir.

Es conveniente una reunión inmediatamente posterior de juicio crítico. Es importante que esta reunión se haga en el plazo más breve posible. Dicha reunión debe repetirse en la fase de Gestión poscrisis para asegurarse de que se están desplegando las acciones de mejora identificadas.

5.3.1.6. Fase 6. Gestión poscrisis

Una de las oportunidades más valiosas para la organización es la generación de conocimiento a partir de las crisis sufridas. La gestión de crisis es un proceso de mejora continua y, por tanto, identificar lecciones aprendidas y puntos de mejora permitirá ganar madurez en el proceso de la gestión de crisis de una empresa. Esta actividad de extraer el conocimiento e identificar puntos de mejora, debe recaer en equipos diferentes de los equipos más técnicos involucrados en la gestión de la crisis dado que se puede caer en el error de obviar esta actividad.

Cuando se producen situaciones extremas que derivan en crisis debe entenderse que, con frecuencia, se van a producir consecuencias futuras, por lo que es preciso que el Comité de Crisis designe acciones del tipo:

- Agradecer el trabajo realizado por todos los involucrados es la resolución de la crisis a todos los niveles (operativo, táctico, estratégico).

- Comunicar las medidas adoptadas y poner en valor el trabajo, los recursos dispuestos, los logros, etc.
- Establecer estrategias para recuperar el daño reputacional, de imagen, etc.
- Priorizar los recursos humanos y técnicos necesarios para atender los frentes latentes existentes, estableciendo un plan de acción.
- Informar convenientemente a los stakeholders
- Modificar los procedimientos existentes de crisis en función de las lecciones aprendidas.
- Revisar los ANS y cláusulas de penalizaciones y términos contractuales en general que se hayan identificado necesarios.
- Comunicar con empatía y asumiendo responsabilidades cuando así sea

Es aconsejable que, transcurrido un plazo razonable (seis meses, por ejemplo), se vuelvan a evaluar las consecuencias de la crisis a nivel de impacto (económico, reputacional, etc.), para asegurarse de que se ha vuelto, o se está volviendo, a la situación precrisis. Asimismo, se deberá hacer seguimiento del plan de acción para verificar que se acometen las acciones necesarias.

Se recomienda realizar un ejercicio crítico y honesto de análisis de causas, gestión realizada y protocolos aplicados, intentando identificar puntos fuertes, para ponerlos en valor, así como carencias, errores cometidos y oportunidades de mejora que permitan a la empresa evolucionar sus protocolos para poder tener mejor respuesta ante futuras crisis.

5.3.1. Stakeholders

Por stakeholders o grupos de interés se entiende todo el ecosistema de relaciones de la empresa, y por consiguiente son específicos de cada empresa, si bien existen algunos que suelen estar en común en buena parte de las empresas:

1. Stakeholders Internos.
    - Accionistas.
    - Equipo Directivo.
    - Mandos intermedios.

- Equipo técnico y administrativo.
- Representantes de los trabajadores.

2. Stakeholders Externos.

- Autoridades reguladoras.
- Administración .
- Fuerzas y Cuerpos de Seguridad.
- Clientes.
- Proveedores.
- Competencia.
- Grupos sectoriales.
- Asociaciones relacionadas.
- Medios de comunicación.

Como se ha visto, los stakeholders o grupos de interés están presentes a lo largo de las fases de gestión de crisis, pero la capacidad de establecer relaciones sólidas y de confianza con cada uno de los stakeholders va a condicionar la evolución y resultado de la situación sobrevenida.

No solo es preciso disponer de protocolos de relación claros con los stakeholders, unos por contratos o por acuerdos específicos, sino también es importante que los mánagers de las distintas áreas de la empresa tengan bien identificados quiénes son y qué relaciones cruzadas existen con ellos.

Todas las partes deben hacer esfuerzos en entender cuál es el umbral mínimo de responsabilidad que le corresponde a cada uno y comprometerse a asumirla y, en caso de incidente grave en que las responsabilidades propias no se puedan garantizar, disponer de canales ágiles y claros de interlocución para pilotar la vuelta a la normalidad.

En este sentido, todo el trabajo de gestión viene claramente influenciado por los nuevos factores de riesgo de un escenario altamente digitalizado en el que cada uno de esos stakeholders se ha convertido en un medio de comunicación en potencia. Por lo tanto, es preciso identificar la capacidad de influencia y de generación de informaciones falsas que poseen.

Asimismo, será esencial definir la estrategia, conscientes de la influencia de nuevos fac-

tores de vulnerabilidad como: el real time de la crisis, la hiperconectividad, la hipertransparencia y, la velocidad de transmisión de la información a escala global.

Estos factores de vulnerabilidad favorecen nuevas tendencias de riesgo como el activismo digital organizado, los ciberriesgos, el descrédito de los medios de comunicación y la desinformación.

A la hora de gestionar una crisis lo primero que deberíamos es ser capaces de determinar a qué tipo de crisis nos enfrentamos. El director de la crisis debe poder determinar en qué rol se encuentra la compañía en función de la atribución de responsabilidad que está recibiendo por parte de los grupos de interés. Por lo tanto, es esencial ser capaces de determinar el rol que se ocupa en la percepción de los stakeholders.

De esta manera tendríamos tres posibles papeles:

1. **Papel de víctima:** La compañía no ha causado la crisis y se ve cómo una víctima más de la misma.
2. **Responsable de un incidente:** La compañía causa el incidente, pero no de forma deliberada. Su responsabilidad es mucho más reducida.
3. **Responsabilidad deliberada:** La mala gestión de la compañía causa la crisis por lo que se considera que ha sido deliberada.

A su vez, y una vez determinado el rol de la compañía respecto al incidente que provocó la crisis, estableceremos una tipología sencilla de stakeholders, para determinar las acciones a realizar durante la gestión de la crisis.

Por tipo de relación:

1. **Poder:** Cuando la compañía posee poder sobre el grupo de interés, o es el stakeholder quien posee poder sobre la compañía.
2. **Dependencia:** Determinando cuál es el grado de dependencia que se tiene entre ambas partes.
3. **Reciprocidad:** Qué reciprocidad existe en la relación entre ambas partes.

Por capacidad de influencia:

1. **Grado de conectividad:** Determinar la estructura de la red, el tipo de red,

cómo se relaciona con otras, la jerarquía de los núcleos y el grado de interconexión del stakeholder, en su calidad de nodo (incluso de portero de la información). Debemos medir su notabilidad (autoridad sobre la conversación) y notoriedad (número de conexiones y transitabilidad).

2. **Grado de viralización:** La capacidad que tiene la información que se traslade de difundirse y alcanzar a un elevado número de organizaciones y personas.

3. **Capacidad de generación de información falsa. Fake Capacity:** Determinar la capacidad que tiene el stakeholder de elaborar y distribuir información manipulada o falsa.

Por generación de daños:

1. **Capacidad de generación de daño reputacional:** Hasta qué punto el stakeholder es capaz de perjudicar a la reputación de la compañía.

2. **Capacidad de generar daños económicos/financieros:** Determinar si el stakeholder podría generar daños económicos o financieros en la compañía.

3. **Capacidad de reclamación legal o contractual:** ¿Puede el stakeholder realizar alguna reclamación legal o contractual sobre la compañía?

4. **Capacidad de reclamación moral:** Además de poder reclamar legal o contractualmente, ¿podría realizar una reclamación moral?

5. **Capacidad de influir en el comportamiento presente o futuro de la empresa:** Las acciones del stakeholder, ¿pueden llegar a producir un cambio en el comportamiento presente o futuro de la compañía?,¿podría cambiar su política empresarial, sus planes de negocio, su código de conducta o sus procesos?

5.3.2. Identificación de interlocutores claros

Parece una obviedad, pero cuando se afronta el ejercicio de identificar todos los stakeholders relevantes para la empresa en situación de crisis, suelen detectarse algunas lagunas de conocimiento.

Es conveniente que, "en tiempo de paz", se realice el ejercicio de:

- Identificar las personas clave que serán interlocutores frente a incidentes graves, siendo recomendable diferenciarlos entre interlocutores de nivel operativo y de nivel estratégico, siendo los primeros los cubiertos por los protocolos de respuesta a incidentes o de continuidad de negocio y los se-

gundos aquellos precisos para encarrilar la resolución de situaciones inesperadas de singular gravedad.

- Contactar con cada uno de ellos para presentarles el modelo de gestión de crisis de la propia empresa, hay que asegurar que entienden y comparten el propósito evaluando cómo encaja con sus expectativas y, si es preciso, realizando las adaptaciones adecuadas para conseguir una coordinación óptima.

5.3.3. Caso especial: los profesionales de ciberseguridad

Cabe destacar que los profesionales que se dedican a la ciberseguridad son muy conscientes de que una amenaza en un proveedor o cliente puede afectar a la empresa propia en muy corto plazo.

Para ello existen canales de colaboración formales (típicamente CERTs y SOCs) así como otros informales, donde se comparten IoCs e información valiosa de respuesta a incidentes.

Incluso en aquellos casos en los que la crisis no esté directamente relacionada con incidentes de ciberseguridad, se recomienda que la organización se apoye en este tipo de grupos de forma que le permita identificar campañas de ciberataques que puedan estar beneficiándose del estado de gestión de crisis de la organización.

Es importante que los responsables de ciberseguridad de las organizaciones conozcan su existencia y establezcan contactos con ellos. A organizaciones pequeñas o medianas que no pueden disponer de SOC, les es de mucha utilidad disponer de medios de notificación de alerta temprana que les permitan disponer de la necesaria anticipación para reducir determinados impactos.

Si en el momento de la lectura de este documento usted no conoce estos canales de colaboración, ISMS Forum puede suponer una buena puerta de entrada para conseguirlo.

5.4 GESTIÓN DE LA COMUNICACIÓN

La gestión de la comunicación en una situación de crisis requiere hoy, igual que con los otros ámbitos, de una **planificación** y de una aplicación férrea del Plan de Comunicación que se haya definido previamente, dado que el ruido interno y externo que se produce en estas situaciones pone en riesgo el éxito de esa gestión y puede situar la empresa a remolque de la situación.

