Aruba Cloud

Gestión del riesgo para la seguridad de la información

ÍNDICE

1 TÉRMINOS Y DEFINICIONES

En este capítulo se recogen algunas definiciones que se consideran importantes para la representación del modelo de cálculo y gestión del riesgo para la seguridad de la información.

***BIA (Business Impact Analysis)*:**

Análisis de los impactos económicos, normativos y reputacionales para el negocio relacionados con la pérdida de confidencialidad, la integridad y la disponibilidad de la información relativa a un determinado proceso/servicio y a la interrupción del mismo.

Disponibilidad:

Garantizar que los sistemas de información y los datos requeridos estén disponibles para su uso cuando sean necesarios.

Gestión del riesgo para la seguridad de la información:

Conjunto de actividades y procesos de negocio destinados a identificar, medir, mitigar y monitorizar los riesgos relacionados con la pérdida de confidencialidad, la integridad y la disponibilidad (RID) de los datos y los servicios.

Impacto:

Consecuencias negativas para la empresa en caso de que existan una o más amenazas.

Incidente:

Un evento relacionado con la seguridad de la información que tiene una probabilidad significativa de comprometer las operaciones comerciales y/o suponer una amenaza para la seguridad de la información.

Integridad:

Entendida como la protección de los datos y de la información por la modificación del contenido, ya sea de forma accidental o voluntaria.

Amenaza:

La causa potencial (deliberada o accidental) de una avería que puede dañar un sistema o una organización que afecta a la **c**onfidencialidad, la **i**ntegridad y la **d**isponibilidad de la información.

Las amenazas pueden ser:

- De naturaleza «informática», que tienen un impacto negativo en la empresa mediante:
    - El uso del sistema de información o de sus componentes (por ejemplo: un ataque por parte de un hacker);
    - La realización de actividades de gestión del sistema de información (por ejemplo: daños causados por miembros del personal interno);

- De naturaleza «no informática», que tienen un impacto negativo en el sistema informático de la empresa mediante:
    - Impacto directo en la prestación de los servicios del sistema de información (por ejemplo: desastres naturales, interrupción de los servicios de soporte);
    - Efectos sobre las modalidades de gestión del sistema de información (por ejemplo, las modalidades de implementación de los procesos de TI).

Para caracterizar los riesgos asociados a cada amenaza es necesario conocer:

- Las vulnerabilidades de los componentes del sistema de información, es decir, a qué pueden afectar las amenazas;
- La exposición de los componentes a la amenaza, es decir, la facilidad con la que la amenaza puede afectar (por ejemplo, un servidor que expone un servicio web a los clientes está más expuesto a sufrir ciberataques);
- Los tipos de consecuencias, ya que algunas amenazas pueden derivar, a su vez, de otras amenazas (por ejemplo, el acceso no autorizado a un servidor web puede permitir a un intruso robar datos, pero también eliminarlos, modificarlos, llevar a cabo acciones fraudulentas, etc.).

Posibilidad o probabilidad de que ocurra:

La probabilidad de que ocurra una amenaza, la probabilidad de que una amenaza afecte a uno o más componentes de TI y cause un impacto negativo en la empresa en un período de tiempo determinado.

Riesgo para la seguridad de la información (en adelante, «riesgo»)

El producto entre la probabilidad de que ocurra una amenaza y el impacto en la empresa en relación con los activos involucrados en el análisis. Según el momento de la medición, el riesgo se clasifica en:

- Riesgo potencial o riesgo inherente (**rRp**)

  Representa el máximo riesgo al que está sujeto un determinado activo en términos de posibilidad de que exista una amenaza que pueda tener un impacto frente a la pérdida de confidencialidad, integridad o disponibilidad de la información. En el servicio de análisis, todos los componentes contribuyen a la determinación del riesgo inherente: procesos, aplicaciones, datos, infraestructura y, por supuesto, el factor humano.

  Es básicamente un valor que se calcula de forma diferente según las metodologías aplicadas y que se consigue sumando todas las posibles amenazas a las que se expone un activo, teniendo en cuenta las respectivas probabilidades de que ocurra y sus impactos.

  En otras palabras, es el riesgo al que puede estar expuesto un activo considerando simplemente su naturaleza y las amenazas asociadas a esta. Un ejemplo sería el caso de un ordenador expuesto en una red pública sin ninguna medida de protección.

