# Gestión del riesgo en *cloud computing*

PID_00286165

Jordi Guijarro Olivares

Tiempo mínimo de dedicación recomendado: 4 horas

Universitat Oberta de Catalunya

**Jordi Guijarro Olivares**

Director de Innovación en Ciberseguridad en i2CAT (http://www.i2cat.net), el Centro de Investigación en Internet. Ingeniero en Informática por la Universitat Oberta de Catalunya (UOC) y máster en Gestión de las Tecnologías de la Información y de la Comunicación por la Universidad Ramon Llull (URL). Experto en cloud computing y ciberseguridad, participa en proyectos de investigación e innovación de la Comisión Europea del programa Horizon 2020.
jordi.guijarro@i2cat.net.

El encargo y la creación de este recurso de aprendizaje UOC han sido coordinados por el profesor: Josep Jorba Esteve

Primera edición: febrero 2022

Av. Tibidabo, 39-43, 08035 Barcelona
Autoría: Jordi Guijarro Olivares
Producción: FUOC

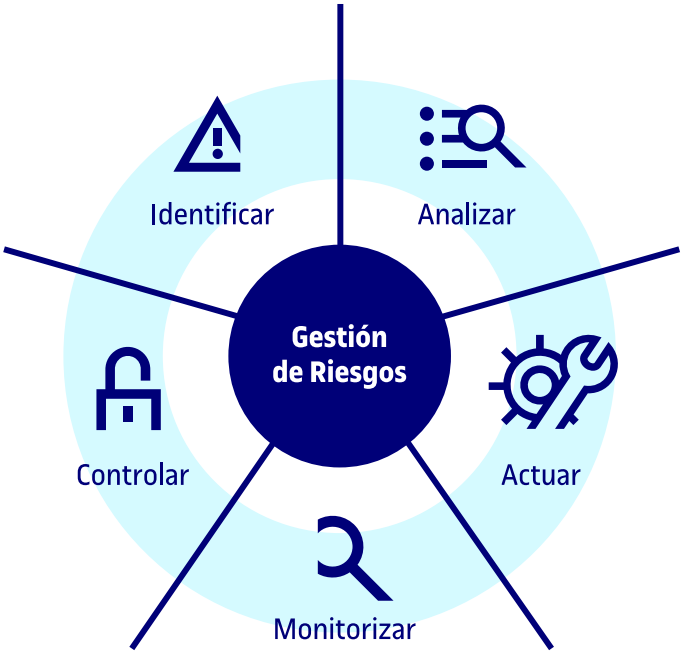
# Índice

# 1. Introducción a la gestión del riesgo

En muchas organizaciones, un enfoque típico de la gestión del riesgo en ciberseguridad se fundamenta en una evaluación anual, ya sea una autoevaluación o una auditoría de terceros de su programa de seguridad cibernética. Sin embargo, **las auditorías anuales no son suficientemente efectivas**, por lo cual, las noticias siguen llenas de casos en los que empresas, que estaban cumpliendo su programa de seguridad, tuvieron de todos modos algún incidente relacionado con la fuga masiva de información. Esto se debe a que las organizaciones tienen un ambiente dinámico, y, en cambio, una auditoría representa el estado del sistema en un momento concreto. Es en el momento del análisis de la causa del incidente cuando se revelan evidencias que apuntan a una respuesta no efectiva por parte de la organización.

Por estos motivos, es posible ver que la mayoría de las organizaciones que basan su gestión del riesgo solo en cumplir con las auditorías de seguridad comienzan su respuesta a incidentes demasiado tarde, en el momento en el que son notificadas por un tercero debido a que sus datos han sido robados, o a que sus sistemas están siendo utilizados por personas ajenas a la organización. En general, esto representa una ejecución ineficaz de las actividades que la organización ha identificado para la protección de sus activos críticos, que han de coincidir con los objetivos deseados de gestión del riesgo de seguridad cibernética.

Figura 1. Modelo de la gestión del riesgo




Fuente: ENISA

Por lo tanto, observamos que, a día de hoy, existe una literatura extensa y suficientes ejemplos de incidentes que apremian a las organizaciones para que trabajen en el proceso de gestión del riesgo de modo adicional con respecto al trabajo requerido por las auditorías anuales incluidas en un programa de seguridad convencional. De esta manera, las organizaciones buscan medir el estado de riesgo en el ámbito de la ciberseguridad y poder tomar decisiones de manera más efectiva.

A continuación, a modo introductorio, respondemos a preguntas esenciales en la gestión de riesgos: ¿Qué está en riesgo? y ¿cómo podemos mejorar?

### 1.1. ¿Qué está en riesgo?

En la actualidad, todavía es común que muchas organizaciones tengan una mentalidad que les incline a pensar que no serán objetivo de ciberataques. Sin embargo, cualquier tipo de organización, por pequeña que sea, tiene que dejar de lado esta mentalidad, ya que todas las organizaciones tienen características que las convierten en objetivo. Algunos motivos y características de las organizaciones por los cuales se convierten en objetivo de ciberataques son:

- Tener la capacidad de generar capital y de gestionar recursos.
- Usar modelos de TI distribuidos acentuados por la adopción de servicios de *cloud computing*.
- Disponer de una infraestructura de computación que puede utilizarse para atacar a otras organizaciones.
- Poseer activos de información (financiera, ecosistema de relaciones personales, etc.) relevantes.

Además, la reputación de una organización es fundamental para su éxito a largo plazo. La buena reputación impulsa la demanda de nuevos retos y oportunidades.

### 1.2. ¿Cómo podemos mejorar?

Es ampliamente conocido que la ciberseguridad es difícil de gestionar, y que ninguna organización dispone de suficientes recursos para proteger todo al máximo nivel. Además, también se sabe que, aunque el gasto sea alto y los controles de ciberseguridad sean efectivos, siempre existe la posibilidad de que los sistemas sean «hackeados». Por este motivo, la estrategia más beneficiosa pasa por tomar un enfoque de gestión del riesgo y desarrollar una buena respuesta a incidentes.

Un enfoque de gestión del riesgo para la seguridad digital permite a una organización priorizar todos los aspectos de su programa de ciberseguridad, como parte de su actual programa de gestión del riesgo empresarial (ERM, *enterprise risk management* en inglés).

En este sentido, el National Institute of Standards and Technology (NIST) desarrolló el **marco de seguridad digital** (NIST CSF, *cybersecurity framework* en inglés) para permitir que los responsables de las decisiones de ERM conozcan sus riesgos de seguridad digital. A pesar de una cierta confusión sobre el papel previsto para el NIST CSF, este no pretende reemplazar los estándares técnicos de ciberseguridad (políticas, procedimientos y controles) como NIST 800-53, COBIT5, ISO 27001, etc. El NIST CSF establece un lenguaje común y una estructura que permiten discutir las mejores prácticas en seguridad digital entre las diversas industrias, organizaciones y grupos, y también dentro de una misma organización. Su objetivo es **cerrar la brecha de comunicación** entre el dominio técnico y el empresarial para que el riesgo de ciberseguridad pueda ser incorporado en la gestión del riesgo global de una empresa.

De forma resumida, el NIST CSF pretende que las organizaciones respondan a las siguientes tres preguntas:

- ¿Cuáles son los activos críticos de la organización?
- ¿Cuáles son las amenazas más probables de alto impacto?
- ¿Cuál es la estrategia para proteger los activos de esas amenazas?

La definición de una estrategia priorizada (donde *estrategia* equivale a las acciones que hay que tomar para alcanzar un objetivo) es un buen comienzo, pero no es suficiente para lograr una postura de seguridad digital medible. Tener la capacidad de ejecutar correctamente la estrategia y medirla es un hecho muy importante y, para ello, toda organización debería poder responder a las siguientes preguntas:

- ¿Cómo se prioriza la respuesta y las acciones cotidianas?
- ¿Cómo se vinculan los esfuerzos hechos por la organización con la estrategia de mitigación de riesgos?
- ¿Cómo se mide la respuesta de la organización?
- ¿Cómo se mide la efectividad de los resultados de las actividades realizadas?
- ¿Cómo se mide el riesgo de ciberseguridad en el riesgo de la cadena de suministro (proveedores de productos y servicios)?

## 2. Gobierno del riesgo

El gobierno o gobernanza y la gestión del riesgo son temas muy amplios. Para profesionales de la seguridad, la computación en la nube impacta en cuatro áreas del gobierno y la gestión del riesgo:

- **El gobierno**, que incluye las políticas, los procesos y los controles internos que incluyen cómo está funcionando una organización. Todo desde las estructuras y políticas hasta el liderazgo y otros mecanismos de gestión.

- **La gestión del riesgo empresarial**, que incluye gestionar el riesgo global para la organización, alineado con el gobierno de la organización y su tolerancia al riesgo. La gestión del riesgo empresarial incluye todas las áreas de riesgo, no únicamente las relacionadas con la tecnología.

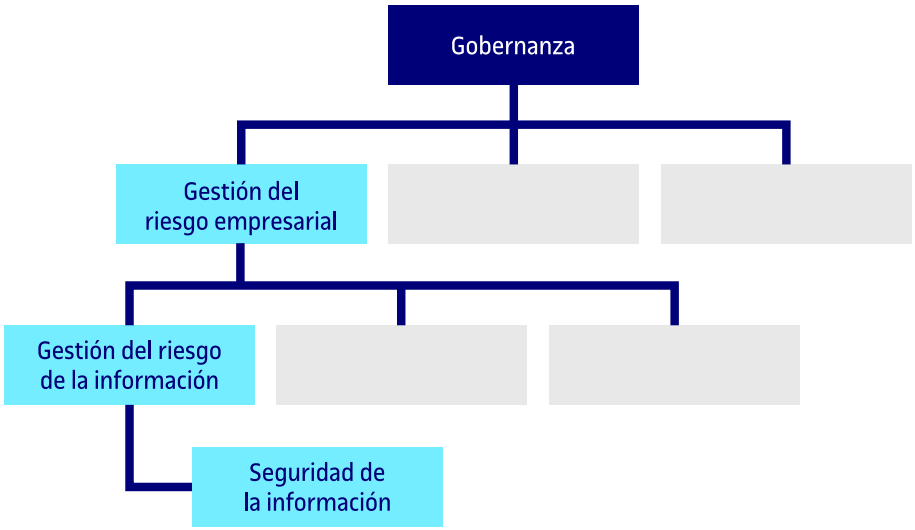
- **La gestión del riesgo de la información**, que cubre la gestión del riesgo de la información, incluyendo la tecnología de la información. Las organizaciones encaran todo tipo de riesgos, desde los financieros a los físicos, y la información solamente es uno de los múltiples activos que una organización necesita gestionar.

- **La seguridad de la información**, que es el conjunto de instrumentos y prácticas para la gestión del riesgo de la información. La seguridad de la información no es la razón de ser de la gestión de los riesgos de la información: políticas, contratos, seguros y otros mecanismos que también tienen un rol (incluyendo la seguridad física para la información no digital).

Sin embargo, el rol principal, si es que no es el único, de la seguridad de la información es proveer de procesos y controles para proteger la información electrónica y los sistemas que se usan para acceder a ella.

En una jerarquía simplificada, la seguridad de la información es una herramienta para la gestión del riesgo de la información, que es un instrumento para la gestión del riesgo empresarial, y que a su vez es una herramienta de gobernanza. Las cuatro están estrechamente relacionadas, pero requieren un enfoque, procesos y herramientas individuales.

Figura 2. Gestión del riesgo empresarial y la seguridad de la información




**Lecturas recomendadas**

Para más Información consultad estos recursos sobre el gobierno del riesgo en *cloud*:

**ISO/IEC 38500:2015** - Information Technology - Governance of IT for the organization https://www.iso.org/standard/62816.html.

**ISACA - COBIT** - A Business Framework for the Governance and Management of Enterprise IT https://www.isaca.org/resources/cobit.

**ISO/IEC 27014:2013** - Information Technology - Security techniques - Governance of information security https://www.iso.org/standard/43754.html.

## 2.1. Impactos principales

La computación en la nube afecta al gobierno, ya que introduce una tercera parte dentro del proceso (en el caso de una nube pública o nube privada gestionada por terceros), o posiblemente altera las estructuras internas de gobernanza en el caso de nube privada propia.

La primera cuestión que cabe recordar en el gobierno de la computación en la nube es que una organización nunca puede externalizar la responsabilidad del gobierno, incluso cuando se utilizan proveedores externos.

Esto es siempre cierto, nube o no, pero es útil tenerlo presente cuando se navega por los conceptos de la computación en la nube de modelos de responsabilidad compartida.

Los proveedores de servicio en la nube intentan aprovechar economías de escala para gestionar los costes y las capacidades. Esto significa crear servicios extremadamente estandarizados (incluyendo contratos y acuerdos de nivel de servicio) que son homogéneos para todos los clientes. Los modelos de gobierno necesariamente no pueden tratar de la misma forma a los proveedores de servicios en la nube que a los proveedores externos de servicio dedicados, los cuales típicamente personalizan sus ofertas, incluyendo los acuerdos legales, para cada cliente.