En el contexto cíber, cuando la crisis se produce, las primeras informaciones suelen salir de los propios trabajadores de la empresa o de trabajadores externos que se comunican con otros compañeros que están desempeñando sus funciones en otra empresa. Este último caso, curiosamente han provocado que las empresas clientes de un proveedor afectado, hayan tenido noticia del incidente de una forma fiable y anticipada a la comunicación formal del proveedor.

En el momento actual, cualquier situación de crisis es **retransmitida en directo** por las redes sociales, que a su vez actúan como fuente de información para los medios de comunicación, los cuales se hacen eco de las mismas. Ese circuito es aprovechado por **múltiples interlocutores que ejercen de portavoces** o bien de presuntos expertos, dimensionando aún más la situación de crisis, "si no dices lo que haces, otros dirán lo que no haces".

Ante esa situación, la única opción de sobrevivir y de ejercer un determinado liderazgo es la **proactividad**, en el sentido de tomar las riendas del incidente, estableciendo un ritmo propio que no suponga quedar a merced del ruido interno o externo.

Para ello se requieren algunas condiciones esenciales: la primera es **disponer de un plan o protocolo previo de comunicación de crisis** que determine los circuitos de información, los argumentarios necesarios, esenciales y recurrentes, los canales, los portavoces, todos los interlocutores involucrados y las acciones a desarrollar.

El tiempo de respuesta en las crisis actuales es cero y por ello es necesario **contar con los liderazgos y con la capacidad de decisión adecuada** para tomar las riendas de la situación. Tal como se ha mencionado anteriormente, la empresa deberá decidir quién, a nivel comunicativo, es el responsable de gestionar la situación en todas su dimensión interna y externa.

En este sentido, la comunicación interna es tan importante como la externa y la comunicación empieza por atender las necesidades de información de los propios colaboradores, los cuales, en una sociedad donde imperan las redes sociales, pueden ejercer de canales de comunicación.

En este sentido, se recomienda actuar con celeridad y elaborar la información a transmitir internamente a todos los trabajadores, no solo en relación con lo que deben hacer técnicamente, sino también aportando esa información que les ayude a hacer frente a preguntas de sus círculos familiares y de amistad.

Al igual que en la gestión técnica del incidente y que la gestión de la crisis, la gestión de la comunicación es un proceso que debe empezar mucho antes de la misma y debe finalizar mucho después. Así pues, a continuación, se destacan las tareas a realizar en el ámbito de la comunicación en cada una de las fases expuestas en el apartado anterior.

5.4.1. Acciones en la fase previa (Fase 1)

En la fase previa se ha de haber elaborado el **Plan de Comunicación de Crisis**, que comprende lo siguiente:

1. Identificación de riesgos.
2. Determinación de los niveles de esos riesgos (incidente/emergencia/crisis).
3. Definición de argumentarios y mensajes internos y externos asociados a esos riesgos que serán adaptados al incidente, pero que tenerlos previamente escritos facilita la toma de decisiones y evita olvidar puntos básicos.
4. Identificación de canales de comunicación vinculados a cada riesgo.
5. Descripción de circuitos de comunicación para cada una de las fases de la crisis.
6. Identificación de todos los interlocutores externos e internos vinculados a esos riesgos.
7. Identificación de portavoces, las personas de la empresa que en este tipo de incidente pueden asumir el rol portavoz, sea por su posición dentro de la empresa, su experiencia y conocimiento o por sus propias habilidades, las cuales pueden reforzarse mediante una buena preparación y formación ad-hoc.
8. Definición de las acciones de comunicación preventivas y las asociadas a cada riesgo.

   Plan editorial de contenidos para cada canal de comunicación.
9. Definición de procesos de capacitación en comunicación de portavoces e interlocutores internos.

En este sentido, el Plan de Comunicación de crisis ha de ir acompañado de un plan de acción, esto es, un plan de implementación en el cual se especifiquen las acciones de comunicación previas que han de asegurar que, cuando llegue el momento de activar el Plan, este se conoce y se disponen de todos los mecanismos necesarios (infraestructuras, gestión de interlocutores, creación de canales de comunicación…)

5.4.2. Acciones previstas durante la crisis (Fases 2, 3, 4 y 5)

Desde el momento en que se detecta el incidente y este deriva en la declaración del

estado de crisis, desde el punto de vista de Gestión de la Comunicación es importante recordar los siguientes puntos:

1. Recopilar toda la información y analizar la situación en base a ésta.
2. Identificar todos los interlocutores vinculados.
3. Actualizar y generar los argumentarios y mensajes.
4. Editar contenidos multiplataforma para todos los mensajes.
5. Gestionar, atender y seguir los medios y canales de comunicación.
6. Definir un cronograma y agenda propia con las acciones de comunicación para ser presentado al Comité de crisis.
7. Identificar posibles nuevos interlocutores.
8. Contar con una política proactiva de comunicación y aplicación de acciones.

5.4.3. Acciones previstas tras la crisis (Fase 6)

Tal como se ha visto en el proceso de gestión de la crisis, el **cierre correcto del incidente y la valoración posterior** por parte de las personas que han participado, son fundamentales para prevenir futuras crisis (que no incidentes) y, si no pueden evitarse, gestionarlas habiendo interiorizado las **lecciones aprendidas** de cada la experiencia.

En esta fase cabe tener presente la conveniencia de realizar las siguientes acciones:

1. Análisis posterior de la situación.
2. Actualización de interlocutores.
3. Actualización de mensajes y contenidos.
4. Recuperar la situación mediante comunicación proactiva y mensajes sobre mejoras y decisiones post.
5. Reforzar relaciones con los medios.
6. Actualizar portavoces.
7. Actualizar Plan de Comunicación.
8. Extraer y difundir las lecciones aprendidas.

5.5 DECÁLOGO DE BUENAS PRÁCTICAS EN LA GESTIÓN DE CRISIS

A modo de síntesis de este capítulo, se presenta un decálogo de 12 buenas prácticas en gestión de crisis[3] las cuales son fruto del trabajo de análisis de muchas crisis relevantes de diferentes índole, origen e impacto de estos últimos años:

LIDERAZGO

BP 1 Liderazgo, valores y control.

PREPARACIÓN

BP 2 Planes y protocolos estructurados, coherentes y con responsables claros.

BP 3 Ejercicio periódico de planes y comités.

BP 4 Gestión adecuada de los grupos de interés.

RESPUESTA

BP 5 Diagnóstico inicial y escenarios posibles.

BP 6 Coordinación.

BP 7 Iniciativa y proactividad.

COMUNICACIÓN

BP 8 Discurso unificado y fuente oficial de información.

BP 9 Transparencia, empatía y asunción de responsabilidades.

BP 10 Puesta en valor de las acciones adoptadas y recursos utilizados.

CIERRE

BP 11 Cierre formal de la crisis y comunicación de la gestión.

BP 12 Implementación de lecciones aprendidas.

Fuente: Institut Cerdà

[3] Referencia: *Buenas prácticas en gestión de crisis*, © Institut Cerdà, diciembre 2018, ISBN 9788409104307

BP 1 Liderazgo, valores y control

Es importante liderar, tomar y mantener la iniciativa durante la crisis y, si ésta se pierde, buscar las oportunidades que permitan recuperarla.

Las compañías que se rigen por unos valores superan en confianza, credibilidad y capacidad de empatía a las que no lo hacen. Las organizaciones que tienen claro cuáles son sus valores antes del inicio de una crisis son las que mejor se manejan, ya que cuando todo parece derrumbarse a su alrededor, tienen principios a los que recurrir. Hoy, más que nunca, ética y comunicación van de la mano en la gestión de las organizaciones, y modelan la configuración de la reputación de la empresa.

BP 2 Planes y protocolos estructurados, coherentes y con responsables claros

Las crisis se preparan en tiempos de normalidad, todo lo que no se prevea entonces es prácticamente imposible improvisarlo durante la emergencia.

Un error relativamente común en los responsables de las compañías en un pasado no tan lejano era confiar en que, dado que su equipo directivo era muy bueno, ya sabría qué hacer en caso de una situación disruptiva. Afortunadamente, esta actitud ha ido cambiando y hay cada vez más organizaciones que dedican esfuerzos y recursos a dotarse de herramientas de gestión. En ocasiones se dispone de continuidad de negocio, de un Plan de Crisis, que actúan como Plan Maestro del cual derivan el resto de los planes específicos en base a los que la empresa activa su respuesta y se prepara para hacer frente a la situación.

Asociada a cada uno de los planes, es de vital importancia que haya una asignación clara de responsables

BP 3 Ejercicio periódico de planes y comités

Un elemento clave es el poner constantemente a prueba los manuales, planes y procedimientos diseñados mediante simulacros, ejercicios, sensibilización y formación de distintos tipos. Es precisamente en los simulacros donde afloran aspectos que sobre el papel parecían resueltos, pero que en el momento de aplicarlos se observa que presentan carencias que es necesario abordar para asegurar su efectividad.
Como paso previo a los simulacros es necesario llevar a cabo la necesaria difusión/formación de los planes desarrollados: que todos los implicados los conozcan para des-

pués aplicarlos correctamente en el ejercicio de simulación. De hecho, además de dicha difusión, es aconsejable que las personas afectadas estén involucradas en el proceso de definición de los procedimientos, de este modo se evita el rechazo habitual de aquello hecho "por quien no conoce los procesos".

BP 4 Gestión adecuada de los grupos de interés

Durante una crisis es seguro que habrá interacción con algunos stakeholders de la compañía. En ciertos casos será en positivo, pero en otros pueden tener una influencia negativa sobre el desarrollo de la emergencia y su impacto reputacional. La gestión de los stakeholders no solo requiere su correcta identificación, sino que impone el establecimiento de una relación profesional colaborativa; por lo tanto, es necesario conocerlos personalmente, visitarlos periódicamente, compartir con ellos los planes y preparativos para afrontar la crisis, y establecer, si cabe, proyectos colaborativos comunes.