- Riesgo residual o final (**rRf**):

  Representa el riesgo que se encuentra en un servicio tras la aplicación de contramedidas para determinar una reducción del riesgo inherente.

- Riesgo final aceptable (**rRfa**):

  Representa el máximo nivel de riesgo aceptable para la organización.

Todos los valores de riesgo indicados anteriormente deben considerarse dinámicos, ya que cambian con el tiempo, pues pueden verse influenciados, por ejemplo, por los siguientes elementos:

- Evolución de las amenazas;
- Modificación de los niveles de servicio solicitados;
- Cambio de las disposiciones legales o de los reglamentos de referencia;
- Modificaciones en la organización que pueden afectar a las debilidades o a la probabilidad de que existan amenazas o cambios en los impactos resultantes.
- Fortalecimiento o debilitamiento de las contramedidas de seguridad.

Riesgos básicos:

Se refiere a los riesgos informáticos que afectan a la seguridad de la información asociados con cada activo y cada escenario de riesgo.

Confidencialidad:

Se refiere a la protección de los datos y de la información para mitigar los riesgos asociados con el acceso o con el uso no autorizado a la información.

RPO (Recovery Point Objective):

La pérdida de datos aceptable se refiere al período máximo de tiempo que transcurre entre el último almacenamiento de datos de un proceso y la existencia del evento que causa la detención del proceso.

RTO (Recovery Time Objective):

Periodo de tiempo después de una avería en el que:

- Se debe retomar el producto o el servicio, o
- Se debe reanudar la actividad, o
- Se deben recuperar los recursos.

Escenario de riesgo:

Combinación de dos o más amenazas que permite la clasificación de las mismas.

Vulnerabilidad:

Debilidad intrínseca de un proceso, de un servicio o de un activo, que, en el caso de una o más amenazas, permite la violación de los objetivos de seguridad de la información (confidencialidad, integridad y disponibilidad). Algunos ejemplos son:

- Redes no segregadas;
- Uso de protocolos sin protección criptográfica;
- Sistemas operativos que no se actualizan con regularidad;
- Bases de datos con datos sensibles no cifrados;
- Virus no actualizados;
- Accesos físicos no supervisados;
- Ausencia de sistemas antiincendio automáticos;
- Insuficiencia de los sistemas de energía suplementaria;
- etc.

2 PRINCIPALES NORMAS DE REFERENCIA

Las principales normas adoptadas para garantizar la realización de las actividades con las mejores prácticas internacionales en el ámbito de la seguridad se describen en los párrafos siguientes.

2.1 Norma ISO/IEC 27001

La norma ISO/IEC 27001:2013 constituye, como norma internacional de seguridad, un verdadero modelo de referencia para la evaluación del nivel de seguridad de la información para analizar tanto los componentes tecnológicos como los organizativos que contribuyen a definir un sistema de gestión de la seguridad de la información (SGSI).
La norma define los requisitos de un SGSI y ayuda a identificar, gestionar y minimizar la variedad de amenazas a las que la información está sujeta normalmente. Esta norma también establece los controles de seguridad que deben adoptarse para proteger la información mediante la protección de las partes interesadas, incluidos los clientes de la organización.

2.2 Norma ISO/IEC 27002

La norma ISO/IEC 27002:2013 define las directrices y los principios generales para la implementación de un sistema de gestión de seguridad de la información adecuado dentro de una organización.

En particular, la norma ISO/IEC 27002:2013 constituye, como norma internacional de seguridad, un verdadero modelo de referencia para la evaluación de los aspectos organizativos, procedimentales, tecnológicos y normativos de la seguridad de un sistema de información, que tiene como objetivo:

- Realizar un examen crítico de los servicios y de las funciones de las que ya dispone o deberá disponer el sistema en cuestión;
- Identificar las vulnerabilidades del sistema;
- Indicar las acciones adecuadas para alcanzar el nivel de seguridad definido en los objetivos.

La norma ISO/IEC 27002 identifica los controles de seguridad a considerar por una organización, pero no reemplaza la actividad de análisis de riesgos propiamente dicha.

2.3 Norma ISO/IEC 27005

La norma ISO/IEC 27005 describe el proceso de gestión del riesgo en materia de seguridad de la información y las acciones asociadas, apoyando los principios generales descritos en la norma ISO/IEC 27001.
La norma, al igual que la ISO 31000, tiene como objetivo ayudar a las empresas a gestionar el riesgo de seguridad de la información de manera similar a la gestión de otros tipos de riesgos.
La figura 1 representa el esquema propuesto por la ISO/IEC 27005:11 relacionado con el proceso de gestión del riesgo en el que se inspira el modelo adoptado y desarrollado por el Grupo Aruba.

