Unidad 10: La transferencia del riesgo

BLOQUE III – La gestión del ciberriesgo como un proceso

Grado en Ingeniería de la Ciberseguridad, curso 2022-2023

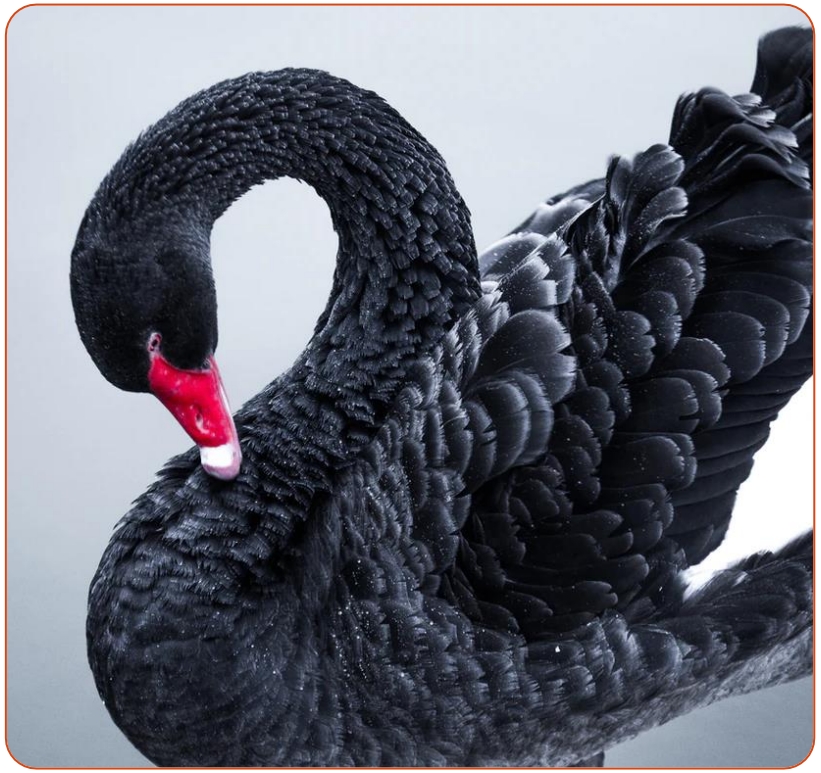
CONTENIDOS

1. El concepto de cisne negro.
2. SLAs y contratos.
3. La ciberpóliza.

1. El concepto de cisne negro

- Ya lo hemos hablado en unidades anteriores, nos referimos con este término a incidentes que ocurren con baja probabilidad pero que podrían tener un impacto alto.

- Con estos riesgos se suele optar por una estrategia de transferencia. Pero hay que mitigar todo lo que sea posible antes….



2. SLAs y contratos

- Una primera forma de transferir el riesgo consiste en subcontratar o externalizar ciertos aspectos de funcionamiento de la organización.
- La ventaja es doble:
  - Se puede recurrir a una organización o persona experta que aporte valor, de manera que nuestra organización se centre en lo que sabe hacer bien.
  - Implica transferir ciertos riesgos.

2. SLAs y contratos

- Esto es típico en algunos escenarios:
  - Se externaliza toda la función TIC.
  - Se externaliza el CISO o el SOC.
  - Se recurre a proveedores cloud de IaaS, PaaS o SaaS.
- Cuidado, externalizar no implica despreocuparse.
- Suelen ser modelos de responsabilidad compartida.

2. SLAs y contratos

- La gestión de esta responsabilidad compartida se realiza mediante la firma de SLAs, contratos y acuerdos de ese tipo.
- Los aspectos relativos a gobernanza, gestión del riesgo, seguridad, privacidad, etc. deben estar reflejados de manera precisa, explícita y exhaustiva.
  - Es conveniente recurrir a expertos técnicos y legales.

2. SLAs y contratos

- Un SLA (Service Level Agreement) no es más que un documento que define la relación entre dos partes: el proveedor de un servicio y su cliente.
- Si se elabora correctamente, debería identificar y definir las necesidades del cliente, proporcionar un marco para la comprensión mutua, simplificar los aspectos complejos, reducir las zonas de conflicto, fomentar el diálogo en el caso de que estos conflictos surjan y eliminar las expectativas poco realistas.
- Por desgracia en la mayoría de las áreas no existen formatos estándar para su definición.