Esta ha de ser una actividad continua, ya que los representantes de los distintos grupos de interés (y los de las organizaciones) van cambiando con el tiempo como lo hace el entorno social y competitivo y es, por lo tanto, necesario mantener y renovar las relaciones de colaboración.

BP 5 Diagnóstico inicial y escenarios posibles

El primer paso en la gestión y posterior resolución de una crisis es llevar a cabo un diagnóstico acertado de lo que está sucediendo. En el análisis de crisis reales, muy a menudo se observa que por no disponer de un diagnóstico correcto (o no disponer de diagnóstico de ningún tipo), la empresa muestra un comportamiento errático durante la emergencia, pierde la iniciativa, va a remolque de los acontecimientos y sufre una clara pérdida de reputación.

A pesar de que, en los primeros momentos de la crisis, la información es a menudo confusa e incompleta, es muy importante entender lo que está pasando y sus posibles afectaciones a corto y medio plazo (posibles escenarios). Este ejercicio permite priorizar actuaciones y tomar las primeras decisiones; a medida que se disponga de más información se irá afinando el proceso. Ante la presión por reaccionar en esos primeros momentos, es mejor indicar que la compañía está analizando la situación para disponer de un buen diagnóstico que permita actuar correctamente y que, por lo tanto, es necesario esperar un poco, que hacer declaraciones voluntaristas o vacías en sentidos que en ese momento son todavía desconocidos y que pueden volverse en contra más adelante.

BP 6 Coordinación

La coordinación es la clave de la buena resolución de una crisis. Incluso empresas que se han preparado adecuadamente para abordar una situación grave de este tipo tienen tendencia a improvisar ante los acontecimientos. La improvisación y la falta de coordinación son ingredientes de una receta segura para el fracaso.

A pesar de que formalmente en ocasiones se perciba como una rémora, el establecimiento de un Comité de Crisis entrenado es una garantía de buena gestión. Por esta razón, el disponer de un gabinete de crisis con experiencia y capacidad de gestión es uno de los primeros y más importantes pasos a seguir durante una crisis.

BP 7 Iniciativa y proactividad

En muchos casos el acontecimiento que desencadena la emergencia encuentra a la compañía con falta de tensión para cambiar su prioridad desde el día a día y hacia la crisis, no realiza un diagnóstico adecuado y pierde un tiempo inicial que, como consecuencia, hace que en adelante vaya a remolque de los acontecimientos. Esto supone la adopción de una política esencialmente reactiva, más enfocada a dar respuesta a las críticas o presiones que se reciben del entorno que a definir y, sobre todo, comunicar la estrategia a adoptar para solucionar la situación.

Por ello es importante que, ante un primer aviso de crisis, la empresa reaccione con rapidez y contundencia, de este modo su versión tiene como mínimo la misma potencia que las que puedan proceder del entorno; de hecho, cuando el posicionamiento de la empresa ante una crisis es robusto, las reacciones de grupos de interés -reales o espurios- y medios de comunicación son menores.

BP 8 Discurso unificado y fuente oficial de información

Lo mejor que puede pasar en caso de estallar una crisis es que la principal fuente de información sea la propia empresa. Para que esto ocurra es imprescindible que –como se ha comentado en el punto anterior- la compañía sea proactiva y lleve la iniciativa, pero además es muy importante que sus distintas posibles fuentes de información estén perfectamente alineadas y transmitan el mismo mensaje sin incurrir en contradicciones.

En casos de crisis es recomendable disponer de un único portavoz que ejerza el liderazgo comunicativo. No obstante, en algunos casos existen distintos frentes de actuación

(operativo, comunicación, stakeholders) y es inevitable que diversas personas deban informar a agentes también distintos. La elección de la figura del portavoz es relevante. Se trata de la persona que aparecerá en los medios para trasmitir los comunicados oficiales de la compañía y ser la cara de la empresa ante la opinión pública.

BP 9 Transparencia, empatía y asunción de responsabilidades

La mentira, la narración sesgada de los hechos, el mutismo o la pasividad son las peores opciones comunicativas cuando ocurre un incidente, ya que, para proteger la reputación de la compañía, debe evitarse la incertidumbre y estar permanentemente presente, incluso cuando no haya mucho que explicar o ello signifique reconocer errores.

Mantener la transparencia durante una crisis no es fácil, pero el daño se puede compensar o minimizar mediante la adopción de una política abierta y responsable que, aunque a corto plazo pueda levantar críticas, a largo plazo produzca una mejora de la credibilidad, la percepción general y, en suma, la reputación de la compañía. Como se ha comentado anteriormente, también el modo de gestionar una crisis se asienta en los valores de la compañía. Desde este punto de vista, el asumir responsabilidades cuando las haya es una muestra de que dichos valores existen y se respetan. Más allá de ello, en general, no asumir las responsabilidades se vuelve en contra de la empresa cuando se hace patente que negándolas pretendía eludir las consecuencias de sus actuaciones.

.

BP 10 Puesta en valor de las acciones adoptadas y recursos utilizados

Las crisis tienen muchos momentos en los que, a pesar del trabajo intenso y de las muchas actuaciones simultáneas que se están llevando a cabo, todavía no hay resultados que se puedan presentar a la opinión pública y grupos de interés. En un contexto como el descrito más arriba de proactividad y transparencia por parte de la compañía en el que haya comparecencia del portavoz o comunicados periódicos, este es un buen momento para poner en valor las medidas tomadas por la empresa, tanto las preventivas (desarrollo de planes, inversión en recursos) como las correctivas (personas en campo, brigadas, ejecución de contratos, etc.).

Cualquier crisis representa una oportunidad para demostrar a la opinión pública la capacidad de la empresa para solventar una situación compleja, demostrando que la gestión de la adversidad ha sido la adecuada.

BP 11 Cierre formal de la crisis y comunicación de la gestión

En ocasiones se cree que la crisis ha pasado cuando ya no se habla de ella en los medios de comunicación, pero eso no es más que un indicador circunstancial que no refleja las relaciones causa-efecto de lo realmente ocurrido.

En este contexto, comunicar que se han llevado a cabo los análisis pertinentes, levantado las conclusiones que se derivan e incluido sus implicaciones en la organización del equipo de crisis, los planes concretos de mejora a desarrollar y que, por lo tanto, se da por formalmente cerrado el episodio, es una buena manera de transmitir, tanto a los stakeholders como a la opinión pública en general, el mensaje de que se aprendió de lo sucedido y que la compañía está mejor preparada para al futuro. Esta comunicación no solo es pertinente de cara al exterior, sino que tiene todo el sentido hacerla en paralelo en clave interna ya que se manda el mensaje de la importancia de estar preparados ante situaciones de este tipo lo cual potencia el estado de alerta de los miembros de la empresa.

BP 12 Implementación de lecciones aprendidas

Un gran porcentaje de empresas sufren con frecuencia crisis o contingencias serias a lo largo de su vida (son prácticamente inevitables) y no todas aprovechan esta circunstancia para corregir errores, extraer conclusiones positivas de lo sucedido y salir reforzadas antes de padecer otro percance. En realidad, toda crisis supone un escalón más en el largo camino hacia la resiliencia, es la gran oportunidad para aprender y no se debe dejar escapar. En muchas ocasiones el día a día hace difícil un análisis detallado y la adopción de las medidas más urgentes y necesarias puede hacer pensar que ya se sacaron conclusiones de lo sucedido y se actuó en consecuencia.

Hay que tratar las crisis como un yacimiento de oro organizacional, obteniendo conclusiones de lo sucedido mediante análisis en profundidad y ajuste a dichos aprendizajes de los planes de acción y de inversión futuros.

6. Ciberseguros

Los ciberseguros son una herramienta adicional, como otro cualquier tipo de producto de aseguramiento dentro del ciclo de vida de la gestión de riesgos. El uso de este tipo de productos debe estar dentro de un marco global de la gestión de riesgos, con objeto a alinear las coberturas y tipos de seguros con dicha estrategia global de gestión de riesgos. La organización puede ya disponer de mecanismos de aseguramiento frente a algunos escenarios mediante las pólizas de Responsabilidad Civil y/o de Interrupción de negocio (que son las que más solapamiento tienen con las de ciberseguro). Los elementos fundamentales sobre los que pivotan las pólizas de los ciberseguros son los siguientes (de manera simplificada):

- **Coberturas:** escenarios que caso de materializarse provocan un daño a la organización que puede erosionar su patrimonio. Estos distintos escenarios son los que activan las distintas protecciones de la póliza.
- **Sublímite:** el máximo capital por el que va a responder la aseguradora para un evento particular dentro de una cobertura. Se especifica un sublímite para cada una de las coberturas.
- **Deducibles:** coloquialmente llamada franquicia, es un límite inferior de capital por el que la aseguradora no responderá de la indemnización. Una vez rebasada dicha cantidad la aseguradora se deberá hacer cargo hasta el sublímite de la cobertura.
- **Límite agregado:** el capital total máximo por el que responderá la aseguradora sumando todas las activaciones de la póliza. Una vez superado dicho límite deberá ser la propia organización la que deberá responder con sus recursos propios.
- **Exclusiones:** condiciones que la organización debe cumplir para la activación adecuada de la póliza, o también se refiere a los escenarios que no estarán cubiertos por la aseguradora.

6.1. FRANQUICIA O DEDUCIBLE

La *Franquicia o Deducible* son conceptos similares que buscan un fin común y es que el asegurado asuma un valor debido a los costos de sus perjuicios asegurados hasta un monto o porcentaje.