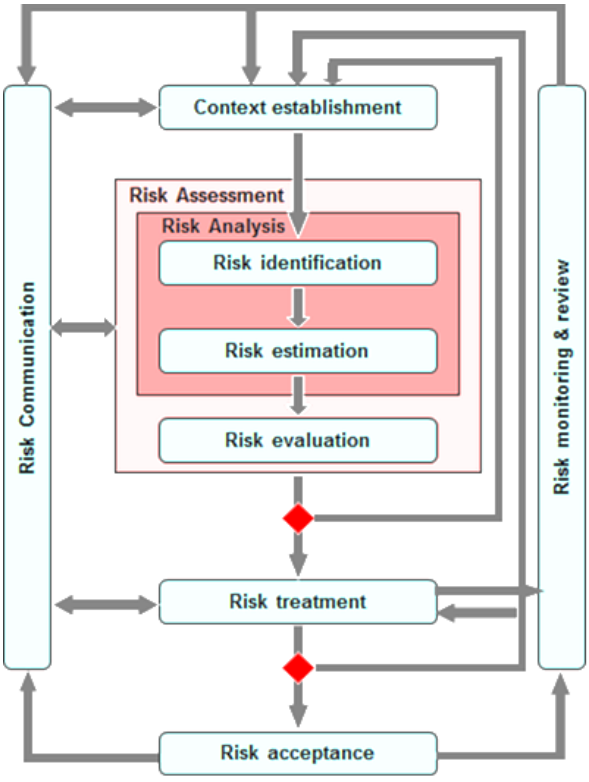

Figura 1 – ISO/IEC 27005: Proceso de gestión del riesgo

3 METODOLOGÍA DE GESTIÓN DE RIESGOS PARA GARANTIZAR LA SEGURIDAD DE LA INFORMACIÓN

Para el Grupo Aruba S.p.A, la información representa un patrimonio que se debe gestionar de forma estratégica para la tutela y el desarrollo del negocio empresarial.

En este contexto, se puede definir como riesgo informático cualquier evento incierto que pueda comprometer una o más de las siguientes tres propiedades principales del patrimonio informativo de la empresa:

- **C**onfidencialidad (acceso a los datos por personas);
- **I**ntegridad(los datos pueden sufrir modificaciones no autorizadas y resultar alterados);
- **D**isponibilidad (el sistema informático no se puede utilizar);

en función de los niveles de gravedad estrictamente dependientes del tipo de información afectada.

La evaluación del riesgo se realizará teniendo en cuenta los posibles impactos de tipo:

- económico;
- normativo;
- reputacional.

La gestión de riesgos de seguridad de la información es un proceso que permite evaluar las interrelaciones entre los activos, las amenazas y las vulnerabilidades que afectan a una organización determinada. Este proceso analítico tiene como objetivo identificar los riesgos asociados con las vulnerabilidades y las amenazas detectadas en los activos y proporcionar la base para establecer un programa de seguridad eficiente.

Las categorías de riesgo identificadas deben estar en consonancia con los tipos aplicables al contexto. Por tanto, los riesgos identificados pueden derivarse de amenazas internas como externas o ambientales, de actos deliberados y de la gestión de la organización inadecuada o negligencia de esta.

El valor del riesgo se entiende como una función del valor de los activos, el valor de las amenazas y de las vulnerabilidades.

Los resultados del análisis de riesgos se documentan e incluyen:

- La clara identificación de los riesgos fundamentales;
- La evaluación del posible impacto de los riesgos identificados en el negocio;
- Un plan de acciones recomendadas para reducir los riesgos hasta un nivel aceptable.

El Grupo Aruba establece un modelo de análisis de tipo cualitativo, ya que es capaz de proporcionar a corto plazo un alto grado de conciencia sobre los mayores riesgos TIC que afectan al entorno tecnológico de referencia.

La metodología adoptada es:

- Utilizada por el Grupo para estimar el valor de la información en los procesos pertinentes y el nivel de riesgo al que está sometida, para poder identificar las medidas de protección adecuadas;
- Aplicable también en el caso de desarrollo de nuevas soluciones de infraestructura o aplicaciones que afectan a la seguridad de los datos tratados. En este caso, la metodología permite evaluar la criticidad de los datos y las amenazas a las que están sometidos para permitir que las personas responsables del análisis de los riesgos implementen las medidas de protección pertinentes en los procesos de desarrollo y adquisición de los sistemas informáticos y reducir así las vulnerabilidades al mínimo.

La evaluación de riesgos y el análisis de las correlaciones entre activos, amenazas y contramedidas se lleva a cabo con el apoyo de una herramienta desarrollada internamente que contiene la información recopilada durante reuniones específicas con las personas involucradas en los procesos objeto de análisis.
La metodología utilizada permite crear un modelo de negocio donde se describen todos los elementos básicos necesarios para el análisis posterior, sus características, su estructura jerárquica y sus conexiones.

4 PROCESO DE GESTIÓN DE RIESGOS

A continuación se describen las principales fases del modelo de análisis para la gestión de los riesgos relacionados con la seguridad de la información adoptado y aplicado por el Grupo Aruba S.p.A.

4.1 FASE 1 – Identificación del contexto

La definición del contexto de análisis prevé la modelización de la realidad empresarial y la identificación de los principales servicios de negocio, procesos, macroprocesos y activos involucrados.

Para la identificación de los recursos, tal como sugiere la norma ISO/IEC 27005 «Information technology – Security techniques – Information security risk management», se identifican dos tipos distintos:

- **Recursos primarios** – información, procesos, macroprocesos y servicios de negocio;
- **Recursos secundarios o activos** – hardware, software, personal, red de trabajo, ubicación y organización.

4.1.1 Identificación de los servicios, procesos y macroprocesos

Para la identificación de los servicios y de los procesos de la Organización se toman como referencia inicial las estructuras organizativas publicadas y puestas a disposición a través del instrumento de comunicación empresarial interno.
Posteriormente, los procesos individuales, que contribuyen a la prestación de servicios, se agrupan en macroprocesos específicos según el contexto analizado.

4.1.2 Identificación de activos

Para garantizar la identificación precisa de los activos, se siguen los siguientes pasos:

1. **Identificación de las categorías** de los activos de información (por ejemplo, hardware, software, ubicación, etc.), de acuerdo con la clasificación establecida en la norma ISO/IEC 27005;
2. **Ponderación de las categorías** de los activos de información según la estrategia de seguridad de la empresa y los requisitos comerciales, legales y contractuales;
3. **Identificación de las dependencias** entre las categorías de activos censuradas.

4.1.3 Vínculo parental entre macroprocesos y activos

Una vez identificados los activos, se han definido las dependencias entre los mismos y los macroprocesos.

Estas dependencias permiten asociar a cada categoría de activos los valores de impacto RID (determinados mediante las entrevistas de BIA), que permiten calcular los riesgos informáticos básicos asociados a cada activo.

4.2 FASE 2 – Análisis de riesgos

4.2.1 Evaluación del impacto

La evaluación del impacto (Business Impact Analysis) se realiza según la metodología adoptada, además de por las principales normas internacionales (ISO 27005, ISO 22301), por los referentes de negocio
A través de una herramienta desarrollada internamente para la recopilación de información, los responsables de los departamentos de la empresa evalúan, durante la entrevista de BIA, la pérdida de confidencialidad, integridad y disponibilidad de la información administrada dentro de su área de competencia en términos de impacto económico, regulatorio y reputacional, según escalas de evaluación bien definidas.

Los procesos individuales, tal y como se especifica en la FASE 1, se agrupan en macroprocesos específicos según el contexto analizado. El impacto asociado estos macroprocesos se calcula como el *«peor caso»* del impacto individual de los procesos que los componen.

4.2.2 Identificación y valorización de los activos

La identificación de los activos es la base de partida sin la cual no es posible proceder a una gestión de la seguridad empresarial eficaz y adecuada. De hecho, el inventario es el punto de partida para la clasificación de los activos de la empresa y para el análisis del nivel de riesgo al que están sometidos.

El objetivo de esta fase operativa es garantizar la elaboración, o la formalización en virtud de metodologías ya existentes, del inventario de los activos informativos, considerados por la empresa como «misión crítica» con el fin de alcanzar sus objetivos de negocio, respetar las obligaciones contractuales y, por último, respetar las normas y la legislación a las que sus actividades estén sujetas.
El valor central de un activo suele estar representado por la información (o los datos) que el sistema trata, y relega la tarea a los otros activos para procesarlos o protegerlos.

En esta lógica, el valor se asigna, en la fase de entrevista de BIA, para cada activo y para cada una de las dimensiones RID (confidencialidad, integridad y disponibilidad) de seguridad aplicables al contexto.

Aprovechando la información recopilada durante las entrevistas de BIA, es posible asociar a cada activo el impacto derivado de los macroprocesos en los que se utilizan.

4.2.3 Análisis de amenazas y evaluación de la probabilidad de que ocurran

La metodología utilizada en el proceso de gestión de riesgos de seguridad de la información define una etapa clave para identificar las amenazas que afectan a los activos del perímetro. Las amenazas representan todos aquellos elementos o eventos que pueden dañar un activo.
El objetivo de esta actividad es identificar las amenazas y las vulnerabilidades que afectan los activos identificados recibidas dentro del proceso de análisis y gestión de riesgos y evaluar la probabilidad de que estas ocurran.
Para garantizar la exhaustividad de la lista de amenazas, se toma como referencia la lista de amenazas de la norma ISO/IEC 27005, a la que se añaden las consideraciones producidas y publicadas por ENISA después de llevar a cabo estudios en la materia.
Las amenazas individuales se agrupan posteriormente en escenarios de riesgo realistas según el contexto analizado.

4.2.4 Análisis de las contramedidas

El objetivo de esta actividad es identificar las contramedidas que se consideran necesarias para cubrir los escenarios de riesgo en función de los activos identificados en el paso anterior.
Para garantizar la exhaustividad de la lista, el Grupo Aruba S.p.A adopta una lista de contramedidas basada en las mejores prácticas estalecidas en el Anexo A de la norma ISO/IEC 27001:2013. Las evaluaciones, dependiendo del tipo de servicio analizado, pueden enriquecerse con temas específicos mediante el análisis de controles adicionales sugeridos por fuentes autorizadas, como ENISA, AgID, NIST, etc.
Una vez definida la lista de controles de seguridad, estos se asignan a los escenarios de riesgo sobre los que actuar para reducir la probabilidad de que ocurran las amenazas que los componen o su impacto.
Las contramedidas se han dividido en:

- **Reactivas** (r), destinadas a reducir el impacto;
- **Preventivas** (p), destinadas a reducir la probabilidad de que ocurran.

4.3 FASE 3 – Evaluación del riesgo

4.3.1 Metodología y modelo del riesgo

El valor del riesgo se entiende como una función$R = f(A, M, V)$, con A el valor de los activos pertinentes, M el valor de las amenazas y V las vulnerabilidades.
En la FASE 2, referida al proceso de gestión de riesgos para la seguridad de la información, se definió el modelo de riesgo (*Threat Modeling*). Este último es un proceso que pretende identificar posibles amenazas y vulnerabilidades,

evaluar la probabilidad de que ocurran, priorizarlas y reducir el riesgo de que se den implementando contramedidas adecuadas.

Una vez definido el contexto básico, el proceso de *Threat Modeling* consiste en:

- Hacer una lista de las posibilidades de ataque/vulnerabilidad que contemplan las formas en las que se puede comprometer la confidencialidad, la integridad y la disponibilidad de los datos;
- Evaluar cuáles son los ataques/vulnerabilidades más probables, descartar los improbables o casi imposibles de evitar, y para el resto de casos, aplicar controles, es decir, contramedidas, que pueden ser técnicas o de procedimiento.

4.3.2 Requisitos de seguridad aplicables y nivel de conformidad

Tras identificar los requisitos de seguridad aplicables en el ámbito del análisis (ver párr. «Análisis de contramedidas»), se lleva a cabo una evaluación del nivel de cobertura de los requisitos relativos a los 14 ámbitos identificados en el Anexo A de la norma ISO/IEC 27001:2013.

El grado de conformidad de cada contramedida se expresa según una escala de valores bien definida que va de 0, en caso de que no exista ninguna contramedida, a 4, en casos de contramedidas completamente implementadas.

Para analizar el nivel de conformidad de los controles establecidos el Anexo A de la Norma ISO/IEC 27001:2013, se utiliza la información y las evidencias recogidas gracias a actividades específicas de evaluación realizadas internamente.

4.3.3 Cálculo de los riesgos básicos inherentes y residuales

Durante esta fase, se calcula el valor de los riesgos básicos de seguridad RID inherentes y residuales (AS-IS, Planificados y TO-BE) asociados al servicio en análisis.

El cálculo de los riesgos elementales inherentes para cada activo y para cada escenario, asociado según las lógicas descritas anteriormente, se efectúa considerando la probabilidad de que se den los escenarios de riesgo individuales y el impacto potencial que los mismos podrían comportar.

Una vez determinados los riesgos inherentes, para obtener los riesgos residuales (AS-IS, Planificado y TO-BE), se tienen en cuenta los valores asociados, en la fase de auditoría interna, a las contramedidas de seguridad necesarias para contrarrestar los escenarios de riesgo identificados, tanto en términos de reducción de la probabilidad de que ocurran las amenazas que los componen como en términos de reducción del impacto.

4.4 FASE 4 – Tratamiento del riesgo

4.4.1 Análisis del riesgo asumido

El riesgo asumido es uno de los conceptos que cabe abordar en relación con la gestión de riesgos. Con este término se indican de manera genérica aquellos riesgos que, por alguna razón, no es conveniente o posible tratar y que simplemente se aceptan.

Por tanto, el objetivo de esta actividad es definir un criterio según el cual se puedan aceptar los pares de amenaza y activos que implican un riesgo menor. Así, más allá de casos concretos, se define un umbral por debajo del cual un cierto riesgo se considera simplemente un coste y, por lo tanto, no se trata.

4.4.2 Resultado del análisis: riesgo residual AS-IS

El trabajo de análisis del riesgo y la evaluación del mismo teniendo en cuenta las contramedidas aplicadas (riesgo residual) se lleva a cabo realizando las siguientes actividades:

- Evaluación de los controles de seguridad con respecto a las mejores prácticas identificadas en el Anexo A de la norma ISO/IEC 27001:2013;
- Análisis de impacto frente a l pérdida de disponibilidad, confidencialidad e integridad de la información para los servicios relacionados;
- Análisis de las vulnerabilidades y las amenazas para los activos;
- Evaluación del riesgo as-is de la seguridad de la información e identificación de una escala de prioridades.

4.4.3 Análisis de lagunas y selección de contramedidas a implementar

Después del trabajo de análisis realizado, para abordar cualquier riesgo/problema relevante en el contexto de los servicios prestados por el Grupo Aruba S.p.A y/o para perseguir la mejora continua del SGSI, se procesan los datos obtenidos en los análisis realizados en la herramienta de análisis de riesgos para identificar las áreas de riesgo para las que se requiere la identificación de intervenciones de seguridad adecuadas.

Por tanto, para identificar acciones de mejora y reducir los riesgos, se define, de vez en cuando, un análisis de lagunas destinado a evaluar la distancia entre el nivel de aplicación actual de las contramedidas de seguridad y el nivel máximo aplicable.

4.4.4 Plan de tratamiento del riesgo - racionalización de las intervenciones

Las acciones identificadas en el análisis de lagunas se agrupan según las iniciativas proyectuales específicas y se documentan dentro del plan de tratamiento de riesgos.

5 FRECUENCIA DE ANÁLISIS

El proceso de gestión de riesgos para garantizar la seguridad de la información debe llevarse a cabo cada 12 meses, o antes en el caso de eventos significativos, como, por ejemplo, pero no limitado a:

- Nuevos activos que pasan a formar parte del ámbito de gestión de riesgos;
- Nuevas amenazas presentes tanto fuera como dentro de la organización y que no han sido evaluadas;
- Posibilidad de que existan amenazas que afecten a nuevas o crecientes vulnerabilidades;
- Revisión de vulnerabilidades ya identificadas para determinar cuáles podrían estar más expuestas a amenazas nuevas o reemergentes.

- Aumento del impacto o de las consecuencias de las amenazas sobre los activos, las vulnerabilidades y los riesgos que, en conjunto, resultan en un nivel general de riesgo inaceptable.
- Averías de seguridad especialmente graves.

Además, se pueden llevar a cabo actividades de análisis con diferentes frecuencias, por ejemplo, según determinadas normas o requisitos de certificación.

Aruba S.p.A.
Via San Clemente 53 - 24036 Ponte San Pietro (BG) – CIF: 01573850516
https://www.arubacloud.com - https://www.arubacloud.fr - https://www.arubacloud.es