La computación en la nube cambia las responsabilidades y los mecanismos para la implementación y la gestión del gobierno. Las responsabilidades y mecanismos para la gobernanza se definen en el contrato, como en cualquier otra relación de negocio. Si el área afectada no está en el contrato, no hay mecanismos disponibles para hacer cumplir al proveedor, y es una brecha de

gobernanza. Las brechas de gobernanza no necesariamente excluyen utilizar el servicio del proveedor, pero requieren que el cliente ajuste sus propios procesos para cerrar las brechas o aceptar los riesgos asociados.

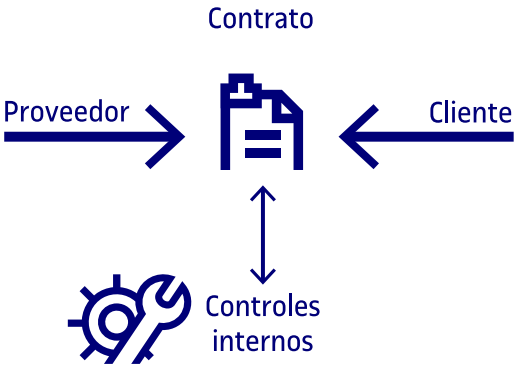
## 2.2. Herramientas para el gobierno de la nube

Como con cualquier otra área, hay herramientas de gestión específicas para la gobernanza. Esta relación se focaliza más en herramientas orientadas a proveedores externos, pero estas mismas herramientas pueden a menudo utilizarse internamente para despliegues privados:

### 1) Contratos

La herramienta principal es el contrato entre el proveedor de servicios en la nube y el cliente de la nube (esto es aplicable tanto a las nubes públicas como privadas). El contrato es su única garantía de cualquier nivel de servicio o compromiso –asumiendo que no hay un incumplimiento de contrato, que mete todo en un escenario legal–. Los contratos son las principales herramientas para extender la gobernanza entre los socios de negocio y los proveedores.

Figura 3. Herramientas de gobierno




Fuente: CSA.

Los contratos definen las relaciones entre los proveedores y clientes y son la herramienta principal para que los clientes extiendan la gobernanza a sus proveedores.

### 2) Evaluaciones de proveedores (proveedor de servicios en la nube)

El cliente potencial de la nube realiza las evaluaciones utilizando la información disponible y los procesos y las técnicas permitidas. Combinan investigaciones contractuales y manuales con análisis de terceros (las declaraciones legales a menudo usadas para comunicar los resultados de una evaluación o auditoría) e investigación técnica. Son muy similares a cualquier evaluación

de proveedores y pueden incluir aspectos como la viabilidad financiera, la historia, las características de las ofertas, las declaraciones de terceros, la retroalimentación entre profesionales y otros.

**3) Informe de cumplimiento legal**

Los informes de cumplimiento legal incluyen toda la documentación sobre los proveedores internos y las evaluaciones externas de cumplimiento legal. Los informes de auditoría de controles, que una organización puede ejecutar por sí misma, que un cliente puede hacer a un proveedor (aunque no suele ser una opción en la nube), o bien ejecutarlo por un tercero de confianza. Se prefieren auditorías y evaluaciones de terceros porque proporcionan una validación independiente (asumiendo que se confía en el tercero). Los informes de cumplimiento legal a menudo están disponibles para los interesados y los clientes de la nube, pero pueden estar solo disponibles bajo NDA (acuerdos de confidencialidad) o para clientes contratados. Esto es a menudo requerido por la firma que ejecutó la auditoría y no necesariamente estará completamente bajo el control del proveedor de servicios en la nube.

Las evaluaciones y auditorías deberían basarse en estándares (hay muchos). Es crítico entender el alcance, no únicamente el estándar utilizado. Estándares como SSAE 16 tienen un alcance definido, que incluye qué se evalúa (por ejemplo, servicios del proveedor), así como qué controles son evaluados. Un proveedor puede «pasar» una auditoría que no incluya ningún control de seguridad, con lo que resulta poco útil para los gestores de la seguridad y del riesgo. También se requiere considerar la confianza de las evaluaciones realizadas por un tercero que ha de ser equivalente en las actividades que se realicen en una evaluación propia. No todas las empresas de auditoría (o auditores) son iguales y su experiencia, historia y cualificaciones deben incluirse en las decisiones de gobierno.

**Programas de seguridad**

El registro de Cloud Security Alliance STAR es un programa de seguridad y de archivo de documentación para las evaluaciones del proveedor de servicios en la nube basadas en CSA Cloud Control Matrix y Consensus Assessments Initiative Questionnaire. Algunos proveedores también distribuyen documentación para certificaciones adicionales y evaluaciones (incluyendo autoevaluaciones).

### 2.2.1. Gestión del riesgo en las organizaciones

La gestión del riesgo empresarial es la gestión global del riesgo para una organización. Al igual que con el gobierno, el contrato define los roles y las responsabilidades para la gestión del riesgo entre el proveedor de servicios en la nube y el cliente en la nube. Y, como con la gobernanza, nunca se puede externalizar en un proveedor externo la responsabilidad general ni la responsabilidad de la gestión de riesgos.

**Lecturas recomendadas**

Para más información sobre la gestión del riesgo, podéis consultar los siguientes recursos:

**ISO 31000:2009** - Risk management - Principles and guidelines

**ISO/IEC 31010:2009** - Risk management - Risk assessment techniques

**NIST Special Publication 800-37 Revision 1** (updated June 5, 2014) (http://nvlpubs.nist.gov/nistpubs/ SpecialPublications/NIST.SP.800- 37r1.pdf).

La gestión del riesgo en la nube está basada en el **modelo compartido de responsabilidades**. El proveedor de servicios en la nube acepta cierta responsabilidad sobre algunos riesgos, pero el cliente en la nube es el responsable de todos los riesgos que no asume el proveedor. Esto es especialmente evidente cuando se evalúan las diferencias entre los modelos de servicio, dado que el proveedor gestiona más riesgos en SaaS, mientras que en IaaS es el usuario el que lo hace. Pero, de nuevo, el usuario de servicios en la nube es en última

instancia el responsable de sus riesgos; solo se delega en el proveedor de servicios en la nube parte de la gestión de riesgos. Esto es cierto incluso con una nube privada propia; en esas situaciones, una unidad organizativa transmite la gestión de algunos de sus riesgos en el proveedor interno de la nube en lugar de en un tercero, y los SLA internos y los procedimientos reemplazan a los contratos externos.

La gestión del riesgo empresarial se basa en buenos contratos y documentación que permiten conocer dónde está la división de responsabilidades y los potenciales riesgos no tratados. Mientras que el gobierno se centra casi exclusivamente en los contratos, la gestión del riesgo puede profundizar en las capacidades tecnológicas y de procesos del proveedor, basada en su documentación.

> Por ejemplo, un contrato rara vez definirá cómo se implementará la seguridad de redes. La revisión de la documentación del proveedor proporcionará mucha más información que ayude a adoptar una decisión más efectiva sobre el riesgo.

La tolerancia al riesgo es la cantidad de riesgo en la organización que están dispuestos a aceptar la dirección y las partes interesadas. Esta varía según el activo, no debe ser general para un proveedor particular; más bien, las evaluaciones deben alinearse con el valor y los requisitos de los activos involucrados. El hecho de que un proveedor de servicios en la nube pública sea externo y que el usuario pueda estar preocupado por la infraestructura compartida para algunos activos no significa que no esté dentro del riesgo tolerado para todos los activos. En términos prácticos significa que se creará una matriz de servicios en la nube con todos los tipos de activos que se permiten en esos servicios.

Mudarse a la nube no cambia la tolerancia al riesgo, simplemente cambia su gestión.

### 2.3. Modelo de servicio y modelo de despliegue

Al considerar las diversas opciones disponibles, no solo con los proveedores de servicios en la nube sino también en la forma en la que se proporcionan dichos servicios en la nube, se debe prestar atención a cómo los modelos de servicio y de despliegue afectan a la capacidad de gestionar la gobernanza y el riesgo.

#### 2.3.1. Software como servicio (SaaS)

En la mayoría de los casos, SaaS es el ejemplo más crítico de la necesidad de un contrato negociado. El contrato protegerá la capacidad de gobernanza o de validar el riesgo en relación con los datos almacenados, procesados, transmitidos con y en la aplicación. Los proveedores de SaaS tienden a agruparse en uno de los extremos del espectro tamaño/capacidad y la probabilidad de contrato negociado es mucho mayor si el proveedor SaaS es pequeño. Desafortunadamente, algunos proveedores pequeños de SaaS no pueden operar con un nivel de madurez que alcance o exceda las capacidades de gobernanza y gestión del

riesgo del cliente. Concretando, el nivel de visibilidad del funcionamiento real de la infraestructura que proporciona SaaS se limita a lo que se muestra en la interfaz desarrollada por el proveedor de servicios en la nube.

### 2.3.2. Plataforma como servicio (PaaS)

Continuando con los modelos de servicio, el nivel de detalle que está disponible (y la consiguiente capacidad de autogestionar el gobierno y los problemas de riesgo) se incrementa. La probabilidad de un contrato totalmente negociado en este modelo es probablemente menor que en cualquiera de los otros. Esto es porque el principal motor del PaaS es desarrollar una prestación sencilla con una alta eficiencia. PaaS, por lo general, se suministra con una API enriquecida, y algunos proveedores han habilitado la recopilación de algunos de los datos necesarios para probar que los SLA se están cumpliendo. Dicho esto, el cliente todavía se encuentra en la posición de tener que hacer un esfuerzo significativo para determinar si las estipulaciones contractuales proporcionan efectivamente el nivel de control o apoyo requerido para habilitar la gobernanza o la gestión de riesgos.

### 2.3.3. Infraestructura como servicio (IaaS)

La infraestructura como servicio es el modelo en la nube que más se acerca a un centro de datos tradicional (o incluso la gestión tradicional de la externalización de un centro de datos), y la buena noticia es que la mayoría de las actividades existentes de gobernanza y gestión de riesgo que las organizaciones han construido y utilizado son directamente transferibles. Sin embargo, hay nuevas complejidades relacionadas con la orquestación subyacente y la gestión por capas que permiten una infraestructura que a menudo se ha pasado por alto.

En muchos sentidos, el gobierno y la gestión de riesgos de la orquestación y la gestión de capas son consistentes con la infraestructura subyacente (redes, energía, etc.) de un centro de datos tradicional. Están presentes los mismos problemas de gobernanza y gestión de riesgo, pero la exposición de esos sistemas es suficientemente diferente, por lo que se requieren cambios en el proceso existente. Por ejemplo, controlar quién puede realizar los cambios de configuración en la red o quién cambia las cuentas en dispositivos individuales en el plano de gestión de la nube.

## 2.4. Riesgos basándonos en los modelos de despliegue

Los clientes de la nube tienen una capacidad reducida para gobernar las operaciones en una nube pública, ya que el proveedor es responsable de la gestión y el gobierno de su infraestructura, empleados y todo lo demás. En la pública, el cliente tiene una reducida capacidad para negociar los contratos, lo que afecta a la forma de extender su gobernanza en la nube. La escasa flexibilidad de los contratos es una propiedad natural del alquiler compartido. Los proveedores

no necesariamente pueden ajustar los contratos y las operaciones para cada cliente, pues todo se ejecuta en un conjunto de recursos compartidos que utilizan el mismo conjunto de procesos. Adaptarse a los diferentes clientes incrementa el coste, lo que ocasiona o introduce una compensación, y a menudo es la línea divisoria entre usar una nube pública o privada. La nube privada hospedada permite una personalización completa, pero a un coste mayor debido a la pérdida de las economías de escala.

Esto no significa que no se deba intentar negociar el contrato, no obstante, se ha de reconocer que no siempre es posible; en vez de esto, se necesitará elegir entre distintos proveedores (cuál puede ser menos seguro), o ajustar las necesidades y usar mecanismos alternativos de gobernanza o de mitigación. Utilizando una analogía, se puede pensar en un servicio de transporte. Cuando se emplea un transportista/proveedor común no se puede definir su funcionamiento. Cuando se ponen documentos sensibles en un paquete y confías en estos (transportista/proveedor), se aceptan sus obligaciones en el despliegue de la seguridad dentro de las expectativas de los acuerdos de nivel de servicio.

### 2.4.1. Nube pública

La nube pública no es el único modelo que impacta en la gobernanza; incluso la nube privada puede tener un efecto. Si una organización permite que un tercero gestione su nube privada (que es muy común), esto afecta a la gobernanza, al igual que cuando se subcontrata a un proveedor. Se compartirán las responsabilidades junto a las obligaciones definidas en el contrato.