Hay que tener en cuenta que los ciberseguros cubren principalmente el "lucro cesante" y los gastos fijos, las multas o sanciones (siempre que sean asegurables) en las que puedan incurrirse a causa de un incidente y los costes de primera respuesta, investigación e incluso comunicación y defensa. En ocasiones, estos gastos son substanciales y el ciberseguro debe estar orientado a cubrir los casos de suficiente envergadura como para activar el ciberseguro y las medidas de control cubiertas. Con esto en mente, se debe considerar que el tipo de franquicia a elegir y las coberturas a las que aplica son un aspecto fundamental de la póliza, donde, por ejemplo, elegir un seguro con una franquicia alta estaría orientado a activar el ciberseguro únicamente en circunstancias excepcionales.

6.2. TERCEROS

Es necesario analizar qué coberturas incluye la póliza sobre los terceros relacionados con la empresa, fundamentalmente con los proveedores y con los clientes.

Dependiendo de cuantos proveedores se tenga, de qué servicios proporcionen y de cuál sea su dependencia y criticidad, se debería considerar un Ciberseguro que cubra "el daño sufrido en los sistemas a raíz de un tercero". Las aseguradoras diferencian entre distintos tipos de proveedores: proveedores de servicios externos, proveedores de servicios cloud con sus distintas modalidades IaaS, PaaS y SaaS, así como el tipo de coberturas para los distintos proveedores, por ejemplo, fallo de sus sistemas, fallo de seguridad del proveedor…

A la hora de evaluar la prima de riesgo la aseguradora evaluará la política interna de gestión de proveedores, si se les audita y clasifica según el riesgo, cada cuanto tiempo y qué análisis/auditorías se les hace y cuantos proveedores se tienen y según qué criterio o metodología (ISAE 3402, PCI-DSS…) el importe del seguro es mayor o menor.

Al contratar una póliza que cubra el daño sufrido a raíz de un proveedor con o sin conexión a la empresa asegurada se debe evaluar si debe contener los siguientes servicios:

- Primera respuesta al proveedor.
- Servicios legales.
- Recuperación de los datos del proveedor.
- Pérdida de beneficio por interrupción en las redes del proveedor.
- Gastos para mitigar la interrupción en las redes del proveedor.
- Servicios de terceros en la Nube.

En cuanto a las coberturas que hacen referencia a los clientes, pueden incluir aspectos como:

- Gastos de notificación a los clientes.
- Coberturas de Responsabilidad Civil, suelen estar recogidas en pólizas específicas, si bien es posible incluirlas en pólizas de ciberseguros.

6.3. COBERTURA DE GASTOS POR IMPACTO REPUTACIONAL Y DE GESTIÓN Y COMUNICACIÓN DE CRISIS

Adicionalmente es buena práctica tener un equipo en reserva que pueda analizar y gestionar el daño reputacional o de "marca" que pueda causar un incidente, siendo por lo tanto necesario analizar si se puede dar este servicio de forma interna o si debe estar incluido en la póliza del ciberseguro incluyendo los gastos de gestión y comunicación de crisis. Normativas como el RGPD y otras normativas sectoriales indican que hay que comunicar los incidentes de seguridad en un plazo determinado (en cuestión de horas), tanto a los reguladores como a los clientes afectados. De manera que una buena gestión de la comunicación en las primeras horas del incidente es algo fundamental para las empresas.

6.4. OTRAS COBERTURAS

Adicionalmente la empresa contratante debe considerar, dependiendo de su actividad cuales de las siguientes coberturas le aplicarían:

- Gastos de defensa por multas y sanciones de organismos reguladores (RGPD, PCI, etc.):
  - Cobertura por multas y sanciones de cumplimiento normativo de tarje-

tas PCI (Payment Card Industry).

- Cobertura en asesoría de PCI.
- Protección frente a reclamaciones de terceros por incumplimiento en casos de custodia de datos, difamación en medios corporativos o infección por malware.
- Paralización de la actividad comercial como consecuencia de un expediente del regulador u otro organismo de la administración.
- Defensa jurídica y asistencia a juicio.
- Gastos de remisión de tarjetas de crédito y débito.
- Responsabilidad por pérdida de datos de carácter personal o riesgos de privacidad.
- Defensa regulatoria, multas y penalizaciones.
- Gastos por perjuicios y de defensa por uso ilegitimo de datos personales o de uso ilícito de información de la compañía.
- Exposición de datos en la Nube.
- Volumen de datos expuestos en la Nube.
- Adecuación personalizada al RGPD.

- Cobertura por fallo en servicios Cloud.
- Fallo de sistemas.
- Transmisión de virus o malware a terceros.
- Impactos derivados de una brecha de seguridad en terceros, con los que la empresa disponga de una relación contractual.
- Pérdida de beneficio por interrupción en redes.
- Gastos para mitigar la interrupción en redes.
- Cobertura de pérdidas de ingresos netos como resultado de una vulneración de seguridad o de un ataque de denegación de servicio.
- Cobertura por Ciberguerra o Ciberterrorismo.
- Gastos para recuperar datos eliminados o cifrados.

- Gastos de defensa ante reclamaciones por fallos de seguridad.
- Gastos por errores tecnológicos y omisiones.
- Cobertura por delito cibernético.
- Extorsión cibernética.
- Fraude de ingeniería social.
- Robo electrónico, Fraude informático y/o de telecomunicaciones.

6.5. RESPUESTA ANTE INCIDENTES EN EL ASEGURADO

- Tiempo de soporte, traslado de personal cualificado a instalaciones de la Empresa.
- Gastos para Mitigar la Interrupción en las Redes.
- Asistencia técnica y gastos de investigación forense del siniestro.
- Gastos de gestión y comunicación de crisis.
- Impactos derivados de una brecha de seguridad en terceros, con los que la empresa disponga de una relación contractual.
- Gastos de un posible análisis forense en caso de que sea necesario (fugas de datos, piratería, ...).
- Asistencia técnica frente a una intrusión de terceros en los sistemas informáticos del asegurado.
- Medidas de prevención como análisis externo e interno de las redes informáticas del cliente.
- Recuperación de los datos del proveedor.

6.6. RESPUESTA ANTE INCIDENTES EN TERCEROS DEL ASEGURADO:

- Primera respuesta al proveedor.
- Servicios legales.
- Recuperación de los datos del proveedor.
- Pérdida de beneficio por interrupción en las redes del proveedor.
- Gastos para mitigar la interrupción en las redes del proveedor.

7. CUMPLIMIENTO

7.1. RESPONSABILIDAD PENAL

7.1.1. Responsabilidad del atacante

El atacante/es podrían incurrir en responsabilidad en la medida en la que hayan podido cometer alguno de los delitos de los recogidos en el Código Penal. La determinacion y/o depuración de dicha responsabilidad no está exenta de problemas: averiguar la identidad del autor o autores, determinar qué organismo o estado es compente para juzgarlo o, incluso, qué ley resultaría aplicable al supuesto o caso concreto.

A estos efectos, resultará crucial la comunicación no solamente a las Autoridades Competentes o Entidades Reguladores sino también a las Fuerzas y Cuerpos de Seguridad para que puedan acometer una investigación para el posible esclarecimiento de los hechos y la depuración de responsabilidades penales.

Por otro lado, el régimen que veremos a continuación para la empresa atacada, también resultaría de aplicación al atacante, en la medida en que el ciberataque fuera articulado claramente por una empresa o persona jurídica.

7.1.2. Responsabilidad de la empresa atacada

En este sentido, la responsabilidad penal en la que podría incurrir la empresa atacada (y/o sus proveedores), en la figura de sus administradores o representantes legales o trabajadores sometidos a su autoridad, de acuerdo con los artículos 31 y 31 bis del Código Penal Español, sería por la posible comisión de los delitos de *descubrimiento y revelación de secretos (artículo 197 CP) o daños informáticos (artículo 264 CP)*. Estos delitos, son los únicos que, a priori, podría cometer la empresa ante un caso de ataque cibernético; y siempre que dichos delitos hayan sido cometidos en nombre o por cuenta de la empresa, y en su beneficio directo o indirecto.

Por lo tanto, si una empresa ha sido "víctima" de un ciberataque, es dificil que se le pueda llegar a atribuir una responsabiliad penal, salvo que los delitos referidos se hayan realizado por cuenta o en nombre de la propia empresa o en su beneficio y hayan intervenido los administradores o representantes legales o trabajadores sometidos a la autoridad de los anteriores. Es conveniente que en estas situaciones la empresa tramite

la pertinente denuncia ante las fuerzas y cuerpos de seguridad del estado.

Con independencia de lo anterior, la empresa atacada (y/o sus proveedores), en su caso, podría quedar exenta de una posible e hipotética responsabilidad penal siempre que cuente, según los artículos 31 bis.2 y 31 bis.5 CP, con un programa real y efectivo de *Cumplimiento* y de prevención de delitos.

Los modelos de empresa y gestión a los que se refiere este requisito del artículo 31 bis.2.1º CP y que pueden llegar a determinar la exención o no de la responsabilidad penal de la empresa, no son otros que los *Compliance Programs*, cuyo contenido básico se regula después en el artículo 31 bis.5 CP:

1. Análisis/mapa de riesgos penales.
2. Políticas, normas, procedimientos necesarios para evitar la materialización de los riesgos.
3. Independencia y Autonomía financiera del órgano de cumplimiento.
4. Canal de denuncias interno.
5. Previsión de un sistema de investigación y sanción interno.
6. Verificar periódicamente dicho programa de Cumplimiento.

Finalmente, las sanciones y/o penas que podrían imponerse a la empresa, sin perjuicio de la responsabilidad personal de administradores o representantes y otras responsabilidades concurrentes o derivadas, de conformidad con el artículo 33.7. CP, son las siguientes:

1. Multa.
2. Disolución de la empresa.
3. Suspensión de actividades (no más de cinco años).
4. Clausura de sus locales y establecimientos por (no más de cinco años).
5. Prohibición de realizar en el futuro las actividades en cuyo ejercicio se haya cometido, favorecido o encubierto el delito (temporal o definitiva).
6. Inhabilitación para obtener subvenciones y ayudas públicas, para contratar con el sector público y para gozar de beneficios e incentivos fiscales o de la Seguridad Social (no más de 15 años).
7. Intervención judicial para salvaguardar los derechos de los trabajadores o de los acreedores (no más de cinco años).

