www.ismsforum.es

Antes, durante y después de ir a la Nube

Respuesta ante Incidentes

Una iniciativa de

isms forum

CSA Spanish Chapter

marzo 2023

Antes, durante y después de ir a la Nube

Respuesta ante Incidentes

AUTORES

COORDINADORES

Olga Forné

Toni García

REVISORES

Miguel Ángel Pérez

Mariano J. Benito

PARTICIPANTES

Ángel Pérez

Antonio Fontiveros

Carlos José Alcón

Carlos Martinez

David Llorente

Eduardo González

Enrique Cervantes

Eva Cristina Cañete

Gemma Déler

Gonzalo Martinez

Iván Sánchez

Javier Sevillano

Jose González

Luis Paredes

Luis Pérez Pau

Rafael Hernández

Ramón Ortiz

Tomás Avila

Trina de Miguel

Xavier Macarrilla

Xavier Rubiralta

GESTIÓN DE PROYECTO

Beatriz García

DISEÑO/MAQUETACIÓN

Cynthia Rica

CONTENIDOS

CONTENIDOS

CONTENIDOS

CONTENIDOS

CONTENIDOS

1 RESUMEN EJECUTIVO

Cuando hablamos de gestión de incidentes de seguridad en la nube, está más que demostrado que la esperanza e inacción son estrategias erróneas como forma de preparación de las organizaciones frente a eventos inesperados que puedan poner en riesgo la actividad del negocio. Si bien esta afirmación a muchas personas nos parece obvia y ha sido demostrada en diversas ocasiones, ¿por qué motivo siguen existiendo muchas organizaciones que, usando servicios en la nube, continúan con la forma tradicional de gestionar las operaciones de negocio esperando que nunca les ocurran incidentes de seguridad que puedan alterar o, inclusive, parar su actividad aunque esto le ocurra a sus competidores, socios, proveedores de servicios, otras plataformas en la nube y hasta a los mismos proveedores de servicios de gestión de incidentes de seguridad?

Habrá quién esté leyendo estas líneas tranquilamente asintiendo y pensando que su organización ya dispone de procesos alineados con las buenas prácticas ITIL, que puede que disponga de una certificación ISO/IEC 20001 para la gestión de los servicios o hasta una certificación ISO/IEC 27001 para la gestión de seguridad de la información y, por lo tanto, un incidente de seguridad en la nube no le desvelará de su sueño porque el negocio está bajo control. Pues bien, estas guías de buenas prácticas son necesarias como base para ayudar a los equipos de tecnología de las empresas a funcionar y acometer algunos de los problemas que pueden surgir, pero son insuficientes si la organización utiliza de forma directa o indirecta servicios en la nube ya que, realizar una petición y esperar a que el proceso escale a través de los distintos niveles de soporte (L1, L2, L3) hasta la persona experta en la materia, aunque necesario, puede llegar a ocasionar un retraso tal que, al atender el problema, el desastre esté servido.

En este contexto y con la rápida evolución de los servicios en la nube, así como la aparición de nuevas tecnologías que le dan soporte y la necesidad de disponer de servicios siempre activos, nos encontramos organizaciones configuradas para gestionar los incidentes de seguridad en este ecosistema de forma clásica, desatendiendo matices importantes como pueden ser los modelos diseñados como software como servicio ("Software as a Service" o 'SaaS') donde las responsabilidades sobre la atención al incidente cambian considerablemente, o los incidentes que pueden surgir en cualquier momento y la rapidez en la actuación y propagación de estos se ha multiplicado y puede tener consecuencias tanto a la propia organización como a sus partes interesadas.

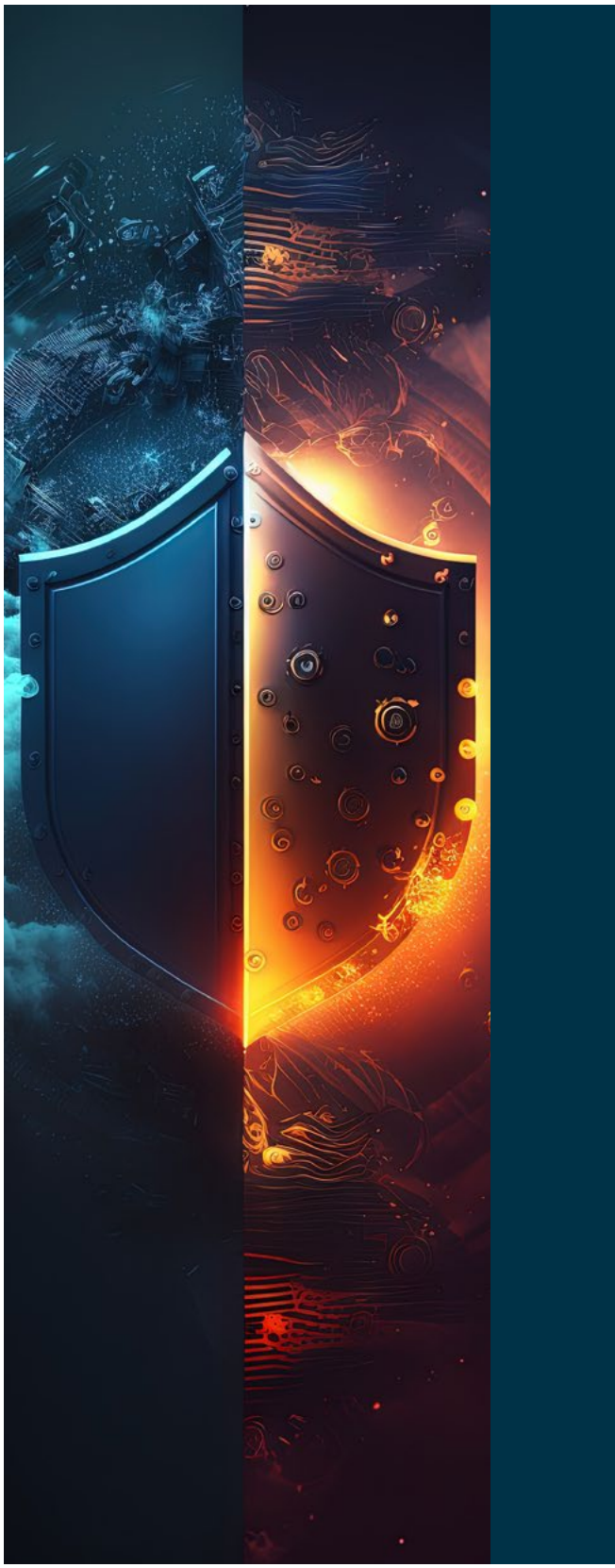
Por lo anterior y para preparar a estas organizaciones frente a incidentes de seguridad en la nube, se ha elaborado la presente guía con la que se introducen los aspectos principales que caracterizan la nube y se proporcionan herramientas para identificar, evaluar, gestionar, resolver y comunicar de forma clara, sencilla y efectiva un incidente de esta índole incluyendo:

- Una descripción sobre qué es, cómo se creó, cuáles son las características y tipologías principales, así como las ventajas y desventajas del uso de la nube en función de cada modelo de implementación y de servicio en que se proporciona.

- Una guía sobre cuáles son las particularidades de los incidentes de seguridad en la nube y qué es necesario tener en cuenta en cada una de las etapas del proceso de anticipación, detección y respuesta ante un evento que pueda poner en riesgo el negocio considerando las fases de un incidente de seguridad, haciendo hincapié en las acciones de prevención y recuperación, así como otros procesos complementarios esenciales en una gestión exitosa como pueden ser el plan de comunicación o el análisis de las lecciones aprendidas.

- El estado del arte en la normativa y legislación española y europea que regulan la implantación y uso de los servicios en la nube, además de las guías y estándares de buenas prácticas internacionales existentes.

- Una hoja de ruta que permita: sentar las bases para evaluar la adopción de la nube; valorar cuáles son las necesidades de la organización para realizar una sólida migración del entrono local a la nube; y aspectos importantes que se deben tener en cuenta una vez se ha realizado el salto a la nube.



Con todo, esta guía nos permite ver y entender que los incidentes de seguridad en la nube, si bien pueden parecer una escisión de los incidentes tradicionales, son más complejos en términos de tecnología y actores que participan durante el proceso, en concreto: cuando en los entornos tradicionales los incidentes pueden tratarse mediante el uso de técnicas y metodologías estándares sin una evaluación muy profunda del negocio, en la nube (tanto si acogemos la nube de forma híbrida o total), es imprescindible el uso de estándares y el conocimiento detallado tanto del negocio, como de las responsabilidades de las partes interesadas y los servicios que forman parte de la cadena de suministro.

2 NOTA DE REDACTORES

¿Cuándo descubrimos el concepto de nube? ¿En qué momento entró en la vida empresarial y en el día a día de muchas organizaciones? Para algunos pocos este concepto puede ser ajeno, a otros les parecerá que hace nada que empezó y el resto dirá que llevan ya una eternidad en ella. Para nosotros, así como para muchas de las personas que lean esta guía, la nube apareció en el entorno profesional y se fue integrando en el negocio en mayor o menor medida dando solución a las necesidades de nuestros clientes y colaboradores o debido a la transformación en la oferta de servicios de los proveedores de servicios. Si bien es cierto que una mayoría de las personas están familiarizadas con la nube, existe un público extenso de profesionales para los que sigue siendo un misterio, una maraña de tecnologías y servicios que prometen ser la barita mágica que impulsará sus organizaciones con una gestión mínima de la tecnología y, sin duda, proporcionando una completa seguridad de sus datos; hasta que, por supuesto, sufren un incidente de seguridad. En ese momento es en el que se dan cuenta de que la nube, como los entornos tradicionales, puede ofrecer las mismas garantías o fallos de seguridad y, por lo tanto, deben prestar atención al gobierno de los incidentes de seguridad de la información.

Durante la elaboración de esta Guía descubrimos que la falta de preparación ante incidentes de seguridad en la nube parece un hecho sistémico en el mundo empresarial; las organizaciones acostumbran a estar preparadas ante un incidente de seguridad tradicional, pero muchas veces -sobre todo aquellas organizaciones de menor volumen y/o recursos- descuidan otros entornos debido a: 1) La falta de recursos y/o personas disponibles para promover los programas de respuesta ante incidencias, 2) La falta de una necesidad de actualizar dichos programas por una falsa sensación de seguridad por defecto derivada de la falta de conocimiento del nuevo entorno y un sesgo optimista.

Por todo ello, nos dirigimos tanto a las pequeñas y medianas empresas como a todas aquellas organizaciones que estén iniciándose en el viaje a la nube (o que tengan pendiente abordar la gestión de incidencias en este entorno) para aportar un rayo de luz que les permita entender los conceptos básicos de este ecosistema, los agentes y actores involucrados en la gestión de la misma, así como los riesgos intrínsecos o circunstanciales más comunes que podemos encontrar y que pueden afectar negativamente a sus organizaciones. Este no pretende ser un manual que deba seguirse a pies juntillas, sino una orientación que permita entender todas las piezas de esa maraña de tecnologías y servicios, así como facilitar los primeros pasos hacía una gestión de incidencias en la nube exitosa.

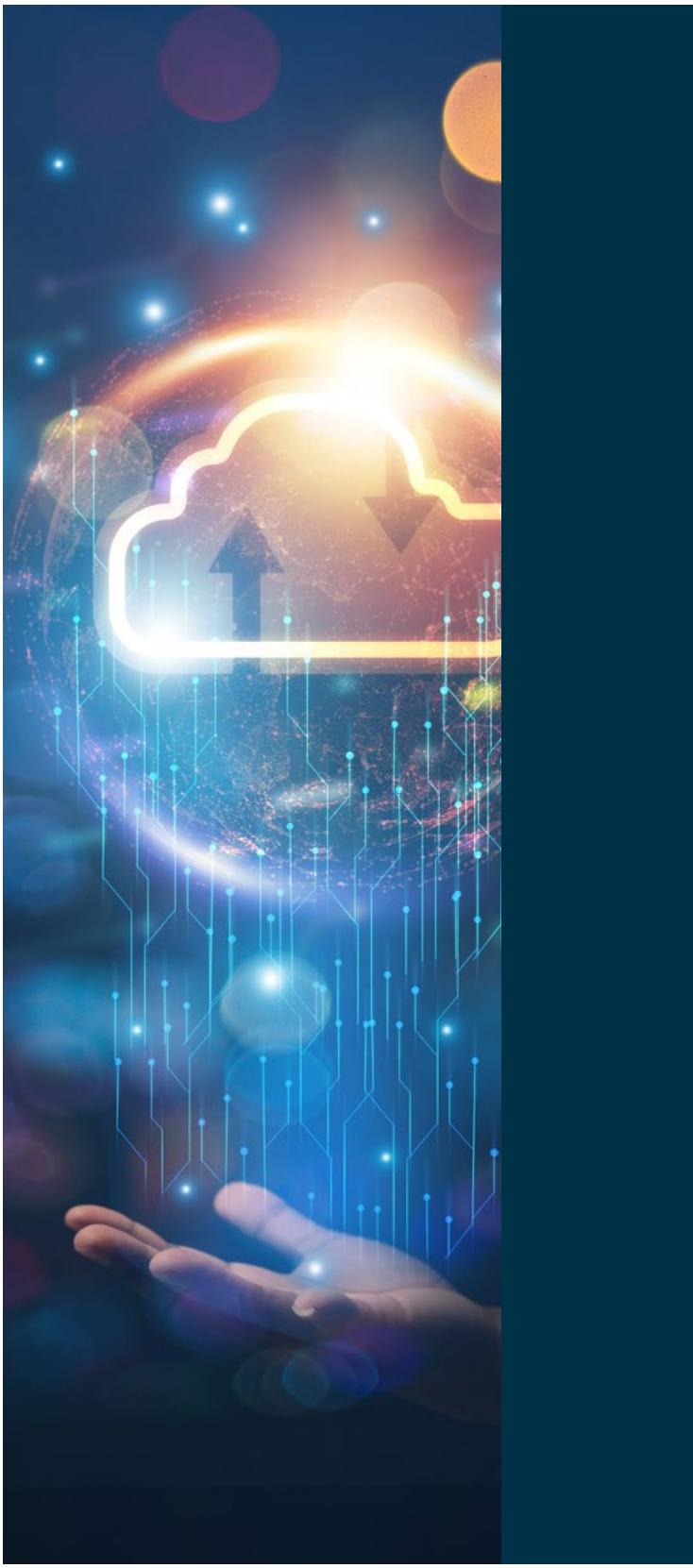
Esta guía se actualizará periódicamente para estar al día de los cambios y riesgos que puedan afectar al ecosistema empresarial considerando tendencias, tecnologías, amenazas y lecciones aprendidas.

La publicación de la Guía ha sido posible gracias a la colaboración entre ISMS Fórum y CSA Alliance que sembraron la idea inicial y han conseguido la involucración de un grupo de profesionales con amplia experiencia en el sector de la seguridad de la información, la privacidad de los datos y el cumplimiento normativo, los riesgos tecnológicos, así como la gestión de operativa de los incidentes de seguridad en la nube.

El éxito de esta Guía habría sido imposible sin la involucración del mencionado grupo de reconocidos profesionales dispuestos a donar parte de su tiempo y esfuerzo con el único fin de contribuir y dar apoyo a las PyMEs y, en consecuencia, a la sociedad en general.

Todas las personas que hemos participado en la creación y publicación de esta Guía deseamos que su contenido sea ágil, interesante y de utilidad y agradeceremos nuevas ideas y aportaciones que ayuden a mejorar la presente publicación.

Os deseamos un agradable viaje por la gestión de incidencias en la nube.



3 INTRODUCCIÓN A LA NUBE

La computación en la nube (en adelante, "la nube") representa tanto un modelo operacional, como un conjunto de tecnologías para administrar grupos compartidos de recursos tecnológicos que, conectados a Internet, permiten la administración, procesado y almacenamiento de datos sin la dependencia de una infraestructura física propia.

La nube es una tecnología con el potencial de mejorar la colaboración, agilidad, escalabilidad y disponibilidad de los servicios tecnológicos, además de facilitar oportunidades para la reducción de costes a través de una optimización y eficiencia de los procesos. Los modelos que ofrecen las distintas tipologías de nube contemplan un ecosistema donde los componentes se pueden orquestar, aprovisionar, implementar, desmantelar y escalar de una forma sencilla y ágil proporcionando modelos que pueden llegar a ser similares a los servicios personalizados.

3.1 ¿Qué es la nube?

El Instituto Nacional de Estándares y Tecnología de EUA ("National Institute of Standards and Technology", conocido como NIST), referente internacional en el campo de la seguridad de la información, define la computación en la nube[1] como:

"La computación en la nube es un modelo para permitir un acceso de red ubicuo, conveniente y bajo demanda a un grupo compartido de recursos informáticos configurables (por ejemplo: redes, servidores, almacenamiento, aplicaciones y servicios) que pueden aprovisionarse y liberarse rápidamente con un mínimo esfuerzo o interacción del proveedor de servicio."

Similar al anterior, la Organización Internacional de Normalización ("International Standard Organization", ISO) junto con la Comisión Electrotécnica Internacional ("International Electrotechnics Commission", IEC), líderes internacionales en la definición de estándares y normas asociadas principalmente enfocadas en el campo tecnológico, a través de la ISO/IEC 27017, "Controles de seguridad para servicios en la nube", define la nube[2] como:

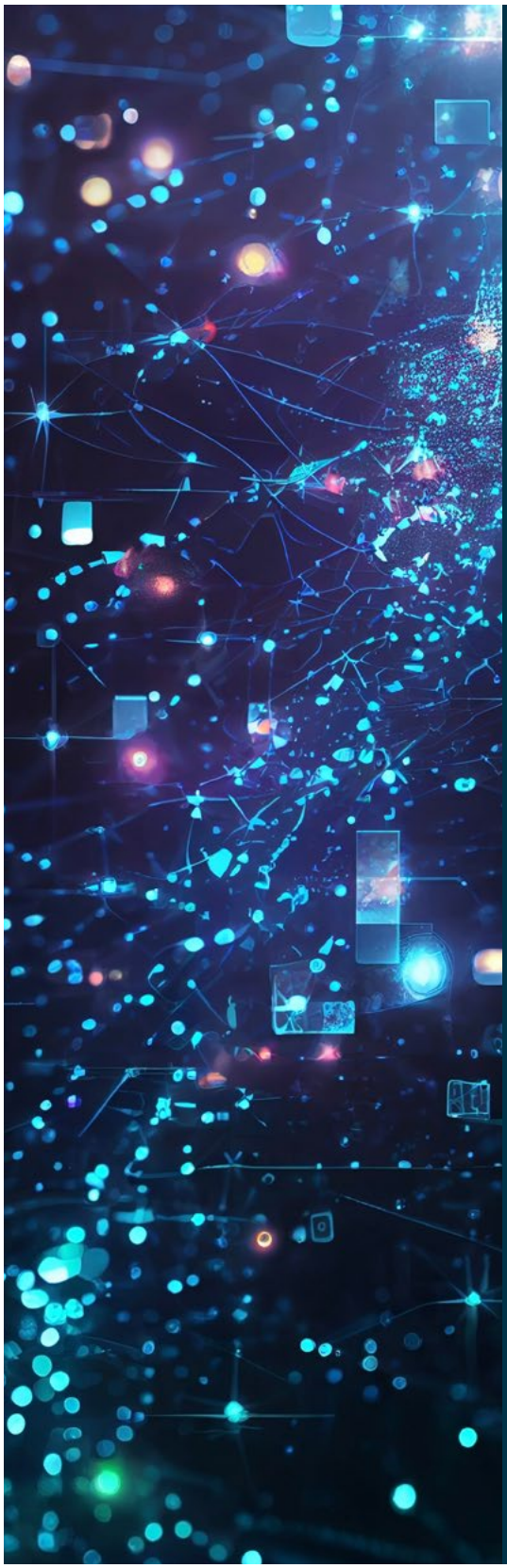
"Paradigma para permitir el acceso de red a un conjunto de recursos compartidos, escalables y elásticos, físicos o virtuales con aprovisionamiento de autoservicio y administración bajo demanda."

Las técnicas clave para crear una nube son la abstracción y la orquestación: los recursos tecnológicos se abstraen de la infraestructura física para pasar a una virtual donde se agrupan; y se orquestan con la finalidad de coordinar la distribución y la entrega de los servicios generados con estos recursos. Estas dos técnicas crean todas las características esenciales que utilizamos para definir hoy la nube.

[1] SP 800-145 The NIST Definition of Cloud Computing https://csrc.nist.gov/publications/detail/sp/800-145/final

[2] ISO/IEC 27017 https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma/?c=N0065228

3.2 Una breve historia sobre la nube



Si bien es cierto que la popularidad de la nube se ha disparado recientemente y se podría pensar que la nube y los servicios que ofrece son relativamente recientes, lo cierto es que lleva ya muchos años entre nosotros.

Existe cierto consenso en aceptar que la computación en la nube comenzó en los años 50, cuando surgieron los grandes computadores (conocidos como 'mainframes') –no sólo el coste era grande, también su volumen– utilizados por algunas organizaciones de gran tamaño para procesar datos de forma masiva o ejecutar aplicaciones críticas y donde los usuarios se conectaban mediante dispositivos ('terminales') muy básicos cuya única función era proporcionar acceso a esos grandes ordenadores.

A finales de los años 60, se empezó a fraguar la idea de conectar los ordenadores formando una red, de forma que estos se pudieran comunicar entre ellos por distintos caminos para que la comunicación se mantuviera en caso de caída de uno de los enlaces. Así, en 1969, se transmitió el primer mensaje a través de la red ARPANET, creada por el Departamento de Defensa de EUA para la comunicación entre las instituciones académicas y estatales, que dio lugar a lo que actualmente se conoce como 'Internet'.

Durante la siguiente década, los años 70, surgió el modelo de arquitectura de software cliente-servidor que permitió centralizar una mayor capacidad de procesado en los servidores, permitiendo orientarlos a tareas específicas (ej.: servidores de correo, servidores de impresión…) y que ponían a disposición de los ordenadores tareas (llamadas 'clientes') cada vez que éstas eran solicitadas. Además, en paralelo, se comenzaron a desarrollar sistemas de virtualización que permitían simular la funcionalidad de un hardware determinado (servidores, nodos de red, almacenamiento…) en servidores alternativos sin ser necesaria la compra del propio hardware.

Con los principales mimbres ya disponibles, pero todavía poco maduros, no fue hasta 1996 cuando, desde la empresa Compaq y por primera vez, se acuñó el concepto de "Cloud Computing" al referirse al futuro de los negocios por Internet. Este hecho provocó que parte del software de las organizaciones empezase a ser trasladado hacia entornos web surgiendo las denominadas "aplicaciones habilitadas para computación en la nube" (o "cloud computing-enabled applications"), servicios específicos para este nuevo entorno que se volverían de uso común (ej.: almacenamiento de archivos en la nube).

En 1999, Salesforce comenzó a comercializar aplicaciones empresariales por Internet directamente para las organizaciones convirtiéndose en la primera empresa en utilizar el Cloud Computing. Sin embargo, hubo que esperar hasta 2006 para que grandes compañías, como Google o Amazon, empezasen a usar el término de cloud computing para describir el nuevo paradigma según el cual se democratizó y extendió el acceso por parte de los usuarios a software, ficheros y capacidad de computación utilizando la web en lugar de sus propios equipos de trabajo.

3.3 ¿Por qué se utiliza la nube? ¿Cuál es su valor añadido? ¿Y sus inconvenientes?

En términos generales, el modelo actual de servicios en la nube ofrece a las organizaciones grandes beneficios, entre los que podríamos destacar:

- Alta disponibilidad de los servicios.
- Gran velocidad para desplegar nuevos servicios de una forma más sencilla.
- Acceso a la información desde cualquier lugar, cualquier dispositivo y en cualquier momento.
- **Escalabilidad**: se pueden redimensionar los recursos de manera flexible de manera rápida y eficaz en cualquier momento.
- Modelo financiero basado en gastos operativos (OPEX) por servicio que permite evitar o reducir los gastos en inversiones (CAPEX).
- **Pago por uso**: el precio varía en función de las necesidades de la organización de manera flexible y la organización únicamente paga por la utilización que haga de los recursos en la nube.
- **Resiliencia frente desastres locales**: la dispersión geográfica de los centros de datos y la información proporciona resiliencia frente a desastres locales físicos y digitales (ej.: desastre natural, ataque de denegación de servicio…).
- **Reducción del coste de la seguridad física**: la concentración de recursos hace que los requisitos de seguridad física para los proveedores de servicios en la nube sean baratos y distribuidos entre todos los clientes.
- **"Automatización" de la instalación de parches y actualizaciones**: si el proveedor de servicios en la nube asume la responsabilidad de este punto, la organización puede automatizar y reducir el tiempo dedicado a instalar los parches y las actualizaciones de los sistemas mejorando la prevención de sistemas obsoletos y vulnerables.
- **Automatización de las copias de seguridad**: los proveedores pueden ofrecer soluciones para automatizar las copias de seguridad, así como soluciones ágiles de restauración.
- **Seguridad como servicio**: una de las principales ventajas de este modelo son las soluciones de ciberseguridad integradas que ofrecen los proveedores sobre sus servicios.
- **Cumplimiento normativo y certificaciones**: la mayoría de los servicios en la nube más extendidos suelen cumplir con los estándares y certificaciones internacionales para este tipo de servicios.

Entre los principales inconvenientes, los servicios en la nube presentan los siguientes:

- Pérdida del control sobre la forma de procesamiento de la información, así como los propios datos, obligando a tener un modelo de gobierno de terceros maduro en el que se recojan de un modo formal las responsabilidades de cada una de las partes.
- Pérdida de la inmediatez o incremento en los tiempos en la atención a la organización para realizar cambios sobre la tecnología o servicios proporcionados, así como el soporte o la respuesta ante incidencias requiriendo la definición de acuerdos de nivel de servicio ('ANS' o, en inglés 'SLA').
- Perdida de flexibilidad y personalización de la tecnología y los servicios de la organización, siendo en algunos casos necesaria la adaptación de los procesos de la propia organización al modelo proporcionado por la nube.

3.4 ¿Qué tipologías de nubes y modelos de servicio existen?

NIST define la computación en la nube mediante la descripción de cinco características esenciales, cuatro modelos de implementación en la nube y tres modelos de servicio.

—3.4.1 Características esenciales de una nube

A continuación, definimos las características que hacen que una nube sea una nube. Podemos considerar que, si algo presenta estas características, estamos ante computación en la nube; en caso contrario, si carece de alguna de ellas, probablemente se trate de otro tipo de tecnología.

- **Agrupación de recursos:** característica principal de la nube; como se discutió anteriormente, el proveedor abstrae los recursos y los recopila en un grupo y, a continuación, estos pueden ser asignados a diferentes usuarios en función de la necesidad de acceso a los mismos.
- **Autoservicio de los recursos bajo demanda de los usuarios** que manejan sus propios recursos sin necesidad de la intervención de un usuario administrador.
- **Amplio acceso a la red**, ya que todos los recursos están disponibles en una red, sin necesidad del acceso físico directo; la red no es necesariamente parte del servicio.
- **Rápida elasticidad y escalabilidad** permitiendo a los usuarios ampliar o contraer los recursos que utilizan del grupo (aprovisionamiento y desaprovisionamiento), a menudo de forma completamente automática, facilitando una relación más estrecha entre el consumo de recursos y la demanda (ej.: agregar servidores virtuales cuando la demanda aumenta y luego apagarlos cuando baja).
- **Medidores de servicio** para garantizar que los usuarios solo usan lo que se ha asignado, y, si es necesario, cobrar por ello.

3.5 Modelos de implementación en la nube

Tanto el NIST (NIST Special Publication 800-145, 'Definition of Cloud Computing') como ISO/IEC (norma 27017) utilizan los mismos cuatro modelos de implementación en la nube. Estos modelos definen la forma en la que las tecnologías se implementan y consumen y se aplican en toda la gama de modelos de servicio.

Los modelos de implementación se definen según el usuario de servicios en la nube, es decir, quién usa la nube. La organización que posee y administra la nube puede variar incluso dentro de un único modelo de implementación.

—3.5.1 Nube pública

La infraestructura de la nube está disponible para el público en general o un gran grupo de la industria y es propiedad de una organización que vende servicios en la nube.

—3.5.2 Nube privada

La infraestructura de la nube se opera únicamente para una sola organización. Puede ser administrada por la organización o por un tercero y puede estar ubicada en sus instalaciones o fuera de su propiedad.

—3.5.3 Nube comunitaria

La infraestructura en la nube es compartida por varias organizaciones y soporta a una comunidad específica que tiene inquietudes compartidas (ej.: misión, requisitos de seguridad, política o requisitos de cumplimiento normativo). Puede ser administrada por las organizaciones o por un tercero y puede estar ubicada en las instalaciones de una de ellas, varias o fuera de ellas.

—3.5.4 Nube híbrida

La infraestructura de la nube es una composición de dos o más nubes (privada, comunitaria o pública) que siguen siendo entidades únicas, pero están unidas por estándares o tecnologías patentadas que permiten la portabilidad de datos y aplicaciones.