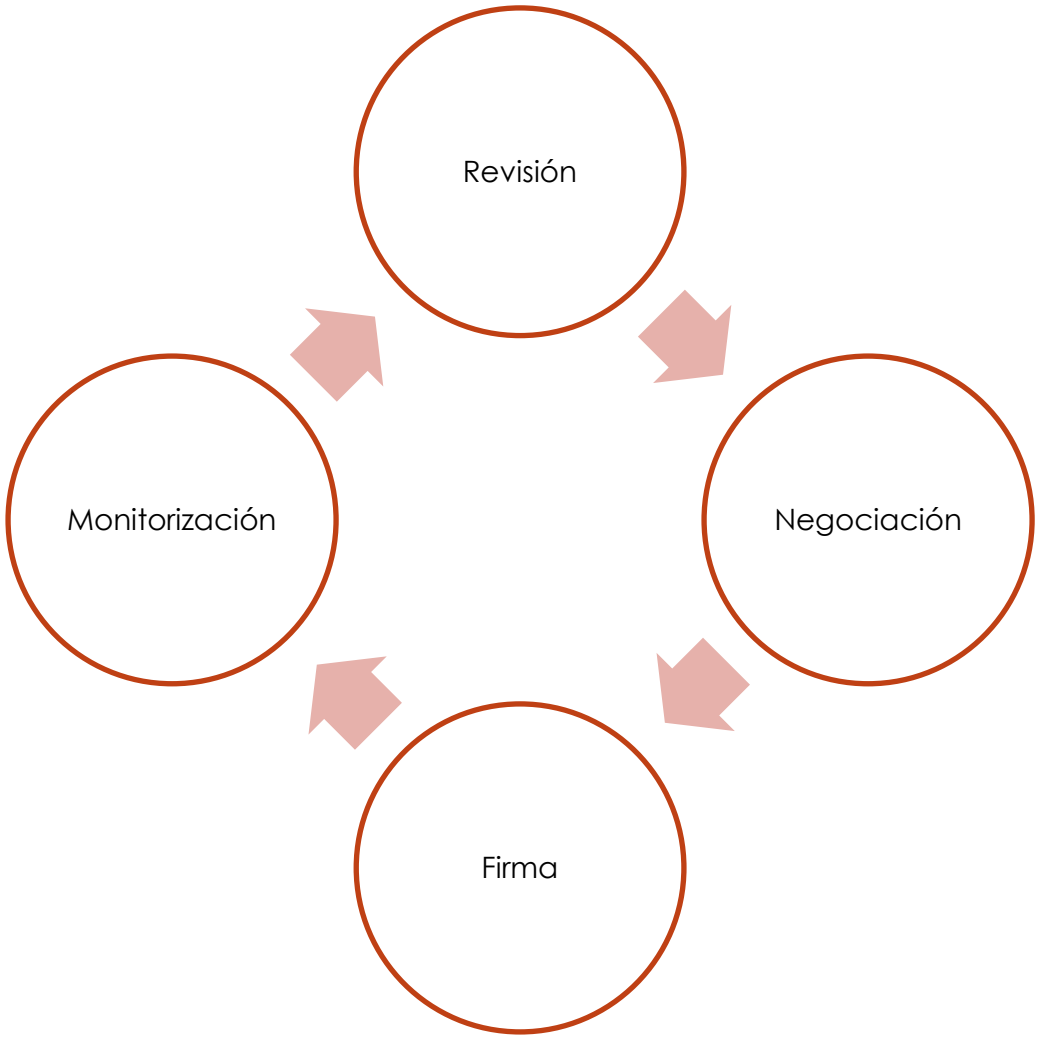
2. SLAs y contratos

- Por ello puede ser muy útil tener en cuenta ITIL, que es una guía de buenas prácticas orientada a la gestión de servicios de TI y a la gobernanza, aunque su campo de aplicación se extiende también a otro tipo de servicios.
  - Puede ser utilizada por y desde los directores de los departamentos de TI y CIOs (Chief Information Officers) hasta los técnicos de apoyo y administradores.
- Y se puede aplicar a todo tipo de proveedores de servicios que proporcionen estos servicios TI a clientes externos.
  - Es el estándar de facto actual para la definición de SLAs.

2. SLAs y contratos

Cumplimiento

Indicadores



Reclamaciones

Soporte

Responsabilidades

3. La ciberpóliza

- La otra forma tradicional de transferencia tiene que ver con la contratación de una póliza de seguros.
- Es algo tradicional en otras áreas, pero relativamente novedoso en los entornos ciber.
  - Todavía evolucionando, el mercado es complejo.

3. La ciberpóliza

Motivos por los que no se contrata en algunas organizaciones

- Falsa sensación de seguridad.
- Confiar en la mitigación como única estrategia.
- Desconocimiento de la ciberpóliza.
- Desconfianza del seguro.
- Creencia de estar cubiertos por otros seguros.
- Análisis coste-beneficio por pago de prima.

3. La ciberpóliza

Eventos que activan una ciberpóliza y sus coberturas

- Eventos relacionados con la privacidad de la información
- Eventos relacionados con la seguridad de la información o de las operaciones
- Eventos relacionados con los fallos de sistemas
- Eventos relacionados con daños causados a la reputación corporativa

3. La ciberpóliza

La ciberpóliza combina coberturas por responsabilidad civil y daños propios e incluyen coberturas ante tres grandes costes/pérdidas

Costes/pérdidas por gastos de primera respuesta, de contención del incidente y de gestión de crisis	Costes/pérdidas de reclamaciones por daños y perjuicios, multas, sanciones y gastos de defensa y consecuencias financieras ante autoridades y/o terceros	Costes/pérdidas de ingresos por interrupción del negocio, por gastos operativos durante el incidente para minimizarlo y por gastos de restauración de sistemas

3. La ciberpóliza

Las ciberpólizas suelen contemplar exclusiones:

- Actos dolosos
- Hechos conocidos
- Falta de mantenimiento tecnológico
- Daños materiales y personales
- Coberturas de las pólizas de responsabilidad civil
- Infracción de secretos comerciales o patentes
- Compensaciones por actos de *trading*
- Actos de guerra y terrorismo

3. La ciberpóliza

- **Ciberriesgo afirmativo:** aquel que está cubierto de forma explícita por una ciberpóliza.