Como hemos apuntado, las mismas normas sobre responsabilidad penal se aplicarían cuando la empresa atacada sea una empresa proveedora o prestadora de servicios.

En este sentido, y sin entrar en el análisis detallado de cada delito (acción, elementos objetivos, subjetivos, tipos agravados, etc.); la empresa proveedora de servicios, con independencia de la relación y responsabilidades contractuales, deberá prestar especial atención al riesgo de comisión de un delito de descubrimiento o revelación de secretos (apoderamiento o interceptación de mensajes de correo electrónico, interceptación de comunicaciones, utilización o modificación de información personal o familiar para vulnerar la intimidad) o de daños informáticos (que regula todo tipo de intromisiones en plataformas ajenas o sistemas externos como: destrucción -*total o parcial*- o alteración -*eliminación, interrupción, supresión o borrado*- de datos, programas o elementos informáticos). A modo de ejemplo, se prevé una modalidad agravada de este último delito, en el caso de que se afecte a los sistemas informáticos de una infraestructura crítica, y que lógicamente podría afectar a la hipotética responsabilidad penal de aquellos proveedores de dicha infraestructura crítica.

7.2. RESPONSABILIDAD ADMINISTRATIVA

7.2.1. Regulación general y autoridades competentes

7.2.1.1. Protección de Datos

La elección de proveedores o terceros solventes en las medidas de protección juega un papel relevante en el cumplimiento del principio de responsabilidad proactiva, que persigue demostrar un tratamiento conforme al RGPD.

La responsabilidad proactiva requiere un análisis continuo y periódico acerca de los tratamientos que se realizan, con qué datos, para qué finalidades y a través de qué operaciones de tratamiento, para garantizar que las medidas tomadas son las adecuadas para el cumplimiento. Esta idea es trasladable al análisis de los proveedores con acceso a datos, traduciéndose en que no únicamente es cumplimiento, sino demostrar el cumplimiento en cualquier momento.

Esta actitud **consciente, diligente y proactiva**, exige del responsable la elección de encargados del tratamiento garantes en términos de privacidad, fiabilidad, seguridad y experiencia probada, que demuestren, además, capacidad para identificar, gestionar y notificar un incidente de seguridad en tiempo y forma.

Cobra especial importancia, por ello, la gestión de los posibles incidentes que se puedan desarrollar con motivo de una violación de datos de carácter personal.

Se entiende por violación de seguridad[4]: *toda violación de la seguridad que ocasione la des-*

[4] Artículo 4.12 RGPD

trucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

Si bien el artículo 28 RGPD desglosa el contenido mínimo (contrato o acto jurídico vinculante) de los acuerdos con personal ajeno a la empresa que, siguiendo instrucciones del responsable, realice tratamientos de datos de carácter personal, es necesario que se tomen las medidas y garantías necesarias para poder gestionar una violación de datos y, en la medida de lo posible, prevenirla.

A estos efectos, en relación con las dimensiones de seguridad afectadas, podemos encontrarnos los siguientes casos[5], que pueden darse de manera individual o agrupada:

1. **Violación de la confidencialidad:** cuando se produce una revelación no autorizada o accidental de los datos personales, o el acceso a los mismos.

2. **Violación de la integridad:** cuando se produce una alteración no autorizada o accidental de los datos personales.

3. **Violación de la disponibilidad:** cuando se produce una pérdida de acceso accidental o no autorizada a los datos personales, o la destrucción de los mismos.

Responsables y encargados deben disponer de planes de control y gestión suficientes y adecuados para afrontar dichas situaciones, que serán diferentes en función del rol que desempeñen.

Los responsables deberán notificar a la Autoridad de Control, sin dilación indebida y a más tardar 72 horas después de haber tenido constancia de una violación de seguridad, a menos que sea improbable que la misma tenga riesgos para los derechos y libertades de los interesados. Deberá, asimismo, informar también a los interesados siempre y cuando el incidente pueda tener efectos adversos para los mismos[6].

El papel del encargado estará regulado por contrato, en el que debe de haberse previsto la obligación de notificar la violación. Aunque no se establece un plazo concreto para la comunicación por parte del encargado[7], el RGPD sí impone al Responsable la comunicación en 72 horas, de manera que siempre que sea posible, se debe intentar negociar una comunicación en un máximo de 24h.

A estos efectos, resulta conveniente tener en cuenta los criterios que se establecen en la *Guía de Notificación de Brechas de Seguridad* preparada por la AEPD e ISMS Forum[8], donde se indican diversos escenarios para considerar cuándo procede o no notificar

[3] Dictamen 03/2014 sobre la notificación de violación de datos personales. GT29.
[6] Artículos 33 y 34 RGPD.
[7] Artículo 33.2 RGPD: El encargado del tratamiento notificará sin dilación indebida al responsable del Tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.
[8] https://www.aepd.es/sites/default/files/2019-09/guia-brechas-seguridad.pdf

cada brecha.
En el caso de los corresponsables, se determinarán las responsabilidades de cada uno de ellos en los acuerdos firmados, donde se determinará qué responsable asume las obligaciones de notificación.

El contenido de las notificaciones debe ser adaptado al destinatario. La comunicación al interesado debe basarse en un leguaje claro y sencillo acerca de la naturaleza del evento, sus posibles consecuencias, las medidas de seguridad adoptadas y el punto de contacto donde obtener más información. En cambio, la notificación a la Autoridad de Control deberá contener, además de una descripción de la naturaleza de la violación, categorías, número de interesados y un número aproximado de registros afectados.

Retomando el principio de responsabilidad proactiva, es necesario que la notificación se encuentre registrada y documentada en un inventario actualizado a disposición de la Autoridad de Control. De este modo se dejará constancia de los tipos de violaciones acontecidas, las medidas de seguridad que mitigaron mayores riesgos y la justificación respecto al proceder de cada una de ellas.

7.2.1.2. Infraestructuras Críticas

Si nos encontramos con un ciberataque a una empresa que haya sido designada como operador crítico de un servicio esencial para la sociedad (administración, agua, alimentación, energía, espacio, industria química, industria nuclear, instalaciones de investigación, salud, sistema financiero y tributario, tecnologías de la información y las comunicaciones y transporte), la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas (Ley PIC) establece que el operador crítico tiene el deber de colaborar con las autoridades competentes del Sistema, con el fin de optimizar la protección de las infraestructuras críticas y de las infraestructuras críticas europeas por ellos gestionados -artículo 13.1. Ley PIC-, imponiéndole dicha Ley, así como su Reglamento de desarrollo (Real Decreto 704/2011, de 20 de mayo) determinadas obligaciones:

1. Prestar su colaboración técnica a la Secretaría de Estado de Seguridad, a través del CNPIC, en la valoración de las infraestructuras propias que se aporten al Catálogo.

2. Colaborar con el Grupo de Trabajo, en la elaboración de los Planes Estratégicos Sectoriales (PES) y en la realización de los análisis de riesgos.

3. Elaborar el Plan de Seguridad del Operador (PSO).

1. Elaborar un Plan de Protección Específico (PPE) para cada Infraestructura Crítica.

2. Designar a un Responsable de Seguridad y Enlace del Operador (RSE).

3. Designar a un Delegado de Seguridad (DS) por cada una de sus infraestructuras consideradas Críticas o Críticas Europeas por el Ministerio del Interior, comunicando su designación a los órganos correspondientes .

4. Facilitar las inspecciones de las autoridades competentes y adoptar las medidas de seguridad que sean precisas en cada Plan, solventando en el menor tiempo posible las deficiencias encontradas.

Sin perjuicio de las responsabilidades en las que pudiese, en su caso, incurrir la propia administración o el operador crítico por el incumplimiento de la normativa de su propio sector estratégico u otro tipo de normativas (civiles, mercantiles, de competencia, protección de datos, etc.), es cierto que la normativa PIC no recogía ningún régimen sancionador específico para las concretas obligaciones que hemos citado con anterioridad.

7.2.1.3. Normativa NIS

El 7 de septiembre entró en vigor el Real Decreto Ley 12/2018, de Seguridad de las Redes y Sistemas de Información (que transpone la Directiva NIS (UE) 2016/1148, de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión) y que resulta aplicable a los operadores de servicios esenciales, entre los que se encuentra la práctica totalidad de los designados como operadores de infraestructuras críticas por la Ley PIC (además de a los prestadores esenciales de un servicio digital -mercados en línea, motores de búsqueda en línea y servicios de computación en Nube-, siempre que no sean pymes o micropymes, estableciendo, entre otras obligaciones, las siguientes:

1. Adoptar medidas técnicas y de empresa, adecuadas y proporcionadas, para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información utilizados en la prestación de los servicios esenciales.

2. Notificar a la autoridad competente, a través del CSIRT de referencia (INCIBE-CERT, operadores sector privado, y el CCN-CERT, operadores sector público), los incidentes en redes y sistemas de información (tanto propios como de proveedores externos) relativos a dichos servicios esenciales.

3. Resolver los incidentes de seguridad que les afecten, y de solicitar ayuda especializada, incluida la del CSIRT de referencia, cuando no puedan resol-

ver por sí mismos los incidentes.

4. Proporcionar a las autoridades competentes la información necesaria para evaluar la seguridad de las redes y sistemas de información, incluida la documentación sobre políticas de seguridad.

5. Designar y comunicar un responsable de seguridad de la información.

A su vez el artículo 26 del citado RDL 12/2018 establece que la Autoridad Competente: *podrá exigir a los operadores de servicios esenciales o a los proveedores de servicios digitales que informen al público o a terceros potencialmente interesados sobre los incidentes cuando su conocimiento sea necesario para evitar nuevos incidentes o gestionar uno que ya se haya producido, o cuando la divulgación de un incidente redunde en beneficio del interés público.*

A diferencia de la Ley PIC, este Real Decreto sí cuenta con un régimen sancionador, por el que una empresa, bien un operador de un servicio esencial, bien un proveedor de servicios digitales que no hubiera adoptado las medidas de seguridad u organizativas adecuadas, no haya notificado un incidente al CSIRT correspondiente o no facilitara la información requerida por el CSIRT, o la autoridad competente, podría verse expuesta a multas que van desde los 100.000€ al 1.000.000€, según la infracción haya sido leve, grave o muy grave, de acuerdo con el catálogo tipificado en la norma referida.