### 2.4.2. Nube privada

Aunque es probable que tenga más control sobre los términos contractuales, es importante asegurarse de que cubran los mecanismos de gobernanza necesarios. A diferencia de un proveedor público, que tiene varios incentivos para mantener su servicio bien documentado y en niveles de rendimiento estándar, funcionalidad y competitividad, una nube privada alojada puede ofrecer exactamente lo que está en el contrato, con todo lo demás a un costo adicional. Esto debe ser considerado y contabilizado en negociaciones, con cláusulas para garantizar que la propia plataforma permanezca actualizada y competitiva. Por ejemplo, al exigir al proveedor que actualice la última versión de la plataforma de nube privada dentro de un cierto periodo de tiempo de lanzamiento y después de su firma.

Con una nube privada alojada de forma autónoma, la gobernanza se centrará en los acuerdos de nivel de servicio interno para el usuario de servicios en la nube (empresas u otras unidades organizativas) y en los modelos de transferencia de costes y facturación para proporcionar acceso a la nube.

### 2.4.3. Nube híbrida

Cuando se contemplan entornos de nube híbrida, la estrategia de gobernanza debe considerar un conjunto mínimo de controles a los que se compromete el proveedor del servicio en la nube en un contrato y los acuerdos internos de gobernanza de la organización El usuario de servicios en la nube está conectando o bien dos entornos en la nube o bien un entorno en la nube y un centro de datos. En cualquier caso, la gobernanza general es la intersección de esos dos modelos.

> Por ejemplo, si se utiliza un enlace a una red dedicada a conectarse a la nube de un centro de datos, se ha de dar cuenta de los problemas de gobierno que afectan a ambos escenarios.

En una nube de tipo «comunitaria» se comparten plataformas con múltiples organizaciones, pero no son públicas; el gobierno se extiende a las relaciones con todos los miembros de la comunidad, no solo entre el proveedor y el cliente. Es una mezcla de la forma de abordar la gobernanza en la nube pública y en la privada, mediante la que se aprovecharán economías de escala en relación con las herramientas generales de gobernanza y los contratos. No obstante, se puede llegar a un consenso entre los miembros de la comunidad, para realizar ajustes que permitan trabajar como si la nube fuese privada. Esto incluye las relaciones entre los miembros de la comunidad, relaciones financieras, así como en la forma de reaccionar cuando un miembro abandona la comunidad.

## 2.5. Intercambios en la gestión de riesgos en la nube

Existen ventajas y desventajas en la administración del riesgo empresarial para los despliegues en la nube. Estos factores son, como era de esperar, más pronunciados en la nube pública que en la nube privada en modo «collocation»:

- Hay menos controles físicos sobre los activos, su gestión y los procesos. No se puede controlar físicamente la infraestructura o los procesos internos del proveedor.

- Hay una mayor dependencia de los contratos, las auditorías y las evaluaciones, ya que se carece en el día a día de visibilidad del estado de la nube y de la gestión.

- Existe la necesidad de una gestión proactiva de las relaciones y de adherencia a los contratos, que se extiende más allá de la firma del contrato inicial y de las auditorías. Los proveedores de servicios en la nube evolucionan constantemente sus productos y servicios para seguir siendo competitivos; estas innovaciones continuas pueden exceder, estirar o no estar cubiertas por los acuerdos existentes y las evaluaciones.

- Los clientes en la nube tienen una necesidad reducida (y una reducción de costes asociada) de gestionar los riesgos que acepta el proveedor de servi-

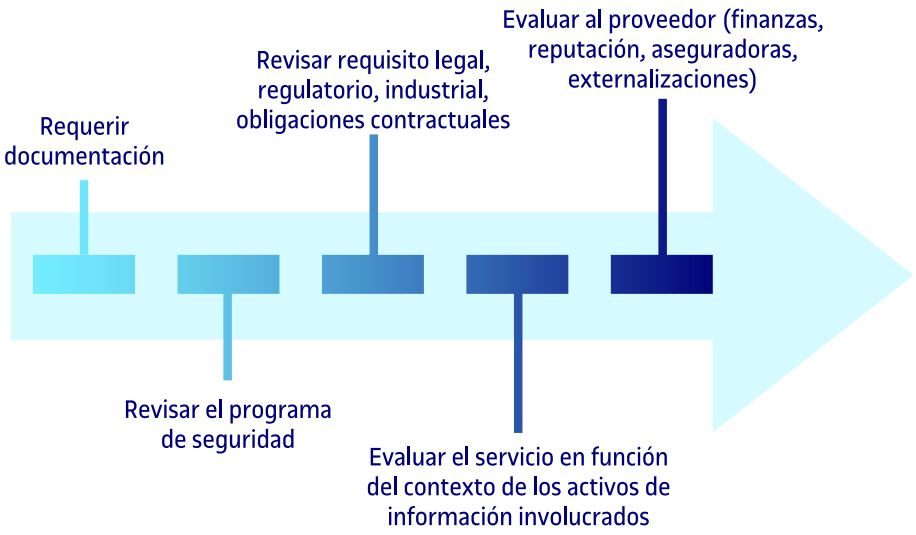
cios en la nube bajo el modelo de responsabilidad compartida. No se externaliza la responsabilidad de gestionar el riesgo, pero sin duda se puede externalizar la gestión de algunos riesgos.

## 2.6. Herramientas para la gestión del riesgo en la nube

Los siguientes procesos ayudan a formar la base de la gestión del riesgo en los despliegues de computación en la nube. Uno de los principios básicos de la gestión de riesgos es que se puede gestionar, transferir, aceptar o evitar riesgos. Sin embargo, todo ha de comenzar con una evaluación adecuada.

La evaluación del proveedor sienta las bases para el programa de gestión de riesgos en la nube:

Figura 4. Proceso de evaluación de referencia




Fuente: CSA.

- Revisar periódicamente las auditorías y evaluaciones para asegurar que están actualizadas.

- No asumir que todos los servicios de un proveedor en particular cumplen con los mismos estándares de auditoría/evaluación. Pueden variar. Las evaluaciones periódicas deben programarse y automatizarse si es posible. Después de revisar y comprender qué riesgos gestiona el proveedor de servicios en la nube, lo que queda es el riesgo residual. El riesgo residual a menudo se puede gestionar mediante la implementación de controles (por ejemplo, encriptación). La disponibilidad e implementación específica de controles del riesgo varía mucho entre los proveedores en la nube, en particular según los servicios/características, los modelos de servicio y su despliegue. Si después de las evaluaciones y los controles que se hayan implementado todavía hay un riesgo residual, las únicas opciones son transferirlo, aceptar el riesgo o evitarlo.

- Transferir el riesgo, a menudo mediante un seguro, es un mecanismo imperfecto, especialmente para riesgos de la información. Algunas de las pérdidas financieras asociadas se pueden compensar con un elemento clave perdido, pero no ayudará con la pérdida de un evento secundario (como la pérdida de clientes) –especialmente una pérdida intangible o difícil de cuantificar, como el daño reputacional–. Desde la perspectiva de las compañías de seguros, el «ciber-seguro» es también un campo incipiente, sin la profundidad de las tablas actuariales utilizadas por otras formas de seguro, como los de fuego o inundación; e incluso la compensación financiera puede no ajustarse al coste asociado con el evento primario perdido. Conviene comprender los límites.

## 2.7. Recomendaciones en el gobierno de servicios de *cloud computing*

**Recomendaciones**

- Identificar las responsabilidades compartidas de seguridad y gestión del riesgo basadas en la elección del despliegue de la nube y del modelo de servicio. Desarrollar un marco de trabajo/modelo de gobernanza de la nube basado en las mejores prácticas de la industria más relevantes, estándares globales y regulaciones como CSA CCM, COBIT 5, NIST RMF, ISO/IEC 27017, HIPAA, PCI DSS, EU GDPR, etc.
- Comprender cómo afecta un contrato a su marco de trabajo/modelo de gobernanza.
- Obtener y revisar los contratos (y cualquier documento referenciado) antes de llegar a un acuerdo.
- No asumir que se puede negociar eficazmente un contrato con un proveedor de servicios en la nube, pero esto tampoco debería impedir el uso de ese proveedor.
- Si un contrato no puede ser negociado eficazmente y percibe un riesgo inaceptable, considerar mecanismos alternativos para gestionar este riesgo (por ejemplo, la monitorización o encriptación).
- Desarrollar un proceso para las evaluaciones del proveedor de servicios en la nube. Proceso que debería incluir:
  - Revisión del contrato.
  - Revisión del cumplimiento legal reportado por la propia organización.
  - Documentación y políticas.
  - Auditorías y evaluaciones disponibles.
  - Revisiones de servicio adaptándose a los requisitos del cliente.
  - Fuertes políticas de gestión del cambio para monitorizar por parte de la organización de los cambios en el uso de los servicios en la nube.
  - Reevaluaciones –si son posibles– que deben realizarse de forma programada o automatizarse.
- Ofrecer un acceso fácil a la documentación y a los informes que se necesiten por los potenciales clientes de cara a las evaluaciones. Por ejemplo, el registro CSA STAR.
- Alinear los requisitos de riesgo con los activos específicos involucrados y la tolerancia al riesgo para esos activos.

- Crear una metodología específica de gestión de riesgos y de aceptación/mitigación de estos para evaluar los riesgos de cada solución.
- Usar controles para gestionar los riesgos residuales. Si los riesgos residuales permanecen, elegir aceptar o evitar los riesgos.
- Utilizar herramientas para buscar proveedores autorizados según el tipo de activo (por ejemplo, vinculado a la clasificación de datos), el uso de la nube y la gestión.

# 3. Gestión de ciberincidentes

Los ataques contra los sistemas de información son, cada día, no solo más numerosos y diversos, sino también más peligrosos o potencialmente dañinos. Aunque las acciones y medidas preventivas, adoptadas según los resultados obtenidos en los preceptivos análisis de riesgos a los que deben someterse todos los sistemas públicos, contribuyen sin lugar a dudas a reducir el número de ciberincidentes, la realidad nos muestra que, desafortunadamente, no todos los ciberincidentes pueden prevenirse.

Por lo tanto, es necesario disponer de una adecuada capacidad de respuesta a ciberincidentes que, al detectar rápidamente ataques y amenazas, minimice la pérdida o la destrucción de activos tecnológicos o de información, mitigue la explotación dañina de los puntos débiles de las infraestructuras y alcance la recuperación de los servicios en la mayor brevedad posible. A continuación, se ofrecen algunas pautas para un buen manejo de ciberincidentes y para determinar la respuesta más adecuada, dependiendo del tipo concreto de incidente, con independencia de la plataforma tecnológica subyacente, el hardware, los sistemas operativos o las aplicaciones.

Gestionar adecuadamente ciberincidentes constituye una actividad compleja que contempla: la adopción de métodos para recopilar y analizar datos y eventos; metodologías de seguimiento; procedimientos de tipificación de la peligrosidad y de priorización; determinar los canales de comunicación con otras unidades o entidades propias o ajenas a la organización, etc.

Debido a la complejidad que entrañan todas estas actividades, la consecución de una capacidad de respuesta eficaz a ciberincidentes exige una planificación escrupulosa y una asignación adecuada y suficiente de los recursos necesarios.

Además, en los casos en los que se requiere la colaboración de personal ajeno a la organización, como en entornos basados en *cloud computing*, la complejidad de la gestión se agrava. En estos entornos, la labor del proveedor se centra básicamente en actividades de respuesta ante la ocurrencia de algún incidente de seguridad. Esto incluye: la verificación, el análisis del ataque, la contención, la recolección de evidencias, la aplicación de remedios y la restauración del servicio.

La colaboración entre proveedores y suscriptores del servicio para la detección y reconocimiento de incidentes es esencial para la seguridad y la privacidad en entornos de *cloud computing*, ya que la complejidad de los servicios puede

dificultar la labor de detección. Para una mejor coordinación entre las diferentes partes, es necesario negociar los procedimientos de respuesta a incidentes y plasmar el resultado de las negociaciones en un contrato de servicio. Entre otros aspectos, es importante que este tipo de contrato contemple:

- La localización de los datos.

- La creación de equipos mixtos (proveedor y suscriptor) que se involucren en la resolución de incidentes que pueden afectar a alguna de las partes de forma individual, a ambas partes conjuntamente, o incluso a otros suscriptores que compartan la infraestructura. De esta manera, se pretende mitigar los incidentes en un tiempo que limite los daños y mejore los tiempos de recuperación.

A continuación, se ofrece una breve introducción al proceso de respuesta de ciberincidentes, y posteriormente se presentan un conjunto de políticas de seguridad de la información como buenas prácticas para ayudar en la gestión de ciberincidentes.

### 3.1. El proceso de respuesta a ciberincidentes

El beneficio más significativo para las organizaciones de poseer una adecuada capacidad de respuesta a ciberincidentes es abordar su gestión de manera sistemática (es decir, siguiendo una metodología consistente y consolidada), lo que facilita la adopción de las medidas más adecuadas.