El término "híbrido" también se usa comúnmente para describir un centro de datos que no está en la nube y está conectado directamente a un proveedor de servicios en la nube.

3.6 Modelos de servicio en la nube

El NIST (NIST Special Publication 800-145, 'Definition of Cloud Computing') define tres **modelos de servicio** que describen las diferentes categorías fundamentales de servicios en la nube:

a. **Software como servicio** (en adelante "SaaS", Software as a Service).

b. **Plataforma como servicio** (en adelante "IaaS", Platform as a Service).

c. **Infraestructura como servicio** (en adelante "IaaS", Infrastructure as a Service).

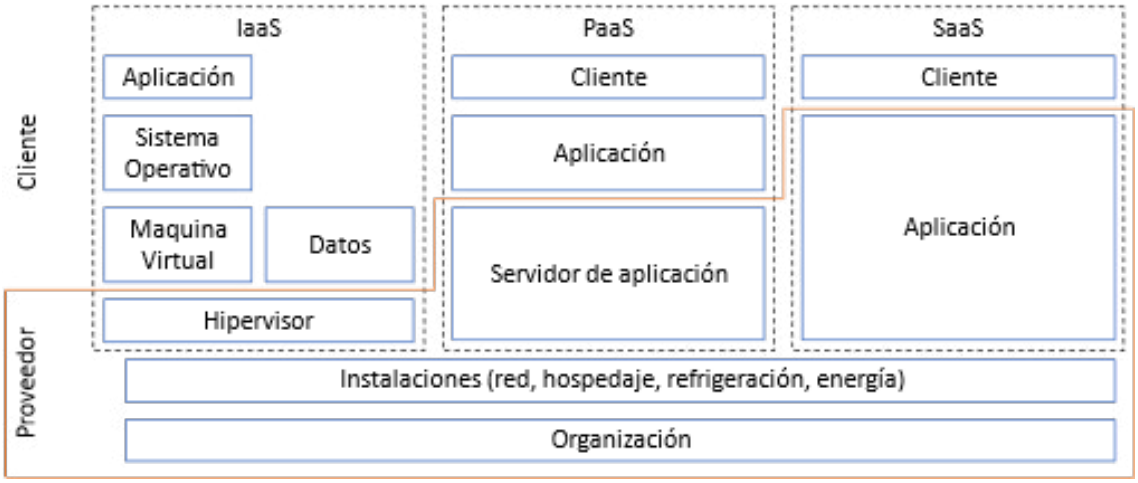


Figura 1. Modelos de servicio en la nube.

En términos generales y aunque entraremos en detalle más adelante, cada uno de estos modelos ofrece distintos niveles de control que el usuario o cliente tendrá sobre el servicio contratado. Debido a esto, aunque los datos siempre serán responsabilidad del cliente por ser de su propiedad, cada uno de ellos tendrá su propio modelo de responsabilidad operativa sobre la nube que deberá consensuarse (entre cliente y proveedor de la nube) y recogerse mediante las correspondientes cláusulas contractuales.

Es importante destacar que la responsabilidad sobre la información, así como su protección, siempre será de su propietario: el usuario o cliente; en función del modelo de responsabilidad, lo que podrá variar será el modelo de gestión y administración de la propia nube, así como la responsabilidad sobre la implementación de las medidas de seguridad requeridas.

Es conveniente destacar la importancia de analizar cuidadosamente el modelo de responsabilidad compartida a la hora de poner en marcha un servicio en la nube con un proveedor en cualesquiera de sus modalidades. En este sentido, es importante tener en cuenta quién es responsable de qué, especialmente en el ámbito de la seguridad de la información (ej.: identificando las responsabilidades del proveedor y de la propia organización para la realización de copias de seguridad, gestión de incidencias de seguridad, etc.).

—3.6.1 Software como servicio (SaaS)

En un modelo de SaaS el proveedor ofrece a las organizaciones la posibilidad de contratar como un servicio aplicaciones o software del proveedor que éste administra y aloja en su propia infraestructura en la nube permitiendo a las organizaciones su acceso online con un navegador web, desde una aplicación móvil o una aplicación de cliente ligera.

Al contrario que en los otros dos tipos de modelo de servicio, en un modelo SaaS el proveedor en la nube es quién dispone, sin intervención de la organización, de la capacidad de administrar o controlar la infraestructura en que se basa el servicio que utiliza.

Actualmente, el modelo SaaS es el más extendido y los proveedores de servicios ofrecen a través de este modelo gran parte de las aplicaciones incluyendo: servicios de correo electrónico, suites ofimáticas, servicios de colaboración o aplicaciones de negocio para la gestión de las relaciones con los clientes, facturación u otro tipo de aplicaciones.

Frente a las soluciones tradicionales de distribución de software, los modelos SaaS proporcionan a las organizaciones una gran escalabilidad adquiriendo el derecho de usar el software sólo en la medida en que lo necesita el cliente. Esto genera una serie de oportunidades muy interesantes para una mayor eficiencia del negocio y, en algunos casos, rendimiento. Algunas de las ventajas que podríamos destacar de este modelo, serían:

- **Despliegue más eficiente de la aplicación.** Las aplicaciones SaaS pueden ser accesibles de una forma muy rápida y económica por los usuarios de la organización sin necesidad de complejos procedimientos de instalación y reduciendo posibles problemas de incompatibilidad con otras aplicaciones del equipo de trabajo del usuario.

- **Uso más eficiente de las licencias del software** permitiendo, incluso, el uso de una única licencia en múltiples equipos en diferentes momentos y evitando la complejidad de sistemas tradicionales como servidores de licencias, etc.

- **Gestión centralizada de la información.** El proveedor gestiona los datos de forma centralizada ofreciendo a la organización la posibilidad de realizar copias de seguridad, recuperación ante desastres, etc.

- **Administración delegada** al proveedor de forma que la organización no se debe preocupar por la gestión de los sistemas operativos, la actualización del hardware, el mantenimiento de los centros de datos, etc.

No obstante, las organizaciones también deben considerar posibles contrapartidas del modelo SaaS, entre las que se destacan:

- **Aparición de nuevos riesgos de seguridad** de la información debido a la necesaria utilización de navegadores web que, en ocasiones, presentan numerosas vulnerabilidades, escasa protección ante ataques avanzados, etc.

- **Mayor dependencia de una conexión a Internet** fiable, robusta y con un rendimiento suficiente que permita acceder al servicio SaaS.

- **Posible dificultad para migrar el servicio**, si la organización así lo considera necesario, de un proveedor a otro. En este sentido, frecuentemente las organizaciones se ven forzadas a descartar la migración por los costes internos que serían necesarios para adaptar su negocio a las especificaciones del servicio del nuevo proveedor.

Las organizaciones y sus departamentos de sistemas de información deben considerar todos estos aspectos a la hora de contratar un modelo de servicio SaaS. Aunque se trata de una modalidad cada vez más extendida, se observa que **principalmente las organizaciones se decantan por el modelo SaaS cuando buscan servicios autogestionados** que den respuesta a necesidades relacionadas con:

- **Gestión del ámbito corporativo**, que permita conectar el negocio con los proveedores, empleados, clientes, etc. (ej.: aplicaciones para la gestión de inventarios, facturación, pagos/transferencias, gestión de las relaciones con los clientes…).

- **Gestión del puesto de trabajo** incluyendo, no sólo aplicaciones ofimáticas con procesadores de texto, hojas de cálculo, presentaciones, etc., sino también aplicaciones que permitan a los usuarios finales trabajar colaborativamente (ej.: aplicaciones de correo electrónico, calendarios, audio y videoconferencias, etc.).

Así, por las desventajas mencionadas anteriormente, el modelo SaaS es desaconsejable actualmente para el uso de aplicaciones en tiempo real que requieran un alto rendimiento y velocidad de conexión (ej.: sistemas de control de vuelos, robótica industrial, etc.), aplicaciones que originen grandes cantidades de datos y cuyo volumen desaconseje la transferencia por Internet, y aplicaciones críticas para la organización cuyo fallo o pérdida pueda ocasionar daños irreparables para la misma.

Con lo anterior, la mayoría de las aplicaciones modernas en la nube (modelo SaaS u otro) pueden usar, a su vez, una combinación de uno de los otros dos modelos de servicio explicados a continuación.

—3.6.2 Plataforma como servicio (PaaS)

En un modelo PaaS el proveedor ofrece a las organizaciones la posibilidad de disponer de una plataforma (servidores de aplicaciones) en la nube para desarrollar, desplegar y administrar directamente sus propias aplicaciones o aplicaciones de terceros.

Los proveedores de servicios PaaS proporcionan un nivel de abstracción intermedio entre el modelo de servicio SaaS y el modelo de Infraestructura como Servicio de forma que la organización delega la gestión o el control de la infraestructura (incluyendo todo lo relacionado con la red, servidores, sistemas operativos o almacenamiento), pero mantiene la administración de las aplicaciones que despliega. Para ello, el servicio PaaS proporciona plataformas de desarrollo de aplicaciones, como bases de datos, plataformas de aplicaciones, almacenamiento de archivos y colaboración o, incluso, procesamiento de aplicaciones propietarias (ej.: aprendizaje de máquina, procesamiento de grandes cantidades de datos).

De todos los modelos de servicio, PaaS es el más difícil de caracterizar debido tanto a la amplia gama de ofertas de tipos de PaaS de los proveedores, así como de las múltiples formas de crear servicios de PaaS que existen.

PaaS agrega una capa adicional de integración con marcos de desarrollo de aplicaciones, capacidades de middleware (Ver Anexo V: Glosario) y funciones como bases de datos, mensajería y colas. Estos servicios permiten a los desarrolladores crear aplicaciones en la plataforma con lenguajes de programación y herramientas que son compatibles con los servicios disponibles en la nube.

En PaaS, el usuario de servicios en la nube solo ve la plataforma, no la infraestructura subyacente. Existen servicios para ejecutar casi cualquier tipo de aplicación en cualquier lenguaje en PaaS, liberando a los desarrolladores de la configuración, creación y mantenimiento de servidores, así como de la complejidad de las agrupaciones y los equilibrios de carga.

Los beneficios y contrapartidas de un modelo de servicio PaaS son muy similares a los mencionados en un modelo SaaS: ambos permiten un despliegue muy eficiente de la aplicación, una gestión centralizada de la información y el proveedor se responsabiliza de la administración de la infraestructura. El **modelo PaaS ofrece**:

- la capacidad a las organizaciones, y más en concreto a sus desarrolladores, **de desarrollar y desplegar aplicaciones de una forma muy ágil.**
- **manteniendo un control centralizado sobre su operación y los datos que se procesan con ellas.**
- **delegando la configuración y mantenimiento de la infraestructura** de servidores, parches, actualizaciones, etc. en el proveedor.

Como contraprestación, el modelo PaaS:

- **dependencia muy alta de la conexión a Internet.**
- **exposición a los riesgos de seguridad intrínsecos de la utilización de los navegadores web.**
- la **migración de las aplicaciones** a servicios de otros proveedores –especialmente cuando se utilizan características de desarrollo específicas y nativas de un proveedor– **puede ser más complicada**,
- **el rendimiento de las aplicaciones puede verse penalizado** en determinadas circunstancias por la naturaleza propia de los desarrollos tipo PaaS
- y es necesario **reforzar el control sobre las medidas de seguridad en los desarrollos**.

—3.6.3 Infraestructura como servicio (IaaS)

En el modelo IaaS, el proveedor ofrece recursos de computación online como capacidad de procesamiento, red o almacenamiento de forma que el cliente pueda desplegar y ejecutar directamente cualquier software, incluyendo sistemas operativos y aplicaciones.

Así, el proveedor se encargaría de proporcionar y gestionar la infraestructura –el hardware, la red, las instalaciones físicas…– mientras el cliente mantendría el control sobre los sistemas operativos, almacenamiento y aplicaciones desplegadas, así como el control de los componentes de red virtualizados. Al contrario que en un modelo PaaS, un servicio IaaS no ofrecería una plataforma para el desarrollo de aplicaciones, administración de base de datos, *middleware*, etc.

Las instalaciones físicas y la infraestructura de hardware forman la base de un modelo IaaS. Con la computación en la nube abstraemos y agrupamos estos recursos, pero en el nivel más básico siempre necesitamos hardware físico, redes y almacenamiento para construir sobre ellos. Estos recursos se agrupan utilizando abstracción y orquestación. La abstracción, a menudo a través de la virtualización, libera los recursos de sus restricciones físicas para permitir la agrupación. Luego, un conjunto de herramientas básicas de conectividad y entrega (orquestación) vinculan estos recursos de abstracción en conjunto, crea los grupos y proporcionan la automatización para entregarlos a los clientes.

Todo esto se facilita mediante el uso de APIs. Las APIs generalmente son el método de comunicación subyacente para los componentes dentro de una nube, algunos de los cuales están expuestos al usuario de servicios en la nube para administrar sus recursos y configuraciones. La mayoría de las APIs en la nube actualmente usan REST (Transferencia de estado representacional), que se ejecuta sobre el protocolo HTTP, lo que lo hace extremadamente adecuado para los servicios de Internet. En la mayoría de los casos, esas APIs son accesibles de forma remota y se envuelven en una interfaz de usuario basada en web. Esta combinación es el plano de administración de la nube, ya que los consumidores lo usan para administrar y configurar los recursos de la nube, como el lanzamiento de máquinas virtuales (instancias) o la configuración de redes virtuales. Desde una perspectiva de seguridad, esta es la mayor diferencia al proteger la infraestructura física (ya que no puede confiar en el acceso físico como control) y la máxima prioridad cuando se diseña un programa de seguridad en la nube. Si un atacante ingresa en su plano de administración, es posible que tenga acceso remoto completo a toda su implementación en la nube.

Con todo, IaaS consta de una instalación, hardware, una capa de abstracción, una capa de orquestación (conectividad básica y entrega) para unir los recursos abstraídos y APIs para administrar de forma remota los recursos y entregarlos a los consumidores.

En general, las organizaciones que opten por este modelo deberán asumir responsabilidades operativas mucho mayores que con los modelos PaaS o SaaS; aunque el proveedor pueda proporcionar numerosas herramientas y soluciones para gestionar y administrar diferentes aspectos del servicio, la mayor parte de la responsabilidad de la operación será de la organización. Esta característica ofrece simultáneamente importantes beneficios y, a su vez, contrapartidas que deben ser consideradas:

- por un lado, la posibilidad de administrar y controlar el almacenamiento, los sistemas operativos, las aplicaciones, etc., permite **aumentar la eficiencia en el uso del hardware** para ejecutar las aplicaciones del modo en que la organización considere más necesario (ej.: con el sistema operativo que considere conveniente)

- o, sin ir más lejos, la **posibilidad de desplegar aplicaciones legacy** que se hayan podido quedar obsoletas pero que siguen siendo necesarias para la actividad del negocio.

En contrapartida:

- **la organización deberá disponer del conocimiento y los recursos necesarios** (bien sea internamente o apoyándose en terceros) para la gestión de las operaciones prestando especial atención a aspectos relacionados con la seguridad de la información y la actualización de los sistemas desplegados.

4 INCIDENTES EN LA NUBE

4.1 Introducción a los incidentes de seguridad

—4.1.1 ¿Qué entendemos por un incidente de seguridad?

Se entiende que un incidente de seguridad es cualquier evento o serie de eventos, inesperados o no deseados, que tienen una probabilidad significativa de provocar efectos adversos reales sobre los principios de la seguridad de la información habituales como:

- **Confidencialidad**: se define como la propiedad de la información que se mantiene inaccesible y no se revela a individuos, entidades o procesos no autorizados. [UNE-ISO/IEC 27000:2014]. Daño que causaría que se revelase información a un tercero sin la debida autorización.
- **Integridad**: se define como la propiedad de exactitud y completitud [UNE-ISO/IEC 27000:2014] consistente en que un activo no ha sido alterado de manera no autorizada. Corrupción, daño o modificación indebida de la información.
- **Disponibilidad**: se define como la capacidad de ser accesible y estar listo para su uso a demanda de una entidad autorizada. [UNE-ISO/IEC 27000:2014]. El perjuicio que causaría la falta de acceso a la información.

Además de otros principios que deben considerarse como:

- **Autenticidad**: se define como la propiedad consistente en que una entidad es lo que dice ser. [UNE-ISO/IEC 27000:2014]. Acceso ilícito a los datos debido a una falta de verificación de la identidad de las personas o elementos que interactúan con el sistema para la validación del acceso a la información.
- **Trazabilidad**: se define como la cualidad que permite que todas las acciones realizadas sobre un sistema de tecnología de la información sean asociadas de modo inequívoco a un individuo o entidad. [CESID:1997].

  - Del uso del servicio: entendido como el daño que causaría no saber quién hizo qué y cuándo.

  - Del acceso a los datos: entendido como el daño que causaría no saber quién accedió a qué datos y qué hizo con ellos.

—4.1.2 Clasificación de los incidentes de seguridad

En el Anexo V: Taxonomía se puede encontrar una taxonomía de incidentes de seguridad (Ver Anexo V: Glosario) basada en las recomendaciones de ENISA ("European Union Agency for Network and Information Security") para su aplicación como buenas prácticas de seguridad que ayudará a reconocerlos con mayor facilidad, ofreciendo una ventaja a la hora de su análisis, contención y erradicación.

En las distintas normas, regulaciones, guías de buenas prácticas... se presentan múltiples formas de clasificación de incidentes que pueden ser adoptadas total o parcialmente por las organizaciones que también pueden crear taxonomías propias adecuadas a situaciones de riesgo concretas. Una propuesta de clasificación podría ser la siguiente:

- Contenido abusivo:
  - **SPAM**: correo electrónico masivo no solicitado; el receptor del contenido no ha otorgado autorización válida para recibir un mensaje colectivo.
  - **Delito de odio**: contenido difamatorio o discriminatorio (ej.: ciberacoso, racismo, amenazas a una persona o dirigidas contra colectivos).
  - **Pornografía infantil, contenido sexual o violento inadecuado**: material que represente de manera visual contenido relacionado con pornografía infantil, apología de la violencia, etc.
- Contenido dañino:
  - **Sistema infectado**: sistema infectado con software malicioso (ej.: sistema, computadora o teléfono móvil infectado con un rootkit).
  - **Servidor C&C ("Mando y Control")**: conexión con servidor de control y mando ("command and control", 'C&C') mediante software malicioso o sistemas infectados.
  - **Distribución de software malicioso**: recurso usado para distribución de software malicioso (ej.: recurso de una organización empleado para distribuir software malicioso).
  - **Configuración de software malicioso**: recurso que aloje ficheros de configuración de software malicioso (ej.: ataque de webinjects para troyano).

- Obtención de información:

  -**Escaneo de redes**: envío de peticiones a un sistema para descubrir posibles debilidades incluyendo (o no) procesos de comprobación o testeo para recopilar información de alojamientos, servicios y cuentas (ej.: peticiones DNS, ICMP, SMTP, escaneo de puertos).

  -**Análisis de paquetes ("sniffing")**: observación y grabación del tráfico de redes.

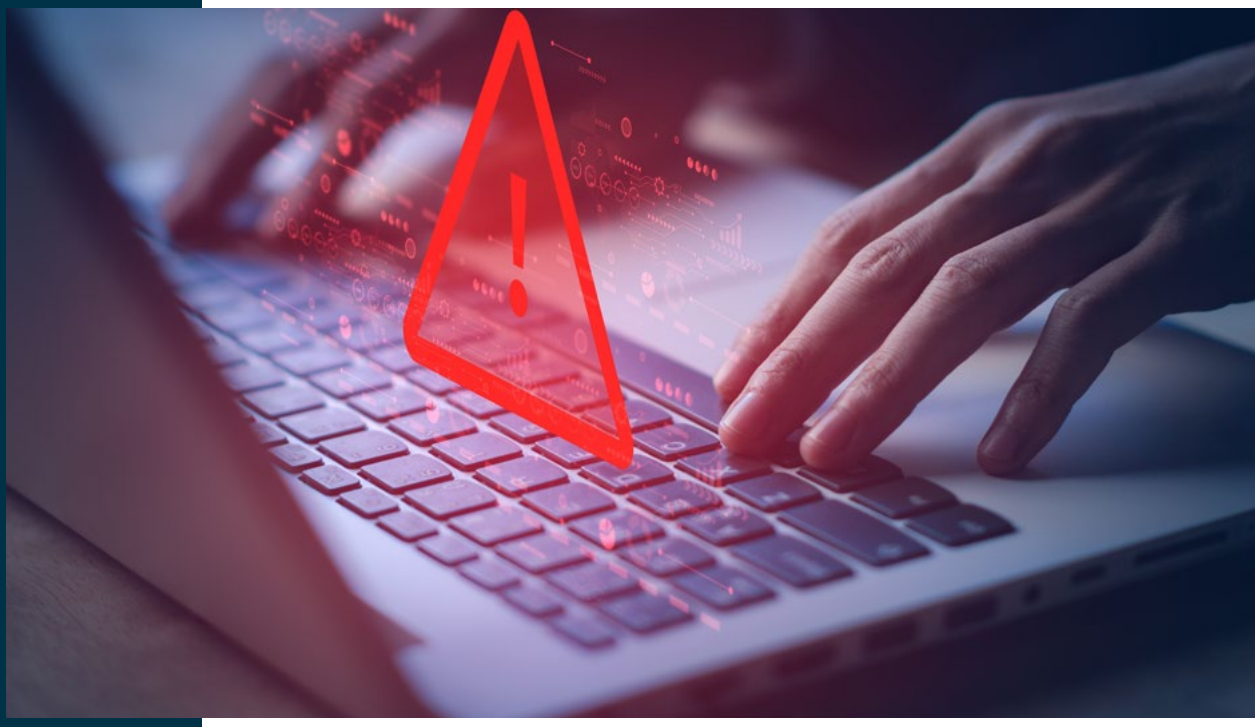
  -**Ingeniería social:** recopilación de información personal sin el uso de la tecnología (ej.: mentiras, trucos, sobornos, amenazas enviadas a los usuarios para obtener información y/o acceso a los sistemas).

- Intento de intrusión:

  -**Explotación de vulnerabilidades conocidas**: intento de compromiso de un sistema o de interrupción de un servicio mediante la explotación de vulnerabilidades con un identificador estandarizado, véase CVE (ej.: desbordamiento de buffer, puertas traseras, cross site scripting (XSS)).

  -**Intento de acceso con vulneración de credenciales**: múltiples intentos de vulnerar credenciales (ej.: intentos de ruptura de contraseñas, ataque por fuerza bruta).

  -**Ataque desconocido**: ataque que emplea una vulnerabilidad de la aplicación, red, sistema operativo y/o hardware desconocido por la organización.



- Intrusión:

  -**Compromiso de cuenta con privilegios**: compromiso de un sistema en el que el atacante ha adquirido privilegios.

  -**Compromiso de cuenta sin privilegios**: compromiso de un sistema empleando cuentas sin privilegios.

  -**Compromiso de aplicaciones**: compromiso de una aplicación mediante la explotación de vulnerabilidades de software (ej.: inyección SQL).

  -**Robo**: intrusión física (ej.: acceso no autorizado al centro de procesado de datos de la organización y sustracción de un equipo y/o hardware).

- Pérdida de disponibilidad:

  -**Ataque DoS (Denegación de Servicio)**: ataque en el que se ocasiona una denegación de servicio mediante el envío de un volumen de peticiones más alto del que es capaz de soportar el sistema (ej.: envío de peticiones a una aplicación web que provoca la interrupción o ralentización en la prestación del servicio).

  -**DDoS (Denegación Distribuida de Servicio)**: similar a un ataque de DoS, pero, en este caso, el atacante lo realiza de forma distribuida para que el ataque sea más difícil de detectar, así como de prevenir y responder a él (ej.: inundación de paquetes SYN, ataques de reflexión y amplificación utilizando servicios basados en UDP).

  -**Mala configuración**: configuración incorrecta del software sobre el que se soporta el servicio y que da lugar a problemas de disponibilidad del servicio. (ej.: un servidor DNS con un KSK de zona raíz DNSSEC obsoleto).

  -**Sabotaje: sabotaje físico** (ej.: cortes de cableados de equipos o incendios provocados).

  -**Interrupción del servicio**: interrupciones de los servicios por causas externas (ej.: desastre natural).

- Compromiso de la información:

  -**Acceso ilícito a información**: acceso no autorizado a información por parte de un agente interno o externo de la organización (ej.: robo de credenciales de acceso mediante interceptación de tráfico o mediante el acceso a documentos físicos).

  -**Modificación ilícita de información**: modificación no autorizada de información por parte de un agente interno o externo de la organización (ej.: modificación por un atacante empleando credenciales sustraídas de un sistema o aplicación o encriptado de datos mediante ransomware).

  -**Pérdida de datos**: pérdida de información (ej.: pérdida por fallo de disco duro o robo físico).

- Fraude:

  -**Uso ilícito de recursos**: uso de recursos para propósitos inadecuados, incluyendo acciones con ánimo de lucro (ej.: uso de correo electrónico para participar en estafas piramidales).

  -**Derechos de autor**: instalación de software u otro material protegido por derechos de autor sin la debida licencia o autorización por parte de su propietario.

  -**Suplantación de identidad**: usurpación de la identidad de una persona o una organización para obtener beneficios ilegítimos.

  -**Phishing**: suplantación de otra entidad con la finalidad de convencer al usuario para que realice alguna acción como puede ser la revelación de sus credenciales privadas, instalación de un software en su equipo u otro tipo de acción.

- Vulnerabilidad:

  -**Criptografía débil**: servicios accesibles públicamente que pueden presentar criptografía débil (ej.: servidores web susceptibles de ataques POODLE/FREAK).

  -**Amplificador DDoS**: servicios accesibles públicamente que puedan ser empleados para la reflexión o amplificación de ataques DDoS (ej.: DNS open-resolvers o Servidores NTP con monitorización monlist).

  -**Servicios con acceso potencial no deseado**: servicios accesibles públicamente potencialmente no deseados (ej.: Telnet, RDP o VNC).

  -**Revelación de información**: acceso público a servicios en los que potencialmente pueda revelarse información sensible (ej.: SNMP o Redis).

  -**Sistema vulnerable**: sistema con una debilidad que puede ser utilizada para un ataque y pone en riesgo la información gestionada en el mismo (ej.: mala configuración de proxy en cliente (WPAD), versiones desfasadas de sistema).

- Otros:

  -**APT**: ataques dirigidos contra organizaciones concretas, sustentados en mecanismos muy sofisticados de ocultación, anonimato y persistencia. Esta amenaza habitualmente emplea técnicas de ingeniería social junto con el uso de procedimientos de ataque conocidos o genuinos para conseguir sus objetivos.

  -**Otros**: todo aquel incidente que no tenga cabida en ninguna categoría anterior.

Cabe destacar que la peligrosidad de cada uno de estos tipos de incidentes de seguridad varía enormemente en función de múltiples factores, por este motivo, organizaciones reconocidas nacional e internacionalmente como el Centro Criptológico Nacional del Centro Nacional de Inteligencia de España (CCN-CERT) y el Instituto Nacional de Ciberseguridad de España (INCIBE-CERT) han desarrollado una guía de apoyo para determinar el nivel de peligrosidad de un incidente de seguridad.

El indicador de peligrosidad se fundamenta en las características intrínsecas al tipo de incidente y su comportamiento general, determinando la potencial amenaza que supondría la materialización de un incidente de seguridad de ese tipo en una organización.

Mediante la consulta de la siguiente tabla, la organización puede tener una idea del nivel de peligrosidad con impacto directamente asociado con la organización de un incidente de seguridad. Es muy importante remarcar aquí que la siguiente clasificación es orientativa y la organización debe realizar un análisis de negocio, así como evaluar el impacto que cada una de estas incidencias pueden tener en la propia organización para determinar el nivel de peligrosidad o riesgo asociado con cada tipo de incidente.

Nivel de peligrosidad	Clasificación	Tipo de incidente de seguridad
Crítico	Otros	APT
Muy alto	Contenido Dañino	Distribución de software malicioso
		Configuración de software malicioso
	Intrusión	Robo y/o acceso a información sensible
	Disponibilidad	Sabotaje
		Interrupción del servicio
Alto	Contenido abusivo	Pornografía infantil, contenido sexual o violento inadecuado
	Contenido dañino	Sistema infectado
		Servidor C&C (Mando y Control)
	Intrusión	Compromiso de aplicaciones
		Compromiso de cuentas con privilegios
	Intento de intrusión	Ataque desconocido
	Disponibilidad	DoS (Denegación de servicio)
		DDoS (Denegación distribuida de servicio)
	Compromiso de la información	Acceso no autorizado a información
		Modificación no autorizada de información
		Pérdida de datos
	Fraude	Phishing
	Contenido abusivo	Delito de odio
Medio	Obtención de información	Ingeniería social
	Intento de intrusión	Explotación de vulnerabilidades conocidas
		Intento de acceso con vulneración de credenciales
	Intrusión Disponibilidad	Compromiso de cuentas sin privilegios ni información sensible Mala configuración
	Fraude	Uso no autorizado de recursos
		Derechos de autor
		Suplantación de identidad
	Vulnerable	Criptografía débil Amplificador DDoS
		Servicios con acceso potencial no deseado
		Revelación de información Sistema vulnerable
Bajo	Contenido abusivo	Spam
	Obtención de información	Escaneo de redes (scanning)
		Análisis de paquetes (sniffing)

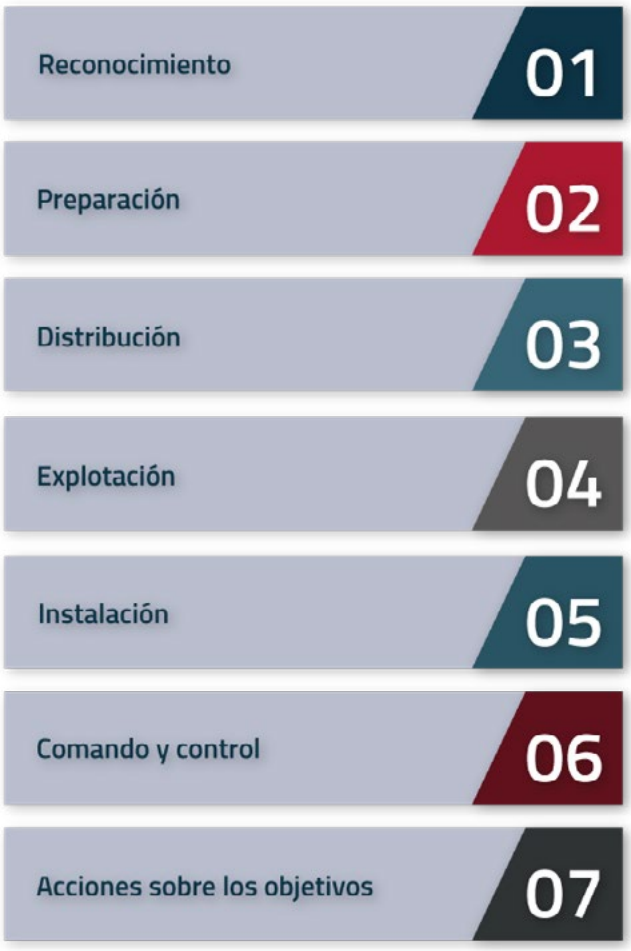
—4.1.3 Fases de un ataque

Un incidente de seguridad se produce tras un ataque, dicho ataque es un proceso dirigido con una intención concreta: conseguir unos resultados sobre un objetivo; robar datos que están en un servidor web o cifrar los contenidos de máquinas o contenedores en la nube para hacer que el usuario pague un rescate. Al tratarse de una secuencia de fases o cadena, una mitigación en cualquiera de ellas romperá la cadena y, por lo tanto, frustrará el ataque.

Además, cada ataque deja una serie de huellas de las que se puede aprender y utilizar para comprender a los adversarios y estudiar cómo realizan sus acciones. Esto permitirá diseñar defensas cada vez más efectivas y comprobar si las que tenemos son las más adecuadas.

La clave para detectar, detener, interrumpir y recuperarse ante un ataque radica en comprender cuál es su ciclo de vida y así desarrollar e implementar todas las operaciones necesarias que garanticen el mayor grado de seguridad y protección. A este ciclo de vida se le conoce en el mundo de la ciberseguridad como "Cyber Kill Chain".

La Cyber Kill Chain está formada por una secuencia de siete pasos, cada uno de los cuales supone una etapa del ataque:



4.1.3.1 Reconocimiento

Se trata de la fase en la que la ciberdelincuencia recopila información sobre su objetivo. Para ello, observa los detalles que la organización publica en fuentes de información públicas y busca información sobre las tecnologías que utiliza, así como datos en redes sociales e incluso puede realizar interacciones por correo electrónico con la organización.

Con esta información, el actor atacante valora qué métodos de ataque podrían funcionar y con qué probabilidad de éxito.

4.1.3.2 Preparación

En esta fase se prepara el ataque de forma específica sobre un objetivo a través del diseñor de software malicioso (ej.: virus, gusano, keylogger) y herramientas para la consecución del objetivo de ataque.

Los equipos informáticos desactualizados, un router o servidor publicado a Internet sin protección, no disponer de antivirus actualizado o una falta de concienciación en la protección de la información de las personas de la organización son algunas de las vulnerabilidades más comunes que acostumbran a poner en riesgo los datos de las organizaciones.

4.1.3.3 Distribución

En esta etapa se produce la transmisión del ataque (ej.: lanzar un software malicioso). Los métodos de distribución varían, pero las técnicas más comunes son:

- Ataque phishing.
- Dispositivos USB infectados.
- Explotación de una vulnerabilidad de software o hardware.
- Obtención de las credenciales de usuario.
- Introducción de software malicioso en programas/software de descarga regular.
- Hackeo de puertos abiertos u otro punto de acceso externo.

4.1.3.4 Explotación

Esta fase implica la «detonación» del ataque, comprometiendo a la máquina infectada y a la red o redes a la que pertenezca. Esto se suele producir explotando una vulnerabilidad conocida para la cual ya existe parche de seguridad, como en el caso de una vulnerabilidad del escritorio remoto que, de no estar parcheada, permitiría entrar en los equipos desde el exterior.

4.1.3.5 Instalación

Fase en la que el atacante instala el software malicioso en el sistema de la víctima. También puede darse la circunstancia de que no se requiera instalación como en el caso del robo de credenciales.

4.1.3.6 Comando y control

Llegados a este punto, el atacante cuenta con el control del sistema de la víctima en el que podrá ejecutar sus acciones maliciosas dirigidas desde un servidor central conocido como C&C ("Command and Control"), pudiendo sustraer credenciales, tomar capturas de pantalla, llevarse documentación confidencial, instalar otros programas, conocer cómo es la red del usuario, etc.

4.1.3.7 Acciones sobre los objetivos

Esta es la fase final en la que el atacante lleva a cabo las acciones concretas por las que ha accedido al sistema (ej.: robo de datos) e intenta expandir su acción maliciosa hacia más objetivos. En este punto, el atacante volverá a ejecutar las distintas fases de la Cyber Kill Chain de cara a infectar a más víctimas.

4.1.3.8 Conclusiones

Para poder romper la cadena de ataque y evitar que un atacante consiga sus objetivos será necesario estar verdaderamente comprometido con la ciberseguridad y disponer de un plan de acción que contemple tanto las personas, como los procesos, la tecnología y la cadena de suministro.

Una organización que mantenga todos sus sistemas y equipos actualizados utilice las soluciones de seguridad adecuadas, monitorice la actividad de sus comunicaciones y sus empleados cuenten con los conocimientos necesarios en ciberseguridad, aumentará considerablemente su capacidad para detectar y responder ante este tipo de incidentes de seguridad, poniéndoselo mucho más difícil a los adversarios y evitando que los sistemas y la información que en ellos se almacena se vean comprometidos.

—4.1.4 ¿Cuál puede ser la afectación de un incidente de seguridad?

Un incidente de seguridad puede tener afectación en una o más dimensiones de la seguridad de la información de los activos de una organización (confidencialidad, integridad y disponibilidad, así como autenticidad y trazabilidad).

Todo activo de la organización es susceptible de generar un impacto sobre la organización debido a la pérdida de cualquiera de las dimensiones de seguridad de la información aplicables. La gravedad de este impacto dependerá tanto de la dimensión de seguridad de la información afectada como del grado de severidad de la afectación. En el peor de los casos, la afectación de un incidente de seguridad podría suponer un perjuicio para la salud de las personas y hasta poner en peligro vidas humanas.

Con carácter ejemplificativo, a continuación, se muestran los posibles niveles de afectación para cada una de las dimensiones de seguridad de la información. En este sentido las organizaciones deben adaptar dichos niveles a las necesidades de sus negocios.

4.1.4.1 Confidencialidad

Niveles de afectación:

- **Muy alto**: la información afectada es confidencial y contiene datos de carácter personal.
- **Alto**: la información afectada es confidencial pero no contiene datos de carácter personal.
- **Medio**: la información afectada es interna y contiene datos de carácter personal.
- **Bajo**: la información afectada es interna pero no contiene datos de carácter personal.
- **No aplica**: la información afectada es de carácter público, por lo que no existen restricciones para su difusión.

4.1.4.2 Integridad

Niveles de afectación:

- **Muy alto**: la recuperación de la integridad de los datos no es viable y la información afectada no se puede reponer.
- **Alto**: la reposición de la información necesaria para recuperar la integridad de los datos supondría un alto coste para la organización.
- **Medio**: la reposición de la información necesaria para recuperar la integridad de los datos supondría un coste moderado, pero asumible para la organización.
- **Bajo**: la reposición de la información necesaria para recuperar la integridad de los datos supondría un bajo coste para la organización.
- **No aplica**: los errores en la información afectada carecen de consecuencias o son fácilmente reparables.

4.1.4.3 Disponibilidad

Niveles de afectación:

- **Muy alto**: la interrupción afectaría a la totalidad de los servicios.
- **Alto**: la interrupción afectaría a algunos servicios críticos.
- **Medio**: la interrupción afectaría a servicios de apoyo (ej.: correo, carpetas compartidas, sistema documental, etc.).
- **Bajo**: la interrupción afectaría a servicios secundarios no críticos cuya función puede dilatarse en el tiempo o realizarse de forma paralela por otros medios.
- **No aplica**: la interrupción del activo no afectaría a la disponibilidad de ningún servicio.

4.1.4.4 Autenticidad

Niveles de afectación:

- **Muy alto**: el descubrimiento de que la información afectada no es genuina o está corrupta causaría daños muy graves a la imagen de la organización o a la privacidad de las personas.
- **Alto**: el descubrimiento de que la información afectada no es genuina o está corrupta causaría daños graves a la imagen de la organización o a la privacidad de las personas.
- **Medio**: el descubrimiento de que la información afectada no es genuina o está corrupta causaría daños leves a la imagen de la organización o a la privacidad de las personas, sin que medie error o negligencia.
- **Bajo**: el descubrimiento de que la información afectada no es genuina o está corrupta causaría daños leves a la imagen de la organización o a la privacidad de las personas, ya que se debe a un error subsanable.
- **No aplica**: el descubrimiento de que la información genuina o está corrupta no es auténtica no causaría daños a la imagen de la organización o a la privacidad de las personas.

4.1.4.5 Trazabilidad

Niveles de afectación:

- **Muy alto**: la incapacidad para rastrear una acción sobre al servicio o a la información afectada impediría enormemente poder subsanar errores muy graves o la capacidad de perseguir delitos graves.
- **Alto**: la incapacidad para rastrear una acción sobre al servicio o a la información afectada impediría poder subsanar errores graves o la capacidad de perseguir delitos.
- **Medio**: la incapacidad para rastrear una acción sobre al servicio o a la información afectada impediría poder subsanar errores.
- **Bajo**: la incapacidad para rastrear una acción sobre al servicio o a la información afectada impediría poder subsanar errores leves.
- **No aplica**: la incapacidad para rastrear una acción sobre al servicio o a la información afectada no impediría poder subsanar errores o no dificultaría la capacidad de rastrear la comisión de delitos por otros medios.

4.2 Identificar – Proteger – Detectar: Preparativos ante incidentes de seguridad en la nube ante incidentes de seguridad en la nube

El objetivo de esta guía se centra en la respuesta y recuperación ante incidentes en la nube, como se detalla en los apartados 4.3 y 4.4. No obstante, en base a las buenas prácticas del NIST (Ver 5.3.2 Marco de Ciberseguridad (CSF) del Instituto Nacional de Estándares y Tecnología (NIST)) que el sector utiliza como estándar de facto, se describen las fases generales para afrontar los desafíos de seguridad en base al propio framework[3]; sin estas fases resumidas a continuación es imposible estar preparado para un incidente de seguridad.

- **Identificar**: desarrollar una comprensión de la organización para gestionar el riesgo de ciberseguridad sobre sistemas, personas, activos, datos y capacidades. Comprender el contexto empresarial, los recursos que respaldan las funciones críticas y los riesgos de ciberseguridad relacionados permite a una organización enfocar y priorizar sus esfuerzos, de acuerdo con su estrategia de gestión de riesgos.
- **Proteger**: desarrollar e implementar salvaguardas apropiadas para garantizar la prestación de servicios críticos.
- **Detectar**: desarrollar e implementar actividades apropiadas para identificar la ocurrencia de un evento de ciberseguridad.

Aunque estas fases pueden agruparse dentro de las actividades preventivas, la fase de detección puede formar parte del inicio de un incidente; durante esta fase se monitorizarán y alertarán las posibles brechas de seguridad que puedan existir en los entornos y sistemas de información, notificando aquellas identificadas con el correspondiente nivel de riesgo.

En este sentido, los indicios de que está ocurriendo un incidente pueden ser por dos tipos de fuentes:

- **Precursores**: indicio de que puede ocurrir un incidente en el futuro.
- **Indicadores**: indicio de que puede haber ocurrido o está sucediendo un incidente de seguridad.

La mayor parte de los incidentes no tienen precursores identificables o detectables. No obstante, uno de los objetivos principales es disponer de las herramientas y controles que puedan detectar la presencia de incidentes, permitiendo adoptar y acondicionar medidas de seguridad que eviten que este suceda.

Asimismo, los indicadores desplegados en la infraestructura de seguridad en la nube pueden proporcionar varios indicios en tiempo real de un posible incidente.

[3]https://www.nist.gov/cyberframework/framework

4.3 Responder: Respuesta ante incidentes de seguridad en la nube

Las organizaciones deben disponer de planes de actuación para cuando ocurra un incidente. La respuesta debe ser considerada como un proceso global y no como algo concreto de un sistema en la nube. No obstante, existen diferencias y características específicas, especialmente en entornos PaaS o SaaS, que deben ser tenidas en cuenta para complementar el proceso de respuesta ante incidentes de seguridad.

En este capítulo nos centraremos en describir lo qué hay que hacer una vez que se detecta un incidente de seguridad en la nube. La fase de respuesta es esencial para actuar de forma ágil y efectiva reduciendo los posibles impactos adversos consecuencia de un incidente de seguridad.

—4.3.1 Principales pasos de un incidente de seguridad en la nube

En esta sección, se describirán los principales pasos a seguir en el suceso de un incidente de seguridad en la nube, incluyendo (i) su identificación, (ii) la definición de objetivos y evaluación de la situación y (iii) las acciones de contención.

Estos pasos no se deben considerar como un listado de acciones a realizar de forma secuencial y sistemática, sino que se podrán acometer de forma paralela estableciendo una priorización.

—4.3.2 Identificación del incidente de seguridad

Una vez se detecta un incidente de seguridad resulta crítico conocer toda la información asociada con el incidente disponible y el impacto de este, con el objetivo de evaluar la situación, definir los objetivos y poder establecer medidas adecuadas de contención lo antes posible.

Las fuentes de datos para conocer más sobre el incidente pueden ser bastante distintas respecto a entornos tradicionales y puede ser más complicado acceder a ellas. En cualquier caso, en incidentes graves, deberíamos intentar que el proveedor nos facilite toda la información disponible y para ello es importante establecer esta necesidad en los contratos de servicio.

A continuación, describimos posibles orígenes que pueden alertarnos del incidente y que aportan información valiosa sobre el incidente:

- **Alertas provenientes de sistemas externos o terceras partes**: como pueden ser: proveedores/clientes que nos informan que han sido comprometidos, proveedores que nos ofrecen servicios de seguridad (como un Centro de Operaciones de Seguridad, 'SOC', o 'Threat hunting') y alertas y/o comunicaciones provenientes de sistemas en nube (ya sea en IaaS, PaaS, SaaS) y de los proveedores que nos dan el servicio en la nube.

- **Alertas provenientes de sistemas internos como pueden ser:** sistemas de protección del puesto de trabajo, sistemas de monitorización de red o de servidores, monitorización específica de seguridad (como SIEM o IDS/IPS), actividad inusual en usuarios (comportamiento anómalo, escalado de privilegiados, cuentas nuevas, etc.).

- **Comunicaciones de los atacantes o evidencias de compromiso en Internet**. En muchas ocasiones no identificamos el incidente hasta que el atacante toma contacto con nosotros (ej.: para pedirnos un rescate económico para liberar los datos que han sido cifrados tras un ataque de ransomware); en otras ocasiones, se evidencia la brecha de seguridad al detectarse información confidencial de la organización publicada en Internet o cuando se detecta a ciberdelicuentes vendiendo información de la organización en la Dark Web (ej.: como credenciales de usuarios con altos privilegios).

Estas informaciones deben ser validadas y complementadas mediante investigaciones adicionales, con el fin obtener información útil para fases posteriores y de identificar posibles falsos positivos. En general, antes de concluir que es un falso positivo, es recomendable el continuar con la investigación y validar las evidencias obtenidas. En ocasiones, se tratarán de incidentes menores o ataques sin éxito que no han evolucionado, pero mejor actuar con cautela. Además, estos eventos nos servirán para probar nuestros procesos de respuesta.

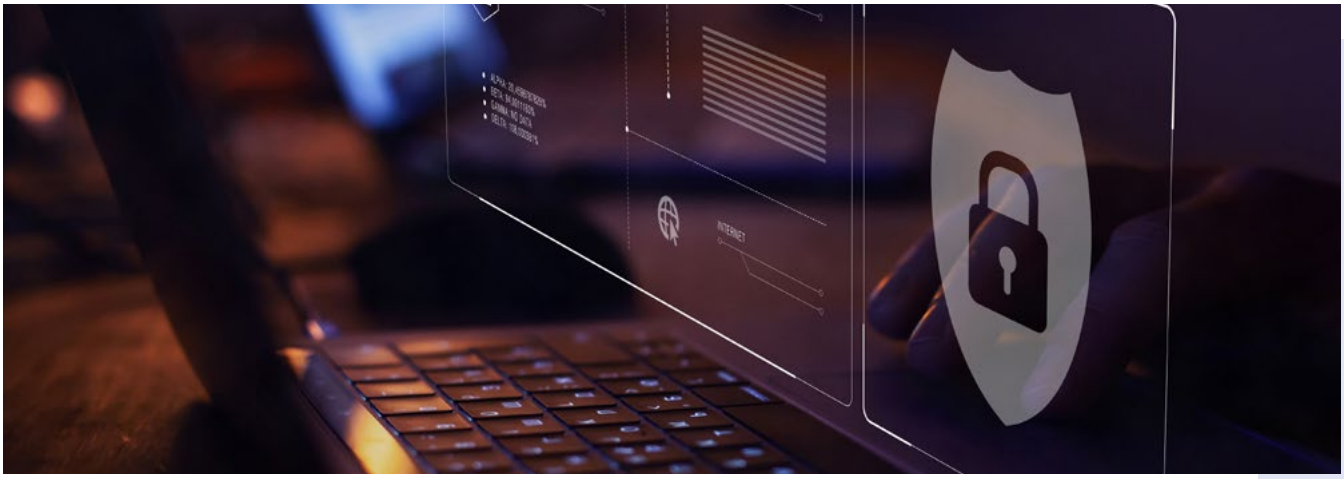
Hay que tener en cuenta que la investigación se realizará de forma muy diferente según el tipo de servicio en la nube y la relación existente con los proveedores (ej.: la resolución de un incidente de seguridad en una nube privada personalizada en un centro de datos de terceros será muy distinta a la que se lleve a cabo en una aplicación SaaS en la que probablemente hayamos aceptado las condiciones estándares del proveedor y quizá no tengamos ni siquiera un contacto directo al que recurrir).

En estas investigaciones se recomienda responder y en colaboración con los actores necesarios (ej.: el proveedor de servicios en la nube) a preguntas como las siguientes:

- ¿Cómo se ha detectado el incidente?
- ¿Qué información y tecnología se han visto afectados? ¿En qué servicios de la nube (IaaS, PaaS, SaaS) y sistemas (ej.: cuentas, procesos, ficheros...)? ¿La información afectada está regulada, es decir, existe una ley que obligue a realizar ciertas acciones en caso de que se produzca un incidente sobre los datos?
- ¿Hay personas involucradas en el incidente? ¿En qué medida?
- ¿Cuándo ha sucedido?
- ¿Por qué se produjo el incidente? ¿Cuál ha sido el vector de entrada o el detonante del incidente?
- ¿Cómo ha sucedido el incidente?

A la hora de clasificar el incidente, como se ha visto en el apartado 4.1.1, es necesario disponer por anticipado de una taxonomía (Ver Anexo IV: Taxonomía) de incidentes.

Adicionalmente se obtendrá la información disponible en los sistemas que dependerá en gran medida del tipo de incidente. Se podrán revisar logs, modificaciones en cuentas, procesos o ficheros críticos, tráficos y conexiones, actividad en el firewall, etc.En este sentido y un aspecto importante, es establecer las medidas adecuadas relativas a la cadena de custodia y la preparación del análisis forense. Hay que evitar que nosotros y nuestros proveedores eliminemos información valiosa. En entornos que están en nube, existen muchas tareas automatizadas que pueden provocar que se pierda información valiosa para la investigación, por lo que habrá que solicitar al proveedor que suspenda esos procesos automáticos o que realice medidas concretas y que serán descritas más adelante (ej.: instantáneas) durante el proceso de análisis de lo sucedido.



—4.3.3 Definición de objetivos y valoración de la situación

Una vez hemos identificado un incidente y antes de iniciar las tareas de contención, erradicación y recuperación, es muy importante definir los objetivos a la vez que valorar la situación.

Los objetivos principales en la gestión de incidentes acostumbran a dividirse en 3 áreas:

Minimizar el tiempo de recuperación:

- El primer objetivo que nos vamos a fijar es el de minimizar el tiempo desde que el incidente ocurre hasta que nos recuperamos de él. Este tiempo incluye la identificación del incidente, el análisis, y las acciones para contener, erradicar y recuperarse;
- Si queremos minimizar el tiempo total, tendremos que definir bien estas etapas, sus procesos de gestión, los equipos involucrados, y la gestión de las comunicaciones. Lo más detallado estén los planes, mejor para la empresa;
- Y si es posible, estos planes de acciones deben de ser probados y mejorados continuamente;

Minimizar los impactos para la empresa:

- Cuando los equipos trabajan en la gestión, contención, erradicación y recuperación del incidente, los equipos operacionales tienen que minimizar los impactos operacionales que puede causar en la empresa, incluidos impactos legales o regulatorios;
- Para esto, es muy importante iniciar con un análisis del impacto en tiempo real, es decir, identificar cuáles son los impactos ahora y en las próximas horas o días. Las acciones, tanto tácticas como estratégicas, que vamos a definir e implementar se harán con el objetivo de minimizar los impactos;
- En esta etapa, hay que también pensar en el proceso de retorno a la normalidad, e identificar las acciones a realizar en función de los impactos identificados y analizados;

Gestión de la relación con nuestros clientes y partes interesadas:

- Si bien ningún cliente quiere que su proveedor de servicios o productos tenga un incidente y sea impactado, acostumbra a suceder que una buena gestión del incidente refuerza la relación con sus clientes. Esto incluye una comunicación proactiva cuando sea necesario y una propuesta de planes alternativos;

- La gestión de la comunicación con los clientes se puede realizar de una forma proactiva, reactiva o las dos a la vez. Esto dependerá del análisis de impacto realizado y de cómo la dirección de la organización quiere gestionar la comunicación con los clientes;

- Para gestionar bien una comunicación con los clientes, es importante que el equipo de comunicaciones prepare un listado de preguntas y respuestas tipo (FAQ) para los equipos que gestionan las relaciones con los clientes y pueda responder de una manera reactiva a las preguntas iniciales. También habría que preparar un informe del incidente, que se pueda enviar por correo electrónico a los clientes cuando sea oportuno;

- Siempre los documentos deben ser revisados por el equipo legal o acudir a terceros si fuese necesario. Es posible que tengamos alguna cláusula de notificación con algunos de los clientes, es importante considerar este aspecto;

- También hay que tener en cuenta si se realizan notificaciones a las autoridades debido a una fuga de los datos de nuestros clientes; aquí el equipo legal tendría que hacer el análisis y decidir la manera de proceder.

Valorar la situación es una de las etapas más importantes en la gestión de incidentes: una vez hemos sido notificados de un incidente, debemos saber cuáles son los impactos en el negocio, pues esto puede variar dependiendo del día y mes del año o incluso de la hora en que acontece el evento.

Si bien la valoración inicial ayudará a definir las acciones a tomar, tanto táctica como estratégicamente, hay que pensar en el peor de los casos e identificar cuáles serían los posibles impactos (de nuevo, en la peor de las situaciones). Esto ayudará a decidir las acciones a realizar, así como cuándo y cómo activar os planes de continuidad.

Los incidentes no llaman a la puerta y, cuando ocurren, hay que tener muy claro los objetivos que queremos y tenemos que cumplir. Una valoración inicial correcta facilitará todas las tareas de recuperación, ayudará en la gestión del incidente y en la reducción dl impacto para el negocio.

—4.3.4 Acciones de contención

Dentro del proceso de contención, el objetivo principal es reducir el impacto de un posible incidente de seguridad aislando los servicios/dispositivos afectados evitando la propagación a otros sistemas en la nube o en nuestra red.

Si bien esto puede parecer simple, hay algunas consideraciones clave durante esta parte del proceso de respuesta que pueden ayudar a limitar el daño y al mismo tiempo preservar la evidencia forense crítica, que es clave. En muchas organizaciones más pequeñas que no cuentan con un equipo de respuesta a incidentes dedicado, ésta será la parte más crítica del proceso de respuesta antes de llamar a un tercero para obtener ayuda en el proceso de análisis y erradicación. Los errores aquí podrían afectar a la red y hacer imposible una mayor investigación.

Veamos algunas de las partes clave del proceso de contención.

4.3.4.1 Pasos para aislar el incidente

Una de las primeras cosas que debe hacer una vez que haya identificado un incidente es determinar si se puede aislar. Si se trata de un solo sistema que se ve afectado, eso puede ser tan fácil como desconectar el cable que lo conecta a su red interna y/o desactivar el adaptador inalámbrico, pero en algunos casos, desconectarlo de una red inalámbrica puede ser imposible debido a que múltiples sistemas a través de la red pueden verse afectados y los sistemas sin afectación pueden ser desconocidos o, incluso peor, tal vez la víctima es uno de los servidores críticos del negocio de la organización y es complicado o inviable desconectarlo.

En cualquier caso, es recomendable disponer de un proceso documentado y probado para determinar el alcance potencial del incidente y luego establecer las acciones oportunas. Estos pasos deben tener como objetivo aislar el incidente.

Hablando de sistemas en la nube, en particular, donde no hay posibilidad de aislamiento físico, es necesario considerar las soluciones de protección de equipos finales, así como los productos EDR que tienen capacidades de aislamiento/sandboxing y que también podrían usarse para cumplir con la intención de esta parte del proceso.

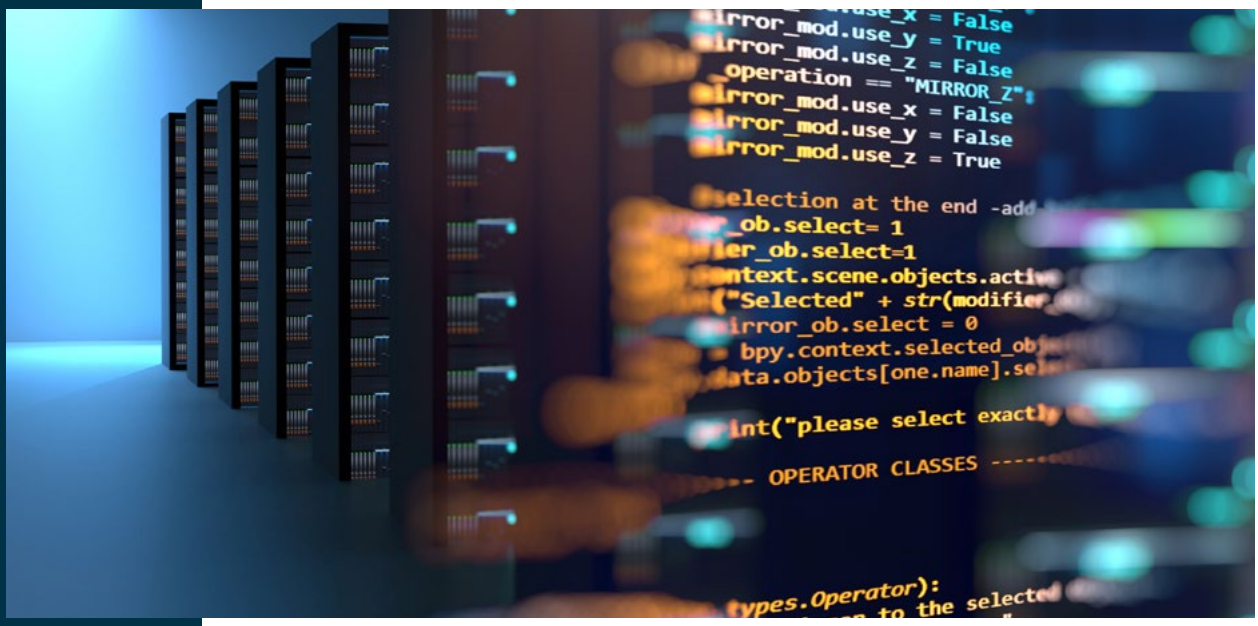
Finalmente, si los sistemas no se pueden aislar fácilmente y son críticos para el negocio, es importante obtener algún tipo de aprobación documentada a nivel ejecutivo para una excepción para ese/os sistema/s que no se pueden aislar y/o parar, mientras trabaja en el resto del proceso de respuesta. Esta aprobación puede resultar fundamental para demostrar que se realizó la diligencia debida en ese caso y, al mismo tiempo, negocio pidió que no se bloquearan los procesos principales.

4.3.4.2 Determinar indicadores de compromiso

Para determinar el alcance del aislamiento o comprender si los pasos de aislamiento que ha tomado fueron efectivos, es posible que deba identificar indicadores de compromiso (IOC). Esto no siempre es posible y puede no ser realista según el tipo de incidente o las capacidades técnicas de su equipo, pero los IOC pueden ayudar a buscar evidencia de propagación en la red, y será información muy válida en el proceso de análisis forense o a la hora de obtener ayuda de una organización de terceros especializada en respuesta a incidentes.

4.3.4.3 ¿Hay disponibles copias/imágenes de los sistemas afectados?

Otra consideración que puede o no ser parte de su repertorio técnico es la capacidad de generar imágenes forenses de los sistemas infectados. Una vez que haya aislado estos sistemas, se pueden tomar copias de máquinas virtuales (ej.: instantáneas) o imágenes forenses para facilitar el proceso de investigación y permitir que su equipo continúe con el proceso de recuperación. Si se está considerando un litigio debido a este incidente, es recomendable dejar los sistemas aislados y dejar que los expertos (terceros certificados que puedan presentar periciales con validez legal) se encarguen de esta parte. Mantener procesos de imágenes de sistemas y una cadena de custodia documentada es fundamental para el caso de determinar el alcance y responsabilidades jurídicas o de cumplimiento, así como para que las pruebas de los análisis forenses sean válidas delante de un juzgado.



—4.3.5 ¿Hay copias de seguridad disponibles para los sistemas afectados?

Junto con la contención, se deben considerar los próximos pasos mientras aislamos y controlamos la propagación de un posible incidente. En un incidente real no hay que olvidar las opciones que pueden cambiar según la afectación del incidente, los datos están en riesgo en los dispositivos infectados ni las opciones de copia de seguridad/recuperación que tenemos disponibles. Documentar las opciones de recuperación y el tiempo de pérdida/recuperación de datos asociado con esas opciones ayudará a informar algunas decisiones potencialmente difíciles que tendrá que tomar (junto con la aceptación de la gerencia) en algún momento de las fases posteriores del proceso de respuesta a incidentes.

En resumen, si bien la pregunta principal que debe responder durante la fase de contención es: "¿tengo este incidente aislado y bajo control para limitar el impacto en el resto de la red?"; es importante pensar y planificar estos elementos con anticipación, incluso si ese plan es simplemente delegar la gestión de la incidencia indicando a quién llamar en caso de que se produzca un evento de este tipo.

4.4 Recuperar

Siguiendo lo establecido por el marco de ciberseguridad de NIST en cuanto a respuesta a incidentes nos hallamos en la última fase del ciclo de vida de un incidente de seguridad de la información.

La norma ISO22301, "Sistema de Gestión de Continuidad de Negocio", así como la "Guía de Gestión de Continuidad de Negocio para Pymes" publicada por ISMS Forum son referencias de buenas prácticas para identificar los procesos, medidas y controles que se pueden tener en cuenta de cara a la recuperación de la actividad de una organización.

Los objetivos principales de la fase de recuperación son:

- Asegurar que la organización tiene procedimientos de recuperación para restablecer los servicios afectados por un incidente reduciendo al máximo un impacto negativo en la organización.
- Implementar mejoras basadas en lecciones aprendidas y revisiones de estrategias existentes.
- Gestionar la comunicación interna y externa durante y después de la recuperación de un incidente de seguridad de la información.
- Garantizar el cumplimiento normativo y legislativo durante la gestión de un incidente.

La recuperación de la actividad, a nivel técnico estará condicionada por los siguientes factores:

- Tipo de servicio contratado en la nube (PaaS, IaaS, SaaS).
- Acuerdos de nivel de servicio establecidos con el proveedor de nube.
- Existencia o no de una estrategia de recuperación ante desastres definida e implementada en el momento del incidente.
- Normativas y/o leyes que aplicables.

Hay dos aspectos clave a considerar para afrontar una adecuada estrategia de recuperación frente a un incidente:

- El momento en que iniciar la recuperación.
- La priorización de servicios a recuperar.

El proceso de recuperación de la actividad digital de una organización frente a un incidente TIC, incluida la nube, debe ser contemplada desde una perspectiva empresarial, considerando no sólo la dificultad tecnológica sino también el impacto en las funciones esenciales de la organización y sus compromisos. Es por ello conveniente identificar una figura de 'coordinación del proceso de continuidad de negocio' que, preferiblemente, será una persona de la organización con el conocimiento de la mayoría de los procesos de negocio y cuyas funciones serán:

- Antes de un incidente: ayudar a la dirección a identificar los procesos críticos de la organización, los riesgos existentes y, en base a ello, desplegar las acciones necesarias de mitigación de estos de acuerdo con las expectativas de la dirección.
- Durante el incidente: colaborar con las áreas implicadas en la respuesta al incidente, aportando su conocimiento experto en la metodología de continuidad de negocio existente, recordando las prioridades de la organización.
- Después del incidente: revisar los procesos y las actividades llevadas a cabo para extraer las lecciones aprendidas y aplicar las medidas correctivas y opciones de mejora oportunas.

Un incidente complejo no requiere sólo de respuestas técnicas, es un ejercicio de liderazgo y trabajo en equipo. En la medida que la coordinación de continuidad de negocio haya tenido oportunidad de preparar a la organización para responder a estos tipos de incidentes se recuperará antes la organización.

—4.4.1 Identificar el momento adecuado para iniciar la recuperación

En función de las características de la incidencia, la estrategia de recuperación será distinta. De este modo, frente a un incidente de seguridad grave se deben considerar varios aspectos clave antes de iniciar el proceso de recuperación de los aspectos técnicos tales como la sofisticación del ataque y la disponibilidad de recursos.

4.4.1.1 La sofisticación del ataque

Los ataques más avanzados consiguen implementar mecanismos de detección y ofuscación del software malicioso frente a la respuesta de forma que, si se inician tareas de recuperación antes de que el incidente esté contenido y erradicado, no se eliminarán los vectores de ataque y/o vulnerabilidades que permitieron el ataque en primera instancia y la incidencia se podrá replicar.

4.4.1.1 La sofisticación del ataque

Los ataques más avanzados consiguen implementar mecanismos de detección y ofuscación del software malicioso frente a la respuesta de forma que, si se inician tareas de recuperación antes de que el incidente esté contenido y erradicado, no se eliminarán los vectores de ataque y/o vulnerabilidades que permitieron el ataque en primera instancia y la incidencia se podrá replicar.

4.4.1.2 La disponibilidad física y emocional de las personas necesarias

Todos los pasos que siguen la respuesta a incidentes son importantes y, aquí, la gestión de la incertidumbre y el agotamiento de las personas puede convertirse en un obstáculo. Por ello es importante proporcionar la información adecuada a las personas resolutoras del incidente y gestionar bien sus periodos de descanso para evitar que el estrés de la situación y el cansancio causen errores y se agrave la incidencia.

—4.4.2 Establecer prioridades para la recuperación

La recuperación de servicios TIC, estén ubicados en la nube o en local, es conveniente abordarla desde una perspectiva global, más allá de los puros servicios tecnológicos y a través de un Plan de Continuidad de Negocio ("Business Continuity Plan" o 'BCP') con el que se clasificarán y se priorizarán los servicios a recuperar.

Para mayor detalle sobre los conceptos básicos de la continuidad de negocio, así como la forma de identificación y evaluación de los riesgos y costes asociados, se puede consultar la "Guía de continuidad de negocio para PyMEs" en la que se aborda el tema de forma sencilla y didáctica.

—4.4.3 Recomendaciones técnicas de recuperación

Una vez establecidas las bases para comenzar la recuperación, se deberá proceder a la carga de los datos y a restaurar los servicios de mayor a menor criticidad para la organización.

El proceso de recuperación consta de dos fases:

- Restauración del servicio.
- Procedimientos de soporte y gestión.

—4.4.4 Restauración del servicio

Las acciones asociadas con la restauración del servicio deben realizarse de forma que se ocasione el menor impacto posible en los usuarios y la organización. En este punto, la organización implementará los planes de contingencia corporativos establecidos en sus respectivos planes de recuperación ante desastres y planes de continuidad priorizando los procedimientos de restauración de los sistemas considerados críticos.

—4.4.5 Procedimientos de soporte y gestión

Una vez restaurados los servicios, se precisa comprobar su correcto funcionamiento y, para ello, cada responsable de servicio deberá verificar que los procesos asociados con este se ejecutan de la forma esperada. En este sentido, la organización deberá determinar si, además de la persona responsable del servicio la restauración de este requiere la intervención de otras áreas de negocio para garantizar no sólo que la operativa funciona adecuadamente, sino que se cumplen los acuerdos establecidos con terceros, así como la normativa, leyes y regulaciones que fueran de aplicación.

4.5 Otras consideraciones técnicas

En el caso de que algún desastre afecte al centro de procesamiento de datos principal de forma irrecuperable, tanto si está ubicado en local como en una nube, es una buena estrategia utilizar los servicios de nube pública, de hecho, es una de las últimas tendencias incorporar los servicios de nube pública para albergar el o los data center de contingencia; una de sus ventajas es la flexibilidad de costes y de administración, así como a la facilidad de establecer arquitecturas en alta disponibilidad.

Las copias de seguridad deberán cifrarse y la administración de las claves de cifrado para la recuperación de copias de seguridad deberá ser rigurosa y sistemática; para ello existen herramientas propias de cada fabricante de soluciones de gestión de copias de seguridad o de servicios en la nube. Además, se deberá contemplar tanto el uso de herramientas de administración de claves de cifrado como el uso de credenciales específicas disponibles en la nube como medio de poder acceder a la claves y credenciales de administración en situación de crisis.

Es importante tener en cuenta que ante la alternativa de disponer un DRP basado en nube, existen distintos planteamientos o mejor dicho “productos o líneas de servicio” para desarrollar el DRP en función de la criticidad de los datos a salvaguardar o al presupuesto destinado para ello.

Así la mayoría de los proveedores de servicios en la nube disponen de productos de almacenamiento capaces de satisfacer objetivos exigentes de tiempo de recuperación (RTO), los objetivos de punto de recuperación (RPO), así como otros requisitos de cumplimiento normativo.

En la sección de referencias se menciona documentación y guías de buenas prácticas de los principales proveedores de servicios en la nube.

4.6 Gestión de la comunicación

Como venimos repitiendo a lo largo del capítulo, la recuperación de la actividad ante un incidente de seguridad supone un proceso empresarial completo, además de técnico, por ende, la gestión de la comunicación forma parte fundamental de una adecuada respuesta.

Pero ¿qué entendemos por "comunicación"? Aquí tomaremos el significado amplio considerando todos los contactos y las notificaciones que establecen interlocutores y canales autorizados de la organización para responder al incidente, desde que se detectan los primeros indicios del incidente hasta que se decreta el cierre.

En este punto, es tan importante que la gestión de la crisis se realice de forma adecuada como que se perciba de esta forma por la opinión pública y de las partes interesadas de la organización (ej.: clientes, colaboradores, accionistas…). Sobre estos últimos, es imprescindible que durante la preparación del plan de respuesta ante incidentes y antes de que se materialice un incidente de seguridad, la organización identifique quienes son estas "partes interesadas", así como las personas que actuaran desde el lado de la organización y desde el otro lado cuando se produzca un incidente; algunos ejemplos de partes interesadas serían:

- Asociados y accionistas.
- Clientes.
- Profesionales de la organización:
    - o Dirección.
    - o Profesionales no directivos.
    - o Otros profesionales.
    - o Representantes de los trabajadores.
- Proveedores de servicios.
- Administración pública (ej.: fuerzas y cuerpos de seguridad, inspectores…).
- Compañía aseguradora.
- Otros (ej.: compañía aseguradora…)

Es recomendable que la organización designe a una persona para el liderazgo del plan de comunicación, en este sentido puede ser el Área de Comunicación u otra área que la organización considere adecuada, pero, en todo caso, para la consecución del plan se deberá involucrar, además del Área de Comunicación, al Área de Asesoría Juridifica, Privacidad, Cumplimiento, TI y Seguridad de la información, así como otras áreas que pudieran verse impactadas por el incidente.

Durante la crisis es imprescindible que haya un único discurso compartido por los distintos miembros de la organización, que exista transparencia y se pongan en valor las acciones realizadas informando de forma periódica a las partes interesadas de las acciones llevadas a cabo.

4.7 Lecciones aprendidas

Para ayudar con la resolución de los incidentes de seguridad, existe un decálogo de aspectos a tener en cuenta en las estrategias de gestión de incidentes:

1. Decir siempre la verdad evitando emitir juicios personales sin base en criterios profesionales. Nunca mentir.

2. El silencio no es rentable. Toda información sobre el incidente y/o activos afectados puede ser de valor. Ocultar información u omitirla por creer que puede ser inútil puede ser perjudicial para el desarrollo de la resolución del incidente.

3. La crisis como oportunidad. Una vez superada, la crisis -al igual que ocurre, por ejemplo, con la gestión de quejas- es una excelente oportunidad para corregir errores y poner los medios para evitarlos en el futuro. Ya que la hemos sufrido, aprovechémosla.

4. La clave: prevención. La correcta gestión de una crisis comienza con su prevención. Cuanto mejor preparados estemos, más ahorraremos posteriormente en daños económicos y de reputación.

5. Proactividad. Es indispensable que exista una clara dirección de la crisis desde el primer momento, los roles de liderazgo en cada una de las etapas deben estar definidos y comunicados a todas las partes que intervienen en el plan de gestión de incidentes para evitar el caos, desorganización o parálisis cuando se produzca un incidente.

6. Transmitir confianza. En todo momento es importante que las partes interesadas mantengan la confianza en la organización, por lo tanto, se debe prestar especial cuidado en las acciones y comunicaciones que se les realicen.

7. Comité de crisis. Las personas que lo integren deben saber en todo momento qué deben hacer para no dejar nada a la improvisación y deben estar informadas de todo lo que está sucediendo entorno al incidente de seguridad.

8. Comunicación interna y externa. Muy centrada en la externa, la comunicación de crisis no debe descuidar su versión interna para evitar que los empleados de una organización, (ej.: publicaciones ilícitas en la prensa).

9. Gestión de las emociones. La gestión de otro tipo de aspectos, incluidos los económicos, debe quedar en un segundo plano cuando nos enfrentamos a una crisis que afecta directamente a personas, especialmente en casos de gravedad.

10. Manual de comunicación de crisis. Es importante disponer de una guía sencilla y práctica como herramienta básica para afrontar cualquier crisis y saber en cada momento quién hace qué y con qué propósito.

Con lo anterior, a pesar de ser una de las partes más importantes de la respuesta a incidentes ya que nos ayuda a identificar los puntos fuertes y aspectos de mejora en el plan de gestión de incidencias, las lecciones aprendidas a menudo se omiten al finalizar la fase de recuperación del incidente y esto puede ocasionar que se repitan errores en eventos futuros.

Una vez concluida una crisis, los equipos de respuesta a incidentes deben valorar las acciones llevadas a cabo para la detección, contención y respuesta del incidente para obtener conclusiones y aprendizajes que les permitan mejorar y optimizar futuras respuestas a otros incidentes. En esta línea, diferentes normas (ej.: ISO/IEC 27001) abogan por celebrar comités de lecciones aprendidas en los que deberán participar los integrantes de los diferentes equipos que hayan intervenido en la respuesta de un incidente y donde se deberían tratar aspectos cómo:

- Causas y evolución del incidente, ¿qué ocurrió exactamente?
- Valoración del papel del personal técnico y directivo en sus respectivos roles.
- Valoración de las políticas y procedimientos de gestión de incidencias (y otros de apoyo) previamente definidos y utilizados en el tratamiento del incidente.
- Valoración de las medidas y los controles existentes.
- Acciones ejecutadas que fueron efectivas y acciones innecesarias o podrían haberse realizado de una forma más óptima.
- Acciones efectivas y mejoras en el plan de comunicación.
- Acciones efectivas y mejoras en la coordinación entre las personas y áreas involucradas.
- Acciones preventivas y correctivas para prevenir incidentes similares en el futuro.
- Herramientas o recursos adicionales que se necesitan para detectar, analizar y mitigar futuros incidentes.

Además de la celebración de comités, otra táctica para extraer lecciones aprendidas de incidentes de seguridad es la de usar un cuestionario de autoevaluación similares al siguiente:

- ¿Cuál ha sido su rol en este incidente?
    - o Formo parte del equipo de respuesta a incidentes de seguridad.
    - o Formo parte del Comité de Continuidad (o órgano similar de coordinación si existe).
    - o No estoy en ninguno de los casos anteriores.
- Describe los puntos fuertes sobre la gestión de este episodio que quieras destacar (ej.: aspectos técnicos, de coordinación, de comunicación...).
- Indica oportunidades de mejora detectadas desde una perspectiva tecnológica (si las has identificado).
- En el caso de que los conozcas, ¿crees que se han cumplido los niveles de servicio de la organización? (S/N); indica comentarios si procede.
- Indica oportunidades de mejora en aspectos asociados con los procedimientos o de servicio.
- Indica oportunidades de mejora en aspectos asociados con el Plan de comunicación.

- ¿Crees que habría sido necesario implicar a algún otro interlocutor en la gestión del incidente? En caso afirmativo explica por favor el motivo.
- Otros aspectos que quieras destacar.

4.8 Acciones generales

Este apartado recopila, a modo de puntos de control, las distintas acciones y tareas que deben ser ejecutadas en cuanto es declarado un incidente de ciberseguridad.

—4.8.1 Prerrequisitos

Los prerrequisitos básicos para agilizar la gestión del incidente son:

- Inventario de activos:
    - o Nombre de máquina, direcciones IP, responsable, clasificación de criticidad o sensibilidad de la información.
    - o Inventario de conexiones remotas (usuarios y accesos de proveedores / clientes).
    - o Listado de propietarios de los activos.
- Mapa de servicios (relaciones entre activos).
- Arquitectura de red y de sistemas con identificación de flujos de tráfico más importantes.
- Lista de contactos de los diferentes departamentos involucrados (ej.: listado de administradores, responsables de los negocios, proveedores...).
- Lista de contactos de los proveedores de los servicios críticos, así como servicios de soporte y servicios de seguridad de la información (incluyendo los proveedores de servicios de respuesta ante incidentes).
- Póliza de ciberseguro (coberturas y franquicias).

5 ESTADO DEL ARTE

Cada día es más frecuente que las PyMEs, siguiendo la tendencia que ya se viene observando en las grandes organizaciones, recurran a servicios en la nube.

Como quiera que sea, una vez que una organización decide contratar a un proveedor los servicios en la nube, es fundamental que esté al tanto de la estrategia de Seguridad de la Información de dicho proveedor y que esté preparada para dar respuesta a los incidentes de seguridad que pudieran surgir con dichos servicios. Entre otros aspectos, es importante que la organización analice qué tipos de datos va a trasladar a la infraestructura de la nube (ej.: si estos son o no de carácter personal, están regulados o son sensibles), cuál es el tratamiento que se va a hacer de éstos, y qué requisitos de ubicación de estos se contempla. Con esto, la organización debe conocer las medidas de seguridad que ofrece el proveedor y la trazabilidad de los elementos que incorporará a sus infraestructuras; de esta forma, en el caso de un incidente de seguridad, podrá tomar las medidas adecuadas para mitigarlo, a la vez que será más fácil su prevención.

Aunque no existe una ley específica relativa al uso de la nube ni a la gestión de incidentes en la nube, sí contamos con un marco jurídico y normativo general, cuya aplicación es de obligado cumplimiento en unos casos y sirve como guía de actuación en otros. Así, podemos abordar los aspectos jurídicos del uso de la nube desde tres niveles:

- Leyes de obligado cumplimiento.
- Normativas y estándares.
- Buenas prácticas desarrolladas y mantenidas por los diferentes foros y organizaciones de referencia en el ámbito de la nube.

5.1 Marco legal aplicable

Como vamos a ver al desarrollar brevemente las leyes implicadas en los servicios en la nube, su obligatoriedad puede venir dada por el tipo de dato manejado o bien, sencillamente, por el sector al que pertenezca la organización.

En el caso concreto de la obligatoriedad de notificar un incidente grave de seguridad al órgano de control pertinente, existen elementos comunes como la fecha y hora del incidente, clasificación de éste, recursos afectados por el incidente, origen del incidente, contramedidas que se han realizado para resolverlo, impacto del incidente, extensión geográfica y hasta una estimación del impacto económico del incidente con los daños reputacionales que pueden generar a la organización.

—5.1.1 Reglamento General de Protección de Datos (RGPD)

Esta ley se aplica a los datos de carácter personal y, desde el punto de vista jurídico, el responsable último del tratamiento de dichos datos es la organización que los ha obtenido y decide su tratamiento. En otras palabras, la organización es responsable de los datos que suba a la nube, mientras que el prestatario del servicio en la nube será el responsable de velar por su correcto tratamiento de acuerdo con las instrucciones recibidas del responsable de los datos.

Como punto de partida a una contratación de servicios en la nube, se debe identificar qué datos de carácter personal van a ser almacenados, procesados y transmitidos, es decir, qué datos forman parte del tratamiento. Para determinarlos, recordemos la definición en el Reglamento General de Protección de Datos (art. 4):

«datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;

Ellos incluyen tanto los datos de carácter personal que la organización obtiene de sus usuarios (identificativos o asociados con información más sensible como, por ejemplo, los de salud), pero también tienen esta consideración otros que no se obtienen directamente de su titular y permiten su identificación. Como indica el Considerando 30 del RGPD:

Las personas físicas pueden ser asociadas a identificadores en línea facilitados por sus dispositivos, aplicaciones, herramientas y protocolos, como direcciones de los protocolos de internet, identificadores de sesión en forma de «cookies» u otros identificadores, como etiquetas de identificación por radiofrecuencia. Esto puede dejar huellas que, en particular, al ser combinadas con o sin identificadores únicos y otros datos recibidos por los servidores, pueden ser utilizadas para elaborar perfiles de las personas físicas e identificarlas.

Una vez analizado el tipo de datos con el que la organización trabaja, habrá que exigir al proveedor de servicios en la nube que cumpla con las medidas de seguridad adecuadas.

A este respecto, hay que tener en cuenta en qué país el proveedor va a almacenar los datos para identificar si existe una transferencia internacional que requiera la aplicación de medidas adicionales.

Se considera que no existe transferencia internacional cuando los datos van a ser tratados en el espacio europeo, es decir, en uno de los estados miembros de la Unión Europea junto a Liechtenstein, Islandia y Noruega. Sin embargo, aunque la legislación es la misma dentro de la Unión Europea ya que los 27 estados miembros deben cumplir con el Reglamento, se debe tener en cuenta la existencia de otras normas en el ordenamiento jurídico de cada uno de los países miembros que puedan añadir requisitos adicionales.

En España, la Agencia Española de Protección de Datos ('AEPD') mantiene una página donde indica cuales son las garantías para la transferencia de datos personales a terceros países o a organizaciones internacionales. La correcta aplicación de estas medidas requiere el conocimiento de la legislación sobre esta materia propia del país destino, entre ellas, se incluye:

- Si los datos más sensibles van a ser cifrados y si la clave la tendrá el proveedor del servicio o la custodiará la organización.
- Si se realizan copias de seguridad de los datos y la localización/cifrado de dichas copias.
- El nivel de protección de los datos que ofrecen los distintos tipos de nube: pública, comunitaria, híbrida y privada.
- Si pueden garantizar la trazabilidad de los datos (qué, quién y cuando se han accedido a los datos).
- La garantía por parte del proveedor de la total devolución o supresión de los datos personales en caso de cancelación del contrato.

Para garantizar que se cumplen estas medidas, el proveedor de servicios de la nube puede disponer de certificaciones de seguridad de la información adecuadas o bien poner a disposición del cliente información suficiente que acredite el cumplimiento en materia de seguridad de la información (ej.: plan de respuesta ante incidentes o plan de continuidad de negocio). Sobre este aspecto, es relevante validar que el alcance de las certificaciones del proveedor sea de aplicación sobre los servicios contratados y que dichas certificaciones sigan vigentes durante la prestación de estos servicios.

De acuerdo con el RGPD, en el caso de un incidente grave que involucre datos de carácter personal con riesgo para los derechos de las personas físicas y dependiendo del volumen de datos afectados, se deberá informar a la AEPD en un plazo máximo de 72 horas desde el momento en que se detecte el incidente. Para garantizar una correcta notificación de una brecha de seguridad dicha notificación se debe realizar de forma electrónica. La falta de notificación se considera como una infracción del Reglamento.

Por otro lado, existe otra obligación de comunicación a los interesados cuando se considere que se hayan producido daños o perjuicios sobre sus derechos y libertades; en esta notificación los interesados deberán conocer que sus datos han podido ser revelados a terceros o que han podido dejar de estar disponibles de forma temporal o permanente. El incumplimiento de este deber de notificación puede acarrear a la organización multas de hasta 10 millones de euros o hasta el 2% de los ingresos totales anuales de la entidad.

Finalmente, mencionar la publicación en 2018 de dos guías sobre los servicios en la nube por parte de la AEPD:

- Guía para clientes que contraten servicios de computación en la nube.
- Orientaciones para prestadores de servicios de computación en la nube.

—5.1.2 Reglamento de Seguridad de las Redes y Sistemas de Información (Reglamento NIS)

El Reglamento de Seguridad de las Redes y Sistemas de Información (conocido como, Reglamento NIS) es aplicable a los operadores de servicios esenciales, así como a los proveedores de servicios digitales y establece los procedimientos para gestionar y resolver los incidentes de seguridad que una organización pudiera sufrir.

Para la evaluación del impacto de un incidente de seguridad el Reglamento NIS pide tener en cuenta los siguientes factores: número de usuarios afectados, duración del incidente, áreas geográficas afectadas por el incidente, alcance del impacto en las actividades económicas y daño reputacional.

En el caso de un incidente de impacto crítico, alto y muy alto, el Reglamento NIS establece que los operadores deben comunicarlo a través del CSIRT del país de referencia o la autoridad competente. El plazo de la comunicación de los incidentes dependerá de la clasificación de éstos (impacto crítico, de forma inmediata; impacto muy alto, a las 12 horas; e impacto alto, a las 48 horas).

Asimismo, si hay más de una organización implicada en un incidente, el Reglamento NIS establece la obligatoriedad de que todas las organizaciones, a través del CSIRT de referencia, intercambien y pongan en común la información disponible, estableciendo así sinergias que permitan abordar óptimamente la resolución del incidente. Para ello se emplea la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes1 ('PNSC'). Para otros tipos de incidentes con menor impacto, no hay obligación de notificación, por lo que las organizaciones pueden decidir libremente si desean comunicar la incidencia.

Estas notificaciones, si se producen sobre datos de carácter personal de ciudadanos españoles, no eximen de la obligatoriedad de notificar igualmente a la AEPD. De hecho, las autoridades competentes y los CSIRTs de referencia colaboran de forma estrecha con la AEPD. Se espera que, con la puesta en marcha de la PNNSC, la AEPD actúe de ventanilla única.

El incumplimiento de la obligación de notificación de incidentes puede traer consigo una serie de infracciones. Estas infracciones pueden ser muy graves, graves y leves (ej.: el incumplimiento reiterado de la obligación de notificar incidentes puede ser una infracción muy grave (a partir del segundo incumplimiento de la notificación de los incidentes) y puede acarrear multas de 500 mil hasta 1 millón de euros.

A fecha del presente documento, la directiva europea NIS2 que sustituirá a la actual Directiva NIS se encuentra a la espera de su adopción formal por parte del Parlamento y del Consejo Europeo. La NIS2 pretende por un lado exigir unas medidas de seguridad más estrictas para evitar los ataques que las organizaciones están sufriendo en materia de ciberseguridad, cuyo número va en aumento y, por otro lado, agilizar las obligaciones de notificación evitando de esta manera la duplicidad en las notificaciones y la sobrecarga que de esta duplicidad se genera en las organizaciones que están sujetas a esta norma.

—5.1.3 Esquema Nacional de Seguridad (ENS)

Recientemente aprobada su actualización, Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS), el mismo se incluye en el paquete de actuaciones urgentes, adoptado el pasado 25 de mayo, para reforzar las capacidades de defensa frente a las ciberamenazas sobre el sector público español y las entidades colaboradoras que suministran tecnologías y servicios al mismo.

El objetivo del ENS es garantizar la protección de los sistemas de información en las entidades de su ámbito de aplicación, reduciendo vulnerabilidades y promoviendo la vigilancia continua, estableciendo a su vez mecanismos de respuesta y medidas de seguridad óptimas, dentro del marco jurídico, tecnológico, estratégico y de ciberamenazas actuales.

Como medidas de seguridad, se han incluido las relativas a servicios en la nube, interconexión de sistemas, protección de la cadena de suministro, medios alternativos, vigilancia y otros dispositivos conectados a la red.

La respuesta a incidentes de seguridad es una parte integral del mismo y los requisitos a cumplir se incluyen a lo largo de todo su articulado. El ENS también establece la obligación de notificación.

Los países pueden tener requisitos similares en sus ordenamientos jurídicos. En Europa, ENISA mantiene en su sitio web la información sobre las estrategias nacionales en materia de ciberseguridad de los estados miembro de la Unión Europea y de la EFTA.

—5.1.4 Ley de Infraestructuras críticas (Ley PIC)

Cuando una organización tiene la consideración de servicio crítico u ofrece servicio a otra organización con esta consideración deberá, en caso de un incidente grave, informar al Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC).

—5.1.5 Directiva sobre los servicios de pago (PSDsd2)

La Directiva sobre los servicios de pago (“Payment Service Directive”, en su segunda actualización, PSD2), es una directiva centrada en la seguridad de la información asociada con los servicios de cobro.

Las organizaciones proveedoras de pago, deben notificar sus incidentes a la autoridad competente (la Autoridad Bancaria Europea, ‘EBA’, en el caso de los países de la Unión Europea; o el Banco de España, en caso de España). En España, el plazo para el envío del informe inicial al Banco de España es de 4 horas después de que el incidente sea clasificado como grave.

5.2 Normativa y estándares

Los principales organismos que desarrollan normativas y estándares en el ámbito internacional son ISO ("International Organization for Standardization") e IEC ("International Electrotechnical Commission"). Ambos cuentan con normativa que aporta luz en el despliegue de procedimientos de respuesta ante incidentes de seguridad y sirven a menudo para que las organizaciones demuestren su madurez en la gestión y respuesta a incidentes. La obligatoriedad del cumplimiento con alguna o varias de estas normas dependerá de los acuerdos internos (ej.: estrategia interna de cumplimiento y control interno de la organización) y externos (ej.: acuerdos con terceros: accionistas, colaboradores, clientes y/o proveedores) de las organizaciones.

—5.2.1 ISO/IEC 20000: Tecnologías de la información. Gestión de Servicios

La norma ISO/IEC 20000, una de las más extendidas, proporciona el marco de mejores prácticas para un sistema de gestión de servicios y, por tanto, es de ayuda en la planificación y gestión de problemas e incidentes. La misma, no solo tiene en cuenta las tendencias emergentes en la gestión del servicio, como son los servicios en la nube y su aplicabilidad es independiente del modelo de servicio utilizado, sino también considera aspectos de seguridad de la información para integrarlos dentro de la gestión de servicios.

—5.2.2 ISO 27002 Tecnología de la Información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información

La norma ISO 27002 recoge las buenas prácticas para gestión de la seguridad de la información. Hoy en día es uno de los referentes principales para la construcción de Sistemas de Gestión de Seguridad de la Información (SGSI), garantizando la continuidad y el mantenimiento de los procesos de seguridad, alineados a los objetivos estratégicos de la organización. Además, esta norma dedica un capítulo específico a los controles para la gestión de los incidentes de seguridad incluyendo guías sobre cómo gestionarlos en las diferentes fases incluyendo la respuesta, notificación y lecciones aprendidas.

La norma ISO 27002 es el punto central utilizado para el desarrollo de sistemas de gestión de la seguridad de la información. Existe una versión de 2013 extendida; sin embargo, a principios de este año 2022 se ha publicado una nueva versión. Además del cambio en su título, la revisión ha incluido nuevos controles relevantes tanto en el despliegue de los sistemas en la nube como en la gestión de incidentes.

La norma ISO 27001 ("Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información.") establece los requisitos para implantar un Sistema de Gestión de la Seguridad de la Información (SGSI) que puede utilizar los controles que proporciona la norma ISO 27002.

La nueva versión de la norma ISO 27002 causa la revisión de otras publicadas durante estos últimos 9 años con el objeto de complementarla, entre ellas: ISO/IEC 27017 e ISO/IEC 27018, relevantes para la gestión de los servicios en la nube[4].

[4]A fecha de la presente Guía, en revisión.

—5.2.3 ISO/IEC 27017 Código de prácticas para los controles de seguridad de la información en la nube

La norma ISO/IEC 27017 es la referencia para la selección de los controles de seguridad de la información específicos de los servicios en la nube.

ISO/IEC 27017 se refiere y usa los controles de seguridad de ISO/IEC 27002 presentando como deben entenderse en el entorno de los servicios en la nube. Tiene en cuenta el papel de la organización que los despliega ya que la forma en que se implementan depende de si son clientes de servicios en la nube o si son proveedores de éstos y añade, en su anexo, controles fuera de la versión anterior de ISO 27002.

—5.2.4 ISO/IEC 27018 Código de prácticas para la protección de la información de identificación personal (PII) en la nube en calidad de procesadores de PII

La norma ISO/IEC 27018 es una extensión de la versión de 2013 de ISO 27002 que tiene en cuenta los requisitos regulatorios para la protección de datos de carácter personal aplicables en el contexto de los entornos de riesgo para la seguridad de la información de los datos personales considerando al proveedor de los servicios públicos de nube.

—5.2.5 ISO 22301 Sistema de Gestión de Continuidad de Negocio

La norma ISO 22301 sobre el Sistema de Gestión de Continuidad del Negocio establece los requisitos para su planificación, establecimiento, implantación, operación, supervisión, revisión, prueba, mantenimiento y mejora.

En concreto, esta norma plantea un sistema diseñado para la protección de las organizaciones ante un eventual incidente. Asimismo, da las pautas para una respuesta ágil y una recuperación rápida poniendo de manifiesto la necesidad de tener una estructura de respuesta bien definida frente a los incidentes.

—5.2.6 Otras normas y documentos ISO

Aunque en los apartados anteriores se han detallado aquellas normas y estándares de referencia más habituales, las que se mencionan a continuación se añaden por su interés.

La mayoría de estas normas y estándares son parte de la familia ISO 27000, algunos de los documentos no son normas sino especificaciones técnicas ('TS', por sus siglas en inglés "Technical Specifications") que se mencionan por ser de utilidad, pero no han sido aprobados como normas, aunque pudieran transformarse en éstas en un futuro (para más información sobre su estado podemos acudir a www.iso.org).

- ISO/IEC TS 27100, "Ciberseguridad - Visión general y conceptos": describe los conceptos de ciberseguridad (iIdentificar, pProteger, dDetectar, rResponder y rRecuperar) y cuenta con apartados sobre la gestión de incidentes en la organización haciendo énfasis en la preparación y en el soporte técnico de los proveedores de producto y de servicio.
- ISO/IEC TS 27110, "Directrices para el desarrollo del marco de ciberseguridad": estrechamente ligada con la anterior, explica cómo definir sistemas robustos para prevenir ciberataques.
- ISO/IEC TS 27102, "Guía para el ciberseguro": proporciona guías para el momento en que se considera gestionar el riesgo adquiriendo un ciberseguro que cubra el impacto de un ciberincidente. Entre otros, proporciona una guía para el momento de la toma de decisión, para la compartición de datos e información entre asegurado y asegurador, etc.
- ISO/IEC 27031: (en revisión a fecha del presente documento), "Directrices para la preparación y la continuidad del negocio": describe los principios y conceptos y proporciona un marco de métodos y procesos para identificar y especificar todos los aspectos de mejora de la preparación de la organización para asegurar la continuidad del negocio.
- ISO/IEC 27035, partes 1 a 4, "Gestión de incidentes de seguridad de la información": se trata de una norma multiparte dedicada a la gestión de incidentes desde una perspectiva estructurada para detectar, reportar, analizar y responder a los incidentes, así como aplicar las lecciones aprendidas.

- ISO/IEC 27041, "Orientación para garantizar la idoneidad y adecuación del método de investigación de incidentes": proporciona guías para asegurar que los métodos y procesos usados en la investigación de los incidentes de seguridad son adecuados.
- ISO/IEC 27042, "Directrices para el análisis y la interpretación de las pruebas digitales". Proporciona guías para el análisis e interpretación de las evidencias digitales de forma que se asegure la continuidad, validez, reproducibilidad y repetibilidad.
- ISO/IEC 27043, "Incident investigation principles and processes": proporciona guías basadas en modelos idealizados, desde la preparación pre-incidente al cierre de la investigación.
- ISO/IEC 27036, partes 1 a 4, "Relaciones con los proveedores": norma multiparte para la gestión de la cadena de suministro.
- ISO/IEC 27701, "Gestión de la privacidad de la información": es una extensión de la 27001 en materia de privacidad de datos, proporcionando un marco para la gestión de dicha la privacidad de los datos personales.

Fuera de la familia ISO 27000, es importante mencionar la ISO/IEC 31000, "Gestión de riesgos": se trata de una guía de referencia para la gestión del riesgo que se aplica a la mayoría de las actividades de las organizaciones, incluyendo la planificación, operaciones de gestión y procesos de comunicación.

—5.2.7 Estándar de la industria de tarjetas de pago (PCI-DSS)

El estándar de la industria de tarjetas de pago ("Payment Card Industry Data Security Standard", 'PCI-DSS') de seguridad de datos elaborado por el PCI Council, al que pertenecen los principales esquemas de pago (VISA, MasterCard, JCB, American Express y Discover entre otros miembros). Afecta a las organizaciones que almacenan, procesan y/o transmiten datos de tarjetas para realizar transacciones de pago y tiene como objetivo que los pagos sean seguros, así como la reducción del fraude.

Los requisitos de seguridad de PCI-DSS se aplican a todos los componentes del sistema incluidos en el entorno de datos del titular de la tarjeta (CDE) o conectados a este Este entorno consta de personas, procesos y tecnologías que almacenan, procesan o transmiten datos de titulares de tarjetas o datos confidenciales de autenticación. El incumplimiento de este estándar puede derivar en la pérdida del permiso para procesar tarjetas.

La normativa es exigente en cuanto a las políticas de identificación y tratamiento del posible incidente, pero no explicita la obligatoriedad de notificación. No obstante, al tratarse de datos de carácter personal, estos datos también estarían sujetos al RGPD mencionado con anterioridad.

—5.2.8 Otras normas

Aunque fue el sector financiero uno de los primeros en elaborar normativa específica y lo ha hecho de forma más intensa por la necesidad de negocio de proporcionar plataformas confiables que acompañaran a los procesos de globalización de las organizacioness y de operar en diferentes jurisdicciones; en la actualidad, prácticamente todos los sectores cuentan con normativa específica de aplicación.

La organización debe investigar y conocer la normativa del sector al que pertenece y con los que realiza negocios para determinar si éstos contienen provisiones adicionales a la de aplicación general mencionada hasta el momento en materia de gestión de incidentes en los servicios en la nube.

5.3 Buenas prácticas

Estas normativas nos llevan a buenas prácticas empresariales en la gestión de los incidentes en la nube que deberían acometerse en cualquier organización. Entre las buenas prácticas queremos destacar la concienciación y formación del personal en materia de seguridad de la información y la aplicación de las medidas de seguridad oportunas sobre la información que la organización considere sensible.

Otro aspecto importante, dados los breves plazos con los que se trabajan en la notificación de incidentes, es la necesidad de rapidez de respuesta y de fluidez de comunicación entre todas las partes afectadas. Por este motivo, es importante que las organizaciones analicen de antemano su contexto, los riesgos de su actividad de negocio y preparen los procesos y procedimientos de prevención y respuesta oportunos en función de sus necesidades concretas.

Podemos nombrar numerosas organizaciones que nos ayudan al desarrollo de las buenas prácticas en la gestión de incidentes de la nube. Entre ellas queremos destacar a ENISA a nivel europeo, al Instituto Nacional de Estándares y Tecnología Departamento de Comercio de los Estados Unidos ("National Institute of Standards and Technology", 'NIST') por su contribución en la materia y, en especial, por su Marco de ciberseguridad; y a la "Cloud Security Alliance" ('CSA') a nivel internacional.

—5.3.1 Agencia de la Unión Europea para la Ciberseguridad (ENISA)

A fecha del presente documento, ENISA está elaborando el Esquema Europeo de Certificación de Servicios de la Nube (EU Cloud Services Scheme, EUCS) que pretende abordar la problemática de la nube para cualquier proveedor de dicho servicio.

El EUCS establecerá unos estándares comunes para todos los proveedores que operen en Europa. Estos estándares están basados en esquemas nacionales existentes y normas internacionales. Con este esquema de certificación de servicios se podrá conocer el nivel de garantía que ofrece dicho proveedor. La certificación en este esquema aumentará la confianza de las organizaciones en los servicios en la nube.

La certificación califica los niveles de garantía en tres: básico, sustancial y alto. Esta certificación será, de momento, voluntaria, aplicable para todos los tipos de servicios de nube y tendrá una validez de tres años.

—5.3.2 Marco de Ciberseguridad (CSF) del Instituto Nacional de Estándares y Tecnología (NIST)

El marco de ciberseguridad del NIST (Cibersecurity framework, CSF) ayuda a las organizaciones a gestionar y reducir los riesgos en materia de seguridad de la información, protegiendo de esa manera sus datos.

Dicho marco está organizado en cinco funciones clave: identificar, proteger, detectar, responder, recuperar. Estas cinco áreas proporcionan una visión integral del ciclo de vida para la gestión del riesgo de ciberseguridad y, consecuentemente, sirve de base en la gestión de incidentes de ciberseguridad en los servicios en la nube.

El marco de ciberseguridad del NIST consta de tres componentes principales:

- El núcleo guía a las organizaciones en la gestión y reducción de sus riesgos de ciberseguridad complementando los procesos existentes; despliega las 5 funciones clave en un conjunto de 23 categorías que cubren los objetivos de seguridad para cualquier organización y, por último, las 108 subcategorías que tienen más detalle que las categorías y mejoran el programa. Las referencias informativas son estándares, prácticas que añaden información adicional.

- Los niveles de implementación del marco facilitan que las organizaciones consideren el nivel apropiado de implementación de su programa de ciberseguridad y, a menudo, se usan como una herramienta para determinar la prioridad en función del riesgo y el presupuesto.

- Los perfiles del marco alinean las funciones, categorías y subcategorías con las necesidades del negocio, la tolerancia al riesgo de ciberseguridad y los recursos que posee la organización. Pueden usarse para determinar el estado actual y el deseado u objetivo y permiten establecer la hoja de ruta para reducir el riesgo,

En el área de respuesta del CSF se encuentran las directrices que hay que seguir en caso de incidente; las categorías pertenecientes a esta área son: planificación de respuesta, comunicaciones, análisis, mitigación y mejoras.

Además del CSF, el NIST tiene disponibles otras normas y documentos relevantes asociados a la gestión de incidentes en la nube: la iniciativa "NIST Cloud Computing Forensic Science" y la "Cybersecurity Supply Chain Risk Management" son de mención especial.

—5.3.3 Cloud Security Alliance (CSA)

La Cloud Security Alliance (CSA) es una organización dedicada a concienciar y fomentar las mejores prácticas para tener un entorno en la nube seguro. Algunas de estas prácticas hablan sobre la arquitectura necesaria para minimizar incidentes en la nube (ej.: como el cifrado de los datos sensibles) o los pasos a seguir cuando estos se materializan.

Con respecto a las notificaciones de Incidentes, la CSA hace hincapié en el nuevo paradigma que se abre al tener responsabilidades de notificación compartidas entre la organización y el proveedor de la nube contratada. La organización, por tanto, deberá entender perfectamente la estrategia de respuesta a posibles incidentes del proveedor contratado.

Con lo anterior, la CSA ha publicado recientemente, el Marco de respuesta ante incidentes en la nube[5] (Cloud Incident Response (CIR) Framework) con el objetivo de guiar a los clientes de la nube en la preparación y la gestión efectiva de los incidentes de ciberseguridad en este entorno; el Marco incluye pautas para la coordinación y la compartición de información con las partes interesadas y otras organizaciones cubriendo las fases de: preparación,; detección, y aAnálisis,; c Contención, erradicación, y recuperación y ; Ppost-mortem de un incidente. Asimismo, el Marco también proporciona referencia a otras normas y marcos aceptados por la industria para planificar y prepararse para la ocurrencia de incidentes en la nube, las estrategias de mitigación y los procesos post-mortem.

—5.3.4 UK Cyber Essentials

El UK Cyber Essentials es un esquema inglés certificable, requerido para los proveedores del gobierno del Reino Unido que gestionan información sensible e información de carácter personal, que comparte el objetivo del NIST CSF al haber sido diseñado con el objetivo de que las organizaciones adopten las buenas prácticas en materia de ciberseguridad y desplieguen los controles para proteger sus activos de información.

El esquema tiene dos niveles de certificación: 1) autocertificación, con el uso de un cuestionario que posteriormente es validado por un tercero cualificado; y, 2) certificación a través de una entidad acreditada independiente.

[5]https://www.ncsc.gov.uk/cyberessentials/resources

—5.3.5 Proveedores de servicios en la Nube

No debemos acabar este apartado sin mencionar que los propios proveedores de servicios en la nube mantienen documentos de buenas prácticas, útiles en la planificación de la respuesta a incidentes. Como ejemplos, citaremos los más extendidos:

- AWS, "Respuesta a incidentes en la nube": toma de referencia la guía del NIST "SP 800-61 Computer Security Incident Handling Guide".
- Azure, "Visión general de los incidentes en la nube": introducción y documentación de Microsoft que apoyan la tarea de la respuesta a incidentes, tanto en las fases de planificación como en el momento de la respuesta.
- Google Cloud Platform, "Proceso de respuesta ante incidentes de datos": recuerda el modelo de responsabilidad compartida, la responsabilidad de Google y como esta organización mantiene la seguridad de la infraestructura y servicios subyacentes en la nube, además de proporcionar directrices y funciones de seguridad para que los clientes realicen un despliegue seguro.

6 HOJA DE RUTA

En este apartado se establece una visión a alto nivel de los pasos necesarios, así como los conceptos útiles para recorrerlos. Se abordará, desde una primera fase muy temprana, dirigida a conocer qué servicios existen en la nube y cómo pueden ayudar a la organización, hasta estadios posteriores en los que se tratará qué tener en cuenta a la hora de comenzar el viaje y tipos de servicio específicos.

6.1 Antes de la nube

Se ha visto en anteriores apartados que el concepto "nube" es muy abierto y se puede contemplar desde diversos prismas, tanto desde los diferentes tipos de nube (pública, privada, comunitaria o híbrida) como desde la tipología de los servicios que se pueden consumir (SaaS, IaaS, PaaS).

—6.1.1 Nube Pública

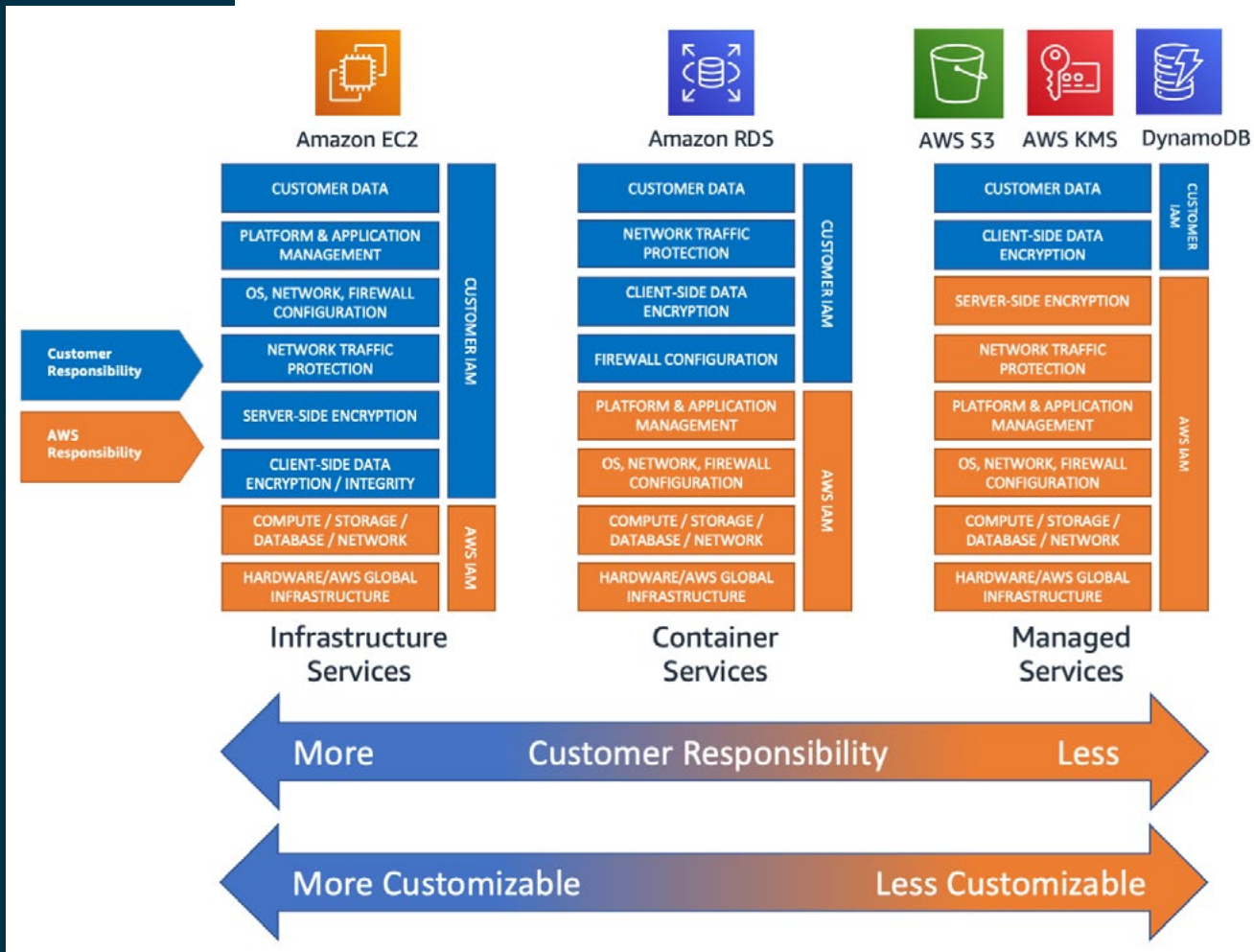
¿Qué ocurre con la seguridad de la información en entornos de nube Pública? ¿Es otro de los servicios ofrecidos por los proveedores? Ésta es una pregunta compleja de contestar ya que dependerá de cuánto de esas capacidades se están consumiendo como servicio y está íntimamente relacionada con el tipo de servicio (IaaS, PaaS, SaaS). Para facilitar un entendimiento general, se podrían presentaremos las diferencias con respecto a un entorno propietario (tradicional o "on-premise") en la siguiente tabla:

	Centro de datos "Tradicional"	Entorno de nube pública
¿Quién es responsable de la seguridad de la información?	La organización ya que es la propietaria de los datos.	La organización ya que es la propietaria de los datos.
¿Quién es responsable de la gestión de la seguridad física?	La organización.	Proveedor de servicios de nube.
¿Dónde están los sistemas y los datos?	Centro de datos gestionados por la organización.	Centro de datos gestionado por el proveedor de servicios de nube.
¿Quién controla el acceso a los datos?	La organización.	La organización y el proveedor de nube pública.
¿Quién es el responsable de los parcheos y gestión de vulnerabilidades de los sistemas?	La organización.	Dependerá del tipo de servicio: **IaaS**: La organización **PaaS**: El proveedor de servicios de nube **SaaS**: El proveedor de servicios de nube
¿Quién es el responsable en caso de incidente?	La organización.	La organización.
¿Quién es el responsable de los aspectos legales de los sistemas y obligaciones con respecto a los datos?	La organización.	La organización.

La responsabilidad de la seguridad de la información tanto en entornos tradicionales como en la nube será siempre de la propia organización ya que es la propietaria de los datos. Cuando esta delega servicios y sistemas en la nube, la organización está delegando la gestión de estos servicios y sistemas y, por lo tanto, la responsabilidad de que los proveedores en la nube apliquen las medidas de seguridad necesarias para garantizar que los datos están seguros. En este punto es donde se introduce lo que llamamos el "modelo de responsabilidad compartida": la organización comparte, en función del modelo de nube elegido, la responsabilidad de la gestión de la seguridad, así como la administración de ciertos sistemas y procesos manteniendo en todo caso la responsabilidad última de la seguridad de los datos.

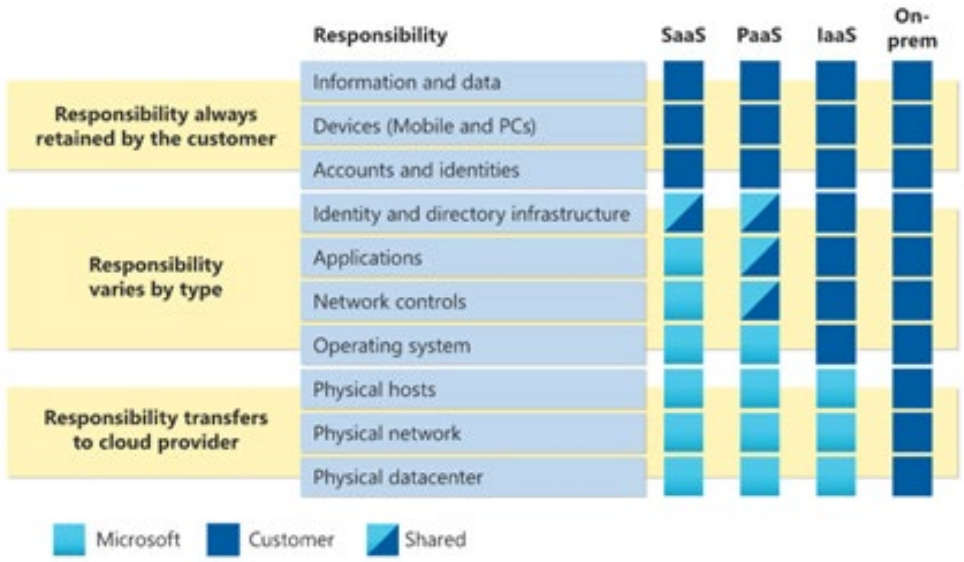
En este sentido, los mayores proveedores de seguridad en la nube muestran de la siguiente forma cuáles son las responsabilidades de la organización y cuáles del proveedor cuando se trata de la gestión de los servicios en la nube:

- AWS[6]:



[6] https://aws.amazon.com/es/blogs/industries/applying-the-aws-shared-responsibility-model-to-your-gxp-solution/

- Azure[7]:



- Google Cloud Platform[8]:

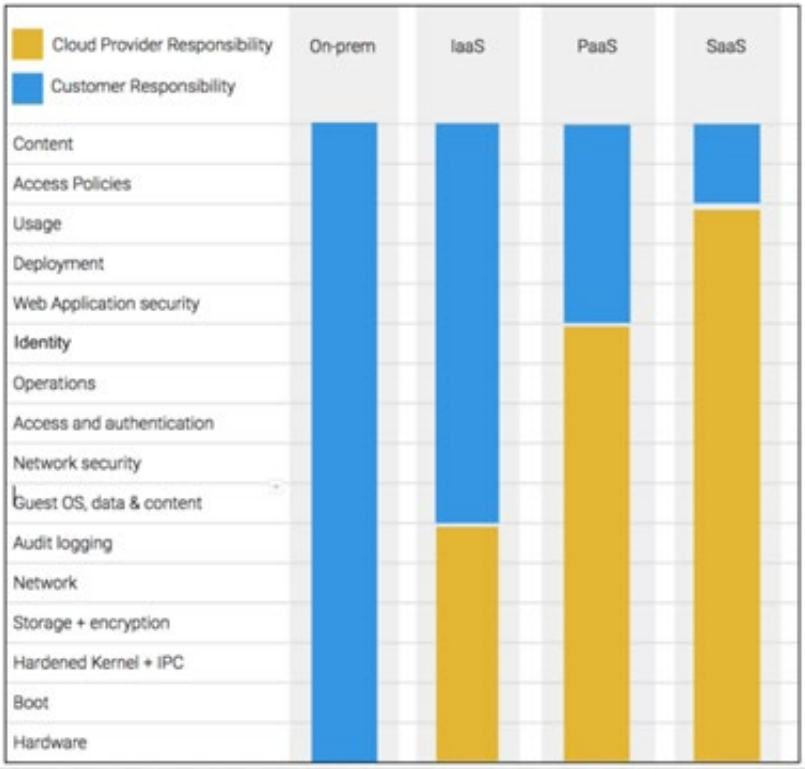


Figure 1.1.1 Shared security responsibilities

[7] https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

[8] https://services.google.com/fh/files/misc/google-cloud-security-foundations-guide.pdf

—6.1.2 Opciones de Nube Pública

Se detallarán, a continuación, las principales alternativas de proveedores de servicios en la nube, por cuota de mercado en Europa, sus peculiaridades y características principales.

6.1.2.1 AWS

Durante las últimas décadas, Amazon ha sido una de las empresas pioneras que mayor impacto ha tenido en el desarrollo de la computación en la nube a nivel mundial. Al principio, su esfuerzo se centraba en el despliegue de una infraestructura potente para soportar su negocio de comercio digital ('e-commerce'); hasta que, una vez diseñados esos sistemas, diversificaron su negocio generando su división Amazon Web Services ('AWS'), que se dedicó a potenciar esa faceta tecnológica para ofrecer servicios de computación a terceros.

En 2006, AWS lanzó por primera vez una beta pública de su servicio más icónico de computación en la nube, la llamada "Elastic Computing Platform" o "Elastic Compute Cloud" ('EC2'), un servicio que ofrecía a los clientes la capacidad de utilizar de manera muy rápida y en autoservicio un servidor alojado en los centros de procesamiento de datos de AWS. Éste fue el germen de lo que ocurrió durante los siguientes años: un crecimiento exponencial en el que en 2008 AWS ofrecía 24 servicios hasta los más de 200 en la actualidad donde se incluyen servicios tan especializados como los relacionados con inteligencia artificial o simulación de computación cuántica.

El acceso a estos servicios se puede hacer a través de la configuración de sus interfaces de red, como se haría en cualquier otro servidor en un centro de procesado de datos clásico o a través de las interfaces de gestión que ofrece AWS, tanto desde su consola web, como de sus diferentes SDK (acceso para desarrolladores) o CLI (interfaz de línea de comandos).

Todos los recursos se pueden instanciar en diferentes regiones y zonas de disponibilidad. Esto significa que AWS deja al cliente elegir en cuál de sus centros de procesado de datos quiere que se alojen sus sistemas permitiéndole crear estrategias de alta disponibilidad y recuperación ante desastres de manera sencilla, así como facilitando el cumplimiento normativo en aquellas regulaciones donde existen requisitos geográficos.

6.1.2.1 AWS

Microsoft Azure fue anunciado en octubre de 2008 con el nombre en clave "Proyecto Red Dog", a partir de ahí, ha pasado por diferentes nombres hasta llegar, en 2014, al actual "Microsoft Azure".

Con evidente foco en sistemas Windows y utilización de lenguajes de programación basados en .NET Framework (como C#) utilizados en sus centros de procesado de datos para ofrecer todos los servicios de computación, también ofrece servicios basados en código abierto, con un catálogo de más de 200 servicios a disposición de los clientes.

Algunas de las características más atractivas de Microsoft a la hora de ofrecer sus servicios a los clientes se basan en la fuerte y sencilla integración con las herramientas ofimáticas y otros productos de la compañía como pueden ser el Directorio Activo o su suite de puesto de trabajo de Office.

Todos los recursos se pueden instanciar, como en el caso anterior, en diferentes regiones y zonas de disponibilidad. Esto significa que Microsoft, como AWS, también deja al cliente elegir en cuál de sus centros de procesado de datos quiere que se alojen sus sistemas.

6.1.2.3 Google Cloud Platform (GCP)

Google es otro de los líderes en la provisión de servicios de computación en la nube no solo por sus números en cuanto a cuota de mercado, sino por su apuesta por la innovación y el empuje que ha tenido durante las últimas décadas en aspectos como las aplicaciones de inteligencia artificial o "machine learning" en la nube. Además, su enfoque en innovación siempre ha sido muy abierto y el trabajo realizado por su división de investigación ("Google Research Division") ha contribuido de una manera crítica al desarrollo de la tecnología y, en concreto, de la computación en la nube de los últimos años, creando, por ejemplo, los Kubernetes.

Google fue una de las primeras organizaciones en explotar la analítica avanzada de gran potencia y la convirtió en el núcleo de su negocio; así, no es de extrañar que entre sus características principales, la organización ofrezca a través de su plataforma en la nube "Google Cloud Platform" ('GCP') servicios con capacidades relacionadas con analítica avanzada, además, como sucede con Microsoft, también permite una integración transparente con toda la suite de servicios ofimáticos de Google (ej.: Gmail, Google Drive, Groups, Docs, Calendar, etc.).

Como en AWS y Microsoft, GCP también se encuentra en este caso un amplio abanico de regiones y zonas de disponibilidad en las que es posible desplegar los servicios.

6.1.2.4 Otros proveedores generalistas de servicios de nube

Además de los proveedores de servicios de computación en la nube expuestos, se pueden encontrar otros proveedores con servicios similares.

Los gigantes tecnológicos chinos Alibaba y Tencent ofrecen sus servicios en Alibaba Cloud y Tencent Cloud, respectivamente. Éstos, por las características y gran extensión del mercado asiático, aunque muy localizados, cuentan con una presencia importante en cuota de mercado a nivel mundial en servicios en la nube.

Del mismo modo, se encuentran otras alternativas de la mano de compañías históricas como IBM Cloud u Oracle Cloud que ofrecen a sus clientes servicios en la nube basados en su tecnología.

6.2 Viajando a la nube

—6.2.1 Necesidades del Negocio

El primer punto es analizar el negocio y sus necesidades tecnológicas para evaluar si el viaje a la nube supondría una ventaja competitiva. Algunas de las consideraciones para tener en cuenta podrían ser las siguientes:

- Servicios de negocio externalizar (ej.: herramientas, webs, correo, CRM, gestor de contenidos, servicios de seguridad, movilidad…).
- Grandes fluctuaciones en el número de usuarios y/o clientes.
- Dispersión geográfica de usuarios/servicios.
- Escalabilidad de los servicios (ej.: computación, almacenamiento, BBDD, red, ciberseguridad…).

—6.2.2 Estrategia de migración

Hay que definir una estrategia clara de migración donde se identifique qué procesos, sistemas e información se van a migrar a la nube y en cuántas fases. Dependiendo de las necesidades y la organización, se podrá realizar una migración total a la nube o ir migrando los servicios de manera escalonada por fases. La complejidad del viaje dependerá del tipo de estrategia seleccionada.

—6.2.3 Alternativas de proveedores de servicios en la nube

Otro de los puntos principales para tener en cuenta en el viaje a la nube es el estudio de las distintas opciones existentes en el mercado y la adaptación de esos servicios a las necesidades de negocio.

En el punto Opciones de Nube Pública se han presentado las principales alternativas de proveedores de servicios en nube, por cuota de mercado en Europa, sus peculiaridades y características principales se trataría, por lo tanto, de considerar las características de cada proveedor junto con las necesidades de negocio y decidir la estrategia a seguir.

—6.2.4 Clausulas legales y condiciones de uso

No se puede olvidar el marco legal existente, tanto en el país en el que reside la organización, como el país del proveedor de servicios en la nube. Algunos de los aspectos básicos a revisar a nivel contractual son los siguientes:

- La privacidad, respecto a los datos de carácter personal.
- Ubicación de los centros de datos del proveedor de nube.
- Revisión del contrato y las condiciones de uso.
- La seguridad de la información.
- Los acuerdos a nivel de servicio (ANS).

—6.2.5 Continuidad de Negocio

Por último, se debe evaluar el Plan de Continuidad de Negocio y el Plan de Recuperación ante Desastres del proveedor de servicios en la nube. Hay que verificar si cubre los Tiempos Objetivos de Recuperación (RTO) y Puntos Objetivos de Recuperación (RPO) de los procesos de negocio que se han externalizado a la nube.

En la medida de lo posible, cuando se traten datos sensibles, se debe evitar la dependencia de un único proveedor de servicios de nube, revisando antes de firmar si ofrece servicios para migrar grandes cantidades de datos o teniendo una estrategia que incluya planes de salida para mover los servicios a otro proveedor.

6.3 En la nube

Ahora que ya conocemos qué servicios desplegaremos en la nube, vamos a ver de qué forma lo llevaremos a cabo. En este apartado se hablará de los diferentes casos de uso básicos para la utilización de la nube, tratando de aterrizar los principales aspectos de su configuración.

—6.3.1 Servicios de Computación

La aproximación más básica a los servicios de computación en la nube es la basada en máquinas virtuales desplegadas en los diferentes proveedores de nube pública deberemos seguir una serie de pasos comunes a la hora de utilizar estos servicios:

- Ajustar los requisitos de la máquina que se va a desplegar a la necesidad de computación.
- Selección de un sistema operativo que se ajuste al caso de uso.
- Configuración del almacenamiento en términos básicos de tamaño, aunque también de otras capacidades, como velocidad, cifrado, etc.
- Configuración de las interfaces de red.
- Despliegue de la instancia.

A partir del momento del despliegue de la instancia, siguiendo el modelo de responsabilidad compartida del proveedor, se estaría consumiendo un servicio IaaS en el que la responsabilidad sobre el mantenimiento del servidor desplegado es responsabilidad del cliente.

Se aconseja seguir las siguientes buenas prácticas en el despliegue de servicios de computación:

1. Utilizar una versión de sistema operativo lo más actualizada posible y con el mínimo número de paquetes necesario para limitar la superficie de exposición ante vulnerabilidades de software.

2. Dentro de lo posible, utilizar los paquetes preparados por los proveedores de servicios de nube.

3. Gestionar de manera responsable y segura las credenciales de acceso a los servidores y evitar, dentro de lo posible la autenticación local utilizando directorios como LDAP o Directorio Activo.

4. Limitar la exposición pública de red y los puertos expuestos de los servidores haciendo uso de las capacidades del proveedor del servicio (ej.: firewalls, VPN, etc.) o utilizar directamente los servicios que ofrecen los proveedores en la nube para la gestión de los servidores.

5. Mantener las instancias actualizadas y dentro de los ciclos de despliegue de parches.

6. Configurar las capacidades de copias de seguridad de los servicios y, dentro de lo posible, considerando que las copias de seguridad se guarden en otra región y se gestionen con cuentas de administración independientes para evitar que el compromiso de credenciales administrativas del entorno principal suponga la vulneración de las copias de seguridad de este.

—6.3.2 Servicios de Almacenamiento

Una de las preguntas más recurrentes a la hora de comenzar el viaje a la nube es ¿estarán los datos seguros fuera del centro de procesado de datos de la organización? La respuesta es que, siguiendo una serie de recomendaciones y buenas prácticas, el nivel de seguridad puede ser el mismo que en un centro de procesado de datos propio. Para ello hay que tener en cuenta que, con respecto a los datos, se debe tener en cuenta su seguridad en términos de:

- Acceso ilícito a datos.
- Filtración de datos.
- Pérdida de datos.

Se hable de S3 de AWS, Storage Accounts de Azure o Google Cloud Storage, se deberá considerar al menos lo siguiente:

1. Restringir de una manera correcta la exposición de los datos a través de las herramientas que proporcionan los proveedores de nube pública (ej.: Acces-control lists (ACLs) o su gestión de controles y accesos).

2. Obligar por configuración el cifrado tanto en tránsito como en reposo de los datos para asegurar su confidencialidad.

3. Auditar las trazas que generan los proveedores de servicios sobre la actividad en los recursos (ej.: creación, modificación, borrado, etc.).

4. Realizar copias de seguridad de toda la información de una manera segura, así como comprobar que los respaldos se hacen de manera periódica y contienen todos los datos necesarios.

—6.3.3 Servicios de bases de datos

Cada proveedor de servicios de base de datos cuenta con su propia metodología para el despliegue de bases de datos. En este sentido, nada impide a la organización de realizar un despliegue tradicional, en una instancia de computación (ej.: un servidor Linux o Windows), de los paquetes y un motor de bases de datos, pero haciendo esto y siguiendo el modelo de responsabilidad compartida, el cliente debería tener la responsabilidad de gestionar todo el sistema operativo, mantenimiento, copias de seguridad, instalación de parches, monitorización, etc. Utilizando directamente el servicio de bases de datos proporcionado por el proveedor de la nube, los consumidores de nube pública directamente acceden a una base de datos correctamente desplegada y dimensionada a través de un entorno de despliegue de tipo autoservicio.

Los principales motivos a la hora de decantarse por este tipo de servicios en detrimento de realizar la instalación desde la propia organización con sus propios recursos son los siguientes:

- El mantenimiento del motor de la base de datos es responsabilidad del proveedor de nube.
- La instalación de los parches de seguridad, tan importantes en este tipo de software, son responsabilidad del proveedor de nube.
- La disponibilidad de la base de datos es responsabilidad del proveedor de nube.
- Las copias de seguridad suelen estar incluidas como parte del servicio.
- El cifrado y la auditoría de eventos en las bases de datos son fácilmente configurables y también se proporcionan como parte del servicio.

Como aspectos básicos a valorar desde el punto de vista de la ciberseguridad de estos servicios:

1. Utilizar en la medida de lo posible usuarios gestionados por el sistema de gestión de identidades del proveedor de nube en vez de usuarios locales.

2. Evitar la exposición en Internet de las bases de datos a través de la configuración de red del servicio, exponerlo sólo en redes privadas (sin conectividad a Internet).

3. Utilizar las configuraciones que facilitan el cifrado en tránsito y en reposo de los datos por defecto.

4. En entornos con datos sensibles, evaluar la posibilidad de utilizar sistemas para que las claves de cifrado sean gestionadas en todo su ciclo de vida por los clientes.

—6.3.4 Servicios de Red

Los servicios de red son servicios especiales, ya que por sí mismos no tienen utilidad y simplemente sirven para realizar conectividad; no obstante, son imprescindibles para el consumo externo de los demás servicios, así como para la interconectividad entre ellos y, por qué no, con servicios de otras nubes de otros proveedores o infraestructura desplegada en los centros de procesado de datos de la organización.

Se hablará en todos los casos de servicios de "redes virtuales" porque para el cliente la parte física de los cables que unen los diferentes servidores del proveedor de servicios de nube es parte del servicio ofrecido y lo gestiona el proveedor.

Hablando, en general, como buenas prácticas para estos servicios, se deberán tener en cuenta los siguientes aspectos:

1. Diferenciar de manera estricta qué servicios deben ser privados (desde Internet no se tendrá acceso a ellos) o públicos (pueden accederse desde internet) y agrupar en subredes aisladas estos recursos.

2. Configuración de reglas de ACL para proteger el acceso desde/hacia los diferentes recursos a nivel de subred. Estas reglas, soportan reglas tanto para permitir tráficos concretos, como para denegarlos. La práctica general debería ser, denegar todo menos aquellos casos de uso que, por las necesidades del caso de uso, deba estar permitido.

3. Limitar la exposición de servicios críticos como SSH/RDP a orígenes conocidos o subredes de administración

4. Limitar la exposición de servicios de compartición de archivos comunes como CIFS/SMB/SFTP a orígenes conocidos

—6.3.5 Servicios de ciberseguridad

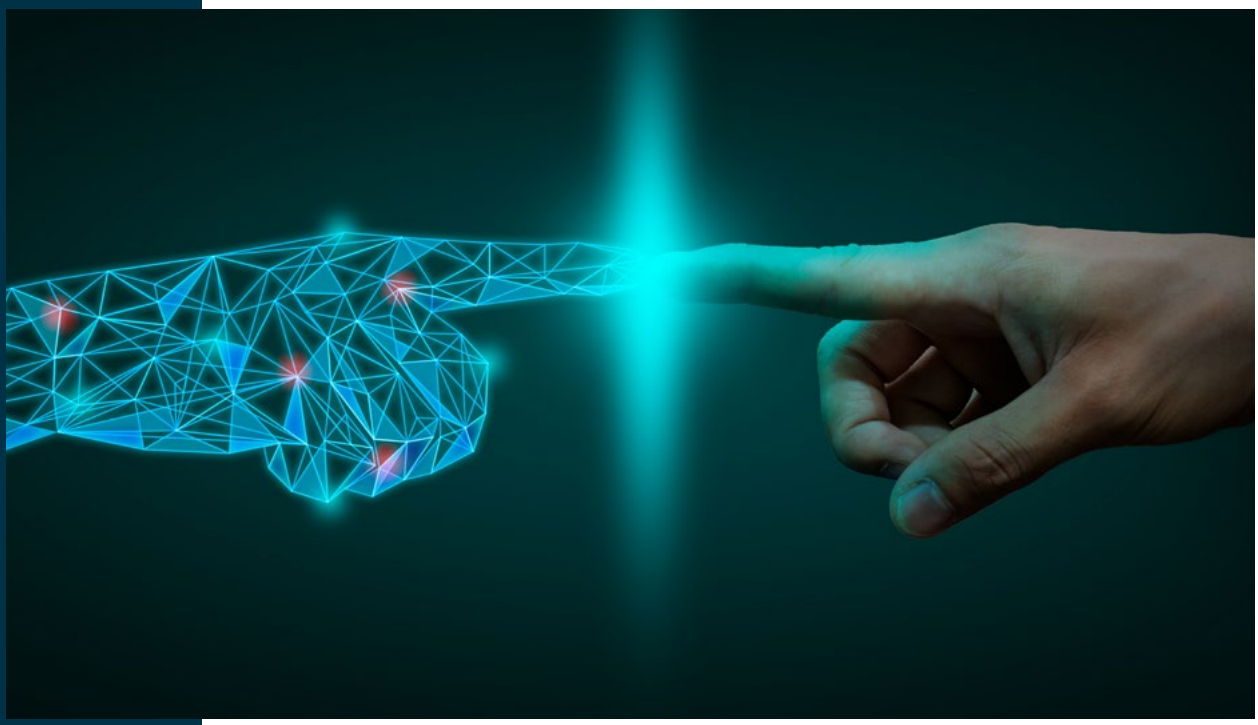
Por último, pero no por ello menos importante, los servicios de ciberseguridad que ofrecen los proveedores de nube pública pueden acercar capacidades de protección que, hasta hace relativamente poco tiempo se limitaban a organizaciones con gran cantidad de recursos, a públicos más modestos como desarrolladores independientes o pequeñas y medianas empresas. Algunos ejemplos:

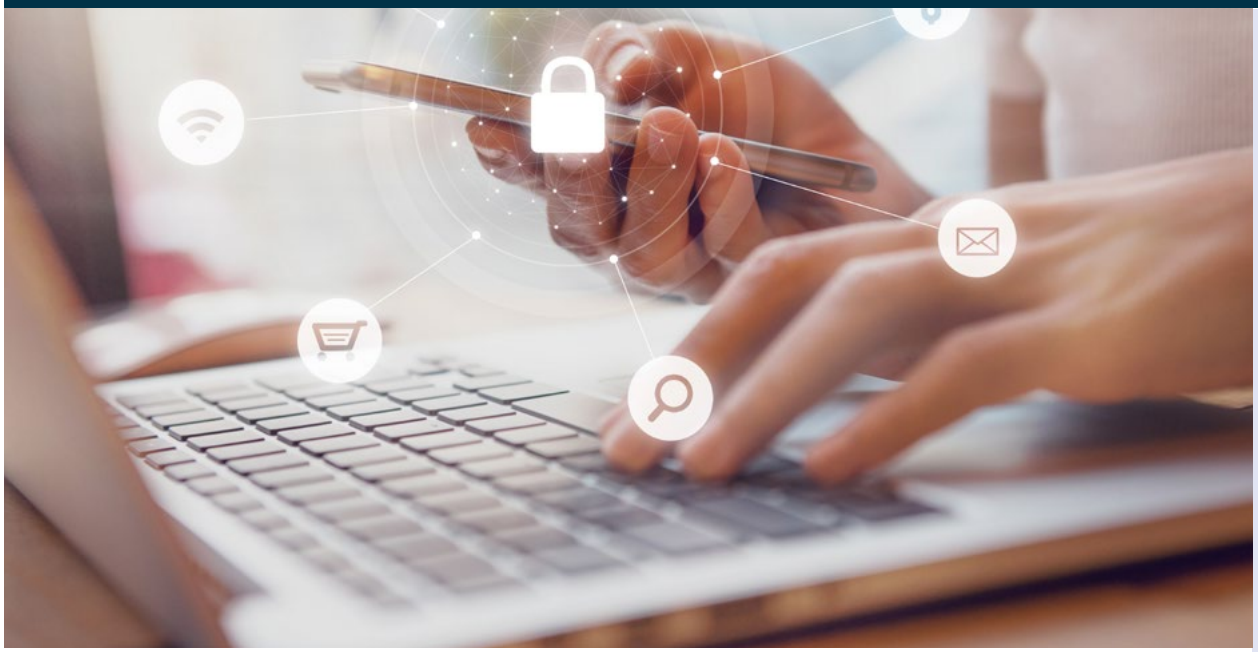
1. Gestión de usuarios: la mayoría de los proveedores de servicios de nube cuentan con robustos sistemas de gestión de usuarios en los que basan gran parte de la seguridad de todos los servicios que ofrecen, a través de los llamados roles. Las identidades, por lo tanto, convertidas en piedra angular de la seguridad de entornos de nube, cuentan con gran cantidad de servicios asociados de ciberseguridad, que de manera nativa se podrán utilizar para que su gestión sea correcta.

2. Cifrado y gestión de secretos: todo lo que tiene que ver con criptografía se trata de simplificar al máximo en entornos de nube, ofreciendo complejos sistemas, como por ejemplo infraestructuras para la gestión de claves públicas o generación de material criptográfico seguro de manera totalmente transparente al cliente. Además, en parte por la importancia que se comentaba en el punto anterior acerca de las identidades, los proveedores de servicios de la nube cuentan con importantes capacidades a la hora de preservar y utilizar contraseñas y otros secretos utilizados por las aplicaciones.

3. Monitorización: los servicios de auditoría y correlación de eventos para la detección de posibles amenazas han sido tradicionalmente capacidades que sólo grandes organizaciones podían pagar; gracias a los nuevos servicios ofrecidos por los proveedores de la nube, en parte soportados por mecanismos de inteligencia artificial y analítica avanzada, se puede disponer de capacidades de monitorización de ciberseguridad robustas de una manera sencilla.

4. Seguimiento del cumplimiento (o postura) de seguridad: el concepto que en inglés se denomina "Cloud Security Posture Management" ('CSPM') es una de las ventajas más importantes desde el punto de vista de ciberseguridad a la hora de desplegar servicios en la nube. Se basa en que, gracias a la gran capacidad de métricas y observabilidad que tienen todos los servicios desplegados en la nube, hay toda una familia de herramientas que, en tiempo real, pueden realizar evaluaciones de la configuración de absolutamente todos los sistemas, es decir, qué configuración tienen todos y ofrecer al cliente una visibilidad de su "postura de seguridad" con respecto, por ejemplo, estándares de la industria. Esto en entornos tradicionales es mucho más complejo por la heterogeneidad de la tecnología, pero en entornos de nube, al estar todo preparado para lanzarse y comprobarse a través de interfaces comunes, facilita sobremanera este tipo de monitorización.





—6.3.6 Principales retos de los impactos más frecuentes de seguridad en la nube

La facilidad y agilidad con que nuevas herramientas en la nube pueden ser implementadas están dificultando su control por parte de los equipos de seguridad. En este sentido, los problemas básicos de supervisión de la seguridad incluyen gobernanza, gestión de vulnerabilidades y configuraciones erróneas siguen siendo los principales factores de riesgo que las organizaciones deberían abordar para garantizar la seguridad de los datos. Por esto y para prevenir o reaccionar de una forma más ágil ante un incidente, pasamos a indicar algunas de las temáticas que deben considerarse en la adopción de la nube.

6.3.6.1 Gestión de identidades, credenciales, accesos y claves.

La preocupación por la identidad y el acceso es uno de los pilares para el colectivo de seguridad de la información ya que es imprescindible para garantizar la protección de los datos.

El acceso a la información encabeza la lista de retos porque la protección de los datos empieza y termina con el acceso y es uno de los principales vectores de ataque. Así, la identidad y el acceso en las plataformas de un proveedor de servicios en la nube son dos elementos cruciales ya que, combinados, proporcionan la entrada a los sistemas y el acceso a los datos pudiendo llegar a representar una amenaza para la estabilidad operativa y la seguridad de cualquier organización.

Los atacantes ya no intentan entrar por fuerza bruta en la infraestructura de las empresas, ya que existen multitud de formas de comprometer y robar credenciales corporativas. En la actualidad, la táctica preferida para el robo de credenciales es hacerse pasar por un usuario legítimo para evitar la detección (suplantación de identidad) o navegar por foros en Internet donde se publican o venden credenciales de servicios hackeados ya que es habitual que los usuarios las reutilicen en múltiples servicios.

Una sólida gestión de claves mediante el cifrado seguro puede salvaguardar los datos y ayudar a garantizar que las partes de confianza sólo tengan acceso a aquella información que es absolutamente necesaria. Desgraciadamente, asegurar los datos a través del cifrado puede causar a menudo un pequeño dolor de cabeza en la gestión de claves, debido al creciente número de éstas y, en ocasiones, su complejidad operativa.

La gestión de la identidad recae casi por completo en el cliente para gestionarla adecuadamente. Los proveedores de la nube proporcionan ayuda, pero la flexibilidad de las plataformas en la nube viene con el requisito de gestionar eficazmente el acceso y los privilegios de los usuarios y del sistema. Es una de las principales responsabilidades de la empresa que aprovecha la nube en un modelo de responsabilidad compartida y, por tanto, ocupa un lugar destacado en su evaluación del riesgo.

Aspectos para tener en cuenta en la gestión de accesos e identidades:

- Las defensas reforzadas en el núcleo de las arquitecturas empresariales han hecho que el hacking se dirija a la identidad de los usuarios de los puntos finales como fruta fácil de conseguir.
- Aislamiento discreto basado en el usuario y la aplicación para lograr una sólida capa de confianza cero más allá de la simple autenticación.
- Uso de herramientas avanzadas (ej.: análisis de comportamiento) para la gestión de derechos de la infraestructura de la nube ("Cloud Infrastructure Entitlements Management", 'CIEM'), las políticas operativas y los modelos de riesgo estructurados.

6.3.6.2 Interfaces y API inseguras

Las API y otras interfaces similares pueden presentar vulnerabilidades debido a una configuración incorrecta, vulnerabilidades de codificación o falta de autenticación y autorización, entre otras cosas. Estos descuidos pueden causar que la organización sea potencialmente vulnerable a la actividad maliciosa.

Las organizaciones se enfrentan a una tarea difícil en la gestión y la seguridad de las API (ej.: la velocidad de desarrollo en la nube se ha acelerado enormemente, los procesos que llevaban días o semanas utilizando métodos tradicionales pueden completarse en segundos o minutos en la nube). Asimismo, el uso de múltiples proveedores de la nube también añade complejidad, ya que cada proveedor tiene capacidades únicas que se mejoran y amplían casi a diario. Este entorno dinámico requiere un enfoque ágil y proactivo para el control y la corrección de los cambios que muchas empresas no dominan.

Los aspectos para considerar sobre las APIs incluyen:

- La superficie de ataque proporcionada por las APIs debe ser revisada, configurada y asegurada.
- Los controles tradicionales y las políticas y enfoques de gestión de cambios deben actualizarse para seguir el ritmo del crecimiento y el cambio de las API basadas en la nube.
- Las organizaciones deben adoptar la automatización y emplear tecnologías que supervisen continuamente el tráfico anómalo de las API y solucionen los problemas casi en tiempo real.

6.3.6.3 Mala configuración y control de cambios inadecuado

Las malas configuraciones de los activos informáticos pueden dejarlos vulnerables a daños indeseados o a actividades maliciosas externas e internas. La falta de conocimiento del sistema o de comprensión de los ajustes de seguridad puede dar lugar a configuraciones erróneas.

Un problema grave de los errores de configuración es que pueden verse magnificados por la nube. Una de las mayores ventajas de la nube es su escalabilidad y la forma en que permite crear servicios interconectados para facilitar los flujos de trabajo. Sin embargo, esto también significa que una mala configuración puede tener ramificaciones magnificadas en múltiples sistemas.

Debido a una canalización automatizada de integración continua/entrega continua (CI/CD), las configuraciones erróneas y las vulnerabilidades sin identificar durante el tiempo de construcción se despliegan automáticamente a la producción.

Los puntos clave a valorar sobre la mala configuración y el control de cambios inadecuado en la nube incluyen:

- Las organizaciones deben adoptar las tecnologías disponibles que escanean continuamente los recursos mal configurados para permitir la remediación de las vulnerabilidades en tiempo real.
- Los enfoques de gestión de cambios deben reflejar la naturaleza incesante y dinámica de las continuas transformaciones empresariales y los retos de seguridad para garantizar que los cambios aprobados se realicen correctamente mediante una verificación automatizada en tiempo real.

6.3.6.4 Falta de arquitectura y estrategia de seguridad en la nube

El rápido ritmo de los cambios y el enfoque prevalente, descentralizado y de autoservicio de la administración de la infraestructura de la nube dificulta la capacidad de abordar la seguridad de la información desde el diseño y en ocasiones se ignoran los riesgos de seguridad.

La mayoría de los equipos de seguridad que se ocupa de la seguridad en la nube debe considerar qué combinación de controles de seguridad por defecto proporciona el proveedor de la nube, controles de seguridad premium que pueden ser necesarios y los productos de seguridad de terceros que pueden complementar las dos opciones anteriores y que abordan su perfil de riesgo específico que puede ser diferente a nivel de aplicación y/o servicio. Esto introduce mucha complejidad frente a las amenazas emergentes.

Entre las principales conclusiones sobre la falta de arquitectura y estrategia de seguridad en la nube se encuentran las siguientes:

- Las organizaciones deben tener en cuenta los objetivos de negocio, el riesgo, las amenazas a la seguridad y el cumplimiento legal en el diseño y las decisiones sobre servicios e infraestructuras en la nube.
- Dado el rápido ritmo de cambio y el limitado control centralizado en las implantaciones de la nube, es más importante y no menos, desarrollar y adherirse a una estrategia de infraestructura y a unos principios de diseño.
- Se aconseja a los clientes de las nubes que consideren las prácticas fundacionales de diligencia debida y evaluación de la seguridad de los proveedores.

6.3.6.5 Desarrollo de software inseguro

Si bien la nube puede ser un entorno atractivo para los desarrolladores, las organizaciones deben asegurarse de que estos comprendan cómo el modelo de responsabilidad compartida afecta a la seguridad de su software (ej.: una vulnerabilidad en Kubernetes podría ser responsabilidad de un proveedor de servicios de nube, mientras que un error en una aplicación web que utiliza tecnologías nativas de la nube podría ser responsabilidad del desarrollador).

Los aspectos para tener en cuenta sobre el desarrollo de software inseguro en la nube incluyen:

- El uso de tecnologías en la nube evita reinventar las soluciones existentes, lo que permite a los desarrolladores centrarse en los problemas exclusivos de la empresa.
- Al aprovechar la responsabilidad compartida, elementos cómo los parches pueden ser propiedad de un proveedor de servicios de nube en lugar de la empresa.
- Los proveedores de servicios de nube dan importancia a la seguridad y proporcionan orientación sobre cómo desarrollar los servicios de forma segura.

6.3.6.6 Recursos de terceros inseguros

Los riesgos de terceros existen en todos los productos y servicios que consumimos. Dado que un producto o servicio es una suma de todos los demás productos y servicios que utiliza, un ataque puede empezar en cualquier punto de la cadena de suministro del producto y proliferar a partir de ahí. Los actores de las amenazas saben que sólo necesitan comprometer el eslabón más débil de la cadena de suministro para propagar su software malicioso, a menudo utilizando los mismos vehículos que los desarrolladores utilizan para escalar su software.

Los aspectos para considerar sobre los recursos inseguros de terceros son las siguientes:

- Uso de productos que cuenten con soporte oficial.
- Productos con certificaciones de cumplimiento, que hablen abiertamente de sus esfuerzos de seguridad, que tengan un programa de recompensas por errores y que traten a sus usuarios de forma responsable informando de los problemas de seguridad y entregando las correcciones rápidamente.
- Identificación y seguimiento de las medidas de seguridad aplicadas por terceros. Esto incluye el código abierto, los productos SaaS, los proveedores de la nube y los servicios gestionados, así como otras integraciones que puedas haber añadido a tu aplicación.
- Revisión periódica de los recursos de terceros. Aquellos productos innecesarios se deben eliminar y revocar los accesos a estos.
- Ejecución de pruebas de penetración en las aplicaciones.
- Formación de los desarrolladores en codificar de forma segura y utilizar soluciones de pruebas de seguridad de aplicaciones estáticas (SAST) y dinámicas (DAST).

6.3.6.7 Vulnerabilidades del sistema

Las vulnerabilidades del sistema son fallos en un proveedor de servicios de nube, que pueden utilizarse para comprometer la confidencialidad, la integridad y la disponibilidad de los datos e interrumpir las operaciones del servicio. Entre las vulnerabilidades típicas se encuentran las de "día cero" (vulnerabilidades muy nuevas para las que aún no existe un parche de seguridad), los sistemas sin los parches de seguridad existentes aplicados, los ajustes vulnerables de configuración, las credenciales débiles o las configuraciones de seguridad por defecto (de fábrica) que los atacantes pueden obtener o adivinar fácilmente.

Los riesgos de seguridad surgidos por las vulnerabilidades del sistema pueden minimizarse en gran medida mediante el escaneo recurrente de los sistemas, las redes y las aplicaciones para la detección rutinaria de vulnerabilidades, la correspondiente aplicación de parches de seguridad y/o aplicación de controles adicionales.

6.3.6.8 Revelación accidental de datos en la nube

La exposición de datos sigue siendo un problema generalizado entre los usuarios de la nube, ya que el 55%[9] de las empresas tiene al menos una base de datos expuesta a Internet y muchas de esas bases de datos tienen contraseñas débiles o no requieren ningún tipo de autenticación, lo que las convierte en objetivos fáciles para los agentes de amenazas.

Los principales aspectos sobre la divulgación accidental de datos en la nube son los siguientes:

- ¿Qué bases de datos están en las nubes? Revisa las bases de datos de tu plataforma como servicio (PaaS), el almacenamiento y las cargas de trabajo informáticas que alojan las bases de datos, incluidas las máquinas virtuales (VM), los contenedores y el software de base de datos instalado en ellos.
- ¿Qué se expone efectivamente desde el entorno de la nube? Elije motores de exposición que tengan visibilidad completa de tu entorno de nube para identificar cualquier enrutamiento o servicios de red que permitan que el tráfico quede expuesto externamente. Esto incluye balanceadores de carga, balanceadores de carga de aplicaciones, redes de entrega de contenido (CDN), emparejamiento de redes y firewalls en la nube.
- Evalúa la exposición externa de un clúster de Kubernetes. El motor de exposición debe tener en cuenta muchos componentes de red de Kubernetes, incluidas las direcciones IP del clúster, los servicios de Kubernetes y las reglas de ingreso.
- Reduce la exposición al acceso asegurándose de que la base de datos está configurada con la política de gestión de accesos e identidades con menores privilegios, que las asignaciones de esta política están controladas y supervisadas, los datos sensibles están cifrados de forma segura y las claves de cifrado están debidamente gobernadas.

[9]Top Threats to Cloud Computing Pandemic Eleven de la Cloud Security Alliance.

6.3.6.9 Configuración errónea y explotación de las cargas de trabajo sin servidor y de los contenedores

La gestión y el escalado de la infraestructura para ejecutar aplicaciones puede seguir siendo un reto para los desarrolladores. Deben asumir más responsabilidad controles de red y seguridad para sus aplicaciones.

Aunque parte de esa responsabilidad puede descargarse a un proveedor de servicios de nube mediante el uso de cargas de trabajo sin servidor y en contenedores, para la mayoría de las organizaciones, la falta de control de la infraestructura de la nube limita las opciones de mitigación de los problemas de seguridad de las aplicaciones y la visibilidad de las herramientas de seguridad tradicionales. Por ello, se recomienda crear prácticas organizativas sólidas centrándonos en la seguridad de las aplicaciones, la observabilidad y control de las configuraciones, así como de los eventos de la propia nube, el control de acceso y la gestión de secretos para reducir el radio de explosión de un ataque.

Entre los principales retos sobre la desconfiguración y la explotación de las cargas de trabajo sin servidor y con contenedores se incluyen:

- Implementar la gestión de la postura o cumplimiento de las medidas de seguridad en la nube (CSPM), el CIEM y las plataformas de protección de la carga de trabajo en la nube para aumentar la visibilidad sobre la configuración de la seguridad, imponer el cumplimiento y lograr el menor privilegio en las cargas de trabajo sin servidor y en contenedores.
- Invertir en formación a las personas de la organización sobre seguridad en la nube, procesos de gobernanza y patrones de arquitectura segura en la nube reutilizables para reducir el riesgo y la frecuencia de las configuraciones inseguras en la nube.
- Garantizar la seguridad de las aplicaciones y las mejores prácticas de ingeniería incluyendo las buenas prácticas dentro de la cultura de la organización.

6.3.6.10 Crimen organizado, hackers y grupos APT

Los grupos de amenazas persistentes avanzadas ("Advanced Persistent Threats", 'APT') suelen centrar su forma de robar en la adquisición de datos. Estos grupos son estudiados de cerca por grupos de inteligencia de amenazas, que publican informes detallados sobre sus métodos y tácticas. Se recomienda a las organizaciones que utilicen este tipo de informes para organizar ejercicios de equipo rojo con el fin de protegerse mejor de los ataques de las APT, así como realizar ejercicios de caza de amenazas para identificar la presencia de cualquier APT en sus redes.

Los puntos clave en el área de las APT incluyen:

- Realizar un análisis del impacto en el negocio de la organización para conocer sus activos de información.
- Participar en grupos de intercambio de información sobre ciberseguridad.
- Comprender cualquier grupo de APT relevante y sus tácticas, técnicas y procedimientos (TTP).
- Realizar ejercicios de seguridad ofensivos para simular las TTP de estos grupos APT.
- Asegurarse de que las herramientas de supervisión de la seguridad están ajustadas para detectar las TTP de cualquier grupo APT relevante.

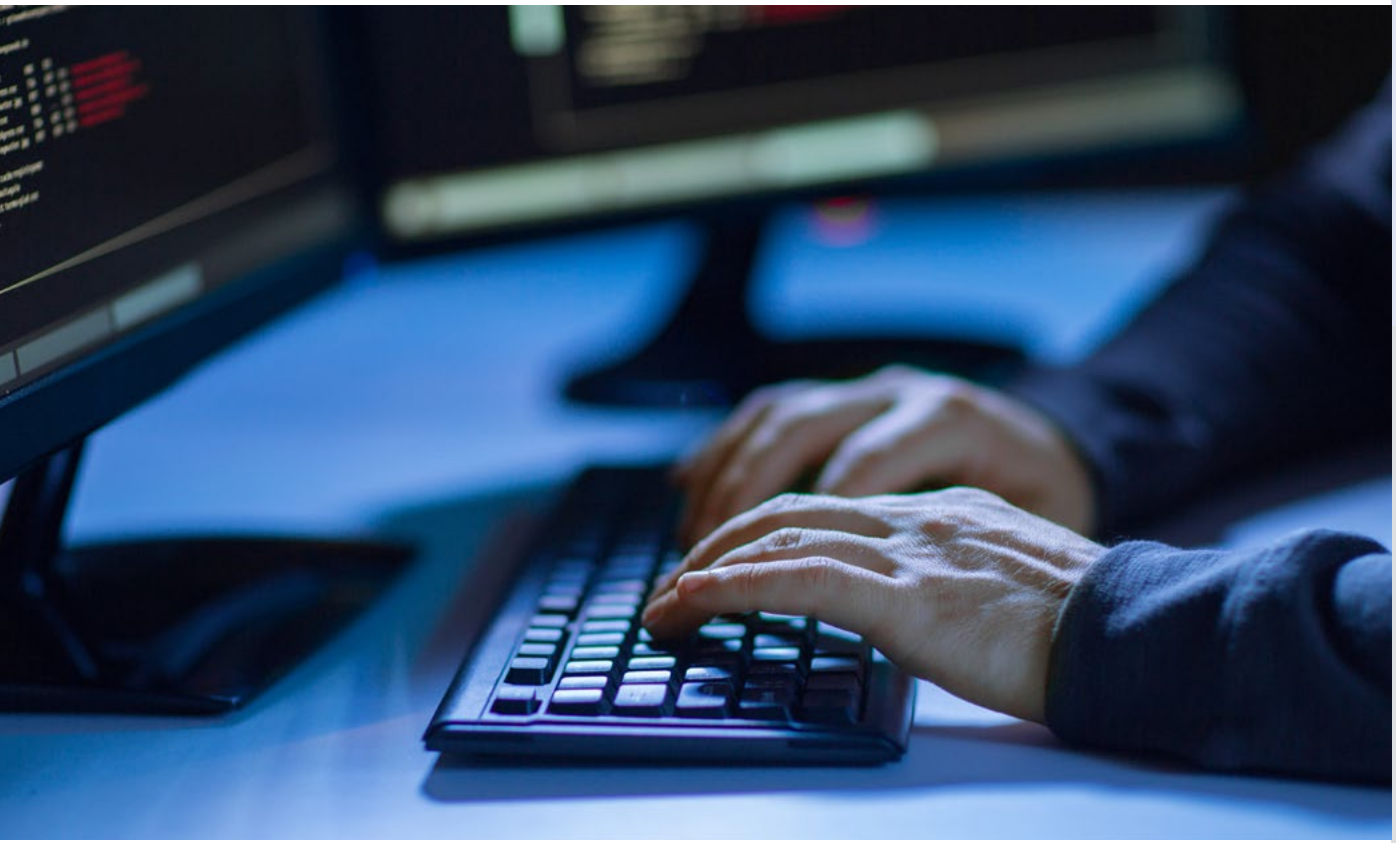
6.3.6.11 Exfiltración de datos en la nube

La exfiltración de datos de almacenamiento en la nube se produce cuando la información sensible, protegida o confidencial es liberada, vista, robada o utilizada por un individuo fuera del entorno operativo de la organización. Muchas veces la exfiltración de datos puede ocurrir sin el conocimiento del propietario de los datos. En algunos casos, el propietario puede no ser consciente del robo de los datos hasta que se lo notifica el ladrón o hasta que aparecen a la venta en Internet.

Aunque la nube puede ser un lugar cómodo para almacenar datos, también ofrece múltiples formas de exfiltrarlos. Para protegerse contra la exfiltración, las organizaciones han empezado a recurrir a un modelo de confianza cero en el que se utilizan controles de seguridad basados en la identidad para proporcionar el acceso menos privilegiado a los datos, esto es, para proporcionar los accesos únicamente a aquella información que los usuarios necesitan para el desarrollo de la actividad de negocio que realicen.

Entre los aspectos a considerar sobre la exfiltración del almacenamiento en la nube se encuentran los siguientes:

- El almacenamiento en la nube requiere un entorno en el que cuya configuración considere la seguridad de los datos (gestión de la postura de seguridad SaaS [SSPM], CSPM), la identificación y remediación de las vulnerabilidades en la infraestructura como servicio (IaaS) y un fuerte control de la identidad y el acceso tanto de personas como de sistemas y redes.
- Para detectar y prevenir los ataques y la exfiltración de datos, es recomendable aplicar las guías de buenas prácticas del proveedor de servicios de nube y las capacidades de supervisión y detección.
- Una formación de concienciación de los empleados sobre el uso del almacenamiento en la nube, ya que los datos están dispersos en varias ubicaciones y controlados por varias personas.
- Una evaluación de la resistencia de la seguridad de los proveedores de la nube y, como mínimo, el cumplimiento de las normas de seguridad, el acuerdo legal y el acuerdo de nivel de servicio ('ANS' o, en inglés, 'SLA').
- Si no está limitado por el negocio, el cifrado del lado del cliente puede proporcionar protección contra los atacantes del proveedor de servicios de nube. Para aplicar el cifrado, se deberán evaluar las capacidades del proveedor en la nube, así como las restricciones operativas tanto del propio operador como del negocio de la organización.
- La clasificación de los datos puede ayudar a establecer diferentes controles y, si se produce una exfiltración, a evaluar el impacto y las acciones de recuperación necesarias.



7 CONCLUSIONES

En la actualidad, la mayoría de las organizaciones utilizan servicios en la nube ya sea de forma directa -contratando infraestructura en la propia nube, servicios o procesos específicos- o indirecta -mediante el uso de proveedores cuya actividad o productos están basados o se apoyan en la nube. Así, los servicios en la nube se han convertido en uno de los servicios críticos de muchas organizaciones ya que, al promover mayor eficacia y agilidad en la realización de la actividad de negocio, han sido integrados en los procesos tradicionales o, inclusive, los han llegado a substituir intensificando así la dependencia de la organización en la nube.

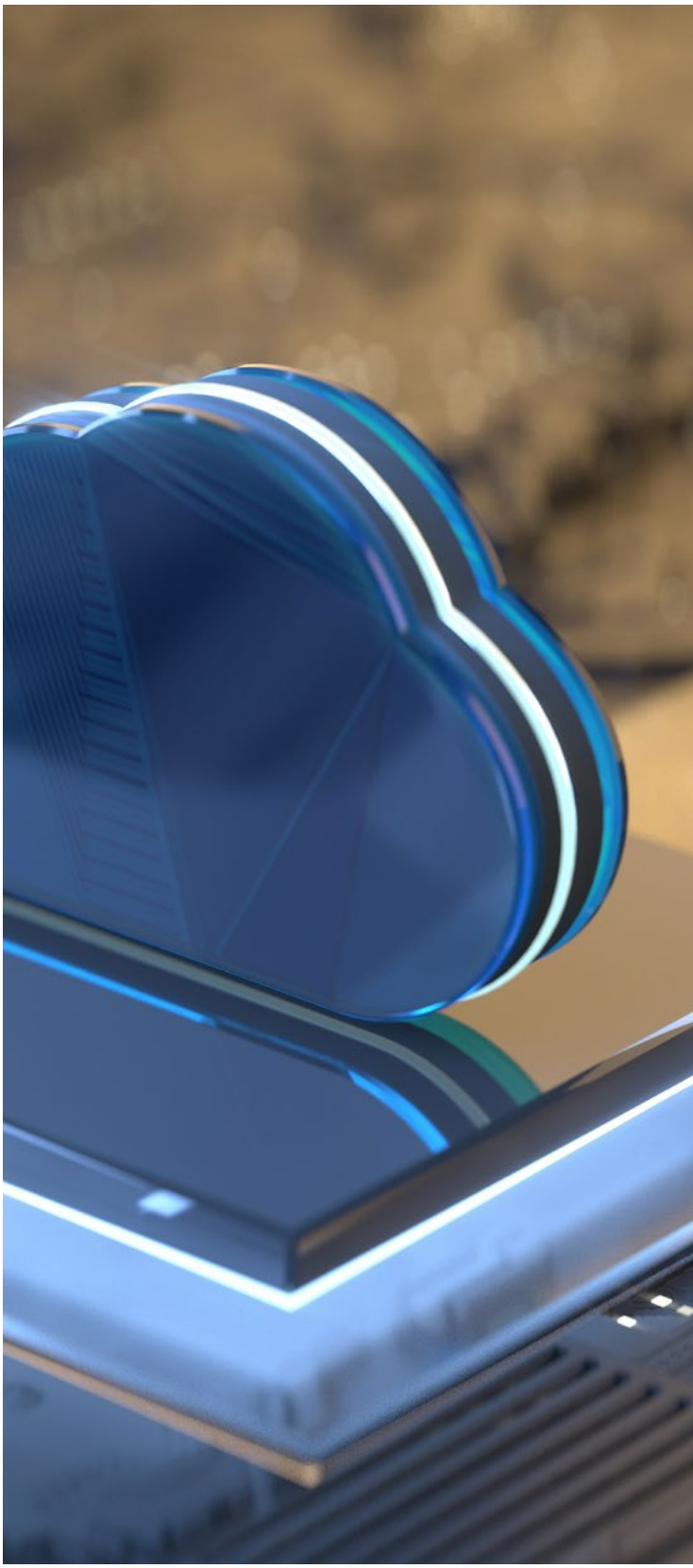
El crecimiento exponencial de los servicios en la nube y la rápida adopción por parte de las organizaciones ha causado una brecha entre los clásicos procesos de gestión y las nuevas necesidades requeridas por esta transformación tecnológica tanto a nivel de formación de las personas, cultura del negocio y recursos.

Además, añadido a esto, los ataques a la seguridad de los datos de las organizaciones siguen creciendo y profesionalizándose sin discernir entre el tamaño de la organización, el objetivo de su actividad ni localización, es decir, su afectación es sistémica y global.

Por todo esto, la necesidad de una Guía de gestión de incidentes en la nube tiene más sentido que nunca. Si bien es cierto que ya se han publicado guías y metodologías de mejores prácticas al respecto, hemos detectado que existen pocos manuales en los que de forma conjunta, sencilla y amena se expliquen las bases de los servicios en la nube y donde se resuman los principales aspectos a tener en cuenta para la gestión de los incidentes en este entorno.

Para simplificar el diseño de un plan de gestión de incidencias en la nube, se han citado las principales nociones a tener en cuenta en estos servicios y que son relevantes en el momento de atender un incidente como pueden ser: leyes y regulaciones que pueden ser de aplicación e introducen obligaciones que se deben cumplir antes, durante y cuando el incidente ha finalizado; las distintas modalidades de nube y la visibilidad que la organización puede tener o no de la infraestructura, procesos y gestión del servicio; el modelo de responsabilidad compartida -que no es más que ser consciente de cuáles son las obligaciones en materia de gestión de incidentes de seguridad de nuestros proveedores, así como ser consciente de que la responsabilidad última de la seguridad del dato es siempre de la propia organización ya que es la propietaria del mismo; los procesos y planes de apoyo a la organización y a la actividad técnica realizada en la gestión del incidente y que son imprescindibles para un buen gobierno y gestión de expectativas (ej.: plan de comunicación); y el seguro de riesgos cibernéticos.

Con todo, las organizaciones que están pensando en iniciar, ya han empezado o llevan años usando servicios en la nube, precisan reestructurar los procesos tradicionales de gestión de incidencias considerando la perspectiva y aspectos fundamentales de la nube para asegurar que tienen controlados los desafíos que esta presenta y están preparadas para reaccionar ante posibles incidencias con la mayor resiliencia posible.



8 ANEXO I: METODOLOGÍA DE GESTIÓN DE INCIDENTES EN PROVEEDORES DE NUBE PÚBLICO

Los principales proveedores de nube pública tienen publicada documentación referente a la Gestión de los Incidentes de Seguridad.

En el momento de la elaboración de esta guía, dicha información está disponible en los siguientes enlaces:

- **Amazon Web Services:**
  - o https://docs.aws.amazon.com/whitepapers/latest/aws-security-incident-response-guide
- **Google:**
  - o https://cloud.google.com/docs/security/incident-response
- **Microsoft:**
  - o https://docs.microsoft.com/en-us/secuity/benchmark/azure/security-control-incident-response
  - o https://docs.microsoft.com/es-es/security/compass/incident-response-overview
- **Oracle:**
  - o https ://www.oracle.com/corporate/security-pracices/corporate/security-inciden-response.html
- **IBM:**
  - o https://www.ibm.com/downloads/cas/QBMEAMAV

8.1 Gestión de incidentes en AWS

Amazon Web Services dispone de una Guía de Respuesta a Incidentes de Seguridad[10].

La guía propone consultar adicionalmente dos enlaces para entender mejor el enfoque de AWS respecto a la gestión de la seguridad en el nube:

- Best Practices for Security, Identity, & Compliance
- Security Perspective of the AWS Cloud Adoption Framework (CAF)

Con relación a AWS, es importante remarcar que las bases de esta nube para el enfoque de un programa exitoso de respuesta a incidentes en la nube son: educar, preparar, simular e iterar.

[10]https://docs.aws.amazon.com/whitepapers/latest/aws-security-incident-response-guide

—8.1.1 Educar

En el apartado de Educar, muestra el "Modelo de Seguridad Compartida"[11] :

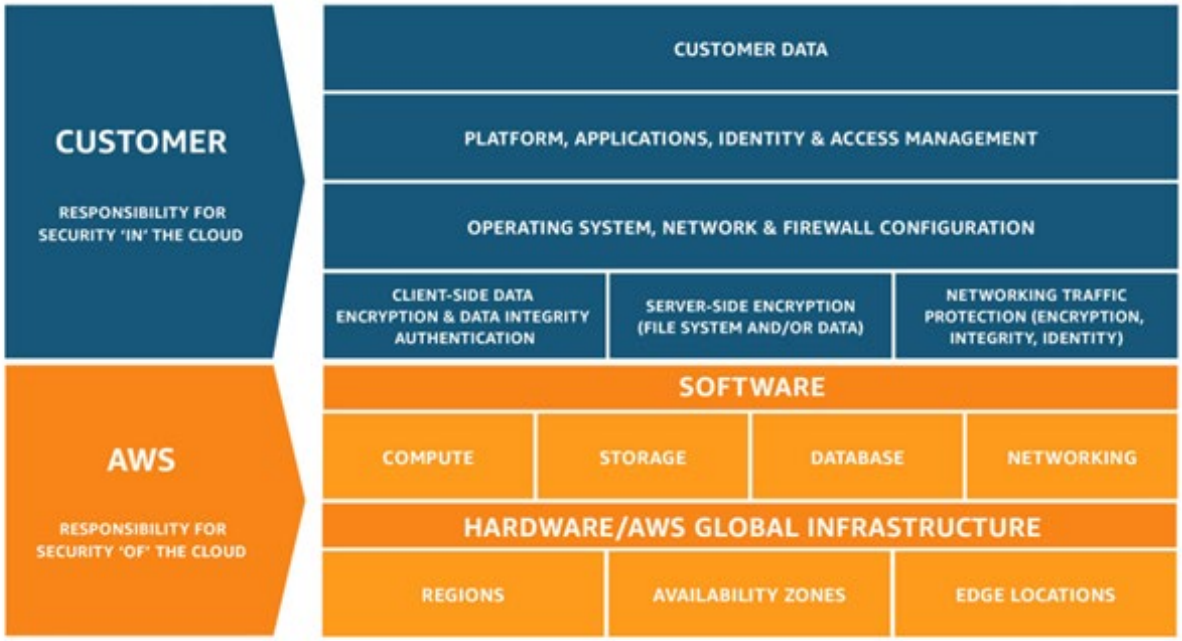


Figure 1: Shared Responsibility Model

En este apartado, AWS aconseja la implantación de procesos de respuesta a incidentes alineados con la NIST SP 800-61 "Guía de gestión de incidentes de seguridad informática" y proponiendo los siguientes objetivos específicos de diseño de la respuesta a incidentes en la nube:

- Establecer objetivos de respuesta.
- Responder usando los servicios disponibles en la nube.
- Disponer de un inventario de los activos, así como de las herramientas y servicios de respuesta necesarios para atender a un incidente de seguridad.
- Utilizar mecanismos de redistribución.
- Automatizar los procesos de respuesta ante incidentes de seguridad cuando sea posible.
- Elegir soluciones escalables.
- Aprender y mejorar el proceso de forma continua.

[11] Aquí se entiende como "Seguridad compartida" como a la distribución de la responsabilidad en la aplicación de las medidas de seguridad; en todo momento la responsabilidad sobre la información y el garantizar que las medidas de seguridad se aplican de forma adecuada es de la Organización.

Con lo anterior, AWS define tres posibles dominios que pueden sufrir un incidente de seguridad: servicio, infraestructura y aplicación. En cada caso los actores implicados en la resolución del incidente pueden variar y la organización no solamente deberá tenerlo en cuenta, sino que deberá disponer establecer los roles y responsabilidades, así como los procedimientos necesarios de forma anticipada.

En este apartado también muestra varios ejemplos interesantes sobre fuentes de eventos de seguridad: registros de eventos y servicios de monitorización de AWS, actividad de facturación, inteligencia de amenazas, herramientas de proveedores colaboradores con AWS, AWS Outreach (identificación de actividad maliciosa o abusiva) y contacto con el equipo de seguridad del cliente.

Por último y de lectura sugerida en caso de usar la nube de AWS, se incluye una breve explicación de las capacidades de seguridad de la nube de AWS.

—8.1.2 Preparar

AWS aconseja preparar tanto a las personas como a la tecnología considerando:

- Personas: definición de roles y responsabilidades, definición de mecanismos de respuesta, creación de una cultura de seguridad receptiva y adaptativa y predicción de la respuesta (anticipación de imprevistos).
- Tecnología: preparación del acceso a las cuentas de AWS, así como de los procesos y obtención del soporte del proveedor de nube.

—8.1.3 Simular

La finalidad de la simulación de respuesta ante un incidente de seguridad es facilitar la oportunidad para practicar el plan de respuesta antes de que se produzca un incidente de seguridad y, así preparar tanto a las personas como la tecnología para cuando el incidente se materialice.

AWS menciona algunos aspectos de valor de las actividades de simulación:

- Verificar si la organización está preparada.
- Desarrollar la confianza entre los equipos y de la Alta Dirección.
- Cumplir con leyes u obligaciones contractuales.
- Generar evidencias para acreditación.
- Mejorar la velocidad y las herramientas.
- Refinar los planes y procesos de comunicación y escalado de incidentes.
- Desarrollar confortabilidad de los equipos y de la organización en general ante situaciones extrañas e inesperadas.

A continuación, se relacionan los pasos que propone AWS para ejecutar una simulación:

- Encontrar un riesgo o amenaza de importancia que pudiera afectar negativamente a la organización.
- Identificar profesionales de seguridad con la preparación suficiente para definir la simulación.
- Construir un modelo realista que considere el estado de la organización, los recursos y las personas disponibles.
- Crear y probar los elementos del escenario.
- Considerar a otras áreas de la organización.
- Ejecutar la simulación.
- Medir, evaluar lecciones aprendidas, mejorar el proceso y repetir.

Por último, AWS menciona algunos ejemplos de simulaciones:

- Cambios ilícitos en la configuración de la red o en los recursos.
- Contenido sensible o credenciales que se han expuesto públicamente por error debido a una mala configuración.
- Aislamiento de un servidor web que se está comunicando con direcciones IP sospechosas.

—8.1.4 Iterar

En el apartado anterior se han observado los beneficios de realizar actividades de simulación del plan de respuesta ante incidentes. Las simulaciones permiten detectar mejoras que se pueden aplicar al plan y sus iteraciones facilitan la mejora continua de los procedimientos de respuesta de la organización.

AWS aconseja recopilar en uno o varios documentos que denomina “runbook”, los pasos para contener un evento específico de seguridad y volver a un estado aceptable. Cada organización debe elaborar sus runbooks a partir de las tareas que se ejecutan tras una alerta y los debe ir mejorando en cada iteración con el objetivo de que se pueda automatizar totalmente y ser invocados directamente por las alertas o eventos.

AWS dispone de múltiples servicios que pueden generar y gestionar alertas, a partir de los eventos generados por estos servicios, se pueden ir desarrollando los runbooks:

- AWS Trusted Advisor
- AWS Security Hub's Foundational Security Best Practices
- AWS Config Rules
- AWS Config Rules Github repository
- Amazon GuardDuty User Guide
- Event-Driven Response

8.2 Gestión de incidentes en Google

La respuesta ante incidentes es un aspecto clave de la seguridad general de Google y, por ello, el proveedor dispone de un riguroso proceso para su gestión que incluye acciones, escalados, medidas de mitigación, resolución y notificación de cualquier potencial incidente que impacte sobre la confidencialidad, integridad o disponibilidad de datos de sus clientes.

En el caso de Google Cloud Platform (GCP), los clientes disponen del "Centro de mando de seguridad en la nube" para obtener más información acerca de los recursos, las vulnerabilidades, los riesgos y las políticas de las organizaciones.

En este panorama, los clientes deben adaptar las funciones de seguridad de forma adecuada y conforme a sus propias necesidades además de encargarse de instalar actualizaciones de software, configurar cortafuegos y zonas de seguridad de red, y asegurarse de que los usuarios finales tienen las credenciales de sus cuentas a buen recaudo y no muestran datos sensibles a usuarios sin autorización.

En la siguiente imagen se ofrece un ejemplo ilustrativo de cómo varía la responsabilidad entre Google y el cliente según la proporción de servicios gestionados que utiliza este último. A medida que el cliente pasa de utilizar soluciones locales a recurrir a productos de la nube, aumenta la proporción general del servicio en la nube que gestiona Google y se reducen las responsabilidades del cliente en cuanto a la aplicación de las medidas de seguridad.

La gestión del programa de respuesta a incidentes de Google recae sobre equipos de expertos en la materia de distintas funciones especializadas. De esta manera, se asegura que todas las respuestas están a la altura de los desafíos específicos que presenta cada incidente. Según el tipo de incidente, el equipo profesional de respuesta de Google puede incluir expertos de las siguientes disciplinas:

- Gestión de incidentes en la nube
- Ingeniería de productos
- Ingeniería de calidad
- Seguridad y privacidad en la nube
- Análisis forense digital
- Investigación mundial
- Detección de señales
- Asesoría de seguridad, privacidad y productos
- Confianza y seguridad
- Tecnología frente a usos indebidos
- Servicio de asistencia
- Proceso de respuesta a incidentes de datos

Cada incidente de datos es único y el objetivo del proceso de respuesta a estos incidentes es proteger los datos de los clientes, devolver el sistema a la normalidad lo antes posible y cumplir tanto los requisitos de las normativas como los contractuales.

En resumen, Google cuenta con un programa de respuesta a incidentes a través de un proceso desarrollado con técnicas líderes en el sector para resolver incidentes y ajustado para funcionar de forma eficiente a escala; cuenta con sistemas de monitorización, analíticas de datos y servicios de aprendizaje automático punteros que detectan y limitan incidentes de forma proactiva; dispone de expertos en la materia dedicados a los que se puede recurrir para responder a incidentes de datos de cualquier tipo y envergadura; y, finalmente, incluye un proceso desarrollado para notificar al instante a los clientes afectados. Todo ello en línea con los compromisos que establece Google en los términos del servicio y en los contratos con los clientes.

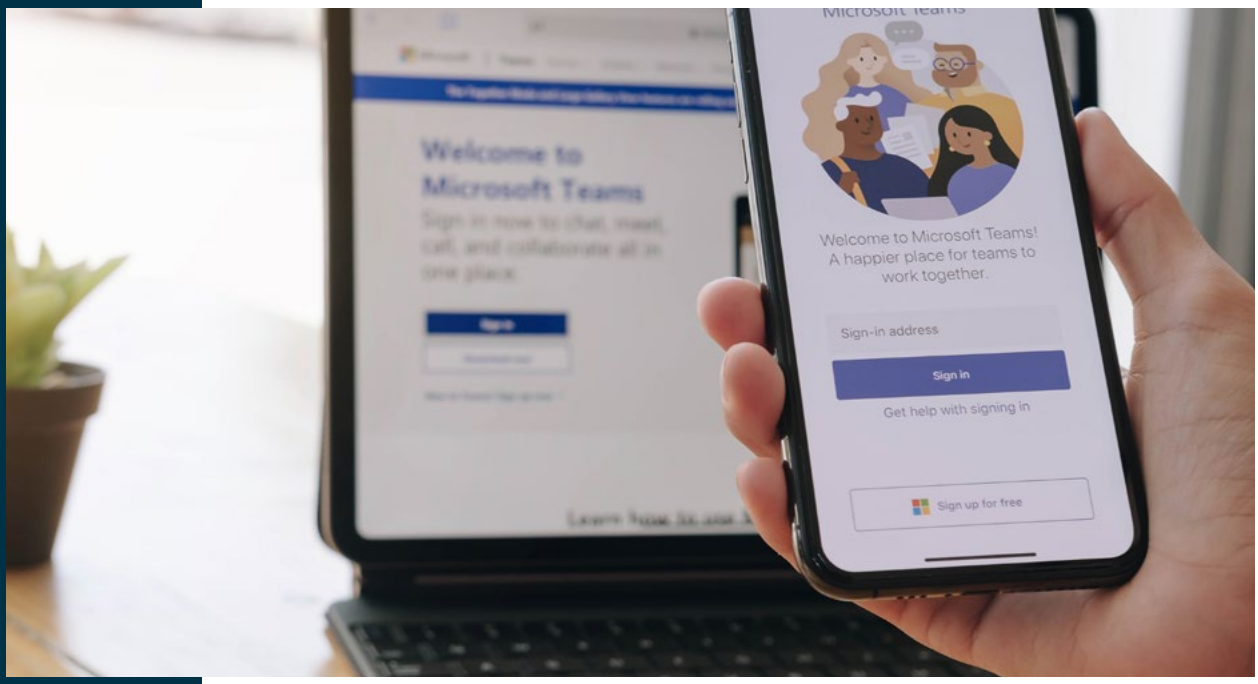
8.3 Gestión de incidentes en Microsoft

La gestión de incidentes en el entorno de los servicios de nube de Microsoft (Azure) se enmarca en los procesos de operación de la seguridad ("SecOps") que están enfocados a reducir el tiempo que un atacante tiene acceso a los recursos mediante la detección, respuesta y ayuda en la recuperación de los incidentes haciendo uso del marco de ciberseguridad de NIST.

Para una efectiva gestión de incidentes, Microsoft define 6 tareas dentro de la nube de Azure:

1. Creación de una guía de respuesta ante incidentes: planes de respuesta documentados y actualizados que describan claramente los roles de la gestión del incidente a lo largo de todo su ciclo: desde la detección hasta la revisión y lecciones aprendidas.

2. Creación de un procedimiento de priorización y valoración de incidentes: cada alerta debe tener asignada una prioridad que permita priorizar las investigaciones a llevar a cabo por el equipo de trabajo. Las herramientas de Microsoft (Security Center) cuentan con una base de conocimiento y de indicadores de compromiso ("IOCs") que permite asignar una severidad a cada incidente.



3. Prueba de los procedimientos de respuesta ante incidentes de seguridad: es fundamental llevar a cabo ejercicios regulares para probar la respuesta de los equipos y su coordinación ante un incidente de seguridad, así como identificar puntos débiles y de mejora.

4. Listado de contactos ante incidentes de seguridad y configuración de notificaciones de alerta para que, en caso de producirse un incidente de seguridad, sea posible el contacto con las personas encargadas de su resolución.

5. Incorporación de alertas de seguridad en el sistema de respuesta ante incidentes: las alertas generadas dentro del entorno de Azure pueden ser exportadas para análisis por parte de los equipos de respuesta; en este sentido, idealmente se debe llevar a cabo una exportación y monitorización continua.

6. Automatización de la respuesta a las alertas de seguridad: Microsoft Azure permite definir características de automatización de los flujos de trabajo y respuesta mediante tareas de "Logic Apps", que desencadenan tareas automáticas para garantizar una rápida respuesta.

Con todo, Microsoft también propone diferentes casos de uso o playbooks de respuesta ante los incidentes más comunes, de manera que las organizaciones tengan la capacidad de parametrizar las tareas del playbook y, por tanto, automatizar la respuesta.

9 ANEXO II: CASOS DE USO

9.1 Casos concretos dependiendo del escenario en la nube

Microsoft ha publicado distintos casos de uso de respuesta a incidentes centrados en los incidentes más comunes:

- Suplantación de identidad (phishing).
- Difusión de contraseñas.
- Concesión de consentimiento de aplicación.
- Ransomware.
- Aplicaciones en peligro y malintencionadas.

Los diferentes playbooks pueden encontrarse aquí: https://docs.microsoft.com/es-es/security/compass/incident-response-playbooks

En el caso de la documentación publica sobre respuesta a incidentes de AWS y de Google, no se detallan los casos de uso. Sin embarfo, en Github (aws-incident-response-playbooks/playbooks at master · aws-samples/aws-incident-response-playbooks · GitHub) se pueden encontrar algunos casos de uso para la respuesta a incidentes en AWS que incluyen:

- Compromiso de credenciales.
- Acceso a datos.
- Denegación de servicio.
- Ransomware.

10 ANEXO III: LISTADO GENERAL DE ACCIONES

Estas son algunas de las acciones principales que se recomienda seguir para la resolución de un incidente de seguridad; su aplicabilidad dependerá de multitud de factores (ej.: tipología de negocio, arquitectura de los sistemas, alcance del incidente de seguridad, tipo de ataque…), se proporciona como una lista amplia para facilitar la comprensión de la gestión de situaciones de resolución de incidentes desde un punto de vista general, así como para orientar sobre las actividades que se pueden aplicar en caso de un incidente de seguridad:

#id	Fase / subfase	Descripción	Acción	Estado de la acción	Responsable
1	Identificación	Clasificación inicial del incidente	Asignación inicial de categoría al incidente según apartado 6.1 del documento		
2	Identificación	Clasificación inicial del incidente	Asignación de subcategoría de incidente		
3	Identificación	Identificación de activos afectados	Activos con afectación confirmada		
4	Identificación	Identificación de activos potencialmente afectables	Activos con probable afectación		
5	Identificación	Identificación de servicios afectados	Listado de servicios indisponibles o comprometidos		
6	Contención	Evaluación y decisión de desconexión/apagado de activos afectados	Solicitud de desconexión de red o apagado de activos afectados		
7	Contención	Activar comité de gestión del incidente	Activar reuniones de coordinación y personas involucradas		
8	Contención	Evaluar viabilidad de activación de planes de continuidad de negocio	Considerar el contexto para decidir si activar plan de continuidad		
9	Contención	Comunicación a responsables de servicio	Comunicación indisponibilidades a usuarios / partners / clientes		
10	Contención	Evaluación y decisión de apagado de activos con potencial afectación inmediata	Reducción superficie de ataque, preservación de evidencias forenses		
11	Contención	Restricción de accesos remotos (usuarios)	Reducción acceso remoto atacante		
12	Contención	Restricción de accesos remotos (proveedores y/o clientes)	Reducción riesgo para partners		
13	Contención	Evaluar restricción acceso a internet	En función de la severidad, cortar internet		
14	Contención	Evaluar restricción acceso a email corporativo	En función de la severidad, cortar email		
15	Contención	Reset de passwords de administradores	Reducción capacidad de movimiento lateral interno del atacante		
16	Contención	Activación MFA administradores, si no lo estaba	Aseguramiento de credenciales críticas para recuperación		
17	Contención	Reset de passwords de usuarios	Reducción capacidad de movimiento lateral interno del atacante		
18	Contención	Verificar y asegurar estado de backups offline	Asegurar capacidad de recuperación		
19	Contención	Parar procesos de backup online a partir de este momento	Asegurar capacidad de recuperación		
20	Contención	Apagado del sistema de backup	Asegurar capacidad de recuperación		
21	Contención	Extracción de logs para investigación forense	Análisis forense: Servidores, elementos de red, accesos remotos…		
22	Contención	Extracción de alarmas de seguridad para investigación forense	Análisis forense: Identidad de usuarios y accesos remotos		
23	Contención	Iniciar identificación de indicadores de compromiso	IPs, URLs, hashes de ficheros		
24	Contención	Rastrear indicadores de compromiso en activos	Búsqueda de posibles rastros de intrusión		
25	Contención	Revisión de servidores o equipos sin antivirus / EDR	Reducción capacidad de movimiento lateral interno del atacante		

#id	Fase / subfase	Descripción	Acción	Estado de la acción	Responsable
26	Contención	Revisión estado despliegue actualizaciones antivirus / EDR	Reducción capacidad de movimiento lateral interno del atacante		
27	Contención	Evaluación preliminar de activación de ciberseguro	Revisar coberturas y franquicias		
28	Contención	Determinar causa más probable de intrusión / infección	Reevaluar la clasificación del incidente (si procede)		
29	Contención	Enviar muestras de software malicioso a fabricantes de seguridad (Antivirus, Intrusion Prevention System, sandbox…) para obtención de firmas específicas	Prevención de infección de máquinas que aún no han sido alcanzadas por el ataque		
30	Contención	Despliegue de firmas de Antivirus / IPS específicas	En cuanto estén disponibles por parte del fabricante se actualizarán las firmas de seguridad		
31	Contención	Revisión de estado de parcheo de servidores y equipos	Determinar método más probable de intrusión o propagación		
32	Contención	Acciones derivadas de revisión de parcheo	Evaluar aplicabilidad de parcheo de emergencia en activos no comprometidos		
33	Contención	Identificar información posiblemente comprometida	Evaluación preliminar de posible afectación a activos con información sensible		
34	Contención	Recopilar información de vulnerabilidades de fuentes públicas sobre nuestros rangos de IPs expuestos	Identificación superficie de ataque pública: www.shodan.io		
35	Contención	Recopilar información de vulnerabilidades de nuestras herramientas de análisis interno	Identificación superficie de ataque: herramientas internas de análisis de vulnerabilidades		
36	Contención	Determinar posibles puntos débiles en servicios expuestos	Acciones de contención derivadas del análisis de vulnerabilidades externo e interno		
37	Contención	Actualizar estado de servicios afectados tras la contención	Informe interno de situación de servicios afectados		
38	Contención	Investigar posible acceso a datos sensibles (en base a activos afectados)	Determinar si ha habido extracción de datos sensibles		
39	Contención	Realizar informe preliminar del incidente	Elaboración del primer informe		
40	Contención	Comunicar internamente el informe	Distribuir según plan de gestión del incidente		
41	Contención	Comunicar externamente el incidente	Según proceda: Aseguradora, Autoridades, reguladores…		
42	Recuperación	Creación nuevas cuentas de administrador con MFA	Erradicación de persistencia		
43	Recuperación	Creación nuevas máquinas de administración	Erradicación de persistencia		
44	Recuperación	Reset de passwords de equipos de gestión de red	Erradicación de persistencia		
45	Recuperación	Obtener lista priorizada de recuperación de servicios	Erradicación de persistencia		
46	Recuperación	Creación de nuevas zonas de red separadas de las afectadas por el incidente	Segmentación (crear nuevos segmentos de red “limpios”) para reconstruir servicios comprometidos		

#id	Fase / subfase	Descripción	Acción	Estado de la acción	Responsable
47	Recuperación	Reinstalación Domain Controllers y DNS desde cero en máquinas nuevas (no reinstalar en máquinas comprometidas)	Reconstrucción de servicios básicos desde cero en máquinas y segmentos de red limpios		
48	Recuperación	Reemplazo progresivo de Domain Controllers y DNS	Revisar coberturas y franquicias		
(no reusar	Reconstrucción de servicios básicos desde cero en máquinas y segmentos de red limpios	Determinar causa más probable de intrusión / infección	Reevaluar la clasificación del incidente (si procede)		
49	Recuperación	Reinstalación de resto de activos desde cero según lista anterior (no reusar máquinas comprometidas o sospechosas de haberlo sido)	Reconstrucción de servicios desde cero en máquinas y segmentos de red limpios		
50	Recuperación	Asegurar y aumentar frecuencia de actualizaciones antivirus / EDR en servidores y endpoints	Mitigación de riesgo de persistencia del atacante		
51	Recuperación	Asegurar y aumentar frecuencia actualizaciones firmas en equipos de seguridad de red	Mitigación de riesgo de persistencia del atacante		
52	Recuperación	Asegurar actualizaciones de parcheado a últimas versiones de parches	Mitigación de riesgo de persistencia del atacante		
53	Recuperación	Asegurar hardening (configuración) servidores, endpoints	Mitigación de riesgo de persistencia del atacante		
54	Recuperación	Asegurar hardening (configuración) equipos de red	Mitigación de riesgo de persistencia del atacante		
55	Recuperación	Revisión y aseguramiento de resolución de causas raíz	Asegurar la recuperación y no reincidencia		
56	Recuperación	Restauración de datos (no sistema) desde backups en los activos afectados	Reconstrucción de servicios desde cero en máquinas y segmentos de red limpios		
57	Recuperación	Evaluar el restablecimiento de servicios restringidos	Mail, internet, accesos remotos		
58	Recuperación	Realización de informe del incidente	Actualización del informe		
59	Recuperación	Comunicación con autoridades (si procede)	Distribución según proceda		
60	Post-incidente	Realización y distribución de informe de lecciones aprendidas del incidente	Contenido: Línea de tiempo, afectación, impacto, exposición a futuros ataques, recomendaciones…		
61	Post-incidente	Actualización de playbooks de gestión de incidentes	Revisión de mejora de procedimientos de respuesta		
62	Post-incidente	Concovar sesión de lecciones aprendidas	Sesión para compartir conocimiento y aspectos de mejora. Ver apartado 6.4.2 del documento		

11 ANEXO IV: TAXONOMÍA

Taxonomía de Referencia para la Clasificación de Incidentes de Seguridad, desarrollada coordinadamente por un grupo internacional de equipos de respuesta a incidentes.

https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy

Tipo de Incidente	Ejemplos	Descripción
Contenido Abusivo	Pornografía Infantil, contenido sexual, violencia	Pornografía infantil, glorificación de la violencia, otros.
	Spam	Correo masivo no solicitado
	Difamación	Desacreditación o discriminación de alguien
Código Malicioso	Software malicioso, Virus, Gusanos, Troyanos, spyware, Dialler, rootkit, ransomware	Software de diferente tipo con propósito dañino.
Fuga de Información	Scanning	Ataques que envían solicitudes a un sistema para descubrir puntos débiles.
	Sniffing	Observar y registrar el tráfico de la red (escuchas telefónicas o redes de datos).
	Ingeniería Social	Recopilación de información de una manera no técnica (ej.: mediante mentiras, trucos, sobornos o amenazas a las personas).
Intentos de Intrusión	Intentos de acceso	Múltiples intentos de inicio de sesión (adivinar / descifrar contraseñas, fuerza bruta).
	Explotación de vulnerabilidades conocidas	Un intento de comprometer un sistema o interrumpir cualquier servicio explotando vulnerabilidades conocidas
	Nueva Firma de Ataque	Un intento de usar una vulnerabilidad explotable desconocida.
Intrusión	Compromiso de Cuenta Privilegiada	Un compromiso exitoso de un sistema o aplicación (servicio). Esto puede han sido causado de forma remota por una vulnerabilidad conocida o nueva, pero también por un acceso local no autorizado. También incluye ser parte de una red botnet.
	Compromiso de Cuenta sin privilegios	
	Compromiso de Aplicación, Bot	
Indisponibilidad	Ataque de denegación de servicio (DoS / DDoS)	Ataques o acciones no intencionadas de diferente tipo que provocan la indisponibilidad de los sistemas e información.
	Sabotaje	
	Interrupción no intencionada	
Acceso y/o modificaciones no autorizadas	Acceso no autorizado a la información	Ataques sobre los controles de accesos que pueden comprometer sistemas e información. También se incluyen los ataques que interceptan y acceden a información durante la transmisión (escuchas telefónicas, spoofing o secuestro) y el error humano / de configuración / software que afecten a la modificación no autorizada.
	Modificación no autorizada de la información	
Fraude	Phishing	Intentos con éxito o no para persuadir al usuario a revelar información privada (ej. credenciales)
	Derechos de Autor	Ofrecer o instalar copias de software comercial sin licencia u otro materiales protegidos por derechos de autor.
	Uso no autorizado de recursos	Usar recursos para fines no autorizados,
	Falsificación de registros o identidad	Tipo de ataques en los que una entidad asume ilegítimamente la identidad de otra
Vulnerabilidades	Sistemas y/o softwares vulnerables	Vulnerabilidades identificadas mediante software y sondas específicas
Otros	Todos los incidentes que no encajan en alguna de las otras categorías dadas	Si la cantidad de incidentes en esta categoría aumenta, es un indicador de que el esquema de clasificación debe ser revisado.
Test	Para pruebas	Pruebas de seguridad controladas e informadas

12 ANEXO V: GLOSARIO

A continuación, se definen los principales términos que aparecen en el contexto de este documento:

- BCP ("Business Continuity Plan" o "Plan de Continuidad del Negocio"): refiere al conjunto de políticas, análisis de riesgos, estrategias de mitigación, organización de los recursos y planes de pruebas de la organización para poder hacer frente a escenarios que provoquen interrupción de sus procesos de negocio. La norma ISO 22301 define el conjunto de buenas prácticas necesarias para desplegar un "Sistema de Gestión de Continuidad de Negocio".
- BIA ("Business Impact Analysis" o "Análisis de Impacto de Negocio"): herramienta clave en un BCP que permite identificar los principales riesgos asociados a procesos de negocio de una organización.
- CSF de NIST ("Cybersecurity Framework"): marco de seguridad promovido por la organización NIST que tiene como objetivo ayudar a empresas de todos los tamaños a comprender, gestionar y reducir los riesgos cibernéticos y proteger sus redes y datos.
- NIST ("National Institute of Standarization and Technology" o "Instituto Nacional de Estándares y Tecnología"): agencia adscrita al departamento de comercio de Estados Unidos que tiene como misión promover la innovación y competencia industrial; esta agencia está especializada en materia de ciberseguridad hasta el punto de que sus publicaciones se consideran estándares de referencia a nivel mundial, muy especialmente su marco de seguridad "CSF" y sus publicaciones ("Special Publications").
- RTO ("Recovery Time Objective" o "Tiempo Objetivo de Recuperación"): periodo máximo definido por la organización para recuperar sus procesos críticos, después de una afectación por alguna una contingencia.
- RPO ("Recovery Point Objective" u "Objetivo de Punto de Recuperación"): periodo máximo que se establece desde la última copia de seguridad y que considera la cantidad de datos que el negocio puede permitirse perder en caso de desastre.
- MTPD ("Maximum Tolerable Period of Disruption" o "Periodo Máximo Tolerable de Parada"): tiempo máximo tolerable de interrupción de un sistema o proceso para una organización.

- Usuario de servicios en la nube: persona u organización que solicita y utiliza los recursos de la nube. Junto a este, el proveedor de servicios en la nube representa la persona u organización que los entrega/presta. En ocasiones se utilizan los términos "cliente" y "consumidor" para hacer referencia al usuario de servicios en la nube o simplemente nube cuando hablamos del proveedor. NIST 500-292 usa el término "actor en la nube" y agrega roles para intermediarios en la nube, operadores y auditores. ISO/IEC 17788 utiliza los términos "servicio al cliente" en la nube, "socio de servicios" en la nube y "proveedor de servicios" en la nube.

- Middleware: el término se refiere al sistema de software que ofrece funciones y servicios de nube comunes para las aplicaciones, de modo que los desarrolladores y los equipos de operaciones puedan diseñarlas e implementarlas con mayor eficiencia, permitiendo conectar las aplicaciones, los datos y los usuarios.

- API: una API (Application Programming Interface) es una pieza de código que permite a diferentes aplicaciones comunicarse entre sí y compartir información y funcionalidades.

- Taxonomía: Clasificación u ordenación en grupos de objetos o sujetos que poseen unas características comunes.

Bibliografía

- Agencia Española de Protección de datos. (2018). Orientaciones para prestadores de servicios de cloud computing. https://www.aepd.es/es/documento/guia-cloud-prestadores.pdf
- Agencia Española de Protección de datos. (2018). Guía para clientes que contraten servicios de Computing. https://www.aepd.es/es/documento/guia-cloud-clientes.pdf
- Parlamento Europeo. (2022). La Directiva NIS2 Un alto nivel común de ciberseguridad en la UE. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333
- European Parliament. (2020). Legislative Train Schedule. https://www.europarl.europa.eu/legislative-train/schedule
- Normas ISO. https://www.iso.org/home.html
- PCI Security Standards Council, LLC. (2013). Normas de seguridad de datos de la industria de tarjetas de pago (PCI), versión 3.0. https://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisite/en/docs/PCI_DSS_v3.pdf
- CSA - Could Security Alliance. (2021). Cloud Incident Response Framework. https://cloudsecurityalliance.org/artifacts/cloud-incident-response-framework/
- NIST (2022). Information Technology Laboratory. https://csrc.nist.gov/
- ENISA - European Union for Cibersecurity. (2013). Incident Reporting for Cloud Computing. https://www.enisa.europa.eu/publications/incident-reporting-for-cloud-computing
- ENISA - European Union for Cibersecurity. (2020). EUCS – Cloud Services Scheme. https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme
- Amazon Web Services. (2022). AWS: Incident Response in the cloud. https://docs.aws.amazon.com/whitepapers/latest/aws-security-incident-response-guide/incident-response-in-the-cloud.html
- Microsoft Ignite. (2022) Incident response overview. https://docs.microsoft.com/en-us/security/compass/incident-response-overview
- INCIBE. (2020). Guía Nacional de notificación y Gestión de ciberincidentes https://www.incibe-cert.es/guias-y-estudios/guias/guia-nacional-notificacion-y-gestion-ciberincidentes
- CCN (2020). Guía de Seguridad de las TIC CCNSTIC 817. Esquema Nacional de Seguridad, Gestión de ciberincidentes. https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html
- AEPD (2021). Guía para la gestión y notificación de brechas de seguridad, AEPD e ISMS Forum https://www.aepd.es/sites/default/files/2019-09/guia-brechas-seguridad.pdf

Bibliografía

- ISMSFORUM. (2020). Guía Gestión de Planes de Continuidad de Negocio para PYMEs, ISMS Forum https://www.ismsforum.es/ficheros/descargas/gestion-de-planes-de-continuidad-de-negocio.pdf
- INCIBE. Plan de Contingencia y Continuidad de Negocio. https://www.incibe.es/protege-tu-empresa/que-te-interesa/plan-contingencia-continuidad-negocio
- CSA: Business Continuity and Disaster Recovery in the Cloud: https://cloudsecurityalliance.org/blog/2021/10/31/business-continuity-and-disaster-recovery-in-the-cloud/
- NIST: Draft - Evaluation of Cloud Computing Services Based on NIST 800-145: https://www.nist.gov/system/files/documents/2017/05/31/evaluation_of_cloud_computing_services_based_on_nist_800-145_20170427clean.pdf
- CSA: Disaster Recovery as a Service: https://cloudsecurityalliance.org/artifacts/disaster-recovery-as-a-service/
- NIST SP 800-184 – Guide for Cybersecurity Event Recovery: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf
- NIST – Cybersecurity Framework Five Functions - https://www.nist.gov/cyberframework/online-learning/five-functions
- Google, clases de almacenamiento: https://cloud.google.com/storage/docs/storage-classes
- Google, Guía de planificación para la recuperación ante desastres: https://cloud.google.com/architecture/dr-scenarios-planning-guide
- AWS, servicio de recuperación ante desastres de Amazon: https://aws.amazon.com/es/disaster-recovery/
- Microsoft, copia de seguridad y recuperación ante desastres: https://azure.microsoft.com/es-es/solutions/backup-and-disaster-recovery/
- https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf
- https://docs.microsoft.com/es-es/security/compass/incident-response-process
- Enrique Alcat, "Y ahora ¿qué?: claves para gestionar una crisis ¡y salir fortalecido ¡" Ed. Empresa Activa - ISBN 9788495787682

Antes, durante y después de ir a la Nube

Respuesta ante Incidentes

www.ismsforum.es
info@ismsforum.es
(+34) 915 63 50 62

@ISMSForum
ISMS Forum

Una iniciativa de

isms forum
CSA Spanish Chapter