En la actualidad, tras haberse designado como operadores de servicios esenciales los que ya habían sido designados anteriormente como operadores críticos, se encuentra en su fase final de aprobación el Reglamento de desarrollo del Real Decreto-Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

7.2.1.4. Guía nacional de notificación y gestión de ciberincidentes

En lo que a incidentes de ciberseguridad se refiere, el pasado 9 de marzo de 2019, el Consejo de Ciberseguridad Nacional aprobó la *Guía nacional de notificación y gestión de ciberincidentes*, siendo aplicable tanto al sector público como privado y a todas aquellas entidades que quedan bajo el ámbito de aplicación de Real Decreto Ley 12/2018 (operadores de servicios esenciales y proveedores de servicios digitales).

Asimismo, la guía establece un capítulo específico destinado a las infraestructuras críticas y a los operadores de dichas infraestructuras, conteniendo una previsión específica dirigida a los proveedores de los operadores señalando que: *aquellos proveedores de*

los sujetos obligados por este anexo que proporcionen sus productos o servicios a estos, y cuyas actividades tengan afección directa a la prestación de un Servicio Esencial, deberán cumplir con los mismos criterios exigibles a los operadores. En todo caso, el operador afectado será el responsable último del cumplimiento de los requerimientos exigibles en este texto.

Igualmente, además de regular un procedimiento de notificación de ventanilla única, una taxonomía y clasificación de los ciberincidentes, se establece la obligatoriedad de los operadores de notificar a la autoridad competente a través del CSIRT de referencia (INCIBE-CERT, operadores sector privado, CCN-CERT, operadores sector público) los incidentes calificados como críticos, muy altos o altos (tanto desde el punto de vista de la peligrosidad como del impacto) en un plazo inmediato, de 12 horas o de 48 horas, respectivamente.

Por lo tanto, si el operador de la infraestructura no cumple con su obligación de notificar el incidente sufrido, podría entrar en juego el régimen sancionador previsto en el citado Real Decreto Ley 12/2018 y ser objeto de una sanción que en función de la infracción cometida oscilaría, como antes se ha indicado, entre los 100.000€ y 1.000.000€.

7.2.2. Regulación sectorial y autoridades competentes

Es habitual que la normativa sectorial que afecta a una empresa, o las directrices de la Autoridad de control que supervise su actividad, establezcan condiciones específicas que deberán tenerse en cuenta para evitar una posible infracción que empeore los efectos del incidente sufrido por un proveedor, de cara a proteger a accionistas, clientes y el mercado en general.

De esta forma, podemos ver que las diferentes normativas, como el RGPD o NIS, establecen elementos comunes a la hora de afrontar incidentes de seguridad, como son los deberes de comunicación a los afectados, establecer plazos máximos para informar a las Autoridades de Control o disponer pautas de gestión del incidente. No obstante, también se da la circunstancia de que en algunos sectores regulados comienzan a anticiparse a la producción del incidente, al establecer pautas específicas a las empresas a la hora de externalizar sus servicios, es decir, procurar que las empresas sean más diligentes para acudir a sus proveedores con mejores garantías, y que estén preparadas para gestionar eficazmente un incidente con el proveedor en caso de que suceda.

A continuación, se reflejan algunos ejemplos en los principales sectores regulados:

7.2.2.1. Banca

El sector bancario, dada su relevancia, es un sector sometido a fuertes requisitos de contratación a la hora de externalizar sus servicios. Así, una entidad bancaria que quiera acudir un proveedor deberá tener en cuenta elementos como:

- El *Informe relativo a las directrices de externalización* de entidades bancarias de la Autoridad Bancaria Europea (EBA, Anexo 2, Referencias) que publicó el pasado 25 de febrero de 2019 y que tiene como objetivo esencial especificar: *los sistemas de gobierno interno, incluida la adecuada gestión de los riesgos, que las entidades, las entidades de pago y las entidades de dinero electrónico deberían aplicar cuando externalicen funciones, en particular en relación con la externalización de funciones esenciales o importantes*, así como *el modo en que las autoridades competentes deberían revisar y supervisar* dichos sistemas. De esta forma, una entidad bancaria que pretenda externalizar su operativa a través de un proveedor deber tener en cuenta elementos como:
  - Disponer de sistemas de gobierno adecuados.
  - Disponer de una política de externalización propia, que deberá tener en cuenta, entre otros, controles de diligencia debida respecto a los proveedores o planes de salida del proveedor.
  - Planes de continuidad de negocio.
  - Evaluar los riesgos derivados de la externalización.
  - Una clara delimitación de lo que se consideran "servicios esenciales" para la entidad.
- Por su parte, la Norma 43 de la Circular 2/2016 del Banco de España, sobre "Delegación de la prestación de servicios o del ejercicio de funciones" nos recuerda que las entidades de crédito deberán tener en consideración a la hora de contratar a un proveedor:
  - El riesgo de incumplimiento de las normas.
  - El riesgo de concentración que pueda suponer la acumulación de servicios externalizados en un mismo proveedor.
  - El riesgo inherente al país de prestación del servicio.
  - El riesgo reputacional.
  - El riesgo operacional, incluido el riesgo legal, derivado de un fallo en la prestación del servicio.

En este sentido, la Autoridad de Control debe tener la capacidad de llevar a cabo sus competencias de supervisión, instando a la entidad bancaria a incluir determinadas cláusulas contractuales con su proveedor en el que delega e incorporar requisitos como el de "incluir la exigencia de que el proveedor de los servicios disponga de un plan de contingencias que permita mantener su actividad y limitar las pérdidas de la entidad en caso de incidencias graves".

7.2.2.2.Seguros

Si bien el sector asegurador en general no cuenta con unas directrices específicas de externalización como sucede en el caso del sector bancario, la orientación del sector va cada vez más encaminada a regular la externalización de servicios y se tiene constancia de que el sector se está preparando para asumir unas directrices de externalización de servicios de manera similar al sector bancario. No obstante, hay algunos elementos a considerar:

- La Autoridad Europea de Seguros y Pensiones de Jubilación (EIOPA) ya ha comenzado a contemplar necesidades de regularización en la externalización de algunos servicios del sector, como es la contratación de servicios en la Nube, cuya publicación llegará pronto al mundo del seguro y las empresas deberán aplicarlo a la hora de acudir a este tipo de proveedores.

- El reciente Real Decreto Ley 3/2020, de 4 de febrero, de medidas urgentes por el que se incorporan al ordenamiento jurídico español diversas directivas de la unión europea en el ámbito de la contratación pública en determinados sectores; de seguros privados; de planes y fondos de pensiones; del ámbito tributario y de litigios fiscales, establece determinadas obligaciones para las entidades gestoras de fondos de pensiones, en concreto: *deberá garantizar el correcto funcionamiento de las actividades externalizadas a través del proceso de selección de un prestador de servicios y el seguimiento permanente de las actividades de dicho prestador de servicios. Para ello deberá designar dentro de la entidad a una persona responsable de la función o actividad externalizada, que cuente con la experiencia y conocimientos suficientes para comprobar la actuación de los proveedores de servicios*.

- Por otro lado, la Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras, regula en su artículo 67 la externalización de funciones esenciales de la entidad aseguradora, condicionando la contratación a que:

  - No se perjudique sensiblemente la calidad de su sistema de gobierno,

  - No aumente indebidamente el riesgo operacional (…) o afecte al servi-

cio continuo y satisfactorio para los tomadores de seguros.

- Deberá designarse dentro de la entidad a una persona responsable de la función o actividad externalizada, que cuente con la experiencia y conocimientos suficientes para comprobar la actuación de los proveedores de servicios.

- Deberá comunicarse previamente a la Dirección General de Seguros y Fondos de Pensiones la externalización de funciones o actividades críticas o importantes, así como de cualquier cambio posterior significativo en relación con dichas funciones o actividades.

- En cualquier caso, las entidades aseguradoras y reaseguradoras que externalicen parte de sus funciones seguirán respondiendo del cumplimiento de todas las obligaciones establecidas en la Ley y en sus normas de desarrollo.

7.2.2.3.Empresas cotizadas

Las empresas cotizadas, por su parte, pueden estar sometidas a directrices o criterios de control por parte de la CNMV, además de estar sometidas a los requisitos de su propia normativa sectorial, como son las empresas del sector energético sobre la necesidad de contemplar requisitos medioambientales para algunos servicios. No obstante, la propia CNMV se ha posicionado de manera puntual sobre el régimen de responsabilidad de las empresas y su relación con los proveedores:

- La propia CNMV recuerda que las empresas pueden mantener su régimen de responsabilidad incluso en un contexto de externalización de servicios, como es el caso de las fintech cuando respondieron a consultas planteadas por el sector, indicando que: *estas empresas no están sujetas a la autorización, registro y posterior supervisión de la CNMV. Son las empresas que utilizan sus servicios tecnológicos, y que realizan los correspondientes servicios de inversión con los clientes finales, las responsables ante la CNMV de la utilización de cualquier tecnología*.

- Por otro lado, la Recomendación 54 del *Código de buen gobierno de empresas cotizadas* de la CNMV nos recuerda que: *la política de responsabilidad social corporativa incluya los principios o compromisos que la empresa asuma voluntariamente en su relación con los distintos grupos de interés e identifique al menos (…) las prácticas concretas en cuestiones relacionadas con (…) proveedores*.

7.2.3. Normativas y estándares

A menudo, el cumplimiento regulatorio debe ser complementado, por motivos sectoriales o de negocio, mediante la adopción de determinados estándares.