- **Ciber-riesgo no afirmativo (ciberriesgo silencioso):** aquel que no está ni explícitamente incluido ni excluido de las pólizas tradicionales, como las de daños, responsabilidad, transportes, etc.

El 10 de noviembre de 2003 se incluyen estas cláusulas que excluían las pérdidas causadas por un incidente de ciberseguridad sobre datos electrónicos o sobre, en general, activos de la organización relacionados con sistemas de información.

- Pólizas de transporte marítimo - *Cyber Attack Exclusion Clause – Cl . 380* o cláusula 380
- Pólizas de daños - *NMA 2914/2915.*

Actualmente se está procediendo a realizar un "write-back"

https://www.infosecurity-magazine.com/opinions/cyberwar-exclusion-cyber-insurance/

16 FEB 2022 OPINION

Cyber-War Exclusion Clauses in Cyber Insurance

Peter Groucutt Managing Director at Databarracks
Follow @databarracks

Lloyd's of London has released four new Cyber War and Cyber Operation Exclusion Clauses. Insurers have been quickly adapting to the rapidly changing cyber landscape. What was initially a very profitable line of business quickly became unsustainable as attacks and claims increased. The industry responded in several ways: reducing coverage, raising prices and increasing requirements for cover. These exclusion clauses are the next step for the industry trying to balance exposure and demand.

The process of attributing a ransomware attack to a perpetrator remains murky, but the new exclusions mean business leaders can no longer rely on insurance companies to bail them out. They must take control of ransomware situations themselves.

Mondelez vs. Zurich

Insurance exclusions for acts of war are common. There are, however, some difficulties in applying these exclusions in the cyber world.

In 2017, NotPetya was aimed (not very carefully) at Ukraine, but it had a massive impact on companies worldwide. Mondelez was hit and claimed on its insurance. Its insurer Zurich refused to payout based on the "war exclusion" clause in its policies.

This is now a legal battle between Mondelez and Zurich. The central issue is whether NotPetya qualified as an act of war.

The new clauses from Lloyd's favor the insurers with broader definitions of cyber activities that can be excluded from coverage.

An Act of War or Just 'Cyber Operations'?

There is a lot going on between nation-states that doesn't qualify as "war." We are not quite in a cyber-cold war, but there's undoubtedly a cold-skirmish or two happening and plenty of cold-jostling. Occasionally, that spills over and affects organizations who want to claim their cyber

Related to This Story

#BHEU: 5 Ways to Approach Ransomwa
70% of Cyber Pros Believe Cyber Insura Exacerbating Ransomware
Uncomplicated Cyber Insurance Progra
Ransomware Hits Over a Quarter of UK
Nation-States Have Right to Hack Back,

What's Hot on Infosecurity Maga

https://www.euronews.com/2021/05/07/cybercrime-insurance-giant-axa-to-stop-covering-ransomwa

euronews. My Europe World Business Sport Green Next Travel Culture Video Programmes

FRANCE

Cybercrime: Insurance giant Axa to stop covering ransomware payments in France

COMMENTS

By Euronews with AP • Updated: 07/05/2021

A Toyota Hybrid during a test for hackers at the Cybersecurity Conference in Lille, northern France, Wednesday Jan. 29, 2020 - Copyright Michel Spingler/AP

SHARE THIS ARTICLE

One of Europe's top five insurers has said it will stop reimbursing people in France who pay up after being targeted by cybercriminals with ransomware.

The global insurance company said on Thursday that it will stop writing cyber-insurance policies that cover customers for extortion payments to ransomware attackers.

Ransomware attacks see criminals break into computer networks, seeding malware and scrambling data. Only after ransoms - often huge sums - are paid do the perpetrators provide software keys to decode it.

As of last year, some ransomware attackers also began stealing sensitive data before encrypting networks and threatening to dump it online unless victims paid up.

This helped drive ransom payments up nearly threefold to an average of around €250,000. The

3. La ciberpóliza

- Punto de partida para contratar una ciberpóliza:
  - Formularios de las aseguradoras.
  - Benchmarking.
  - Análisis de riesgos.
- Todo esto ayuda a fijar las coberturas, límites y sublímites y a analizar las franquicias, periodos de carencia, etc.

Para leer e investigar…

- "Understanding Cyber Insurance - A Structured Dialogue with Insurance Companies". EIOPA (2018).
- "Encouraging Clarity in Cyber Insurance Coverage: THE ROLE OF PUBLIC POLICY AND REGULATION" OECD (2020).

Referencias

- Fotografías
  - https://unsplash.com
- Iconos
  - https://www.flaticon.es/