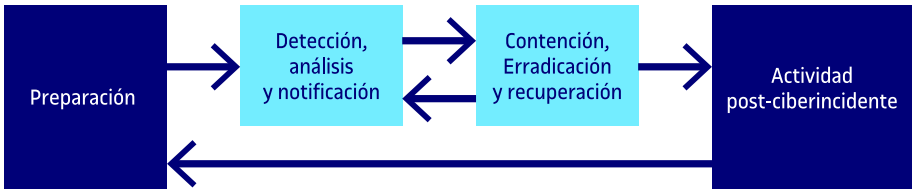
Así, una correcta capacidad de respuesta ayuda a los equipos de seguridad a minimizar la pérdida o exfiltración de información, y también a minimizar la interrupción de los servicios. Otro de sus beneficios es la posibilidad de utilizar información obtenida durante la gestión de los ciberincidentes para mejorar la respuesta a incidentes de seguridad futuros y, en consecuencia, proporcionar una mayor y mejor protección de los sistemas.

El siguiente apartado contiene una breve introducción a las principales fases de la gestión de ciberincidentes que permite a las organizaciones tomar una aproximación adecuada y sistemática de este proceso.

### 3.2. Fases en la gestión de ciberincidentes

Tal y como se puede apreciar en el diagrama de la figura de abajo, la gestión de ciberincidentes consta de cuatro fases principales: preparación; detección, análisis y notificación; contención, erradicación y recuperación, y actividad posciberincidente.

Figura 5. Ciclo de vida de la respuesta de un ciberincidente




Fuente: CCN-CERT.

La fase inicial contempla la formación de un equipo de respuesta a incidentes (ERI) y la selección de las herramientas y los recursos necesarios. Durante esta **fase de preparación**, la organización, atendiendo a un análisis previo de riesgos, identifica y despliega un determinado conjunto de medidas de seguridad.

La adecuada implantación de estas medidas ayuda, posteriormente, en la **fase de detección, análisis y notificación**, a detectar posibles brechas de seguridad en los sistemas de información de la organización, lo que desencadena procesos de notificación.

En la **fase de contención, erradicación y recuperación** de un ciberincidente, la organización debe, en primera instancia, mitigar el impacto producido. Posteriormente, se procederá a la eliminación de la causa del incidente de los sistemas afectados y, por último, a recuperar, en la medida de lo posible, el modo normal de funcionamiento del sistema. Durante esta fase, es necesario persistir cíclicamente en el análisis de las amenazas, de cuyos resultados se desprenden, paulatinamente, nuevos mecanismos de contención y erradicación.

En la **fase de actividad posciberincidente**, los responsables de la organización emiten un informe del ciberincidente para detallar su origen, su coste (especialmente, en términos de información comprometida o de impacto en los servicios prestados) y las medidas que la organización debe tomar para prevenir futuros ciberincidentes de naturaleza similar.

### 3.3. Políticas de seguridad de la información y de gestión de ciberincidentes

Las buenas prácticas en seguridad señalan la necesidad de disponer de una política de seguridad reconocida y que sea ampliamente conocida por los miembros de la organización. Normativas como el Esquema Nacional de Seguridad (ENS) establecen los requisitos mínimos que debe contemplar toda política de seguridad. Entre estos requisitos, toda organización ha de especificar:

- La posición del equipo de respuesta a incidentes (ERI), sus competencias y autoridad, dentro de la estructura de la organización, y la definición de los roles y responsabilidades de cada unidad.

- La normativa de seguridad.

- Una definición de ciberincidentes que considerar teniendo en cuenta un análisis de riesgos y términos de referencia usados.

- Criterios para la comunicación de ciberincidentes y para el intercambio de información, interna y externamente.

- Un nivel de peligrosidad de los ciberincidentes.

- Procedimientos operativos de seguridad.

- Mecanismos para la notificación de informes de ciberincidentes.

- Formularios de notificación, comunicación e intercambio de información.

- Un plan de respuesta a ciberincidentes.

Es recomendable que los organismos posean un plan de respuesta a ciberincidentes que dé adecuada respuesta a sus requisitos específicos, atendiendo a la misión, el tamaño, la estructura y las funciones de la organización. El plan debe, asimismo, determinar y asegurar que se disponen de los recursos humanos y materiales necesarios, y ha de contar con el imprescindible apoyo por parte de la dirección.

Una vez que la dirección de una organización ha redactado y aprobado el plan de respuesta a ciberincidentes, se inicia su implantación. El plan debe ser revisado, al menos, anualmente, para asegurar que la organización está siguiendo adecuadamente la hoja de ruta para una mejora continua.

# 4. Gestión de riesgos e incidentes de seguridad en *cloud*

La manera de empezar que hemos considerado para este apartado no es en ningún caso la habitual, pero en el camino de la adopción del *cloud computing* y todo lo que implica es importante situar el punto en el que nos encontramos y el objetivo.

**Gestión de riesgos - cuestionario de evaluación**

Las preguntas críticas que las organizaciones deben hacerse a sí mismas y a sus proveedores de la nube durante cada paso son las siguientes:

**1. Asegurar eficazmente la gobernanza, el riesgo y los procesos de cumplimiento**

- ¿Qué normas de seguridad y privacidad de la información o qué regulaciones se aplican a la nube de dominio por el cliente?
- ¿El cliente tiene procesos de gobierno y de cumplimiento para el uso del servicio en la nube?
- De acuerdo con los requerimientos del cliente, ¿el proveedor tiene procesos apropiados de gobernanza y notificación?
- ¿Está claro qué controles legales y regulatorios se aplican a los servicios del proveedor?
- ¿Qué contemplan los acuerdos en cuanto a servicio sobre la división de responsabilidades de seguridad entre proveedor y cliente?
- ¿Existe un riesgo relacionado con la ubicación de los datos?

**2. Auditoría. Presentación de informes operacionales y procesos de negocio**

- ¿Existe alguna certificación demostrable por parte del proveedor? La información de auditoría se ajusta a una de las normas para la auditoría de seguridad, como ISO 27001/27002.
- ¿Tiene el proveedor mecanismos para informar a los clientes tanto de aspectos rutinarios como de comportamiento excepcional relacionado con sus servicios?
- ¿Los controles de seguridad abarcan no solo los propios servicios en la nube, sino también las interfaces de gestión ofrecidas a los clientes?
- ¿Existe un proceso de notificación de incidentes y gestión de incidentes críticos?

**3. Administrar a las personas, roles e identidades**

- ¿Ofrecen los servicios del proveedor un control de acceso de tipo granular?
- ¿Puede el proveedor proporcionar informes para supervisar el acceso de los usuarios?
- ¿Es posible integrar o federar sistemas de gestión de identidad de clientes con las instalaciones de gestión de identidad del proveedor?

**4. Asegurar la correcta protección de datos e información**

- ¿Existe un catálogo de todos los activos de datos que se utilizarán o almacenarán en la nube?

- ¿Hay una descripción de roles responsables?
- ¿Se ha tenido en cuenta el tratamiento de todas las formas de datos, en particular datos como vídeos e imágenes?
- ¿Existe una separación de entornos adecuada entre clientes?
- ¿Se han aplicado las medidas adecuadas de confidencialidad e integridad de los datos almacenados?

**5. Políticas de privacidad**

- ¿Los servicios del proveedor cuentan con controles apropiados para manejar datos personales?
- ¿Existen restricciones de localización geográfica de los datos en el acuerdo de servicio?
- Si hay un incumplimiento sobre el tratamientos de los datos, el proveedor es responsable de informar y resolverlo. ¿Están claras las prioridades y los plazos?

**6. Evaluar la seguridad de las aplicaciones**

- Basándose en el modelo que se aplique (IaaS, PaaS, SaaS), ¿está claro quién tiene la responsabilidad de la seguridad de las aplicaciones (cliente o proveedor)?
- Si es el cliente, ¿tiene políticas y metodologías establecidas para asegurar los controles de seguridad apropiados para cada aplicación?
- Si es el proveedor, ¿el acuerdo de servicio en la nube hace que sus responsabilidades sean claras y que existan controles de seguridad específicos para ser aplicados a la aplicación?
- En cualquier caso, ¿la aplicación hace uso de técnicas de cifrado adecuadas para proteger los datos y las transacciones de los usuarios?

**7. Asegurar la red**

- ¿Es posible la detección o inspección del tráfico de la red?
- ¿Qué capacidad tiene el proveedor para hacer frente a los ataques de denegación de servicio?
- ¿Tiene la red del proveedor la capacidad de detener y prevenir intrusiones?
- ¿Está el acceso a la red del cliente separado del acceso a la red del proveedor?

**8. Controles de la infraestructura física**

- ¿Puede el proveedor de servicios en la nube demostrar los controles de seguridad apropiados aplicados a su infraestructura física e instalaciones?
- ¿Dispone el proveedor de servicios de instalaciones para garantizar la continuidad frente a amenazas o fallos en el equipamiento?

**9. Términos del acuerdo de nivel de servicio**

- ¿El acuerdo de servicio especifica las responsabilidades de seguridad del proveedor y del cliente?
- ¿El acuerdo de servicio requiere que todos los términos de seguridad deban también aplicarse a cualquier proveedor de servicios utilizado por el proveedor?
- ¿El acuerdo de servicio cuenta con métricas para medir el desempeño y eficacia de seguridad?
- ¿El contrato de servicio documenta explícitamente los procedimientos de notificación y gestión de incidentes de seguridad?

**10. Requerimientos de seguridad del proceso de salida o fin de contrato**

- ¿Existe un proceso documentado de salida como parte del servicio?
- ¿Está claro que todos los datos de los clientes del servicio en la nube se borran en el momento de finalizar el proceso de migración o salida?
- ¿Los datos de los clientes de servicios en la nube están protegidos contra pérdidas o incumplimientos durante la salida?

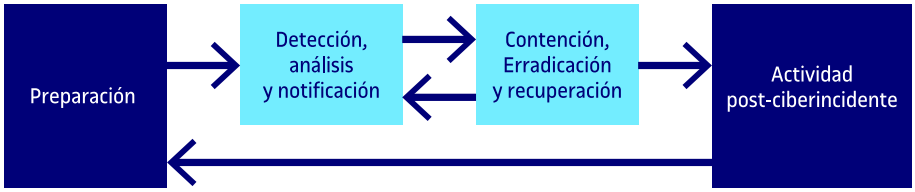
### 4.1. Respuesta a incidentes en entornos *cloud*

La labor del proveedor es básica en las actividades de respuesta ante la ocurrencia de algún incidente de seguridad. Esto incluye la verificación, el análisis del ataque, la contención, la recolección de evidencias, la aplicación de remedios y la restauración del servicio.

La colaboración entre los proveedores y los suscriptores para la detección y el reconocimiento de los incidentes es esencial para la seguridad y la privacidad en *cloud computing*, ya que la complejidad de los servicios puede dificultar la labor de la detección.

Se hace necesario entender y negociar los procedimientos de respuesta a incidentes antes de firmar un contrato de servicio. La localización de los datos también puede impedir una investigación, por lo que es otro de los puntos que se deben negociar en los contratos.

Figura 5. Ciclo de vida de la respuesta a ciberincidentes




Fuente: CCN-CERT.

La solución que se negocie ha de tener la finalidad de mitigar el incidente en un tiempo que limite los daños y que mejore los tiempos de recuperación. Los equipos para la resolución deberían ser mixtos (proveedor y suscriptor), porque la solución puede involucrar a alguna de las partes de forma individual o a ambas conjuntamente, y el incidente puede incluso afectar a otros suscriptores que comparten la infraestructura.

#### 4.1.1. Eventos y ciberincidentes

Los ataques contra los sistemas de información son, cada día, no solo más numerosos y diversos, sino también más peligrosos o potencialmente dañinos. Aunque las acciones y medidas preventivas, adoptadas sobre la base de los resultados obtenidos de los preceptivos análisis de riesgos a los que deben so-

meterse todos los sistemas públicos, contribuyen sin lugar a dudas a reducir el número de ciberincidentes, la realidad nos muestra que, desafortunadamente, no todos los ciberincidentes pueden prevenirse.

Por tanto, se hace necesario disponer de la adecuada capacidad de respuesta a ciberincidentes que, detectando rápidamente ataques y amenazas, minimice la pérdida o la destrucción de activos tecnológicos o de información, mitigue la explotación dañina de los puntos débiles de las infraestructuras y alcance la recuperación de los servicios a la mayor brevedad posible. Este apartado ofrece pautas para el manejo de ciberincidentes y la determinación de la respuesta más adecuada a cada tipo, independientemente de la plataforma tecnológica subyacente, el hardware, los sistemas operativos o las aplicaciones.

Puesto que gestionar adecuadamente los ciberincidentes constituye una actividad compleja que contempla la adopción de métodos para recopilar y analizar datos y eventos, metodologías de seguimiento, procedimientos de tipificación de su peligrosidad y priorización, así como la determinación de canales de comunicación con otras unidades o entidades, propias o ajenas a la organización, la consecución de una capacidad de respuesta eficaz a ciberincidentes exige una planificación escrupulosa y la correspondiente asignación de recursos, adecuados y suficientes.

### 4.1.2. La respuesta a los ciberincidentes

Para las organizaciones, el beneficio más significativo de poseer una adecuada capacidad de respuesta a ciberincidentes es abordar su gestión de forma sistemática (es decir, siguiendo una metodología consistente y consolidada), lo que facilita la adopción de las medidas adecuadas.

Así, una correcta capacidad de respuesta a ciberincidentes ayuda a los equipos de seguridad responsables a minimizar la pérdida o exfiltración de información o la interrupción de los servicios. Otro de sus beneficios es la posibilidad de utilizar la información obtenida durante la gestión del ciberincidente para preparar mejor la respuesta a incidentes de seguridad futuros y, en su consecuencia, proporcionar una mayor y mejor protección a los sistemas.

### 4.1.3. Política de seguridad de la información y gestión de ciberincidentes

Las buenas prácticas en seguridad señalan la necesidad de una política de seguridad reconocida y conocida en la organización. Normativas como el Esquema Nacional de Seguridad (ENS) establecen los requisitos mínimos que debe contemplar toda política de seguridad, entre estos, los incidentes de seguridad, para los que debe especificarse:

- La posición del equipo de respuesta a ciberincidentes (ERI), sus competencias y autoridad, dentro de la estructura de la organización y la definición de los roles y las responsabilidades de cada unidad.

- La normativa de seguridad.

- La definición de los ciberincidentes considerados a tenor del análisis de los riesgos y los términos de referencia usados.

- Los criterios para la comunicación de ciberincidentes y, en su caso, el intercambio de información, interna y externamente.

- El nivel de peligrosidad de los ciberincidentes.

- Los procedimientos operativos de seguridad.

- Los mecanismos para la notificación de informes de ciberincidentes.

- Los formularios de notificación, comunicación e intercambio de información.

- Los elementos del plan de respuesta a ciberincidentes.

Los organismos del ámbito de aplicación del ENS, en este caso la Administración pública, deben poseer un plan de respuesta a ciberincidentes que dé adecuada respuesta a sus requisititos específicos, atendiendo a la misión, el tamaño, la estructura y las funciones de la organización. El plan debe, asimismo, determinar y asegurar que se disponen de los recursos humanos y materiales necesarios y ha de contar con el imprescindible apoyo por parte de la dirección.

Una vez que la organización ha redactado y aprobado por su dirección el plan de respuesta a ciberincidentes, se iniciará su implantación. El plan debería ser revisado, al menos, anualmente, para asegurar que la organización está siguiendo adecuadamente la hoja de ruta para una mejora continua.

### 4.1.4. La gestión de los ciberincidentes

La gestión de ciberincidentes consta de varias fases:

La fase inicial contempla la creación y formación de un equipo de respuesta a ciberincidentes (ERI) y la utilización de las herramientas y recursos necesarios.

Durante esta fase de **preparación**, la organización, atendiendo a un previo análisis de riesgos, habrá identificado y desplegado un determinado conjunto de medidas de seguridad. La adecuada implantación de las medidas ayudará

a detectar las posibles brechas de seguridad de los sistemas de información de la organización y su análisis, en la fase de **detección, análisis y notificación**, desencadenando los procesos de notificación a los que hubiere lugar.

La organización, en la fase de **contención, erradicación y recuperación** del ciberincidente, y atendiendo a su peligrosidad, deberá intentar, en primera instancia, mitigar su impacto, procediendo después a su eliminación de los sistemas afectados y tratando finalmente de recuperar el sistema al modo de funcionamiento normal. Durante esta fase, será necesario, cíclicamente, persistir en el análisis de la amenaza, de cuyos resultados se desprenderán, paulatinamente, nuevos mecanismos de contención y erradicación.

Tras el incidente, en la fase de **actividad posciberincidente**, los responsables de la organización emitirán un informe del ciberincidente que detallará su causa originaria y su coste (especialmente, en términos de compromiso de información o de impacto en los servicios prestados) y las medidas que la organización debe tomar para prevenir futuros ciberincidentes de naturaleza similar.

### 4.2. Cómo afecta la nube al proceso de respuesta a incidentes

Cada una de las fases del ciclo de vida se ve afectada, en distinto grado, en un despliegue en la nube. Algunas de las fases son similares a la respuesta ante incidentes en un entorno externalizado, en el que es necesaria la coordinación con un tercero. Otras diferencias son más específicas de la naturaleza abstracta y automatizada de la nube.

#### 4.2.1. Preparación

Estas son las consideraciones más importantes a la hora de prepararse para la respuesta ante incidentes en la nube.

- SLA y gobierno: Todo incidente que involucre a un proveedor de alojamiento o una nube pública requiere la comprensión de los acuerdos de nivel de servicio (SLA, *service level agreements*), y probablemente la coordinación con el proveedor de servicios en la nube. Hay que tener en cuenta que, dependiendo de la relación con el proveedor, es posible no disponer de puntos de contacto directos, estando limitados a lo que pueda estar disponible en el soporte estándar. Una nube privada personalizada en un centro de datos de terceros tendrá una relación muy distinta de una aplicación SaaS que requiere el registro en un sitio web y la aceptación de un acuerdo de licencia.

- IaaS/PaaS frente a SaaS: ¿Cómo se proveen los datos específicos de la nube de tu organización en un entorno multiusuario? Para cada servicio principal se debería entender y documentar qué datos y registros estarán disponibles en caso de un incidente. No se debe asumir que se puede contactar

con un proveedor después de un incidente y recoger datos que normalmente no están disponibles.

- Herramientas de análisis forense: Conjunto de herramientas necesarias para realizar una investigación de forma remota (como suele suceder con recursos basados en la nube). Por ejemplo: ¿se tienen herramientas para recoger registros y metadatos de la plataforma en la nube? ¿Se tienen los conocimientos necesarios para interpretar la información? ¿Cómo se obtienen imágenes de máquinas virtuales en ejecución y a qué tipo de datos se tiene acceso: almacenamiento en disco o memoria volátil?

- Diseño de un entorno en la nube para una rápida detección, investigación y respuesta (contención y recuperación). Esto significa asegurar que se tiene una arquitectura y configuración adecuadas para facilitar la respuesta ante incidentes:
  - Habilitar la instrumentación de la información, como los *logs* de API ofrecidas por la nube, y garantizar que son enviados a una localización segura para que los investigadores los tengan disponibles en caso de un incidente.
  - Utilizar el aislamiento para asegurar que los ataques no pueden propagarse y comprometer el entorno por completo.
  - Implementar mapas de la pila de aplicación para comprender dónde van a residir los datos para, de esta forma, tener en cuenta diferencias geográficas que afecten a la captura de datos y monitorización.
  - Realizar un modelado de amenazas y ejercicios sobre el papel puede ser muy útil a la hora de determinar las estrategias más efectivas de contención de distintos tipos de ataques a diversos componentes de la pila del servicio en la nube.
  - Incluir, en cada caso, las diferencias a la respuesta en IaaS, PaaS y SaaS.

### 4.2.2. Detección y análisis

La detección y el análisis en un entorno en la nube pueden parecer prácticamente lo mismo (para entornos IaaS) o ser muy diferentes (en entornos SaaS). En cualquier caso, el alcance de la monitorización debe cubrir toda la gestión del servicio en la nube (plano de gestión), no solo los activos desplegados.

De cara a acelerar el proceso de respuesta, es posible aprovechar la monitorización propia de la nube y las alertas capaces de iniciar un flujo automatizado de RI. Algunos proveedores de servicios en la nube ofrecen estas características dentro de sus plataformas, y también están disponibles soluciones de monitorización de terceros. Estas soluciones no tienen por qué ser específicas de

seguridad: muchas plataformas en la nube (IaaS y posiblemente PaaS) ofrecen una variedad de métricas de monitorización en tiempo real o cuasi real por motivos operativos y de rendimiento.

Estas métricas pueden ser utilizadas desde el punto de vista de seguridad. Las plataformas en la nube ofrecen también una variedad de registros que pueden ser, en algunos casos, integrados en las operaciones de seguridad y monitorización. Se pueden tener desde registros operacionales hasta un registro completo de todas las llamadas a API, o la actividad de gestión del servicio. Hay que tener en cuenta que no están disponibles en todos los proveedores; es más habitual tenerlos en entornos IaaS y PaaS que SaaS.

Cuando no existen mecanismos de envío de registros, es posible usar la consola que proporciona acceso al «tenant» contratado para identificar cambios en la configuración o en el entorno. Las fuentes de datos en incidentes en la nube pueden ser bastante distintas de aquellas empleadas en la respuesta ante incidentes tradicional. Aunque hay un solapamiento significativo (como en los registros de sistema), existen diferencias en las formas en las que recopila la información en lo relativo a las nuevas fuentes, como los mecanismos de alimentación de los entornos de gestión en la nube.

Como se ha mencionado, los registros de las plataformas de servicios en la nube pueden ser una opción, pero no están disponibles de manera universal. Idealmente, estos registros deberían mostrar toda la actividad del entorno de gestión.

> Es importante comprender qué información se guarda, así como los vacíos que pudieran afectar al análisis de un incidente. ¿Se registran todas las actividades de gestión? ¿Se incluyen todas las actividades automatizadas del sistema (como el autoescalado) o las actividades de gestión del proveedor de servicios en la nube?

En el caso de un incidente grave, los proveedores pueden tener acceso a otros registros que habitualmente no están disponibles para los clientes.

Un reto a la hora de la recolección de información puede ser la visibilidad limitada de la red. Los registros de red de un proveedor tienden a ser registros de flujos, no una captura completa de paquetes.

Donde existan vacíos siempre es posible instrumentar la pila de tecnología con mecanismos propios de registro. Esto puede aplicarse a instancias, contenedores y código de aplicación para permitir obtener telemetría vital en una

posible investigación. Hay que prestar atención especial a las arquitecturas de aplicación sin servidores y a PaaS; es probable que sea necesario añadir registros personalizados en el ámbito de la aplicación.

La inteligencia de amenazas externa puede ser también útil, como en los servicios de computación más tradicional, a la hora de identificar indicadores de compromiso y conseguir información sobre los adversarios. Hay que ser consciente de los retos potenciales existentes cuando la información que un CSP (*cloud service provider*) provee se enfrenta a cuestiones relativas a la cadena de custodia. Hoy en día, no hay precedentes fiables establecidos al respecto. El soporte para las investigaciones y el análisis forenses debe también adaptarse y entender los cambios producidos a las fuentes de datos. Hay que fijarse siempre en lo que el CSP puede proveer y si cumplen los requisitos de cadena de custodia. No todos los incidentes provocan una acción legal, pero es importante trabajar con el equipo legal para entender los límites y dónde se puede terminar teniendo problemas con la cadena de custodia.

Hay una mayor necesidad de automatizar muchos de los procesos forenses y de investigación en la nube, debido a su naturaleza dinámica y de alta velocidad.

**Ejemplo**

Es posible perder evidencias debido a una actividad normal de autoescalado, o si un administrador decide apagar una máquina virtual involucrada en una investigación.

Algunos de los ejemplos de tareas que pueden ser automatizadas incluyen:

- Realizar una instantánea (*snapshot*) del almacenamiento de la máquina virtual.

- Capturar los metadatos en el momento de la alerta, para que el análisis pueda basarse en cómo estaba la infraestructura en dicho momento.

- Si el proveedor lo soporta, «pausar» la máquina virtual, lo que guardará el estado de la memoria del sistema. Siempre se puede aprovechar las capacidades de una plataforma en la nube para determinar el alcance potencial de un compromiso.

- Analizar flujos de red para comprobar si el aislamiento de red fue eficaz. Es posible usar llamadas a una API para realizar una instantánea del estado de la red y de las reglas del cortafuegos virtual, lo que puede aportar una imagen exacta de toda la pila en el momento del incidente.

- Examinar los datos de la configuración para comprobar si otras instancias similares fueron comprometidas en el mismo ataque.

- Revisar registros de acceso a datos (para el almacenamiento basado en la nube, si están disponibles) y del panel de gestión para ver si el incidente ha afectado o alcanzado a la plataforma en la nube.

- Las arquitecturas PaaS y sin servidor requerirán una correlación adicional entre la plataforma en la nube y cualquier registro de aplicación autogenerado.

### 4.2.3. Contención, erradicación y recuperación

Siempre hay que empezar garantizando que el plano de control de los servicios en la nube y su metaestructura están libres de ataques. Esto incluirá con frecuencia la invocación de procedimientos de urgencia, para tener acceso a las credenciales maestras de la cuenta en la nube, para confirmar de esta manera que la actividad del atacante no está siendo ocultada o enmascarada a la vista de cuentas de menor privilegio que la del administrador. Hay que recordar que no es posible contener un ataque si los atacantes mantienen acceso al panel de gestión. Los ataques a activos en la nube, como las máquinas virtuales, pueden en ocasiones revelar credenciales del panel de gestión que luego son usadas como un puente a un ataque más amplio y serio.

La nube ofrece, a menudo, mucha más flexibilidad en esta fase de la respuesta, especialmente en IaaS.

La infraestructura definida por software permite una rápida reconstrucción desde cero en un entorno limpio, y para ataques más aislados, las características inherentes de la nube –grupos de autoescalado, llamadas a API para cambiar la configuración de redes o máquinas virtuales y las instantáneas– pueden acelerar los procesos de cuarentena, erradicación y recuperación.

Por ejemplo, en muchas plataformas es posible poner en cuarentena, de forma instantánea, una máquina virtual moviéndola fuera del grupo de autoescalado, aislándola con un cortafuegos virtual y reemplazándola. Esto implica, a su vez, que no hay una necesidad inmediata de «erradicar» al atacante antes de identificar sus mecanismos de explotación y el alcance de la brecha, ya que como la nueva infraestructura o instancia están limpias es posible, en su lugar, simplemente aislarlo.

De todas formas, sigue siendo necesario asegurar que el camino de explotación utilizado está cerrado y no puede ser usado para infiltrarse, de nuevo, en otros activos en producción. Si existe alguna duda de que el panel de administración ha sido comprometido, hay que estar seguro de que las plantillas o configuraciones para las nuevas infraestructuras o aplicaciones no han sido comprometidas a su vez.

Dicho esto, estas capacidades no son siempre universales: con SaaS y algunos PaaS se puede estar muy limitado y por ello depender, en mayor medida, del proveedor de servicios en la nube.

### 4.3. Actividades posincidente

Como con cualquier ataque, hay que trabajar con el equipo de respuesta interno y el proveedor para analizar qué funcionó bien y qué no funcionó para identificar los puntos de mejora. Se debe prestar especial atención a las limitaciones de los datos recogidos y averiguar cómo resolver los problemas encontrados. Es complicado cambiar los SLA, pero si los tiempos de respuesta, datos o cualquier otro apoyo acordado fueron insuficientes, hay que intentar renegociarlos.

**Recomendaciones**

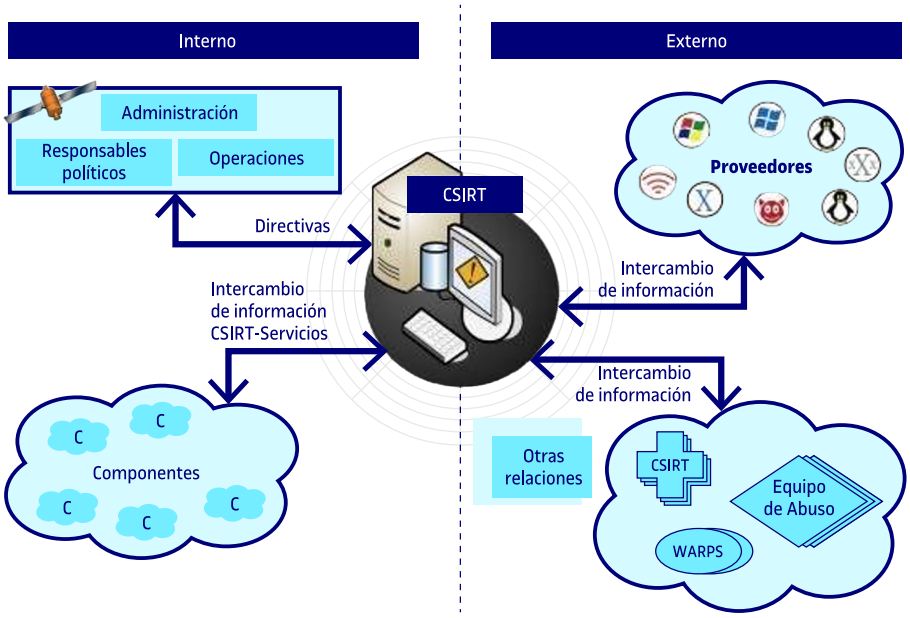
- Los aspectos más importantes de la respuesta ante incidentes en entornos en la nube son los SLA y el establecimiento de las expectativas sobre qué tiene que hacer el cliente frente a qué tiene que hacer el proveedor. Una comunicación clara de roles y responsabilidades y la práctica, tanto de la respuesta como de los trasvases de información, son críticas.
- Los clientes deben establecer canales de comunicación claros con el proveedor que puedan ser empleados en el caso de un incidente. Los estándares abiertos existentes pueden facilitar la comunicación del incidente.
- Los clientes deben comprender el contenido y formato de los datos que el proveedor de servicios en la nube puede proporcionar para su análisis, y evaluar si los datos forenses satisfacen los requisitos legales de la cadena de custodia.
- Los clientes en la nube deberían adoptar esquemas de monitorización continua y de recursos en la nube para detectar los problemas de forma más temprana que en centros de datos tradicionales.
  - Las fuentes de datos deberían de ser almacenadas o copiadas en localizaciones que mantengan la disponibilidad durante incidentes.
  - Si fuera posible y necesario, deberían de ser manejadas de forma que se mantenga una cadena de custodia apropiada.
- Las aplicaciones basadas en la nube deberían aprovecharse de la automatización y la orquestación para optimizar y acelerar la respuesta, incluyendo la contención y la recuperación.
- Para cada proveedor de servicios utilizado, la aproximación para detectar y gestionar incidentes que afecten a los recursos alojados en dicho proveedor, debe ser planificada y descrita en el plan de respuesta ante incidentes corporativos.
- Los SLA de cada proveedor de servicios en la nube deben garantizar el soporte a las tareas de gestión de incidentes requeridas para una ejecución efectiva del plan de respuesta ante incidentes corporativos. Se debe cubrir cada etapa del proceso de gestión del incidente: detección, análisis, contención, erradicación y recuperación.
- Las pruebas deben llevarse a cabo anualmente, o cada vez que se produzcan cambios significativos en la arquitectura de la aplicación. Los clientes deberán integrar sus procedimientos de prueba con los de sus proveedores (y otros asociados) en la mayor medida posible.

# 5. Equipos de repuesta a incidentes (CERT/CSIRT)

Un equipo de respuesta ante incidentes de seguridad (CSIRT o *computer security incident response team* en inglés) es un equipo de expertos en seguridad de las TI cuya principal tarea es responder a los incidentes de seguridad informática. El CSIRT presta los servicios necesarios para ocuparse de estos incidentes y ayudar a las organizaciones a recuperarse después de sufrir alguno.

Para mitigar los riesgos y minimizar el número de respuestas necesarias, la mayor parte de los CSIRT ofrece también a sus clientes servicios preventivos y educativos. Por ejemplo, publican avisos sobre las vulnerabilidades de software y hardware en uso e informan a los usuarios sobre programas maliciosos y virus que se aprovechan de estas deficiencias. De este modo, los clientes atendidos pueden corregir y actualizar rápidamente sus sistemas.

Figura 6. Modelo de relación de un CSIRT




Fuente: ENISA.

El término CSIRT es el que se suele usar en Europa en lugar del término protegido CERT, registrado en Estados Unidos por el CERT Coordination Center (CERT/CC). Además, también hay otras siglas para referirse a este tipo de equipos. A continuación listamos las más populares:

- CERT o CERT/CC (equipo de respuesta a emergencias informáticas/centro de coordinación o *computer emergency response team* / *coordination center*).

- CSIRT (equipo de respuesta a incidentes de seguridad informática o *computer security incident response team*).

- IRT (equipo de respuesta a incidentes o *incident response team*).

- CIRT (equipo de respuesta a incidentes informáticos o *computer incident response team*).

- SERT (equipo de respuesta a emergencias de seguridad o *security emergency response team*).

La creación del primer CSIRT se remonta a finales de los años ochenta con la aparición del gusano Morris 2, que se propagó rápidamente e infectó numerosos sistemas de TI en todo el mundo, hasta convertirse en la primera amenaza global a la infraestructura de TI creada por un gusano.

Este incidente generó una alarma que manifestó la necesidad de cooperación y coordinación entre administradores de sistemas y gestores de TI para enfrentarse a este tipo de casos. Era necesario establecer un enfoque más organizado y estructurado de la gestión de los incidentes relacionados con la seguridad de las TI que tuviera en cuenta el tiempo como un factor decisivo. Así, unos días después del incidente con el gusano Morris, la DARPA (Agencia de Investigación de Proyectos Avanzados de Defensa o Defence Advanced Research Projects Agency) creó el primer CSIRT: el CERT Coordination Center (CERT/CC 3), ubicado en la Universidad Carnegie Mellon de Pittsburgh (Pensilvania).

Poco después, el modelo se adoptó en Europa, y en 1992 el proveedor académico holandés SURFnet puso en marcha el primer CSIRT de Europa, denominado SURFnet-CERT. Posteriormente, se crearon otros muchos equipos, y en la actualidad el inventario de actividades de CERT en Europa, redactado por la Agencia Europea de Seguridad de las Redes y de la Información (ENISA, European Union Agency for Network and Information Security, en inglés) incluye más de cien equipos de reconocido prestigio localizados en el continente europeo.

Con el tiempo, los CERT ampliaron sus capacidades y pasaron de ser una mera fuerza de reacción a ser prestadores de servicios de seguridad completos, incluyendo servicios preventivos, como alertas, avisos de seguridad, formación y servicios de gestión de la seguridad, etc. Pronto, el término «CERT» se consideró insuficiente, y a finales de los años noventa se acuñó el término «CSIRT». En la actualidad, tal y como hemos comentado anteriormente, ambos términos (CERT y CSIRT) se usan como sinónimos, si bien CSIRT es el más preciso de los dos. A continuación, detallaremos los sectores y los servicios que ofrecen estos equipos.

### 5.1. Servicios prestados por un CSIRT

Cuando se pone en marcha un CSIRT es muy importante, como con cualquier otro negocio, formarse una idea clara de quiénes forman su grupo de clientes y a qué tipo de entorno se enfocarán los servicios que se presten. Actualmente, los CSIRT suelen prestar servicio a entidades de los sectores siguientes:

- CSIRT del sector académico.
- CSIRT comercial.
- CSIRT del sector de la protección de la información vital y de la información y las infraestructuras críticas (CIP/CIIP).
- CSIRT del sector público.
- CSIRT interno.
- CSIRT del sector militar.
- CSIRT nacional.
- CSIRT del sector de la pequeña y mediana empresa (PYME).
- CSIRT de soporte.

Los servicios que puede llegar a prestar un CSIRT son muy diversos y, de hecho, actualmente ningún CSIRT los presta todos. A continuación, se presenta una breve visión general de todos los servicios conocidos que prestan los CSIRT, tal y como se definen en el Manual del CSIRT publicado por el CERT/CC:

- Alertas y advertencias.
- Tratamiento de incidentes.
- Análisis de incidentes.
- Apoyo a la respuesta a incidentes.
- Coordinación de la respuesta a incidentes.
- Respuesta a incidentes *in situ*.
- Tratamiento de la vulnerabilidad.
- Análisis de la vulnerabilidad.
- Respuesta a la vulnerabilidad.
- Coordinación de la respuesta a la vulnerabilidad.
- Comunicados.
- Observatorio de tecnología.
- Evaluaciones o auditorías de la seguridad.
- Configuración y mantenimiento de la seguridad.
- Desarrollo de herramientas de seguridad.
- Servicios de detección de intrusos.
- Difusión de información relacionada con la seguridad.
- Análisis de instancias.
- Respuesta a las instancias.
- Coordinación de la respuesta a las instancias.
- Gestión de la calidad de la seguridad.
- Análisis de riesgos.
- Continuidad del negocio y recuperación tras un desastre.
- Consultoría de seguridad.

- Sensibilización.
- Educación/formación.
- Evaluación o certificación de productos.

La mayor parte de los CSIRT empiezan ofreciendo servicios de distribución de alertas y advertencias, emiten comunicados y ofrecen tratamiento de incidentes a los distintos clientes. Estos servicios básicos suelen resultar valiosos para los clientes atendidos y normalmente se consideran «valor añadido» real.

En general, se considera una buena práctica al empezar un nuevo CSIRT el hecho de seleccionar un grupo de clientes pequeño, a los que prestar servicios básicos durante un periodo de tiempo piloto, y posteriormente pedirles su opinión y una evaluación del servicio prestado.

Sin embargo, además de tener la opción de externalizar los servicios que ofrece un CSIRT, también existe la opción de tener un CSIRT propio dentro de la propia organización. Las ventajas de contar con un CSIRT propio son:

- Ayudar a las organizaciones a mitigar y evitar los incidentes graves y a proteger su patrimonio.

- Disponer de una coordinación centralizada para las cuestiones relacionadas con la seguridad de las TI dentro de la organización.

- Reaccionar a los incidentes relacionados con las TI y tratarlos de un modo centralizado y especializado.

- Tener al alcance de la mano los conocimientos técnicos necesarios para apoyar y asistir a los usuarios que necesitan recuperarse rápidamente de algún incidente de seguridad.

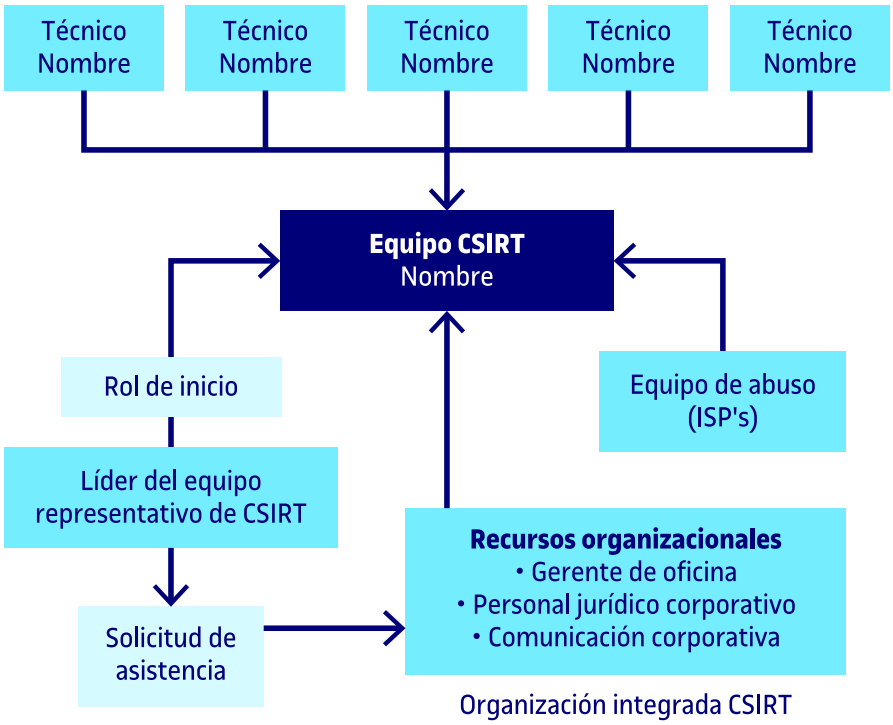
- Tratar las cuestiones jurídicas y proteger las pruebas en caso de pleito.

- Realizar un seguimiento de los progresos conseguidos en el ámbito de la seguridad.

- Fomentar la cooperación en la seguridad de las TI entre los clientes del grupo atendido.

Uno de los modelos organizativos que se suelen seguir cuando una organización decide tener un CSIRT propio es el **modelo incrustado**. Este modelo se crea usando un departamento de TI ya existente. El CSIRT lo dirige un jefe de equipo responsable de las actividades. El jefe de equipo reúne a los técnicos necesarios en el momento de resolver incidentes o trabajar en actividades propias del CSIRT.

Figura 7. Modelo organizativo de un CSIRT interno




Fuente: ENISA.

Este modelo puede evolucionar según el crecimiento de servicios y competencias del equipo de respuesta en la organización. En casos como el de los proveedores de servicios de internet (ISP) está totalmente justificado disponer de personal dedicado a tiempo completo.

## 5.2. Buenas prácticas para el seguimiento efectivo de incidentes

El seguimiento efectivo de los incidentes debe seguir un proceso formal, con personal apropiado y capturando ciertas piezas de datos durante cada caso. Los CSIRT deben considerar cómo los datos de incidentes supuestamente aislados podrían estar vinculados entre sí, de modo que los patrones y las tendencias de estos puedan contribuir tanto a la misión de respuesta a incidentes como a la postura de seguridad general de la organización. Para una buena gestión de los datos de seguridad es esencial el uso de herramientas de seguimiento. A continuación, daremos una explicación introductoria a este tipo de herramientas.

### 5.2.1. Construir el proceso de respuesta con herramientas de seguimiento

Como hemos mencionado anteriormente, los CSIRT consolidados normalmente separan el proceso de respuesta ante incidentes en fases y usan estas fases para guiar el trabajo de los investigadores, analistas y personal de operaciones de TI. Las diferentes tareas propias de cada fase pueden involucrar miembros de diferentes equipos. Para la buena coordinación de todas las personas involucradas en la resolución de incidentes, es conveniente el uso de herramientas de seguimiento que ayuden al grupo a registrar y monitorizar el

desarrollo de las diferentes fases y tareas; analizar alertas, marcar su validez y gravedad, y en consecuencia actuar según un protocolo previamente establecido.

A continuación, mostramos una serie de buenas prácticas que incluyen el uso de herramientas de seguimiento, el registro de los datos importantes para la investigación, la mejora de búsquedas, la revisión de los *tickets*, la formación de los empleados y la seguridad operacional.

### 5.2.2. Herramientas de gestión de incidentes y de seguimiento

En una herramienta de gestión de incidentes, el incidente y sus datos relevantes se almacenan en una sola unidad, a la que normalmente se conoce como ***ticket***. Así, la progresión de la investigación de un incidente a través del proceso de respuesta puede ser visto como un movimiento lógico del *ticket* mediante una serie de pasos repetitivos. Por ejemplo, al comienzo de una investigación, un *ticket* puede aparecer en la cola del equipo de identificación y el investigador asignado puede, entonces, revisar los indicadores o la evidencia que lo inició. Este investigador puede también asignar una nueva tarea para recopilar datos de una máquina sospechosa. Alternativamente, el investigador podría buscar entre los *tickets* anteriores y concluir que se ha producido una violación de seguridad y enviar el *ticket* a la cola del equipo de contención. Al recibir el *ticket*, este equipo podría comenzar a actuar para restringir los movimientos del atacante.

El *ticket* puede progresar así a través del flujo de trabajo, de equipo a equipo y de cola a cola, hasta que la gestión del incidente se haya completado. De esta forma, el uso de herramientas de seguimiento se considera una buena práctica para garantizar que los pasos correctos se realicen en el orden correcto y por el personal adecuado durante todo el flujo de trabajo.

Así, con herramientas de gestión es posible construir un flujo de trabajo que quede registrado y vinculado al propio incidente. Por ejemplo, en un incidente en el que ya se ha confirmado que se ha comprometido el sistema, el suceso puede enviarse a un equipo de análisis para determinar el alcance de la actividad y presencia del atacante en la red. Todo este trabajo se registra en una herramienta de seguimiento. De esta manera, en el caso de un falso positivo, la alerta inicial puede ser enviada a un equipo de operaciones de seguridad o inteligencia de amenazas para encontrar la causa y así actualizar las firmas en uso en los sistemas de detección.

### 5.2.3. Del dato a la información

La investigación de incidentes no implica solamente recopilar lo datos, sino que la mayor parte del trabajo consiste en interpretar, analizar y actuar sobre los datos recogidos, que suelen ser bastante complejos. Estos datos pueden describir al atacante, al usuario objetivo, a un sistema, a otros datos, a una

aplicación, a programas, a código, a métodos de comunicación y a redes, así como a muchos otros aspectos del entorno informático o de las operaciones comerciales.

De entre la gran cantidad de datos que podrían registrarse en una herramienta de seguimiento, es recomendable que los investigadores sigan una plantilla que les indique qué datos registrar, y que de esta manera no quede a criterio del investigador el descarte de datos, que en un futuro podrían ser material crítico para el futuro de una investigación. A continuación, listamos algunos ejemplos de los campos recomendables de registrar asociándolos a un *ticket* de un incidente:

- Activos comprometidos o sospechosos de haber sido comprometidos, ubicación geográfica, propietario, sistema operativo, detalles del hardware y el indicador principal que llevó a la conclusión de que el activo está comprometido.

- Datos que fueron robados o son sospechosos de haber sido robados, su ubicación de almacenamiento, propietario y nivel de clasificación.

- Información sobre el actor de la amenaza, incluyendo las cuentas o herramientas utilizadas, los *hosts* remotos de los que están operando y el motivo potencial.

- Resultados del análisis, de ingeniería inversa de malware o de herramientas, forense, pruebas y artefactos descubiertos.

- Enlaces a bases de conocimiento internas o de terceros.

Además, es necesario establecer mecanismos para restringir el acceso a los datos sobre atacantes, herramientas, vulnerabilidades o datos robados (por ejemplo, el número de la Seguridad Social o de la tarjeta de crédito, credenciales de usuario, etc.), de modo que su difusión inadvertida no exponga a la organización a nuevos daños.

### 5.2.4. Mejorar la efectividad de las búsquedas

Pocos problemas ralentizan tanto el progreso de una investigación como la búsqueda de información relevante. En la actualidad, todavía hay investigadores que pierden mucho tiempo buscando respuestas clave entre notas en papel, o en archivos individuales en sus ordenadores.

Herramientas como las mencionadas anteriormente incluyen algoritmos modernos de búsqueda que convierten este problema en irrelevante. La mayoría de las herramientas de seguimiento de incidentes pueden configurarse para

indexar algunos o todos los campos de un *ticket* de incidente. El objetivo al que debe aspirar un CSIRT es que un investigador pueda buscar cualquier cadena de texto en cualquier campo de todos los *tickets*.

Por ejemplo, un investigador puede querer saber si un dominio conocido se ha utilizado en algún ataque. Estos datos pueden existir en un campo creado específicamente para almacenar *hosts* de comando y control, pero también puede existir en un fragmento de un archivo de registro almacenado en un campo de texto general de «notas». Implementar un sistema que permita la búsqueda de texto en cualquiera de los campos registrados del sistema ayuda a los investigadores a mejorar su eficiencia y contribuye con un ahorro muy significativo del tiempo de una investigación. Además, también mejora la capacidad de búsqueda incorporar etiquetas con palabras clave vinculadas a los *tickets*. Modelos de este tipo de etiquetas podrían ser el nombre coloquial usado para referirse a una amenaza o un código interno del CSIRT. Por ejemplo, si varios incidentes implican el robo de dibujos esquemáticos de una organización, la etiqueta «esquemas» podría aplicarse a todos estos incidentes.

### 5.2.5. Revisión regular de los *tickets* de incidentes

Una buena práctica dirigida a los gestores de un CSIRT es la revisión periódica del contenido de un incidente para asegurarse de que los investigadores siguen los procesos establecidos. Esto es especialmente importante porque en ocasiones se tiende a tomar atajos o a caer en malas prácticas, sobre todo en investigaciones de incidentes repetitivos que ocurren varias veces por semana y que se convierten en rutinas para los investigadores.

Además, también es recomendable hacer de vez en cuando revisiones de las políticas que determinan qué datos registrar obligatoriamente. Ya que la importancia de los datos va variando con el tiempo, y datos que pueden considerarse poco importantes un día pueden volverse críticos en el futuro.

### 5.2.6. Formación de los trabajadores

Como hemos visto, los procesos de respuesta ante incidentes y las investigaciones pueden ser complejas y requerir el uso de herramientas de seguimiento que no son sencillas de utilizar. Es común que los nuevos investigadores no comprendan y no estén familiarizados con las características de estas herramientas, ni con los procedimientos de *incident response* (IR), ni con la implementación concreta de los procesos de cada CSIRT. Por este motivo, es importante dar formación a las nuevas incorporaciones.

También es importante realizar un entrenamiento regular para todos los miembros del equipo, no solo para que aprendan a utilizar nuevas funciones, sino también para formarlos en el uso correcto de las herramientas disponibles. Esto, además, ofrece la oportunidad a los miembros del equipo de hacer preguntas que pueden haber quedado pendientes durante algún tiempo y da la oportunidad de sugerir nuevas características o cambios.

### 5.2.7. Seguridad operacional

Un intruso inteligente conoce su objetivo y localiza inmediatamente las herramientas y las bases de conocimiento utilizadas por los equipos de seguridad de la información empleados por el objetivo. Las herramientas de seguimiento de incidentes son de gran interés para cualquier atacante, ya que, por un lado, el atacante puede simplemente querer averiguar lo que el equipo de seguridad sabe sobre este. Por otro lado, es posible que el atacante quiera ir más allá y desee interrumpir la capacidad de respuesta, registrar nuevos datos o modificar datos almacenados en el sistema para inducir a error a los investigadores.

Por estos motivos, es recomendable tomar medidas operativas de seguridad para proteger la confidencialidad, integridad y disponibilidad de la herramienta de seguimiento. Por lo tanto, diariamente se deben hacer copias de seguridad que incluyan tanto los datos como el sistema operativo, la aplicación de seguimiento y su base de datos. Las copias de seguridad deben estar encriptadas y la capacidad de recuperación ha de ser probada regularmente. Además, es importante parchear el sistema operativo, las herramientas de seguimiento y las otras aplicaciones siempre que sea necesario.

Finalmente, también hay que tener en cuenta las medidas típicas de seguridad para el acceso a la herramienta de seguimiento, incluyendo una autenticación fuerte para usuarios y administradores; cifrado para las sesiones con la aplicación servidor en las arquitecturas cliente/servidor; etc. En los casos en que haya sospechas o se espere interferencias de un atacante, podría ser necesario operar la herramienta de seguimiento de incidentes fuera de banda. La herramienta podría funcionar en una red separada físicamente de la que está conectado un cliente, o se podría usar una conexión VPN para su acceso.

## 5.3. CSIRT-KIT PROJECT: un kit de herramientas para respuestas de seguridad

CSIRT-KIT Project (http://csirt-kit.org/), es un proyecto colaborativo entre varios CSIRT que tiene el objetivo de facilitar el acceso a herramientas populares y a herramientas desarrolladas por la comunidad a empresas e instituciones que dan sus primeros pasos en la gestión de respuesta a ciberincidentes. Básicamente, el proyecto elabora un kit de herramientas ya instaladas y configuradas en una imagen virtual. A continuación, listamos las herramientas incluidas más destacadas:

**Plataforma de inteligencia de amenazas de código abierto**

La plataforma para compartir MISP es un software gratuito y de código abierto que ayuda a compartir información de inteligencia sobre amenazas, incluidos los indicadores de seguridad cibernética.


**Información sobre manejo de incidentes**

IntelMQ es una solución CERT para recopilar y procesar fuentes de seguridad, pastebins, tweets y archivos de registro mediante un protocolo de cola de mensajes.


**Plataforma de respuesta a incidentes de seguridad**

The Hive es una plataforma de respuesta a incidentes de seguridad gratuita, de código abierto y escalable diseñada para facilitar la vida de los SOC, CSIRT, CERT y cualquier profesional de seguridad de la información.


**Análisis forense de redes**

NfSen permite mantener todas las ventajas convenientes de la línea de comando usando nfdump directamente y también proporciona una descripción gráfica de sus datos de netflow.


**Inteligencia operacional**

Elastic permite buscar, monitorear, analizar y visualizar datos legibles por máquina.


**Plataforma de seguridad de código abierto**

Wazuh es una solución de monitoreo de seguridad gratuita, de código abierto y lista para la empresa para la detección de amenazas, monitoreo de integridad, respuesta a incidentes y conformidad.


**Remitente ligero para datos de red**

Packetbeat es un analizador de paquetes de red ligero que envía datos desde sus hosts y contenedores a Logstash o Elasticsearch.


**Gestión de registros bien hecha**

Graylog proporciona respuestas a las preguntas de seguridad, aplicaciones e infraestructura de TI de su equipo al permitirle combinar, enriquecer, correlacionar, consultar y visualizar todos sus datos de registro en un solo lugar.


**Automatización de flujo de trabajo ampliable**

N8N mueve y transforma datos entre diferentes aplicaciones y bases de datos sin quedar atrapado en documentos API y soluciones de errores CORS.

# 6. Comunidades CSIRT

Como hemos comentado anteriormente, es importante que los CSIRT colaboren entre sí. Por este motivo, se considera una buena práctica ponerse en contacto con otros CSIRT lo antes posible para establecer la relación necesaria con otros colectivos. Por lo general, los CSIRT en funcionamiento se muestran dispuestos a ayudar a los nuevos equipos a establecerse.

Un buen punto de partida para buscar otros CSIRT establecidos en España es consultar el *Inventario de actividades del CERT en Europa*, o también asistir a actividades nacionales de colaboración entre CSIRT. A continuación, se presenta un resumen de las actividades más destacadas de los colectivos CSIRT. En el *Inventario de actividades del CERT en Europa* se puede encontrar una descripción más completa e información más detallada.

## 6.1. Iniciativa de los CSIRT europeos

Foro CSIRT.es. Equipos de ciberseguridad y gestión de incidentes españoles.

Proteger el ciberespacio español, intercambiando información sobre ciberseguridad, y actuar de forma rápida y coordinada ante cualquier incidente que pueda afectar simultáneamente a distintas entidades en nuestro país es el principal objetivo del foro CSIRT.es Este foro es una plataforma independiente de confianza y sin ánimo de lucro compuesto por los equipos de respuesta a incidentes de seguridad CSIRT/CERT, cuyo ámbito de actuación o comunidad de usuarios en la que opera se encuentra dentro del territorio español.

TF-CSIRT (http://tf-csirt.org/), el grupo de trabajo CSIRT, promueve la colaboración entre los CSIRT europeos. Las actividades del grupo de trabajo CSIRT se centran en Europa y sus países vecinos, de conformidad con el mandato aprobado por el comité técnico de Gèant. Las metas más destacadas del grupo de trabajo son:

- Ofrecer un foro de intercambio de experiencias y conocimientos.
- Crear servicios piloto para los grupos CSIRT europeos.
- Fomentar unas normas y procedimientos comunes para responder a los incidentes de seguridad.
- Ayudar a la creación de nuevos CSIRT y a la formación del personal de los CSIRT.

Dentro de sus iniciativas cabe destacar el servicio *Trusted Introducer* (TI). Este servicio constituye la columna vertebral de los servicios de infraestructura y sirve como centro de intercambio de información para todos los equipos de seguridad y de respuesta a incidentes a nivel europeo. Entre otras responsabi-

lidades, el servicio *Trusted Introducer* lista equipos y acreditaciones reconocidas, y certifica equipos según su nivel de madurez demostrado y verificado. A su vez presta servicios vitales que permiten a los equipos de seguridad y de respuesta a incidentes acreditados interactuar de forma más eficiente entre sí.

### 6.2. Iniciativa de CSIRT a nivel global: FIRST

FIRST es la organización de CSIRT más importante y es líder mundial reconocido en la respuesta a incidentes. Los equipos de respuesta a incidentes que pertenecen a FIRST pueden dar a los incidentes de seguridad una respuesta más eficaz, tanto reactiva como proactiva.

FIRST reúne a diferentes equipos de respuesta a incidentes de seguridad informática de organizaciones públicas, comerciales y educativas. FIRST intenta fomentar la cooperación y la coordinación en la prevención de incidentes, estimular una reacción rápida ante los incidentes y promover la puesta en común de información entre sus miembros y todo el colectivo.

### 6.3. Caso de uso: Catalonia-CERT

Catalonia-CERT es el equipo de respuesta a incidentes de ciberseguridad en Cataluña y proporciona un punto de contacto fiable y de confianza para la comunicación y gestión de incidentes de ciberseguridad.


La Agencia de Ciberseguridad de Cataluña dispone de un equipo de respuesta a incidentes que opera, bajo la marca Catalonia-CERT®, como CSIRT (*computer security incident response team*) del **Gobierno de Cataluña**, para desarrollar medidas preventivas, reactivas, de coordinación y de gestión frente a incidentes de ciberseguridad en los colectivos que son ámbitos de relación y a quien se dirige la Agencia de Ciberseguridad de Cataluña.

El diseño del **equipo de respuesta a incidentes** sigue unos procesos y metodología de gestión de incidentes según el modelo de buenas prácticas estándar reconocido internacionalmente, definido por el Software Engineering Institute (SEI) de la Carnegie Mellon University (CMU) de los Estados Unidos de América. Esta manera de trabajar es una garantía de calidad y seguridad en las diversas funciones realizadas durante el ciclo de vida de gestión de incidentes, donde por ejemplo se realizan acciones de triaje considerando aspectos técnicos, legales y judiciales.

Catalonia-CERT® es miembro oficial desde el año 2010 de la red internacional FIRST, formada por más de 350 centros de respuesta a incidentes de ciberseguridad de todo el mundo.

**1) Servicios del Catalonia-CERT®**


Los servicios ofrecidos por el Catalonia-CERT se organizan en tres categorías principales:

**a) servicios reactivos:** servicios destinados a responder a una amenaza o un incidente de seguridad sufrido por un sistema de información y minimizar su impacto. Estos servicios se clasifican en:

- Avisos y alertas
- Tratamiento de incidentes:
  - Análisis de incidentes
  - Soporte remoto de respuesta de incidentes (información estándar)
  - Soporte remoto de respuesta de incidentes (información personalizada)
  - Orientación remota para incidentes en tiempo real
  - Soporte de incidentes en línea
  - Orientación de incidentes en el sitio
  - Respuesta de incidentes coordinada con terceras partes

- Tratamiento de vulnerabilidades:
  - Análisis de vulnerabilidades
  - Respuesta a vulnerabilidades
  - Respuesta a vulnerabilidades coordinada
  - Orientación remota y en el sitio para resolver vulnerabilidades

- Tratamiento de artefactos:
  - Análisis de artefactos
  - Respuesta a artefactos
  - Respuesta a artefactos coordinada

– Análisis forense

**b) Servicios proactivos:** son servicios cuya función es reducir los riesgos de seguridad de la comunidad mediante la distribución de información e implantación de sistemas de protección y detección. Estos servicios están diseñados para mejorar los procesos de infraestructura y seguridad antes de que se produzca un incidente o sea detectado. El objetivo principal es evitar incidentes y reducir su impacto y abastecimiento en el caso de que sucedan. Estos servicios se clasifican en:

- Publicación y anuncios.
- Configuración y mantenimiento de herramientas de seguridad, aplicaciones e infraestructuras.
- Servicio de detección de intrusiones.
- Difusión de información relativa a seguridad.

**c) Servicios de gestión y coordinación:** Servicios mediante los cuales se pretende mejorar los procesos de trabajo tanto de la comunidad a la que se da servicio como del propio ERI. Estos servicios se clasifican en:

- Educación y formación.
- Campañas de sensibilización.

Figura 8. Sello de acreditación a EU de un CSIRT por parte del servicio Trusted Introducer


Fuente: TF-CSIRT- Gèant. https://www.trusted-introducer.org/directory/teams/csuc-csirt.html.

Se pueden encontrar más detalles sobre Catalonia-CERT en su RFC2350.

**2) Colaboraciones con organismos externos**

Catalonia-CERT se coordina con otros grupos de respuesta a incidentes existentes y establece lazos de colaboración con las fuerzas policiales para el tratamiento de incidencias de seguridad informática.

Algunas de las instituciones con las que colabora Catalonia-CERT son las siguientes:

- CSUC-CSIRT, equipo de seguridad del Consorcio de Servicios Universitarios de Cataluña (CSUC).

- esCERT-UPC, equipo de seguridad para la coordinación de emergencias telemáticas de la UPC.

- CCN-CERT, equipo de respuesta ante incidentes del Centro Criptológico Nacional (CCN), que depende del Centro Nacional de Inteligencia.

- INCIBE-CERT, equipo de respuesta ante incidentes de seguridad del Instituto Nacional de Tecnologías de la Comunicación (INTECO).

También Catalonia-CERT participa en diferentes foros o asociaciones de profesionales de seguridad, que permiten disponer de información y contactos de primera mano en la detección, contención y resolución de los diferentes incidentes que se pueden producir. Algunos de los grupos en los que participan son:

- ABUSES, que gestiona incidentes de seguridad y difunde medidas reactivas y proactivas para resolver incidentes de seguridad relacionadas con *spam*, distribución no autorizada de contenidos, infecciones por código malicioso, etc.

- Trusted Introducer (TF-CSIRT), plataforma de confianza y certificación de equipos de respuesta a incidentes.

- FIRST es la organización de CSIRT más importante y es líder mundial reconocido en la respuesta a incidentes.

# Bibliografía

**CSA. «Certificate of Cloud Security Knowledge»** [en línea]. <https://cloudsecurityalliance.org/education/ccsk/>

**Dotson, Chris** (2019). *Practical Cloud Security* [en línea]. O'Reilly Media. <https://www.oreilly.com/library/view/practical-cloud-security/9781492037507/>

**ENISA «Cloud security»** [en línea]. <https://www.enisa.europa.eu/topics/cloud-and-big-data/cloud-security>

**ENISA** (2020, 10 de diciembre). «How to set up CSIRT and SOC» [en línea]. <https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc>

**Guijarro Olivares, Jordi; Caparrós, Joan; Cubero, Lorenzo** (2019). *Devops y Seguridad Cloud*. [en línea]. Editorial UOC. <http://devopsyseguridadcloud.cloudadmins.org/>

**NIST** (2020, 31 de julio). «General Access Control Guidance for Cloud Systems: NIST Publishes SP 800-210» [en línea]. <https://csrc.nist.gov/News/2020/nist-publishes-sp-800-210-ac-guidance-for-cloud>

**Novak, Justin; Manley, Brittany; McIntire, David; Mudd, Sharon; Hueca, Angel Luis; Bills, Tracy** (2021). *The Sector CSIRT Framework: Developing Sector-Based Incident Response Capabilities* [en línea]. Software Engineering Institute. <https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=734783>