Un ejemplo muy extendido es la Norma de Seguridad de Datos para la Industria de Tarjetas de Pago (PCI DSS). Pese a no existir ninguna exigencia legal para su cumplimiento, la mayoría de nuestras empresas están expuestas en mayor o menor medida (en función de los servicios de pago en nuestro negocio) a este estándar. Y no solo hablamos del claro ejemplo de las compañías financieras que actúen como emisoras de tarjetas. A cualquier otro actor que desee establecer una pasarela de pagos se le exigirán las mismas medidas de seguridad.

Estar adherido a PCI DSS conlleva el cumplimiento de 12 requisitos, que ayudarán a mitigar el riesgo de sufrir un incidente de seguridad. Desplegar controles de acceso lógico, de seguridad de red, de protección frente a malware, de desarrollo seguro, etc., son requisito indispensable para garantizar el cumplimiento del estándar y para establecer una protección razonable sobre los datos de tarjetas.

Además, el apartado 10.8 pone de relieve la importancia de la gestión de los incidentes relacionados con este tipo de datos, especialmente en aquellas compañías prestadoras de servicio, y que podrían ser origen, por tanto, de un incidente global. La normativa es exigente en cuanto a la definición de políticas para la identificación y el tratamiento del incidente y, si bien no explicita una necesidad de notificación y escalado a los afectados, sí hace hincapié en la importancia de la documentación, estudio y registro de los incidentes, de modo que se identifiquen las causas raíces y se establezcan controles para evitar la reproducción de los eventos.

A todo esto, debemos añadir la regulación europea PSD2, de aplicación a cualquier servicio de pago y traspuesta a la legislación española (RD 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera).

En este caso sí es explícita la necesidad de mantener procedimientos de gestión de incidentes que incluyan la notificación de incidentes de importancia a la autoridad competente (EBA o BdE), con el objetivo de mitigar el daño a los usuarios, a otros proveedores o a cualquier servicio de pago.

La seguridad de la información se está convirtiendo en un ámbito especialmente inten-

so en términos de regulación y estándares. Por ello, merece la pena que las compañías tengan en cuenta, también, otros marcos de referencia (Swift, eIDAS, Sepa, etc. para el sector financiero, guías de UNESPA para el sector asegurador, NIST, SOC, etc. para el resto).

7.3. BUENAS PRÁCTICAS PARA HITOS CONTRACTUALES

Para poder conseguir la adecuada gestión de los riegos derivados de la contratación de proveedores, conviene analizar las diferentes fases que intervienen en la formalización de una relación comercial entre la empresa y la sociedad sobre la que se quiere externalizar una actividad. De esta forma, se pueden identificar los siguientes escenarios y algunos de los elementos a contemplar en cada uno de ellos:

7.3.1. Fase precontractual

La fase precontractual supone el filtro inicial que puede garantizarnos el inicio de relaciones con terceras entidades en un escenario de mayor seguridad, así como cumplir con las obligaciones de "diligencia debida" que ya se imponen en las normativas de protección de datos, ciberseguridad, Cumplimiento, etc. Una empresa que identifique sus requisitos legales, técnicos y formales a la hora de externalizar sus servicios tendrá la capacidad de establecer procedimientos o soluciones que le ayuden a identificar empresas proveedoras con mayores garantías y seguridad. Algunas recomendaciones serían:

- Disponer de un procedimiento de homologación de proveedores. Para que el procedimiento de homologación sea eficaz, la empresa deberá tener un cuestionario que contemple los diferentes escenarios de riesgo que puedan afectar a las partes o la naturaleza del servicio, así como información de fuentes abiertas, certificaciones, auditorías, etc. de cara a tomar la mejor decisión posible en base a:
    - El sector de actividad.
    - Los requisitos legales de contratación establecidos por la normativa sectorial.
    - La captación de evidencias que acrediten los hitos de cumplimiento del proveedor.
    - Disponer de un sistema de ponderación que le permita determinar los diferentes criterios de valoración de manera objetiva.

La solicitud de códigos éticos, normas de cumplimiento interno y protocolos de actuación, y la comprobación de su compatibilidad con los valores y requisitos de contratación general de la compañía.

7.3.2. Fase contractual

No debemos olvidar que las cláusulas delimitarán el alcance de la responsabilidad de cada una de las partes y no bastará solo con haber identificado los riesgos y las necesidades por parte de la empresa, sino de reflejarlo adecuadamente. Por ello, un contrato de prestación de servicios debería contemplar elementos como:

- Las cláusulas de responsabilidad respecto a su contenido, limitación y, en su caso, exención. Solo serán eficientes si en ellas se contemplan todos los posibles riesgos a los que se expone no solo la empresa, sino también el propio proveedor. De esta forma, se podrán tener en cuenta:
  - Un catálogo completo de causas de exoneración de responsabilidad.
  - Cuantías económicas máximas de responsabilidad que tengan en cuenta no solo la posible responsabilidad derivada de los daños propios o frente a terceros, sino también teniendo en consideración el régimen sancionador que pueda ser de aplicación por motivo de la actividad de la compañía o el sector en el que se externaliza el servicio.
- Los ANS también serán un instrumento esencial para establecer los parámetros en los cuales el proveedor va a tener que ejecutar el servicio contratado, y será importe como es el conocer la actividad sancionadora de la Autoridad de control que supervise cada sector de actividad o los requisitos técnicos del servicio para delimitar un adecuado ANS.
- Por otro lado, la inclusión de cláusulas de continuidad de servicio prevendrá a la empresa ante las consecuencias de una interrupción del servicio del proveedor, incluyendo los casos en los que sufra un incidente o un evento sobrevenido.
- La inclusión de la contratación de un seguro apropiado para hacer frente a posibles incidentes de seguridad.
- La identificación de personas competentes para una interlocución adecuada en términos de seguridad y privacidad (DPOs, CISOs, Compliance Officers, etc.)
- La voluntad de las partes a trabajar en adecuar y complementar dicha relación ante nueva normativa sobrevenida que pudiera aplicar a la prestación del servicio y tratamiento de la información objeto del contrato.

7.3.3. Fase poscontractual

Si bien podemos pensar que la responsabilidad de una empresa respecto a la producción de un incidente de un proveedor acaba con la finalización del servicio, no debemos olvidar que todavía existen riesgos específicos que pueden afectar a la propia sociedad no solo de forma directa sino frente a terceros. En este sentido, que un proveedor sufra un incidente de seguridad que, por ejemplo, suponga un riesgo a la confidencialidad de nuestros datos o la de nuestros clientes, puede reactivar la esfera de responsabilidad que la empresa creía acabada con la finalización del contrato. De esta forma, es recomendable contemplar algunos aspectos que regulen circunstancias posteriores a la finalización del contrato, tales como:

- **Cláusulas de destrucción o devolución de la información suministrada al proveedor.** De esta forma, aminoraremos los riesgos de que el posible evento sufrido por un proveedor tenga efectos negativos sobre activos de nuestra empresa.

- **Cláusulas de transición.** Si el servicio externalizado se pretende continuar a través de otro proveedor, es conveniente regular un proceso de transición de estos proveedores de manera que se regulen aspectos como:

  - Plazos para llevar a cabo la transición del servicio.

  - Coordinación de reuniones para transmitir el *know how* adquirido durante el servicio.

  - Modo en el que se realizará el trasvase de información entre los proveedores.

  - Plazos de limitación de responsabilidad. Las cláusulas de exención de responsabilidad indicadas anteriormente deben tener en cuenta no solo el alcance de dicha responsabilidad, sino su duración.

- Asimismo, habrá que **acudir al ordenamiento jurídico general** y toda la teoría general de daños cuando sucedan incidentes que provoquen tales daños, aunque no se hubieran incluido clausulas específicas en el contrato que ya no esté vigente.

8. ANEXOS

8.1. ANEXO 1 – CUESTIONARIO AUTOEVALUACIÓN PROVEEDORES

Para poder evaluar el riesgo de ciberseguridad de un proveedor se ofrece un cuestionario de controles estructurado en 7 grupos que debería permitir a las organizaciones obtener una visión más ajustada del grado de riesgo y mitigación en materia de ciberseguridad:

Cada control tiene tres tipos de respuestas:

- ¿Cumple el control? Sí, No, N/A (No Aplica).
- Grado de Madurez del control, que se mide en la típica escala de madurez:
  - **0.** No se realiza.
  - **1.** Se realiza, pero no está documentado.
  - **2.** Está documentado, pero no hay procedimiento.
  - **3.** Está procedimentado, pero no se evalúa.
  - **4.** Está procedimentado y se evalúa.
  - **5.** Está procedimentado, se mide y se aplican mejoras.
- Comentarios sobre el control.

8.1.1. Grupo 1 - Controles de seguridad general

CONTROL	ID	DESCRIPCIÓN	EVALUACIÓN DEL PROVEEDOR	MADUREZ DEL CONTROL	COMENTARIOS
Concienciación	SG.1	¿Tiene la empresa un programa de formación de concienciación sobre seguridad integral?			
Transparencia	SG.2	¿Tiene la empresa contratado un ciberseguro con cobertura a clientes?			
	SG.3	En caso de fabricante de software, ¿tiene la empresa un programa de *bug bounty* y/o un programa de *vulnerability disclosure*? En caso afirmativo, indicar la URL desde donde se presentan cada uno de los programas.			
Rating	SG.4	¿La empresa tiene contratado algún servicio de rating de ciberseguridad a un tercero? En caso afirmativo indicar cual..			

8.1.2. Grupo 2 - Controles sobre los activos

CONTROL	ID	DESCRIPCIÓN	EVALUACIÓN DEL PROVEEDOR	MADUREZ DEL CONTROL	COMENTARIOS
Gestión de activos de la información	SG.1	¿Tiene la empresa un programa de formación de concienciación sobre seguridad integral?			
	AV.1	¿Dispone la empresa de una política de seguridad de la información actualizada?			
	AV.2	En caso afirmativo en AV.1, ¿define claramente la política lo que se considera información sensible o confidencial?			

CONTROL	ID	DESCRIPCIÓN	EVALUACIÓN DEL PROVEEDOR	MADUREZ DEL CONTROL	COMENTARIOS
Gestión de activos de la información	AV.3	¿La información sensible (confidencial o secreta) está separada física o lógicamente del resto de la red? Aplica también a entornos Cloud.			
	AV.4	¿Dispone la empresa de un procedimiento definido e implantado para la clasificación de la información?			
	AV.5	¿La empresa dispone de mecanismos de detección de accesos no autorizados a través de las redes de comunicaciones? En caso afirmativo, por favor describa cómo en comentarios.			
	AV.6	¿Tiene la empresa una solución antimalware gestionada de forma centralizada para todas las estaciones de trabajo, servidores y dispositivos móviles?			
	AV.7	Qué porcentaje de cobertura del antimalware hay actualmente en todos los sistemas informáticos, incluidos dispositivos móviles y ordenadores dedicados a OT. Indicar en comentarios.			
Hardening	AV.8	¿Se aplican guías de bastionado (*hardening*) en los sistemas?			
	AV.9	¿Las guías de bastionado incluyen el cambio de las passwords por defecto?			
	AV.10	¿Dispone la empresa de guías de bastionado (*hardening*) para configurar servidores, estaciones de trabajo y dispositivos móviles?			

8.1.3. Grupo 3 – Controles de confidencialidad

CONTROL	ID	DESCRIPCIÓN	EVALUACIÓN DEL PROVEEDOR	MADUREZ DEL CONTROL	COMENTARIOS
Confidencialidad	CN.1	¿La empresa hace firmar a sus empleados una cláusula de confidencialidad referente a la difusión de información de los proyectos/servicios de sus clientes?			
Datos Personales RGPD	CN.2	¿Dispone la empresa del informe periódico de cumplimiento con los aspectos exigidos en cuanto a RGPD? En caso afirmativo indicar en comentarios cuál es el grado de cumplimiento de la última auditoría RGPD.			

8.1.3. Grupo 4 – Controles de resiliencia

CONTROL	ID	DESCRIPCIÓN	EVALUACIÓN DEL PROVEEDOR	MADUREZ DEL CONTROL	COMENTARIOS
Resiliencia	RS.1	¿Se realizan copias de seguridad de los datos de sus clientes? En caso afirmativo indicar en comentarios la frecuencia con que se realizan.			
	RS.2	¿Dónde se almacenan las copias de seguridad? Indicar en comentarios			
	RS.3	¿Qué política de retención se aplica a los datos de clientes? Indicar en comentarios			
	RS.4	¿Se cifran las copias de seguridad de los datos?			
	RS.5	En caso de desarrollar software, ¿dónde se almacena el código fuente de clientes? Indicar en comentarios.			

CONTROL	ID	DESCRIPCIÓN	EVALUACIÓN DEL PROVEEDOR	MADUREZ DEL CONTROL	COMENTARIOS
Resiliencia	RS.6	En caso de desarrollar software, ¿se realizan copias de seguridad del código fuente de clientes?			
Continuidad de Negocio	CDN.1	¿Dispone de una política de Continuidad de Negocio? ¿Qué escenarios cubre?			
	CDN.2	¿Cuenta con un Plan de Continuidad de Negocio (PCN)? En caso afirmativo, ¿el servicio ofrecido está respaldado en ese PCN?			
	CDN.3	¿Está en condiciones de activación parcial del Plan de Continuidad de Negocio? Si la respuesta es afirmativa, ¿el respaldo del servicio prestado se puede activar independientemente?			
	CDN.4	¿Cuenta con certificaciones en materia de Seguridad y/o Continuidad de Negocio? En caso afirmativo, indique cuáles.			
	CDN.5	¿Dispone de un calendario de pruebas de planes de contingencia?			
	CDN.6	¿Realiza informes de las pruebas incluyendo planes de acción?			
	CDN.7	¿Qué OTR y OPR garantiza para los servicios dentro del alcance?			

8.1.5. Grupo 5 – Controles de protección

CONTROL	ID	DESCRIPCIÓN	EVALUACIÓN DEL PROVEEDOR	MADUREZ DEL CONTROL	COMENTARIOS
Incident Response Plan	PR.1	¿Dispone la empresa de un plan de respuesta antes incidentes de ciberseguridad y/o seguridad de la información?			
	PR.2	En caso afirmativo de la respuesta anterior, ¿qué fases incluye el plan de respuesta ante incidentes? Incluir una breve descripción de cada fase en comentarios.			
	PR.3	En caso afirmativo a las preguntas PR.1 y PR.2, ¿el plan incluye una matriz de responsabilidades?			
	PR.4	¿Cuenta la empresa con un plan de contingencia de las instalaciones físicas desde las que prestará el servicio?			
Protección de email	PR.5	¿La empresa dispone de un sistema de protección para el correo electrónico? En caso afirmativo indicar cuál.			
	PR.6	¿El sistema de protección de correo electrónico tiene configurada una *sandbox* para analizar los archivos adjuntos?			
Protección de navegación	PR.7	¿La empresa dispone de un sistema de protección de navegación web y/o filtrado DNS?			
Protección de información	PR.8	¿La empresa restringe el uso de medios extraíbles (USB, discos duros portátiles, etc.) en las estaciones de trabajo?			

CONTROL	ID	DESCRIPCIÓN	EVALUACIÓN DEL PROVEEDOR	MADUREZ DEL CONTROL	COMENTARIOS
Gestión de parches	PR.9	¿Existe un proceso gestionado de parcheo de sistema operativo y software? En caso afirmativo, ¿cómo se implementan los parches en los sistemas operativos y el software?			
SSDLC	PR.10	Respecto a los equipos de desarrollo y pruebas, ¿Están formados en las directrices de OWASP Top 10 (Ref. 4) u otras directrices de programación segura?			
	PR.11	¿Están definidos los procesos de QA y de prueba de seguridad (pentest, scans por release, etc.)? En caso afirmativo haga un breve resumen de cómo se realizan en la columna de comentarios.			

8.1.6. Grupo 6 – Controles de accesos

CONTROL	ID	DESCRIPCIÓN	EVALUACIÓN DEL PROVEEDOR	MADUREZ DEL CONTROL	COMENTARIOS
Control de Acceso	AC.1	¿Tiene definido el proveedor una política de control de accesos a las aplicaciones?			
	AC.2	¿Tienen implementados los proveedores controles de acceso físico a los lugares donde se hallen instalados equipos que den soporte a los sistemas de información?			
	AC.3	¿Ha implantado el proveedor un sistema de gestión de credenciales/ contraseñas?			

CONTROL	ID	DESCRIPCIÓN	EVALUACIÓN DEL PROVEEDOR	MADUREZ DEL CONTROL	COMENTARIOS
Accesos no autorizados	AC.4	¿Existe un *log* para registrar accesos fallidos en cuentas de usuarios incluidos los administradores y cuentas privilegiadas?			
Autenticación	AC.5	¿Todas las cuentas administrativas están configuradas con doble factor de autenticación?			
	AC.6	¿Está habilitado el doble factor de autenticación para todas las cuentas de usuarios no administrativos?			
	AC.7	¿Qué porcentaje de usuarios tienen acceso administrativo o privilegiado en sus estaciones de trabajo? Por qué lo requieren.			

8.1.7. Grupo 7 – Controles de exposición

CONTROL	ID	DESCRIPCIÓN	EVALUACIÓN DEL PROVEEDOR	MADUREZ DEL CONTROL	COMENTARIOS
Exposición	EX.1	¿La empresa realiza escaneos de vulnerabilidades sobre los activos de la empresa? Indicar en comentarios.			
	EX.2	¿La empresa realiza ejercicios de *red team*? En caso afirmativo indicar la frecuencia en comentarios.			
	EX.3	¿La empresa participa en ejercicios de ciberseguridad multisectoriales o sectoriales?			
	EX.4	¿Dispone la empresa de una política de Seguridad de la Información en relaciones con proveedores?			

8.2. ANEXO 2 - REFERENCIAS

1. "The Global Risks Report 2020" del World Economic Forum (https://www.weforum.org/reports/the-global-risks-report-2020).

2. "Protocolo de actuación frente a incidente en proveedor", ISMS Forum 2020 (https://www.ismsforum.es/ficheros/descargas/protocolo-de-actuacion-frente-a-incidente-en.pdf).

3. "All together now. Third party governance and risk management", Deloitte 2019 (https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-extended-enterprise-risk-management-global-survey-2019.pdf).

4. Owasp Top 10 (https://owasp.org/www-project-top-ten/).

5. "Informe relativo a las directrices de externalización" de entidades bancarias de la Autoridad Bancaria Europea (EBA) 2019 (https://www.bde.es/f/webbde/INF/MenuHorizontal/Normativa/guias/EBA-GL-2019_02_ES.pdf).

6. "Guía Nacional de notificación y Gestión de ciberincidentes" (https://www.incibe-cert.es/guias-y-estudios/guias/guia-nacional-notificacion-y-gestion-ciberincidentes).

7. "Guía CCN-STIC 817, Esquema Nacional de Seguridad, Gestión de ciberincidentes" (https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html).

8. "Libro Blanco del CISO", ISMS Forum (https://www.ismsforum.es/ficheros/descargas/segunda-edicion-del-libro-blanco-del-ciso-de-isms.pdf).

9. "Guía para la gestión y notificación de brechas de seguridad", AEPD e ISMS Forum (https://www.aepd.es/sites/default/files/2019-09/guia-brechas-seguridad.pdf).

11. Indicadores para la Mejora de la Ciberresiliencia (https://www.incibe-cert.es/guias-y-estudios/guias/imc-indicadores-mejora-ciberresiliencia).

12. ISAE 3402 - International Service Organization Assurance Standard (http://isae3402.com/)

Más información en:

www.ismsforum.es

isms forum INTERNATIONAL INFORMATION SECURITY COMMUNITY

DSN · CCN centro criptológico nacional · CNPIC CENTRO NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURAS Y CIBERSEGURIDAD · incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD · AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA