Obraz zawierający mapa

Opis wygenerowany automatycznie**LECTURAS**

1. Cibersegurança
2. Princípios de estabelecimento da ciber-segurança
3. Equipa de segurança (tarefas, papéis, processos, etc.)
4. Equipas CERT e CSIRT (estrutura, hierarquia)
5. Ancoragem legal das equipas CERT e CSIRT (direitos e obrigações)
6. Direitos e obrigações das equipas de segurança
7. Tratamento de incidentes (IH)
8. Análise de fonte aberta dentro da IH
9. Possibilidades de transferência de dados e informações

**WORKSHOPS**

1. Análise da necessidade de criar uma equipa de segurança na organização
2. Definição de activos individuais e análise SWOT contra eles
3. Criação e integração de uma equipa de segurança na organização - adopção de regras e políticas
4. Simulação de um incidente ou evento cibernético contra uma organização
5. Tratamento de incidentes
6. Análise das medidas tomadas
7. Partilha de informação com outras entidades

Conteúdos

[1. Introdução 5](#_Toc74220868)

[1.1 Ciber-segurança 6](#_Toc74220869)

[1.2 Princípios de ciber-segurança 9](#_Toc74220870)

[1.2.1 A Tríade da CIA 10](#_Toc74220871)

[1.2.2 Elementos de ciber-segurança 19](#_Toc74220872)

[1.2.3 Ciclo de vida da ciber-segurança 24](#_Toc74220873)

[1.3 Risco, activo, vulnerabilidade 30](#_Toc74220875)

[1.3.1 Risco 30](#_Toc74220876)

[1.3.2 Bens 33](#_Toc74220877)

[1.3.3 Vulnerabilidade 33](#_Toc74220878)

[1.4 Ameaças cibernéticas, eventos, incidentes e ataques 34](#_Toc74220879)

[1.4.1 Ameaça cibernética 34](#_Toc74220880)

[1.4.2 Evento de ciber-segurança 40](#_Toc74220881)

[1.4.3 Incidente cibernético (segurança) 41](#_Toc74220882)

[1.4.4 Cyberattack 42](#_Toc74220883)

[1.4.5 Cibercriminalidade 42](#_Toc74220884)

[2 Equipas CERT/CSIRT 46](#_Toc74220885)

[2.1 História 46](#_Toc74220886)

[2.2 Equipas CERT e CSIRT 46](#_Toc74220887)

[2.3 Como é formada uma equipa CERT/CSIRT 48](#_Toc74220888)

[2.4 Cooperação em infra-estruturas CERT/CSIRT 49](#_Toc74220889)

[2.5 Hierarquia das equipas CERT/CSIRT? 51](#_Toc74220890)

[2.6 Equipas nacionais e governamentais CERT/CSIRT 51](#_Toc74220891)

[2.7 Situação na República Checa e no mundo 52](#_Toc74220892)

[2.8 CSIRT Nacional da República Checa 53](#_Toc74220893)

[2.9 CERT do Governo da República Checa 53](#_Toc74220894)

[2.10 Qual a equipa CERT/CSIRT a contactar? 54](#_Toc74220895)

[3. Quadro legislativo do CSIRT/CERT 58](#_Toc74220896)

[3.1 República Checa 60](#_Toc74220898)

[3.1.1 CERT nacional 60](#_Toc74220899)

[3.1.2 CERT do Governo 69](#_Toc74220900)

[3.2 Polónia 73](#_Toc74220901)

[3.3 Portugal 73](#_Toc74220902)

[4. Conclusão 76](#_Toc74220903)

[5. Referências 77](#_Toc74220904)

## Introdução

A informação e os dados representam um potencial económico e político considerável. A informação, como dados em bruto e fluxo de dados, pode determinar não só a existência ou não existência de um indivíduo ou empresa, mas também, pela sua natureza, influenciar o desenvolvimento global. [[1]](#footnote-1)

Precisamos de compreender que quanto mais dependemos das tecnologias de informação e comunicação[[2]](#footnote-2) , e quanto mais dados estas tecnologias recolhem e partilham sobre nós, mais vulneráveis nos tornamos.

Muitas das consequências causadas por ciberataques, imprudência humana ou ignorância podem ser evitadas se os princípios básicos da ciber-segurança forem seguidos. [[3]](#footnote-3)

A ciber-segurança é, na sua essência, um processo em constante evolução e mudança que depende de uma série de variáveis. É claro que estas variáveis podem ser dados ou os próprios elementos das TIC, que são objecto de protecção, processos definidos à medida e as suas revisões, etc. No entanto, o elemento mais importante é o utilizador (seja utilizador final ou administrador) que aplica os elementos de ciber-segurança.

É aqui que encontrará esse obstáculo teórico, ou seja, onde lhe serão dadas as informações, instruções e procedimentos que adoptámos e testamos de boa fé. O que aqui será apresentado é a nossa opinião sobre a questão da ciber-segurança e os processos a ela associados. Estas instruções, procedimentos e recomendações funcionam para nós, mas podem não funcionar para si porque, na implementação efectiva de quaisquer procedimentos de segurança, é bom basear-se em certas recomendações comprovadas, mas acima de tudo é benéfico adaptar, modificar ou alterar estes procedimentos em função das condições específicas quer do utilizador individual quer da organização.

A Directiva da UE sobre Segurança das Redes e da Informação (Directiva NIS) visa criar uma Rede CSIRT "para contribuir para o desenvolvimento da confiança entre os Estados-Membros e para promover uma cooperação operacional rápida e eficaz". [1] A Directiva estabelece que cada Estado-Membro designará um ou mais CSIRT que devem cumprir os requisitos estabelecidos no ponto (1) do Anexo I (requisitos) da Directiva, abrangendo pelo menos os sectores referidos no Anexo II e os serviços referidos no Anexo III, responsáveis pela gestão de riscos e incidentes, de acordo com um processo bem definido. A Directiva prevê requisitos de alto nível que os CSIRTs designados devem observar, e tarefas que devem desempenhar.[[4]](#footnote-4)

## Ciber-segurança

*"A proeminência da ciber-segurança cresceu na última década e tornou-se uma das principais prioridades em muitas políticas nacionais. Isto deve-se principalmente à sobreposição com outras esferas de segurança e também a incidentes que deram notoriedade a este conceito e forçaram o público em geral a pensar sobre a necessidade de segurança no ciberespaço. Ligado a isto está a necessidade de proteger o ciberespaço para que a segurança abrangente da República Checa seja preservada tanto quanto possível, bem como o direito dos indivíduos à autodeterminação informativa".*[[5]](#footnote-5)

A definição de ciber-segurança pode ser algo problemática. Para muitas pessoas, a ciber-segurança é uma área que é essencialmente tratada exclusivamente pelos departamentos de tecnologias de informação e comunicação.

Esta premissa está errada desde o início porque a ciber-segurança diz respeito a cada um de nós que utiliza qualquer elemento das TIC na nossa vida diária. Se não nos apercebemos de que somos um elemento chave, e em muitos casos crucial, da cibersegurança (seja na nossa vida privada ou no trabalho), então estamos de facto a aumentar a probabilidade de ciberataques bem sucedidos.

Actualmente, a ciber-segurança não pode ser subestimada ou subestimada. É uma área crucial para muitas organizações, mas também para indivíduos, pelo que deve ser abordada de uma forma sistemática e a longo prazo.

*"A gestão organizacional deve compreender e aceitar que a gestão da cibersegurança recai muito mais sobre outras áreas da segurança e da gestão de crises. Afinal, mesmo os ataques sofisticados de hoje em dia são frequentemente multidisciplinares e combinam as áreas das TIC, engenharia social, pessoal e segurança de objectos".[[6]](#footnote-6)*

Voltando ao próprio conceito de ciber-segurança, é apropriado partir de uma análise deste termo. A palavra **cibersegurança** representa uma interconexão com elementos das tecnologias da informação e da comunicação e do ciberespaço enquanto tal.

**Segurança**

Existem muitas definições de **segurança**[[7]](#footnote-7) , mas não existe uma única, geralmente aceite. A maioria das definições do termo segurança são dadas na literatura e não na própria legislação. [[8]](#footnote-8)

Marés define segurança como *"um Estado em que as ameaças a uma instalação (geralmente um Estado, ou mesmo organizações internacionais) e os seus interesses são limitados ao nível mais baixo possível, e esta instalação está efectivamente equipada e disposta a cooperar na eliminação de ameaças existentes e potenciais".*[[9]](#footnote-9)

Pozár define *"segurança como uma característica de uma instalação ou entidade que determina o grau, nível da sua protecção contra potenciais danos e ameaças".*[[10]](#footnote-10)

Esta definição foi especificada com mais pormenor no *Výkladový slovník kybernetické bezpečnosti (*Cybersecurity Glossary):

***Segurança***

*Uma característica de um elemento (por exemplo, um sistema de informação) que é protegido contra perdas a um determinado nível, ou também o estado de protecção (a um determinado nível) contra perdas. A segurança informática inclui a protecção da confidencialidade, integridade e acessibilidade no processamento, armazenamento, distribuição e apresentação da informação.* [[11]](#footnote-11)

É de notar que a segurança não é actualmente apenas uma preocupação do Estado, que, no entanto, ainda desempenha um papel primordial na garantia da segurança, mas que é um processo implementado por outras entidades (entidades jurídicas e pessoas singulares), que recentemente foram forçadas a lidar mais com a questão da segurança, ou mais precisamente a garantir as suas actividades contra ataques.

Dada esta expansão do âmbito da segurança, é necessário abordar, entre outras, as seguintes questões:

* **De quem é a segurança** (organização internacional, Estado, organização, indivíduo, etc.)**?**
* **Que valores são protegidos** (organização, pessoas, dados, etc.)**?**
* **Quais são (devem ser) estes valores protegidos contra** (ataques físicos, cibernéticos, ataques combinados, etc.)**?**
* **Que recursos devem ser despendidos para proteger estes valores**? [[12]](#footnote-12)

O objectivo ideal da segurança é criar um estado de "segurança absoluta". Contudo, este estado é uma utopia, porque não pode ser realisticamente alcançado,[[13]](#footnote-13) uma vez que haverá sempre uma ameaça ou risco que não foi considerado no conceito de criação de segurança ou foi intencionalmente negligenciado.

Contudo, o objectivo da segurança não é cobrir todos os riscos reais, menos reais ou completamente imprevisíveis e improváveis em todas as circunstâncias, uma vez que tal implementação criaria um complexo completamente disfuncional, que essencialmente negaria ou mesmo eliminaria completamente a aplicação e implementação da segurança.

**Exemplo:** *Na vida quotidiana, também lhe pode acontecer, por exemplo, que se feche fora do seu apartamento. Se tiver considerado esta possibilidade, provavelmente tem chaves sobresselentes com a sua família, amigos, ou noutro lugar. No entanto, se não tiver chaves sobresselentes, provavelmente chamará um serralheiro ou arrombará a porta.*

**Ciber-segurança**

Tal como com o conceito de segurança, a ciber-segurança não tem uma única definição geralmente aceite. A ciber-segurança é um subconjunto da segurança enquanto tal.

Ao definir a ciber-segurança, é apropriado partir de definições já estabelecidas. Aqui estão algumas destas definições:

* 1. **Ciber-segurança** é **um conjunto de medidas tomadas para proteger um sistema informático contra acesso ou ataque não autorizado.** [[14]](#footnote-14)
  2. O Dicionário Oxford afirma que a **ciber-segurança** é **o estado de protecção contra a utilização criminosa ou não autorizada de dados electrónicos.** A ciber-segurança deve então incluir as medidas que têm de ser tomadas para o conseguir.[[15]](#footnote-15)
  3. Segundo Jirásek et al., **cybersecurity** é "**um conjunto** de **instrumentos** jurídicos, organizacionais, técnicos e educativos **concebidos para assegurar a protecção do ciberespaço.** ”[[16]](#footnote-16)
  4. De uma forma relativamente semelhante, a cibersegurança é definida em "*Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020". (*A Estratégia Nacional de Cibersegurança da República Checa para 2015-2020). Esta estratégia afirma que: "Cybersecurity é um **conjunto** de **medidas e ferramentas** organizacionais, políticas, jurídicas, técnicas e educativas **destinadas a garantir um ciberespaço seguro, protegido e resiliente na República Checa**, tanto para entidades do sector público e privado como para o público checo em geral".[[17]](#footnote-17)

Embora estas definições procurem definir o conceito de ciber-segurança, são um pouco imprecisas.

A primeira definição centra-se apenas no computador e no sistema informático e na sua protecção contra dois tipos de ciberataques, enquanto que o espectro de ambos os alvos dos ataques e especialmente dos próprios ataques é muito mais diversificado.[[18]](#footnote-18)

A segunda definição protege então apenas os dados electrónicos e não os sistemas informáticos enquanto tal.

A terceira definição centra-se na adopção de meios para proteger os elementos das TIC no ciberespaço. Esta definição é relativamente precisa, mas a sua restrição ao ciberespaço só pode ser enganadora uma vez que a cibersegurança também pode ser aplicada aos elementos das TIC que não estão envolvidos no ciberespaço ou que criam o seu próprio "ciberespaço fora de linha".[[19]](#footnote-19)

A última das definições é então explicitamente limitada ao ciberespaço na República Checa, ignorando completamente a possibilidade de proteger os interesses dos cidadãos da República Checa ou outras entidades que não estejam estabelecidas na República Checa. Acreditamos que o estreitamento da ciber-segurança ao ciberespaço na República Checa é compreensível do ponto de vista da implementação da Lei de Ciber-segurança, mas inadequado do ponto de vista da implementação da ciber-segurança.

Outra definição de cibersegurança pode ser encontrada, por exemplo, na **Definição de Cibersegurança - Lacunas e sobreposições na normalização**[[20]](#footnote-20) pela ENISA, a Agência Europeia para a Segurança Cibernética[[21]](#footnote-21) : *"Cybersecurity" refere-se à segurança do ciberespaço, onde o ciberespaço se refere a um conjunto de ligações e relações entre objectos acessíveis através de uma rede geral de telecomunicações e a um conjunto de objectos cujas interfaces permitem o seu controlo remoto, acesso remoto a dados, ou a sua ligação a acções de gestão dentro do ciberespaço. A cibersegurança incluirá o paradigma "CIA" da tríade de relações e objectos no ciberespaço, e será alargada para assegurar a protecção da privacidade das entidades (pessoas singulares e colectivas) e a resiliência [recuperação de um ataque]".*

Dado o esforço para definir o conceito de ciber-segurança, é apropriado proceder a partir das regras processuais que cobrem a ciber-segurança.

A Directiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de Julho de 2016, relativa a medidas destinadas a assegurar um elevado nível comum de segurança das redes e sistemas de informação em toda a União, declara[[22]](#footnote-22) no n.º 2 do artigo 4.º que *"segurança das redes e sistemas de informação significa a capacidade de as redes e sistemas de informação resistirem, com um determinado nível de confiança, a qualquer acção que comprometa a disponibilidade, autenticidade, integridade ou confidencialidade dos dados armazenados ou transmitidos ou processados ou dos serviços conexos oferecidos ou acessíveis através dessas redes e sistemas de informação".*

A definição de Ciber-segurança pela lei polaca é - resistência dos sistemas de informação a actividades que violem a confidencialidade, integridade, disponibilidade e autenticidade dos dados processados ou serviços relacionados oferecidos por estes sistemas (Lei de 5 de Julho de 2018 sobre o sistema nacional de ciber-segurança Journal of Laws de 2018, item 1560).

As definições acima procuram de várias formas definir o leque de relações, interesses e entidades contra as quais a ciber-segurança é aplicada. Ao mesmo tempo, definem também o ciberespaço como o ambiente em que a cibersegurança é aplicada.

Devido a uma certa inconsistência nas opiniões sobre o que é e o que não é ciber-segurança, é apropriado apresentar a nossa própria definição de ciber-segurança, que surgiu tanto com base numa análise das definições anteriores como com base na nossa própria experiência.

**A ciber-segurança pode ser definida como:**

* **um conjunto de instrumentos jurídicos, organizacionais, técnicos e educativos destinados a assegurar a protecção dos sistemas informáticos e outros elementos das TIC, aplicações, dados e utilizadores,**
* **a capacidade dos sistemas e serviços informáticos utilizados para responder a ameaças ou ataques cibernéticos e suas consequências, bem como o planeamento da restauração da funcionalidade dos sistemas informáticos e serviços relacionados.**

**A ciber-segurança é implementada tanto dentro como fora do ciberespaço.** Não é adequado limitar a aplicação dos meios e princípios acima referidos, geolocamente, de qualquer forma (seja no território de um determinado Estado, da União ou do próprio ciberespaço).

## Princípios de ciber-segurança

**Ao aplicar a ciber-segurança, são instituídos os seguintes princípios, que também são chamados as tríades da ciber-segurança.**[[23]](#footnote-23)

Para os fins desta monografia, serão definidas as três tríades seguintes:

1. **CIA** (**C** - **Confidencialidade**; **I** - **Integridade**; **A - Disponibilidade**).
2. **Elementos de ciber-segurança** (Pessoas, Tecnologia, Processos).
3. **Ciclo de vida da ciber-segurança** (Prevenção, Detecção, Resposta)

## A Tríade da CIA

A tríade de segurança cibernética mais conhecida e mais amplamente utilizada é a tríade **da CIA**, mas a simples utilização desta tríade básica de princípios de segurança cibernética sem pôr em prática outros princípios é actualmente insuficiente para manter um nível adequado de segurança cibernética.

Na literatura, por exemplo, é feita referência à aplicação do **hexad Parkerian**[[24]](#footnote-24) , que é essencialmente a tríade da CIA, mas complementada por três outros elementos: **P/C - Possessão/Controlo**, **A - Autenticidade** e **U - Utilidade.**

O objectivo da ciber-segurança é assegurar tanto a segurança das TIC como tal e, em particular, os dados e informações que são transmitidos, processados e armazenados por estes elementos.

Muito frequentemente, a tríade da CIA está principalmente relacionada com a informação.

Este conceito mais restrito resulta principalmente da própria definição de **segurança da informação**, que se centra na protecção da informação. Sob esta protecção, o tipo de portador (papel, meios electrónicos, etc.) ou sistema de processamento de informação não é um problema. A segurança da informação é então aplicada à informação ao longo de todo o seu ciclo de vida.

A segurança da informação é também definida por uma série de normas ISO 27000. As normas básicas de segurança da informação incluem:

* ISO/IEC 27001:2014 Tecnologia da informação - Técnicas de segurança - Sistemas de gestão da segurança da informação - Requisitos
* ISO/IEC 27002:2014 Tecnologia da informação - Técnicas de segurança - Código de prática para controlos de segurança da informação

A questão é se a definição de segurança da informação é actualmente adequada e suficiente, ou se se aplica a todos os elementos-chave da segurança no ciberespaço.

Apesar de o termo segurança da informação ser mais comummente utilizado na literatura profissional e nas regras processuais, estamos convencidos de que em relação às actividades relacionadas com a utilização das TIC ou às actividades relacionadas com o ciberespaço, o termo cibersegurança é um termo mais apropriado.

Como mencionado acima: *"a segurança da informação refere-se à informação enquanto tal"*. No entanto, isto omite elementos chave relacionados com a segurança no ciberespaço.

Consideramos estes elementos importantes como **dados** e depois os próprios **sistemas informáticos** (ou elementos individuais das TIC), que permitem a transmissão efectiva de dados e informações.

Existem várias definições dos termos dados e informações na literatura profissional e na legislação. Para efeitos da presente publicação, são seleccionadas definições relacionadas com a protecção de informações, dados ou cibersegurança.

De acordo com a Convenção sobre o Cibercrime[[25]](#footnote-25) , **dados informáticos** significa *"****qualquer representação de factos, informações ou conceitos numa forma adequada ao processamento num sistema informático****, incluindo um programa adequado para levar um sistema informático a executar uma função".*

Assim, os dados são qualquer elemento com um valor de informação que é processado por um sistema informático, e são processados para posteriormente criar informação.

**A informação** *"são dados que foram processados numa forma útil para um destinatário. Assim, cada informação é um dado, mas qualquer dado armazenado não se torna necessariamente informação".*[[26]](#footnote-26)

Wiener afirma que *"a informação é o nome para o conteúdo do que é trocado com o mundo exterior à medida que nos ajustamos a ela e fazemos sentir o nosso ajustamento".* Diz também que a informação não é nem matéria nem energia, mas sim uma categoria física separada.[[27]](#footnote-27)

**A informação é, portanto, entendida como algo "mais qualificado" do que os dados.** Os dados são factos que se tornam informação quando são percebidos ou expressos em contexto e têm um significado que é compreensível para as pessoas.[[28]](#footnote-28)

É a ligação de dados "insignificantes" e a criação de um determinado contexto, que apenas compõe informações "significativas" a partir dos dados, que podem ser fundamentais do ponto de vista da ciber-segurança. Se respeitarmos a tese de segurança da informação acima referida, na qual apenas a informação enquanto tal é protegida, então poderá haver uma violação significativa da segurança.

O gráfico seguinte demonstra a relação entre os dados e a informação.[[29]](#footnote-29)

Os dados e informações são transmitidos no ciberespaço utilizando sistemas informáticos[[30]](#footnote-30) , que são parte integrante da segurança cibernética ou da informação.

Com base no acima exposto, estamos convencidos de que a tríade CIA[[31]](#footnote-31) deve ser aplicada não só à própria informação, mas também a outros elementos de ciber-segurança (dados, sistemas informáticos, etc.)

**Confidencialidade**

Confidencialidade significa uma situação em que apenas as entidades autorizadas a fazê-lo têm acesso a informação, dados ou TIC.

Dada a grande quantidade de informação processada, é apropriado introduzir ou aplicar uma das classificações de informação. Estas classificações podem então ser aplicadas a outros elementos de ciber-segurança e acesso aos mesmos.

As normas de segurança ISO/IEC 27000 definem isso:

* *"A informação deve ser classificada de acordo com o seu valor, requisitos legais, sensibilidade e criticidade".*
* *"Os procedimentos de acordo com o esquema de classificação adoptado por uma organização devem ser estabelecidos e implementados para a marcação e tratamento da informação".*
* *"A fim de impedir o acesso não autorizado ou a má utilização da informação, devem ser estabelecidas regras para o tratamento e armazenamento da informação".*

Exemplos de alguns esquemas de classificação:

1. **Classificação da informação de acordo com a Lei 412/2005 Sb., sobre a Protecção da Informação Classificada e sobre a Autorização de Segurança**[[32]](#footnote-32) :

* **Top secret** - o tratamento não autorizado de informações pode causar danos extremamente graves aos interesses da República Checa.
* **Segredo** - o tratamento não autorizado de informações pode causar danos substanciais aos interesses da República Checa.
* **Confidencial** - o tratamento não autorizado de informações pode causar danos simples aos interesses da República Checa.
* **Restrição** - o tratamento não autorizado de informações pode ser desvantajoso para os interesses da República Checa.

1. **Classificação das informações utilizadas na esfera comercial**:

* **Protegido - o** tratamento não autorizado de informação pode causar danos substanciais ou destruição da organização (por exemplo, fuga de informação estratégica, código fonte, esquemas de segurança, palavras-passe, etc.).
* **Interno - o** tratamento não autorizado de informações pode causar danos à organização (por exemplo, fuga de dados pessoais, contratos, etc.).
* **Sensível - o** tratamento não autorizado de informação pode ter um impacto negativo na empresa (por exemplo, informação não publicada anteriormente sobre projectos, eventos planeados, etc.).
* **Público - o** tratamento não autorizado de informação não deve prejudicar ninguém e não deve ter qualquer impacto na empresa (por exemplo, contactos disponíveis ao público, apresentações de projectos, etc.).[[33]](#footnote-33)

Para além das duas classificações acima mencionadas, existem várias outras classificações que são aceites por organizações ou indivíduos, quer com base na legislação, quer à discrição do utilizador.

As classificações, desde que sejam respeitadas e cumpridas, podem mitigar significativamente o impacto de um possível ciberataque.

1. **Protocolo de Semáforos**

No seio da comunidade de cibersegurança, houve no passado a necessidade de partilhar informações e dados sensíveis (normalmente sobre ciberataques). Por esta razão, o **TLP** (***Traffic Light Protocol***)[[34]](#footnote-34) foi criado no Centro Nacional de Coordenação de Segurança de Infra-estruturas[[35]](#footnote-35) no início de 2000. Este protocolo visa acelerar a troca de informações entre os interessados e, ao mesmo tempo, estabelece regras para o tratamento da informação transmitida. A entidade que transmite a informação (a fonte da informação) marca sempre a informação com uma determinada cor que determina a forma como o destinatário deve tratar a informação.

O protocolo TLP é melhor definido na tabela seguinte, que foi retirada do US-CERT[[36]](#footnote-36) :

|  |  |  |
| --- | --- | --- |
| **Cor** | **Quando utilizar** | **Como partilhar?** |
| **TLP:**VERMELHO  TLP:RED **Não se destina a publicação**, apenas para os participantes. | As entidades podem utilizar o TLP: RED nos casos em que a informação não permite uma resposta eficaz por parte de outras entidades e pode levar a implicações para a privacidade, reputação ou operações dessas entidades em caso de utilização indevida. | Os beneficiários não podem partilhar informações classificadas no TLP: categoria VERMELHO com qualquer entidade que não seja a troca, reunião ou conversa específica na qual a informação do TLP:RED foi originalmente divulgada. Por exemplo, numa reunião, o TLP: A informação VERMELHO é limitada àqueles que estão a participar directamente na reunião.  Na maioria dos casos, a **informação marcada com TLP: VERMELHO só deve ser trocado verbalmente ou pessoalmente**. |
| **TLP:AMBER**  TLP:AMBER **Divulgação limitada.** A revelação só é possível na organização dos participantes. | As entidades podem utilizar TLP: AMBER nos casos em que a informação requer uma resposta eficaz de outras entidades e representa um risco para a privacidade, reputação ou operações, se for partilhada fora das organizações participantes. | Os beneficiários podem partilhar informações classificadas na categoria TLP: AMBER com membros da sua própria organização e com clientes ou clientes que necessitem de conhecer estas informações a fim de proteger ou prevenir novos danos potenciais. **As entidades são livres de estabelecer regras de partilha adicionais, e estas devem ser seguidas.** |
| **TLP:VERDE**  TLP:GREEN Divulgação limitada, limitada à comunidade. | As entidades podem utilizar TLP: GREEN se a informação for útil para aumentar a sensibilização entre todas as organizações participantes. É também possível partilhar esta informação com outras entidades dentro de uma comunidade ou sector mais vasto. | Os beneficiários podem partilhar informações classificadas na categoria VERDE com parceiros e organizações parceiras dentro do seu sector ou comunidade. No entanto, a informação não pode ser partilhada através de canais acessíveis ao público. A informação nesta categoria pode ser massivamente divulgada dentro de uma dada comunidade. **A informação incluída no TLP: A categoria VERDE não pode ser divulgada fora da comunidade.** |
| TLP:BRANCO  TLP:WHITE A revelação não é de forma alguma restrita. | As entidades podem utilizar TLP: BRANCO se a informação contiver pouco ou nenhum risco previsível de má utilização, de acordo com as regras e procedimentos de divulgação aplicáveis. | De acordo com as regras e a protecção dos direitos de autor, as **informações incluídas no TLP: categoria BRANCO podem ser distribuídas sem restrições.** |

*"Em ciber-segurança, a divulgação não desejada de certas informações é referida como uma violação da sua confidencialidade ou fuga".*[[37]](#footnote-37)

1. **Avaliação da confidencialidade de acordo com o Decreto n.º 82/2018 Sb.** , sobre **Medidas de** Segurança**, Incidentes de Segurança Cibernética, Medidas Reactivas, Requisitos para o Registo no Campo da Segurança Cibernética e Eliminação de Dados** (Decreto sobre Segurança Cibernética)[[38]](#footnote-38)

O Decreto sobre Ciber-segurança retoma em grande parte o Protocolo de Semáforo mencionado acima para a escala de classificação de confidencialidade (ver Apêndice 1 do DoCS).

|  |  |  |
| --- | --- | --- |
| **Nível** | **Descrição** | **Exemplos de requisitos de protecção de bens** |
| **Baixo** | Os bens estão disponíveis ao público ou foram destinados à divulgação. A violação da confidencialidade dos bens não prejudica os interesses legítimos de um devedor.  No caso de partilha de tal bem com terceiros e utilizando a classificação de acordo com o Protocolo de Semáforo (doravante "TLP"), é utilizada  a designação **TLP:WHITE.** | Não é necessária qualquer protecção.  Liquidação/apagamento do bem ao nível baixo - ver Apêndice No. 4. |
| **Médio** | Os bens não estão disponíveis ao público e constituem o saber-fazer de um devedor; a protecção dos bens não é exigida por qualquer acto legislativo ou acordo contratual.  No caso da partilha de tal bem com terceiros e utilizando a classificação de acordo com o TLP, é utilizada em particular a designação **TLP:GREEN** ou TLP:AMBER. | Os instrumentos de controlo de acesso são utilizados para proteger a confidencialidade.  Liquidação/apagamento do bem ao nível do Meio - ver Apêndice No. 4. |
| **Alto** | Os bens não estão publicamente disponíveis e a sua protecção é exigida por regulamentos legais, outros regulamentos ou disposições contratuais (por exemplo, segredos comerciais, dados pessoais).  No caso de partilha de tal bem com terceiros e utilização da classificação de acordo com o TLP, é utilizada em particular  a designação **TLP:AMBER.** | Ferramentas para assegurar o controlo de acesso e gravação são utilizadas para proteger a confidencialidade. As transmissões de informação através de redes de comunicação são protegidas por meios criptográficos.  Liquidação/apagamento do bem a Alto Nível - ver Apêndice No. 4. |
| **Crítico** | Os bens não estão disponíveis ao público e requerem um nível de protecção acima da categoria anterior (por exemplo, segredos comerciais estratégicos, categorias especiais de dados pessoais).  No caso de partilhar um tal bem com terceiros e de utilizar a classificação de acordo com o TLP, é utilizada em particular  a designação  TLP:RED **ou TLP:AMBER.** | Ferramentas para assegurar o controlo de acesso e gravação são utilizadas para proteger a confidencialidade. Além disso, métodos de protecção que impedem uma utilização indevida dos bens pelos administradores. As transmissões de informação são protegidas por meios criptográficos.  Liquidação/apagamento do bem ao nível crítico - ver Apêndice No. 4. |

**Integridade**

De acordo com o Cybersecurity Glossary[[39]](#footnote-39) , a **integridade** é definida como "*a propriedade da exactidão e da integralidade.* " A **integridade dos dados** é então definida no mesmo glossário como "a *certeza de que os dados não foram alterados". Também se refere à validade, consistência e exactidão dos dados, tais como bases de dados ou sistemas de ficheiros. É fornecido por checksums, funções de hash, códigos de auto-cura, redundância, jornalismo, etc. Na criptografia e segurança da informação em geral, integridade significa validade dos dados". A* **integridade do sistema** é então *"uma propriedade de que o sistema desempenha a função a que se destina de forma não perturbada, sem manipulação intencional ou acidental não automatizada com o sistema".*

**A integridade representa, portanto, a impossibilidade de interferir com informações, dados, sistemas informáticos, suas configurações,** etc., **por uma pessoa que não seja a autorizada para o fazer.**

Ao mesmo tempo, a integridade é uma espécie de garantia da integridade do sistema, da informação ou dos dados.

*"Alteração indesejada (alteração) é portanto referida na segurança da informação como uma violação da integridade".*[[40]](#footnote-40)

No caso de uma violação da integridade, estar ciente de que se ocorrer uma alteração indesejada dos dados, a alteração indesejada pode não ser detectada de todo e pode decorrer um período de tempo considerável antes de a violação da integridade ser detectada.

O Decreto sobre Ciber-segurança no Apêndice 1 também representa uma escala para avaliar a integridade.

|  |  |  |
| --- | --- | --- |
| **Nível** | **Descrição** | **Exemplos de requisitos de protecção de bens** |
| **Baixo** | Os bens não necessitam de protecção em termos de integridade. A violação da integridade dos bens não compromete os interesses legítimos de um devedor. | Não é necessária qualquer protecção. |
| **Médio** | Os bens podem exigir protecção em termos de integridade. Uma violação da integridade de um bem pode prejudicar os interesses legítimos de um devedor e pode ter efeitos menos graves sobre os bens primários. | Ferramentas padrão (tais como restrições aos direitos de acesso de escrita) são utilizadas para proteger a integridade. |
| **Alto** | Os bens requerem protecção em termos de integridade. Uma violação da integridade de um bem conduz a danos aos interesses legítimos de um devedor com efeitos significativos sobre os bens primários. | Para proteger a integridade, são utilizados meios especiais que permitem seguir o historial das alterações efectuadas e registar a identidade da pessoa que efectua a mudança. A protecção da integridade da informação transmitida pelas redes de comunicação é assegurada por meios criptográficos. |
| **Crítico** | Os bens requerem protecção em termos de integridade. Uma violação da integridade leva a danos muito graves aos interesses legítimos de um devedor com efeitos directos e muito graves sobre os bens primários. | Para proteger a integridade, são utilizados meios especiais para identificar de forma única a pessoa que faz a alteração (por exemplo, utilizando tecnologia de assinatura digital). |

**Disponibilidade**

De acordo com o Cybersecurity Glossary[[41]](#footnote-41) , a **disponibilidade** é definida como "*uma propriedade de acessibilidade e usabilidade a pedido de uma entidade autorizada".* ”

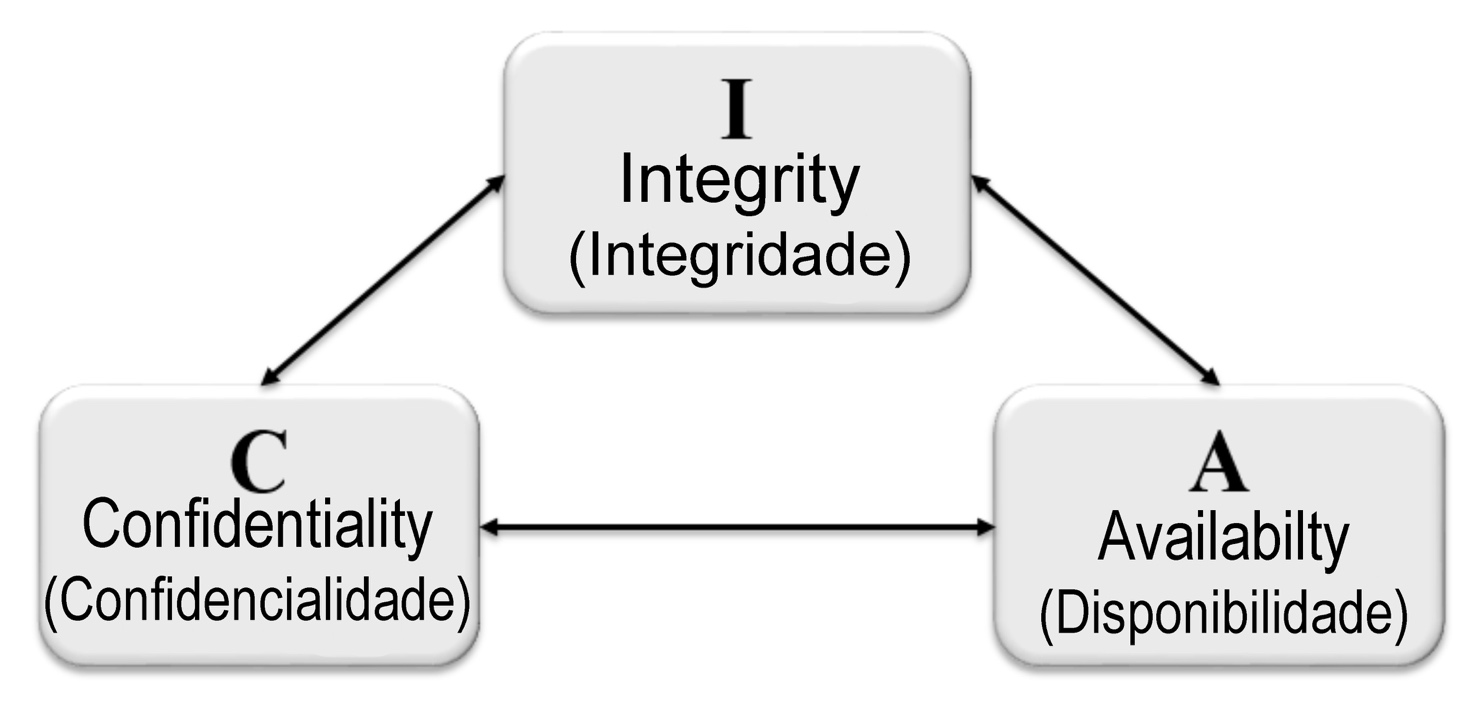
A disponibilidade pode portanto ser definida como uma garantia de acesso à informação, aos dados ou a um sistema informático no momento da necessidade. Não importa como o sistema garante a integridade e permite o acesso ao próprio sistema, dados ou informação, este será inutilizável se não proporcionar um acesso fiável conforme necessário.[[42]](#footnote-42)

"*A destruição de certas informações é referida na segurança da informação como uma violação da sua disponibilidade".* [[43]](#footnote-43)

O Decreto sobre Ciber-segurança no Anexo 1 também representa uma escala para avaliar a disponibilidade.

|  |  |  |
| --- | --- | --- |
| **Nível** | **Descrição** | **Exemplos de requisitos de protecção de bens** |
| **Baixo** | A interrupção da disponibilidade de bens não é importante e, em caso de interrupção, é normalmente tolerado um período de correcção mais longo (aproximadamente até 1 semana). | Os backups regulares são suficientes para proteger a disponibilidade. |
| **Médio** | A perturbação da disponibilidade de bens não deve exceder um dia útil, uma paragem a longo prazo conduz a uma possível ameaça aos interesses legítimos de um devedor. | São utilizados métodos comuns de backup e recuperação para proteger a disponibilidade. |
| **Alto** | A interrupção da disponibilidade de bens não deve exceder um período de várias horas. Qualquer falha deve ser tratada imediatamente, uma vez que conduz a uma ameaça directa aos interesses legítimos de um devedor. Os bens são considerados muito importantes. | Os sistemas de backup são utilizados para proteger a disponibilidade, e o reinício da prestação de serviços pode ser condicionado à intervenção do operador ou à troca de activos técnicos. |
| **Crítico** | A perturbação da disponibilidade dos bens não é admissível e mesmo a indisponibilidade a curto prazo (na ordem de vários minutos) conduz a uma séria ameaça aos interesses legítimos de um devedor. Os bens são considerados críticos. | Os sistemas de backup são utilizados para proteger a disponibilidade, e o reinício da prestação de serviços é de curto prazo e automatizado. |

A tríade da CIA é frequentemente representada visualmente para melhor compreender os seus atributos e relações individuais. Por esta razão, também, uma representação típica da tríade da CIA é mostrada aqui. Na parte seguinte deste capítulo, esta tríade é complementada por certos elementos (tecnologia, pessoas, processos).



**A Tríade da CIA**

Se tentássemos definir o espaço de ciber-segurança dentro da implementação da tríade CIA, então este espaço poderia ser exibido como uma intersecção de princípios individuais desta tríade.

Obsah obrázku text, hodiny, vektorová grafika

Popis byl vytvořen automaticky

Tríade da CIA e ciber-segurança



Vista hexadecimal de Parkenian[[44]](#footnote-44)

## Elementos de ciber-segurança

Os três elementos seguintes, ou a sua interacção mútua, tornam possível criar ou estabelecer uma certa medida de ciber-segurança. Estes elementos são:

* **pessoas**,
* **tecnologias** e
* **processos**.

Acreditamos que é utópico pensar que é possível criar uma segurança cibernética absoluta ou um sistema absolutamente seguro em que elementos das TIC são utilizados.

Teoricamente, seria possível conceber um sistema informático completamente isolado (incluindo uma fonte de alimentação, por exemplo, através de um agregado), encerrado numa jaula de Faraday, com um grupo claramente definido de pessoas que estão autorizadas a trabalhar neste sistema informático, assegurando que nenhum meio (electrónico ou outro) é trazido ou removido deste ambiente único.

No entanto, a questão é saber qual seria o objectivo de um sistema assim assegurado e como seriam utilizados os resultados do trabalho neste sistema, ou como esses resultados poderiam ser trazidos à vida quando não é possível trazer os resultados da actividade. O contra-argumento poderia então ser a alegação de que os resultados só serão entregues no final do projecto, até lá tudo será protegido e o acesso será sujeito ao regime acima mencionado.

Contudo, a questão é se um sistema criado artificialmente e completamente isolado está protegido contra outras ameaças, que podem ser a ausência de cópias de segurança, a possibilidade de destruição física do sistema informático, a divulgação de informação parcial por pessoas que trabalham com o sistema, etc.

Qualquer sistema é tão seguro como o seu elo mais fraco (elemento).

**Pessoas**

*"As pessoas representam frequentemente o elo mais fraco da cadeia de segurança e são cronicamente responsáveis pela falha dos sistemas de segurança".*

Bruce Schneier[[45]](#footnote-45)

As pessoas que interagem com a ciber-segurança podem ser vistas como:

* **autor (criador) desta segurança** (ou seja, tipicamente pessoas que tentam impor e implementar elementos individuais de ciber-segurança, quer em relação a si próprios, quer em relação à organização),
* **destinatários das regras de cibersegurança** (ou seja, pessoas que tenham decidido ou sejam forçadas a implementar as regras de cibersegurança existentes),
* **entidades que precisam de ser protegidas contra ciberataques**,
* **entidades que necessitam de ser informadas e formadas sobre as regras e princípios da ciber-segurança**,
* **um risco ou ameaça à criação e manutenção da ciber-segurança**.

Se nos concentrarmos no papel das pessoas na construção e manutenção da cibersegurança, especialmente em ligação com o AoCS, então é necessário definir e recrutar os seguintes cargos de uma forma apropriada:

* Comité de Ciber-segurança,
* Gestor de Ciber-segurança,
* Arquitecto de Ciber-segurança,
* Auditor de Ciber-segurança,
* Equipa de Segurança Cibernética,
* Garante,
  + de bens primários,
  + de bens acessórios,
* Administrador Factual,
* Administrador Técnico,
* Operador (por vezes também referido como o fornecedor),
* Administrador,
* Utilizador.

As pessoas são um elemento chave de qualquer segurança. No caso da ciber-segurança, o seu papel está a intensificar-se, e tipicamente as pessoas são o elemento mais fraco e ao mesmo tempo o alvo mais comum dos atacantes.

Há várias razões que nos levam a esta declaração.

O primeiro é o tempo relativamente curto que temos estado a utilizar sistemas informáticos. A maioria dos utilizadores só começou a utilizar um dos sistemas informáticos depois de 1990. Começámos a ligar-nos mais à Internet em grande escala por volta de 1995, e temos vindo a utilizar telemóveis "inteligentes" desde cerca de 2007. Vários sítios de redes sociais, que são actualmente considerados uma parte necessária da vida, sem os quais não podemos imaginar as nossas actividades diárias, não têm sido utilizados por nós há mais de 10 anos.

A segunda razão reside na enorme dinâmica do desenvolvimento tanto do hardware como especialmente do software, que está inextricavelmente ligado à nossa interacção no mundo digital. É a dinâmica do desenvolvimento de software que não permite a muitos utilizadores abordar mais detalhadamente as questões de segurança que estão inevitavelmente associadas à utilização de software.

A terceira e última razão é o facto de que a vida sem tecnologias de informação e comunicação é agora inconcebível ou impossível para a nossa sociedade. As TIC e as aplicações associadas a estas tecnologias criam avatares digitais de nós próprios, mas com uma quantidade de informação muito maior do que nós, como indivíduos, somos capazes de recordar ou armazenar. Para além dos fornecedores de hardware e software, os atacantes estão cientes deste facto, e é por esta razão que estão a visar pessoas no ciberespaço.

"*Amadores hackeam sistemas, profissionais hackeam pessoas".*

Bruce Schneier[[46]](#footnote-46)

Na nossa opinião, é essencial que as pessoas que utilizam as TIC e optam por interagir no ciberespaço:

* **compreender** pelo menos os **princípios e regras básicas** relacionadas com a **ciber-segurança**,
* **compreender** pelo menos as **funções básicas dos sistemas informáticos** (por exemplo, PC, portátil, telemóvel, televisão inteligente, etc.) **que utilizam** para esta interacção,
* **analisar as aplicações que utilizam** para esta interacção e, se necessário, se a actividade destas aplicações ou as suas condições contratuais não lhes convêm, não utilizaram as aplicações,
* **educar-se** em ciber-segurança.

Portanto, a fim de facilitar pelo menos o último item da lista acima, decidimos criar esta publicação e resumir pelo menos algumas das conclusões que podem ser utilizadas tanto por utilizadores leigos como por profissionais de TI que decidiram prestar maior atenção à ciber-segurança.

**Tecnologias**

*"Se pensa que a tecnologia pode resolver os seus problemas de segurança, então não compreende os problemas e não compreende a tecnologia".*

Bruce Schneier[[47]](#footnote-47)

As tecnologias são normalmente um meio para os utilizadores se ligarem à Internet, às redes sociais, e a outras aplicações. É uma ferramenta que utiliza vários pacotes de escritório quando cria documentos, envia e-mails, verifica vídeo, etc. O utilizador médio normalmente percebe e interage com as tecnologias finais (PC, tablet, telemóvel, etc.), que ele próprio utiliza, enquanto que normalmente não está interessado noutras camadas tecnológicas necessárias para o seu funcionamento no ciberespaço.

Para as organizações, as tecnologias representam toda uma gama de dispositivos, desde tecnologias destinadas aos utilizadores (desktop, dispositivos móveis, etc.), através de uma infra-estrutura de rede completa (LAN, elementos activos, elementos Wi-Fi, etc.) e serviços (servidores, aplicações, etc.), até elementos que servem para garantir a segurança tanto no perímetro (firewall[[48]](#footnote-48) , IDS/IPS[[49]](#footnote-49) , honeypot[[50]](#footnote-50) , etc.) como dentro da infra-estrutura (elementos concebidos para autenticação e autorização, monitorização, análise, etc.).

Como parte da construção e manutenção da ciber-segurança, é necessário analisar os bens existentes e, com base nesta análise, eventualmente complementar ou modificar os sistemas existentes. Dentro das tecnologias, os seguintes elementos devem ser parte integrante de uma organização TIC, tendo em conta as especificidades dessa organização:

* sistemas de detecção - Sistema de Detecção de Intrusão (**IDS**) / Sistema de Prevenção de Intrusão (**IPS**),
* administração central de utilizadores e funções,
* gestão centralizada da classificação da informação,
* protecção contra código malicioso (firewall de aplicação, antivírus, antispam e outras soluções),
* tecnologia para registar as actividades de elementos individuais das TIC, administradores e utilizadores (**sistema de registo**),
* sistemas de backup activos e offline; backups de servidores, aplicações e bases de dados vitais (**sistema de recuperação**),
* gestão da segurança da rede (VLAN, DMZ, firewall, etc.).

As tecnologias são normalmente a parte da ciber-segurança onde nós, como utilizadores ou organizações, não poupamos dinheiro. Estamos dispostos a pagar uma grande parte dos fundos para a tecnologia, ou porque "precisamos do telefone mais recente" ou por uma razão real e justificada baseada na obsolescência e na continuação do não apoio (actualização) do sistema informático.

Portanto, a fim de garantir a ciber-segurança, é necessário manter as tecnologias em tal estado que elas sejam capazes de responder às mudanças associadas ao desenvolvimento das TIC. Em particular, as tecnologias (tanto hardware como software) devem ser mantidas actualizadas e seguras.

Embora as tecnologias sejam certamente uma parte importante do processo de criação e manutenção da cibersegurança, elas são, na nossa opinião, a parte menos importante. Elementos muito mais importantes da ciber-segurança são processos devidamente estabelecidos e pessoas que podem aplicar ou modificar os processos em questão na prática e seguir regras pré-acordadas.

**Processos**

*"O mantra de qualquer bom engenheiro de segurança é: '****A segurança não é um produto, mas sim um processo.*** *"É mais do que conceber uma criptografia forte num sistema; é conceber todo o sistema de modo a que todas as medidas de segurança, incluindo a criptografia, funcionem em conjunto".*

Bruce Schneier[[51]](#footnote-51)

Os processos são actividades que precisam de ser feitas para que as pessoas e as tecnologias possam utilizá-los.

Em termos da passagem do tempo, é possível monitorizar os processos de:

* gestão de activos e riscos,
  + definição e categorização dos bens,
  + análise e categorização do risco,
* implementação das TIC e aplicações,
* gestão de utilizadores e funções,
* autorização e autenticação,
* manutenção (actualização) de sistemas e serviços,
* testes de segurança de sistemas e serviços informáticos individuais,
* análise das medidas correctivas,
* implementação de medidas correctivas,
* auditoria de ciber-segurança,
* detecção de anomalias ou ciberataques,
* resposta a ciberataques ou outros incidentes,
* processos para assegurar a continuidade,
* treino e exercícios, etc.

A lista acima referida de processos individuais associados à criação e manutenção da ciber-segurança não é certamente exaustiva, e os processos delineados podem ser granularizados. Os processos individuais são implementados dentro de todo o ciclo de vida das TIC, informação, dados e em relação aos utilizadores. [[52]](#footnote-52)

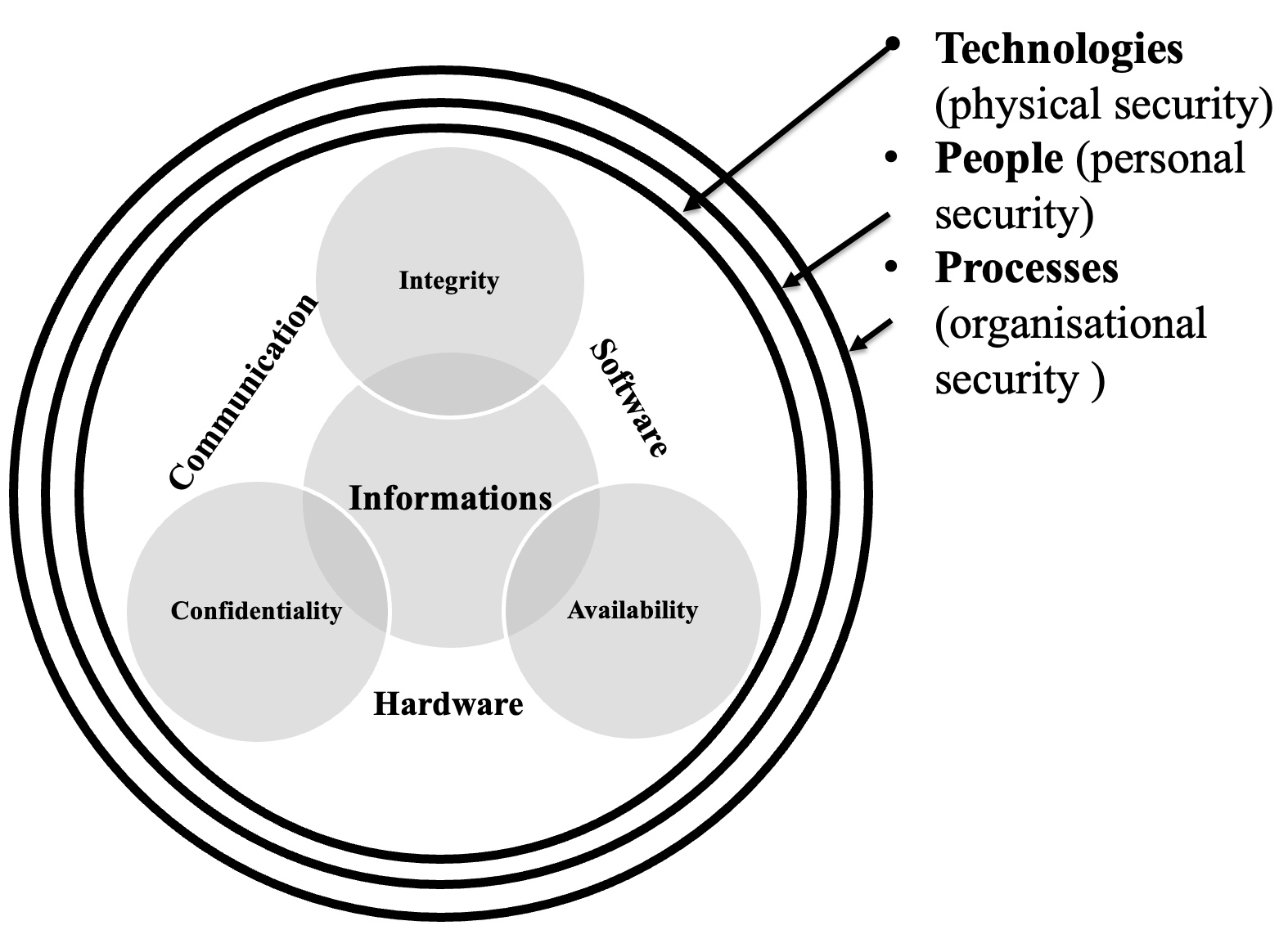
A definição real dos processos, a sua manutenção ou modificação constante é a parte mais exigente da construção de ciber-segurança. Ao mesmo tempo, esta actividade coloca as mais elevadas exigências aos administradores de sistemas individuais.

Se a organização decidir implementar as regras de ciber-segurança, então é obviamente apropriado manter o hardware e o software actualizados, seguir as regras que são estabelecidas para o acesso a sistemas individuais, etc.

Se possível, é aconselhável realizar simulações de ciberataques típicos na organização (por exemplo, phishing, e-mail comercial, etc.) a fim de demonstrar realisticamente estes ataques e possíveis impactos se uma pessoa for vítima de tais ataques.

Os testes de penetração também lhe permitem encontrar erros em processos já definidos.

No entanto, ao criar e estabelecer regras de cibersegurança, a organização deve concentrar-se principalmente nos recursos humanos e na sua educação.

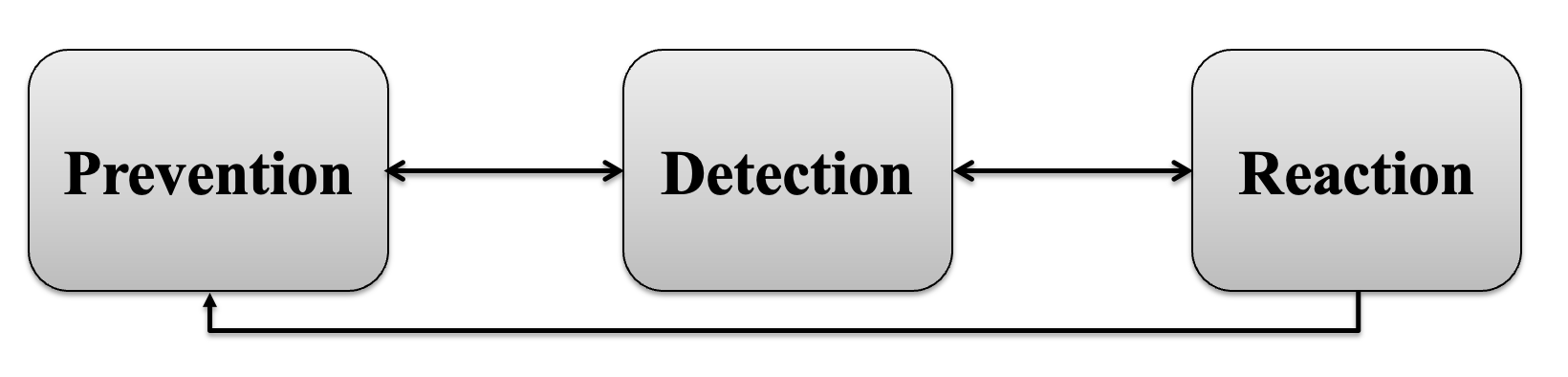


Tríade da CIA complementada por tecnologias, pessoas e processos[[53]](#footnote-53)

## Ciclo de vida da ciber-segurança

Do ponto de vista da passagem do tempo, é necessário aplicar ou modificar tanto a tríade da CIA como elementos parciais de ciber-segurança durante todo o ciclo de vida na implementação da ciber-segurança. Em particular, trata-se de prevenção, detecção e reacção ao ataque. [[54]](#footnote-54)

Muito frequentemente, o ciclo de vida da ciber-segurança é representado por vários diagramas. Para maior clareza, apresento alguns deles.



Representação simplificada do ciclo de vida da ciber-segurança

Texto sobre a figura: **Prevenção - Detecção - Resposta**



Ciclo de vida da ciber-segurança de acordo com kybez.cz[[55]](#footnote-55)

Texto sobre a figura: **Ciber-segurança** - ciclo de vida

ADMINISTRAÇÃO - AUDITORIA - RISCOS - MEDIDAS - IMPLEMENTAÇÃO

Quando se trata de ciber-segurança, não há "ponto de referência" dentro do qual se possa dizer: *"Conseguimos! Estamos protegidos contra ciberataques ou ameaças. Estamos ciberneticamente seguros".*

A construção e manutenção da ciber-segurança pode ser comparada a uma análise de risco sem fim, mas esta análise de rotina precisa de ser complementada por outros processos de apoio que podem ajudar a aumentar a ciber-segurança na organização.

Figura 7: Análise de risco

* análise padrão do funcionamento de sistemas e serviços,
* análise forense, etc.
* ameaças,
* incidentes e ataques,
* eventos do sistema, etc.
* para restaurar a funcionalidade do sistema e dos serviços,
* recomendações baseadas na análise de incidentes,
* as melhores práticas,
* formação e aperfeiçoamento profissional, etc.
* actividades de sistemas e serviços,
* prestar apoio aos utilizadores finais,
* CSIRT/CERT, etc.
* auditoria,
* implementação de medidas, etc.

Ciclo de vida da ciber-segurança

A representação real do ciclo de vida da ciber-segurança pode ser muito mais complexa.[[56]](#footnote-56)



Exemplo de solução de ciber-segurança

**Evolução da ciber-segurança**

No final deste subcapítulo, seria possível fazer uma simples pergunta: *"Porque deveria eu (como indivíduo) ou uma organização lidar com a ciber-segurança de forma alguma?*

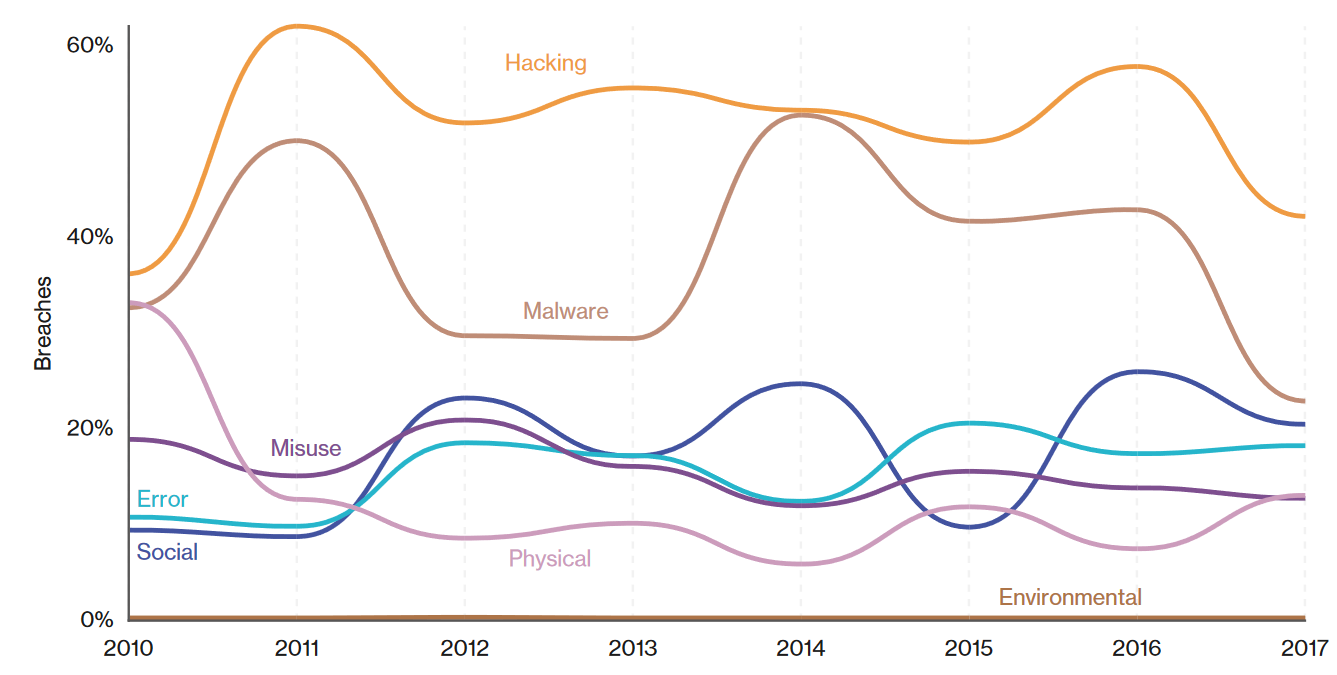
A resposta não será tão complicada, embora seja necessário dissipar o mito muitas vezes enraizado de que outra pessoa, quer sejam grandes organizações como a Microsoft, Google, Apple ou fornecedores de serviços de nuvem, conectividade, etc., já está a abordar a questão da ciber-segurança para mim.

É verdade que estas organizações introduziram e aplicaram subelementos de ciber-segurança, mas a ciber-segurança, como qualquer outra segurança, começa e termina sempre com uma pessoa ou organização específica que se quer assegurar, sempre no que diz respeito às especificidades dessa pessoa ou organização.

Os seguintes factos emergem do Data Breach Investigations Report[[57]](#footnote-57) para 2017, que trata das violações de segurança que conduzem ao comprometimento de dados:

* atacante foi
  + **uma pessoa fora da organização - 73%**
  + uma pessoa dentro da organização - 28%
  + **um grupo de crime organizado - 50%**
* um dos métodos dos ataques foi:
  + **hacking - 48%**
  + **malware - 30%**
    - **49% do malware** foi distribuído por um atacante e subsequentemente instalado **via e-mail**
  + **engenharia social - 43%**
  + ataque físico - 8%[[58]](#footnote-58)
* As vítimas são organizações que operam em:
  + cuidados de saúde - 24%
  + sector público (tipicamente administração estatal e auto-governo, etc.) - 14%
* motivo de ataque:
  + **enriquecimento - 76%**
  + ganho de dados e informação (espionagem) - 13%
* **68% dos ataques só foram detectados após vários meses ou após um período mais longo**

O gráfico seguinte apresenta o desenvolvimento de ataques individuais de 2010 até ao final de 2017.



Tipos de ataques utilizados para comprometer a segurança[[59]](#footnote-59)

**De acordo com um relatório da Agência Nacional de Cibersegurança e Segurança da Informação**,[[60]](#footnote-60) "***é de esperar um novo aumento das ameaças cibernéticas em 2018****, especialmente novos ataques de phishing da próxima geração, ataques a mercados, carteiras e trocas de moeda criptográfica, variantes de resgate sem ficheiros, utilização de inteligência artificial para ciberataques, ataques de dados em soluções Cloud, ataques à Internet das Coisas, sistemas industriais, etc.* ***Espera-se que a percentagem de actores estatais ou apoiados pelo Estado em ciberataques aumente, e as fugas maciças de dados pessoais, palavras-passe e dados de acesso continuarão.*** *É por isso que é necessário construir a ciber-segurança dos sistemas de informação e comunicação importantes para o funcionamento do Estado e da sua infra-estrutura crítica".*[[61]](#footnote-61)

A área da ciber-segurança será uma das áreas mais importantes no futuro, uma vez que se pode assumir que a utilização das TIC e dos serviços relacionados com estas tecnologias não será reduzida. A ciber-segurança destina-se a ajudar a identificar lacunas na configuração destes sistemas e serviços.

"A cibersegurança também ajuda a identificar, avaliar e enfrentar as ameaças no ciberespaço, reduzir os riscos cibernéticos e eliminar o impacto dos ciberataques, crimes de informação, ciberterrorismo e espionagem cibernética, reforçando a confidencialidade, integridade e disponibilidade de dados, sistemas e outros elementos das infra-estruturas de informação e comunicação.

O principal objectivo da ciber-segurança é a protecção do ambiente para fazer respeitar os direitos de informação humana".[[62]](#footnote-62)

## Risco, património, vulnerabilidade

## Risco

Antes de definir os termos de ameaça, acontecimento, incidente e ataque, consideramos necessário definir pelo menos uma definição geral do termo "risco", que está directamente relacionada com os termos definidos subsequentemente.

O Glossário de Ciber-segurança define risco como: "(1) *Perigo, possibilidade de danos, perda, falha. (2) O efeito da incerteza sobre a realização dos objectivos. (3) A possibilidade de uma determinada ameaça explorar a vulnerabilidade de um activo ou grupo de activos e causar danos à organização.* "[[63]](#footnote-63)

**O risco** também **pode** ser definido como **o potencial para uma ameaça se tornar real e explorar a vulnerabilidade de um activo.** De acordo com o Artigo 4 (9) do NIS, **risco** é *"****qualquer circunstância ou evento razoavelmente identificável que possa ter um impacto negativo na segurança das redes e dos sistemas de informação". "***No ciberespaço, os utilizadores, bem como os sistemas e aplicações informáticas estão em risco, bem como outros elementos das TIC.

O termo **"risco" expressa a probabilidade com que um evento indesejado pode ocorrer**. O grau de probabilidade de este evento ocorrer é expresso através da análise de risco. Os valores-padrão mínimos para métodos de identificação, análise, avaliação e tratamento de riscos são definidos em ČSN EN 31010.

Valášek et al[[64]](#footnote-64) declaram que a avaliação de risco é geralmente baseada em três questões básicas:

* **Que pode correr mal (ser indesejado)? O que pode falhar?**
* **Qual é a possibilidade/probabilidade de isto acontecer?**
* **Quão graves (intensidade, dimensão, etc.) podem ser os efeitos (impactos, consequências)?**

Segundo Valášek, porém, estas questões representam apenas um quadro básico capaz de definir o seu próprio risco. Para além destas três perguntas, são feitas as seguintes perguntas complementares, que se relacionam com factores significativos que influenciam a caracterização do risco:

|  |  |
| --- | --- |
| **Factor** | **Pergunta** |
| Hora | "Durante quanto tempo estaremos expostos ao risco (ameaça)"? |
| Instabilidade | "Quão próximas estão as estimativas dos impactos de  um evento de risco para a realidade?" |
| Complexidade | "É difícil compreender o risco?" |
| Relações mútuas | "Até que ponto estão os diferentes riscos ou factores de risco  relacionado?" |
| Influência | "É possível gerir o risco?" |
| Ciclo de vida | "Como é que o risco muda com o tempo?" |
| Relação custo-eficácia | "Qual é o custo das medidas em relação ao risco?" |

Para cada risco, é calculado o grau de significância do risco, que pode ser expresso da seguinte forma:

**Significado** do risco = **Impactos** do risco \* **Probabilidade** de ocorrência do risco

*"O resultado da análise de risco é determinar o significado dos riscos definidos. Cada risco, em relação à tarefa atribuída, tem diferentes impactos que pode causar. Avaliamos os impactos do risco ou das consequências numa escala de cinco pontos, por exemplo, da seguinte forma:"*

|  |  |  |
| --- | --- | --- |
| **Pontos** | **Probabilidade de ocorrência de risco** | **Descrição da ocorrência** |
| 5 | SURE | O risco ocorre quase sempre ou com uma probabilidade de 90-100%. |
| 4 | LIKELY | O risco é susceptível de ocorrer |
| 3 | POSSÍVEL | O risco pode por vezes ocorrer (por exemplo, em condições específicas). |
| 2 | UNLIKELY | O risco pode por vezes ocorrer, mas é improvável. |
| 1 | Impossível | O risco ocorre apenas em casos excepcionais e sob condições específicas. |

*Para além do impacto, podem ou não ocorrer riscos individuais. Por conseguinte, é determinada a probabilidade de ocorrência de riscos. A ocorrência é novamente avaliada numa escala de cinco pontos da seguinte forma*: [[65]](#footnote-65)

|  |  |  |
| --- | --- | --- |
| **Pontos** | **Impacto do risco** | **Descrição do impacto** |
| 5 | CRISIS | A situação irá fundamentalmente reduzir ou terminar as operações da empresa (por exemplo, falência, perda de vidas, etc.). |
| 4 | SIGNIFICANTE | A situação afecta muito perigosamente o funcionamento interno e externo da empresa (por exemplo, a ocorrência de perdas financeiras significativas - 100% sobre o orçamento, o tempo, o surgimento de litígios, ferimentos, etc.). |
| 3 | MÉDIO | A situação afectará perigosamente o funcionamento interno e externo da empresa (por exemplo, ocorrerão perdas, mas a empresa poderá continuar a funcionar, ocorrerão perdas financeiras até 30% do orçamento, etc.). |
| 2 | INSIGNIFICANTE | A situação limita o funcionamento interno da empresa (por exemplo, haverá atrasos de tempo até 30 dias). |
| 1 | NEGLIGÍVEL | Embora a situação limite negativamente o funcionamento da empresa, não causa perdas superiores a 5%. |

Para além das circunstâncias acima referidas, outras circunstâncias devem ser tidas em conta na avaliação do risco, que são

* a própria natureza (tipo) do risco ou ameaça,
* vulnerabilidade dos bens,
* probabilidade de que o risco se transforme num evento ou incidente de segurança.

A análise de risco é muito difícil e requer conhecimento dos bens, ameaças e, em particular, alguma experiência nesta área é necessária. Com base na análise de risco, podem ser identificadas medidas para minimizar ou eliminar os riscos.

## Bens

**Um bem é qualquer coisa que tenha um certo valor para uma pessoa, organização ou estado.**

Um bem pode ser um **objecto tangível** (edifício, sistema informático, redes, energia, bens, etc.) ou um **intangível** (informação, conhecimento, dados, programas, etc.) do ponto de vista do direito civil.

Contudo, um bem pode também ser uma **qualidade** (por exemplo, disponibilidade e funcionalidade do sistema e dos dados, etc.) ou um **bom nome**, reputação, etc. **As pessoas** (utilizadores, administradores, etc.) e os seus conhecimentos e experiência são também uma mais-valia do ponto de vista da ciber-segurança.

De acordo com a Secção 2 (f) e (g) do DoCS, os **bens** são divididos em **subsidiários** e **primários.**

Um **activo auxiliar** é um activo técnico, empregados e fornecedores envolvidos na operação, desenvolvimento, administração ou segurança do sistema de informação e comunicação.

Um **bem primário** é a informação ou um serviço processado ou fornecido por um sistema de informação e comunicação.

## Vulnerabilidade

Vulnerabilidade refere-se à fraqueza de um bem, software, segurança, que é explorado por uma ou mais ameaças.

A vulnerabilidade, bem como uma ameaça, pode ser causada por uma série de factores fundamentados no comportamento humano, falhas técnicas, e possivelmente de força maior.

No domínio da ciber-segurança, as vulnerabilidades dividem-se em:

* **vulnerabilidades conhecidas** (publicado)
  + **fixo** (tratado) - um caso típico são as vulnerabilidades de software para as quais o fabricante já emitiu uma actualização
  + **não corrigida** (não tratada) - uma entidade afectada (fabricante, administrador, etc.) conhece a vulnerabilidade, mas não assegurou a sua correcção
* **vulnerabilidades desconhecidas** 
  + escondido
  + não descoberto

No caso de vulnerabilidades desconhecidas, é importante que sejam descobertas por um atacante, um fabricante, um analista de segurança, um testador de penetração, ou um utilizador. Igualmente importante é a motivação da pessoa que descobre a vulnerabilidade.

As vulnerabilidades de segurança são potenciais ameaças à segurança. As vulnerabilidades de segurança podem ser eliminadas, até certo ponto, actualizando e corrigindo consistentemente todo o software.[[66]](#footnote-66)

O Decreto sobre Ciber-segurança no Apêndice 3 lista algumas das vulnerabilidades como exemplo. **De acordo com** este **decreto, a vulnerabilidade é:**

1. manutenção insuficiente do sistema de informação e comunicação,
2. obsolescência do sistema de informação e comunicação,
3. protecção insuficiente do perímetro exterior,
4. sensibilização insuficiente dos utilizadores e administradores em matéria de segurança,
5. fixação inadequada dos direitos de acesso,
6. procedimentos insuficientes para identificar e detectar fenómenos de segurança negativos, eventos de ciber-segurança e incidentes de ciber-segurança,
7. controlo insuficiente das actividades dos utilizadores e administradores e incapacidade de detectar o seu comportamento inadequado ou defeituoso,
8. definição insuficiente das regras de segurança, definição imprecisa ou ambígua dos direitos e obrigações dos utilizadores, administradores e funções de segurança,
9. protecção insuficiente dos bens,
10. arquitectura de segurança inadequada,
11. grau insuficiente de controlo independente,
12. incapacidade de detectar erros de forma atempada pelos empregados.

## Ameaças cibernéticas, eventos, incidentes e ataques

Lidar com a questão dos "fenómenos cibernéticos negativos" pode ser algo problemático, uma vez que literatura científica diferente, bem como regras processuais, utilizam frequentemente sinónimos diferentes, o que deveria significar a mesma coisa, para definir o fenómeno negativo específico.

A razão para a persistência da terminologia é, por um lado, o tempo relativamente curto que temos lidado com ameaças, ataques e incidentes cibernéticos, e, por outro lado, a tradução nem sempre idêntica do inglês, que é utilizada principalmente em TI.

## Ameaça cibernética

Uma ameaça pode muito simplesmente ser definida como algo que é capaz de perturbar o estado normal ou ordenado e interferir com os direitos de outras entidades. Este é um efeito negativo que pode ou não ser levado a cabo. É suficiente para a própria definição que a possibilidade de um estado negativo ameace e seja real.

De acordo com o Ministério do Interior da República Checa, "*qualquer fenómeno que tenha o potencial de prejudicar os interesses e valores protegidos pelo Estado é considerado uma ameaça. A gravidade de uma ameaça é determinada pela magnitude dos possíveis danos e pela escala temporal (geralmente expressa em probabilidade ou risco) da possível aplicação dessa ameaça.* ”[[67]](#footnote-67)

O Cybersecurity Glossary define vários termos que estão directamente relacionados com as ameaças cibernéticas.

**A ameaça** é definida como "*a causa potencial de um incidente indesejado que poderia resultar em danos para um sistema ou organização. "* [[68]](#footnote-68)

Directamente relacionado com este conceito básico está o conceito de **ameaça à segurança da informação**[[69]](#footnote-69) , que é definido como "*uma causa potencial de um evento adverso que pode resultar em danos ao sistema e aos seus activos, tais como destruição, divulgação indesejada (compromisso), modificação de dados ou indisponibilidade de serviços*" [[70]](#footnote-70)

Além dos dois termos acima mencionados, os autores definem também **ameaça activa**, **ameaça passiva** e ameaça **avançada** e **permanente** no glossário . [[71]](#footnote-71)

O dicionário de Oxford afirma que uma **ameaça cibernética é a possibilidade de uma tentativa maliciosa de danificar ou perturbar uma rede ou sistema informático.**[[72]](#footnote-72) Neste contexto, um sistema informático é considerado como um sistema.

**A ameaça cibernética** também pode ser definida como um acto destinado a modificar[[73]](#footnote-73) informação, aplicações ou o próprio sistema.

Jirovský define quatro grupos de ameaças básicas e, ao mesmo tempo, caracteriza a sua relação:[[74]](#footnote-74)

1. **O vazamento de informação** é uma condição em que a informação protegida é vazada a uma entidade não autorizada.
2. **A violação da integridade** representa dano, alteração ou eliminação de dados.
3. **A supressão de um serviço** significa obstruir intencionalmente o acesso à informação, às aplicações, ou ao sistema.[[75]](#footnote-75)
4. **A utilização não autorizada** é a utilização de informação por uma entidade não autorizada ou de uma forma não autorizada.[[76]](#footnote-76)

**Classificação das ameaças cibernéticas**

Há uma série de classificações de ameaças cibernéticas, e na maioria das vezes estas ameaças são divididas de acordo com elas:

1. **Fonte de ameaça**
   1. **Ameaças feitas pelo homem.** No caso de uma ameaça ser causada por uma pessoa, é apropriado concentrar-se na forma de culpa que levou ao início da ameaça. Deste ponto de vista, é possível distinguir as ameaças causadas:
      * **intencionalmente,**

As ameaças cibernéticas intencionalmente causadas incluem, por exemplo:

* + - * eliminação intencional de dados, configuração do sistema, etc..,
      * danos físicos a um sistema informático ou outro elemento das TIC,
      * roubo de dados e informações,
      * ciberataques (malware, DoS, DDoS, phishing, espionagem não autorizada, etc.).[[77]](#footnote-77)
    - **por negligência.**

As ameaças cibernéticas causadas por negligência incluem, por exemplo:

* dados apagados acidentalmente,
* danos físicos a um sistema informático ou outro elemento das TIC (por exemplo, por queda, tropeçar em cablagem estruturada, etc.),
* danos de dados, sistemas ou outros elementos devido à não familiarização com actos internos (legais ou técnicos),
* outro erro do utilizador.
  1. **Erros técnicos** (por exemplo, erro de software ou hardware).
  2. **Força maior.**

As ameaças cibernéticas causadas por força maior incluem, por exemplo:

* + - * falha de energia não planeada (a menos que se trate de uma ameaça de negligência por parte do homem),
      * acontecimentos naturais (trovoadas, tempestades, etc.) ou catástrofes (inundações, terramotos, etc.),
      * fogo (a menos que seja uma ameaça feita pelo homem).

1. **Fonte de acção**
   1. **ameaças internas** (a origem da ameaça está localizada dentro da organização)
   2. **ameaças externas** (a fonte da ameaça está fora da organização)[[78]](#footnote-78)
2. **Alvo da ameaça**
   1. **Ataque à tríade da CIA.**
      * **Confidencialidade** - por exemplo, roubo de dados, dados de acesso e chaves, hardware, etc.
      * **Integridade** - erros nas bases de dados, definições de permissões, etc.
      * **Disponibilidade** - por exemplo, ataques DoS e DDoS; ataques físicos a servidores e cablagem estruturada; falhas de energia, etc.
   2. **Ataque a qualquer um dos elementos da ciber-segurança.**
      * **Pessoas** - ataques por engenharia social (no mundo real, mas também no ciberespaço), phishing, malware, roubo, etc.
      * **Tecnologias** - todas as ameaças enumeradas no ponto 1 desta classificação. Tipicamente, as ameaças podem afectar:
        + hardware (sistemas de computadores endpoint, servidores, controladores de rede, IoT, etc.),
        + bases de dados,
        + rede e infra-estrutura de rede,
        + software (sistema operativo ou outras aplicações),
        + informação e dados armazenados em sistemas informáticos.
      * **Processos -** testes não autorizados de segurança ou funcionalidade de processos estabelecidos na organização, etc.
3. **Motivação**

Se uma ameaça for causada por comportamento humano intencional, é apropriado lidar com a sua motivação ao abordar a ameaça. Com base na análise da motivação de tal comportamento, é possível criar medidas correctivas no âmbito do processo de resposta à ameaça, para que não haja incentivos para essa motivação no futuro.

Com base na motivação, pode controlar:

* ameaças, a fim de obter ganhos financeiros,
* ameaças, a fim de ganhar uma vantagem competitiva,
* ameaças, a fim de demonstrar as capacidades de alguém,
* ameaças de retaliação,
* ameaças devidas ao não cumprimento de obrigações.[[79]](#footnote-79)

1. **Tipo de ameaça**

* engenharia social,
* botnet,
* malware,
* resgate,
* spam/scam,
* ofertas fraudulentas,
* phishing, pharming, spear phishing, vishing, smishing,
* hacking,
* farejar,
* DoS, DDoS, DRDoS ataca,
* distribuição de conteúdos defeituosos,
* roubo de identidade,
* APT (Ameaça Persistente Avançada),
* ciberterrorismo,
* extorsão cibernética.

O Decreto sobre Ciber-segurança no Apêndice 3 lista algumas das ameaças como exemplo. **De acordo com** este **decreto, uma ameaça é:**

1. uma violação da política de segurança, execução de actividades não autorizadas, utilização indevida de permissões por utilizadores e administradores,
2. danos ou falhas de hardware ou software,
3. fraude de identidade,
4. utilização de software em violação das condições da licença,
5. código malicioso (tais como vírus, spyware, trojans),
6. violação da segurança física,
7. interrupção da prestação de serviços de comunicações electrónicas ou do fornecimento de electricidade,
8. utilização indevida ou modificação não autorizada de dados,
9. perda, roubo ou dano de um bem,
10. não cumprimento da obrigação contratual por um fornecedor,
11. uma falha por razões imputáveis aos empregados,
12. uso indevido de meios internos, sabotagem,
13. interrupção a longo prazo na prestação de serviços de comunicações electrónicas, fornecimento de electricidade ou outros serviços importantes,
14. escassez de empregados com um nível profissional exigido,
15. ciberataque direccionado utilizando engenharia social, utilização de técnicas de espionagem,
16. utilização indevida de suportes de dados electrónicos amovíveis,
17. ataque à comunicação electrónica (escuta, modificação).

## Evento de ciber-segurança

Prosise e Mandiva caracterizam "**evento de segurança informática**" (que pode ser entendido como um ataque informático ou crime informático), como uma acção ilegal, não autorizada e inaceitável que envolve um sistema informático ou uma rede informática. Tal acção pode centrar-se, por exemplo, no roubo de dados pessoais, spam ou outro tipo de assédio, desvio de fundos, divulgação ou posse de pornografia infantil, etc.[[80]](#footnote-80)

Jirásek et al. definem um evento de segurança como: "***um evento que possa causar ou conduzir a uma violação*** *dos sistemas e tecnologias de informação e das regras definidas para a sua protecção (política de segurança)*".[[81]](#footnote-81)

A definição de um evento de segurança também pode ser encontrada no artigo 3.5 da ISO/IEC 27001, que estabelece que tal evento é: "***um estado identificável*** *de um sistema, serviço ou rede,* ***indicando uma possível violação da política de segurança ou falha das medidas de segurança"****. Pode também ser outra situação que não tenha acontecido anteriormente que possa ser importante do ponto de vista da segurança da informação".*

Uma definição semelhante pode ser encontrada em NIST, 800-61 Computer Security Incident Handling Guide, que afirma que um evento de segurança é um evento de segurança: "*um evento desfavorável com um efeito negativo, tal como falhas do sistema, inundação de pacotes, utilização não autorizada dos privilégios do sistema, acesso não autorizado a dados sensíveis ou execução de código malicioso que destrói os dados*". " [[82]](#footnote-82)

**Um evento de ciber-segurança** é também definido pela Lei sobre Ciber-segurança na Secção 7 (1) como "***um evento que possa causar uma violação da segurança da informação nos sistemas de informação ou uma violação da segurança dos serviços ou da segurança e integridade das redes de comunicações electrónicas"***.

De facto, **é um acontecimento sem uma consequência negativa real** para um determinado sistema de comunicação ou informação. No fundo, é apenas uma ameaça, mas deve ser real.

Ao mesmo tempo, os autores utilizam as tautologias, explicando um evento como um evento.

Acreditamos que seria mais apropriado e provavelmente mais compreensível rotular e interpretar o termo "incidente de cibersegurança" como uma **ameaça cibernética**, porque na realidade só existe uma causa potencial que pode causar um evento adverso.

**Exemplo:** *Uma mensagem de correio electrónico contendo código malicioso (malware) é entregue ao correio interno da empresa de um utilizador. Contudo, este malware é comprimido (por exemplo, utilizando WinZip) e não pode ser instalado sem uma acção adicional do utilizador. Tal evento não significa necessariamente uma quebra de segurança em si mesmo, mas é, em certas circunstâncias, capaz de a violar.*

## Incidente cibernético (segurança)

Jirásek et al. definem um incidente de segurança como "*uma violação ou ameaça iminente de uma violação das políticas de segurança, dos princípios de segurança, ou das regras normais de segurança para o funcionamento das tecnologias de informação e comunicação".* ”*[[83]](#footnote-83)*

A norma ISO/IEC 27001 fornece a sua própria definição de um **incidente de segurança da informação**. No artigo 3.6 desta norma, um incidente de segurança da informação é definido como: "*um ou mais eventos de segurança indesejados ou inesperados em que existe uma elevada probabilidade de comprometer uma organização e de comprometer a segurança da informação".*

Uma definição muito semelhante de **incidente de segurança informática** pode também ser encontrada no manual do NIST, Guia de Tratamento de Incidentes de Segurança Informática 800-61, que afirma que se trata de "*uma violação ou ameaça iminente de violação de políticas de segurança, políticas de utilização aceitável (sistema, serviço) ou prática padrão de segurança*".[[84]](#footnote-84)

**Um incidente de ciber-segurança** é também definido na Secção 7 (2) da Lei sobre Ciber-segurança como "***uma violação da segurança da informação nos sistemas de informação ou uma violação da segurança da prestação de serviços ou uma violação da segurança e integridade das redes de comunicações electrónicas devido a um evento de ciber-segurança"***.

Decorre da redacção do acto que um incidente pode ser causado tanto por acções intencionais como por negligência de uma pessoa, mas também por força maior. É essencial que **a segurança da informação, ou dos serviços e sistemas de informação e comunicação a eles associados, seja comprometida.**

Um incidente de cibersegurança representa assim uma verdadeira violação da segurança da informação nos sistemas de informação ou uma violação da segurança dos serviços ou da segurança e integridade das redes de comunicações electrónicas, ou seja, uma violação de um sistema de informação ou de comunicação com um impacto negativo.

Acidentes, erros de hardware e software, erros cometidos pelos administradores durante a configuração, erros dos utilizadores do sistema, etc. são também responsáveis por uma certa parte dos incidentes de cibersegurança.

**Exemplo:** *Se nos basearmos no exemplo anterior, então quando o utilizador executa código malicioso no computador, já estamos a referir-nos à ocorrência de um incidente de segurança.*

## Cyberattack

Jirásek et al. definem um ciberataque como: *"Um ataque a uma infra-estrutura informática para causar danos e obter informação sensível ou estrategicamente importante". É mais frequentemente utilizado no contexto de ataques de motivação política ou militar".*[[85]](#footnote-85)

Uma tal definição de ataque cibernético reduziria significativamente e não afectaria todas as actividades negativas dos utilizadores do ciberespaço[[86]](#footnote-86) , espesialmente porque combina cumulativamente as condições de danos informáticos e de recuperação de informação. Um ciberataque pode também incluir acções sob a forma de engenharia social, onde o único objectivo é obter informação, ou, inversamente, um ataque DoS ou DDoS, onde o único objectivo pode ser suprimir (ou seja, não danificar) a funcionalidade de um ou mais sistemas ou serviços informáticos.

A diferença entre um incidente de ciber-segurança e um ataque cibernético reside principalmente na questão da culpa. Como mencionado anteriormente, um incidente de cibersegurança pode ser causado tanto por comportamento humano intencional como por negligência, ou por força maior. No entanto, um ataque cibernético é um acto intencional de uma pessoa.

Com base no acima exposto, um **ataque cibernético**[[87]](#footnote-87) pode, portanto, ser definido como **qualquer conduta intencional de um agressor no ciberespaço que seja dirigida contra os interesses de outra pessoa.**

Um ciberataque também pode ser definido como as acções de um atacante ou grupo de atacantes que utilizam tecnologias de informação e comunicação para atacar outra infra-estrutura de informação e comunicação, quer para comprometer a disponibilidade, confidencialidade, ou integridade dos dados.

## Cibercriminalidade

No final da discussão dos incidentes e ataques informáticos, consideramos necessário definir, pelo menos em termos gerais, a relação entre estes ataques ou incidentes e a cibercriminalidade.

Ao definir o conteúdo do conceito de **cibercrime**, é necessário perceber que, juntamente com o crescimento das possibilidades de utilização de ferramentas de informação e comunicação, a possibilidade da sua utilização (abuso) para cometer crimes está também a crescer. Por conseguinte, não existe praticamente nenhuma definição universal, geralmente aceite, que afecte plenamente o âmbito e a profundidade deste conceito.

De um modo geral, o cibercrime pode ser definido como uma **conduta dirigida contra um sistema informático, rede informática, dados ou utilizadores, ou uma conduta em que um sistema informático é utilizado como uma ferramenta para cometer um crime.** Um critério indispensável para a aplicação da definição de crime cibernético é o facto de a rede informática, ou ciberespaço, ser então o ambiente em que esta actividade tem lugar.

O cibercrime representa o conjunto mais amplo para todos os crimes que ocorrem no ambiente das tecnologias de informação e comunicação. O "crime clássico" é muitas vezes transferido para o ciberespaço, uma vez que é possível cometer crimes mais rápida e eficazmente (por exemplo, fraude, disseminação de material sobre abuso de crianças, etc.). Para além desta transferência de crimes familiares, existem até agora novos ataques muitas vezes não abrangidos pela lei.

É de notar que nem todos os ciberataques devem ser um crime, mas todos os crimes cibernéticos devem ser um ciberataque ao mesmo tempo. Muitos ciberataques, mesmo devido à ausência de uma norma de direito penal, podem ser subsumidos a uma conduta que terá a natureza de delito civil ou administrativo, ou não pode ser uma conduta punível por qualquer norma legal (pode ser, por exemplo, apenas uma conduta imoral ou intolerável).

**RESUMO / PRINCIPAIS RESULTADOS DO CAPÍTULO** 

* Para compreender a questão dos ciberataques e da cibersegurança, é necessário conhecer a terminologia básica que está directamente relacionada com a área seleccionada. Este capítulo apresenta os termos técnicos e jurídicos seleccionados.
* conceito de ciber-segurança não tem uma definição uniforme ou geralmente aceite. A ciber-segurança é um subconjunto da segurança enquanto tal.
  + Ao definir a ciber-segurança, é apropriado partir de definições já estabelecidas. Aqui estão algumas destas definições:
  + Ciber-segurança é um conjunto de medidas tomadas para proteger um sistema informático contra o acesso ou ataque não autorizado.
* Dicionário Oxford afirma que a ciber-segurança é o estado de protecção contra a utilização criminosa ou não autorizada de dados electrónicos. A ciber-segurança deve então incluir as medidas que têm de ser tomadas para o conseguir.
  + Segundo Jirásek et al., a ciber-segurança é "*um conjunto de instrumentos jurídicos, organizacionais, técnicos e educativos concebidos para assegurar a protecção do ciberespaço".*
* A definição de cibersegurança pode ser encontrada, por exemplo, na Definition of Cybersecurity - Gaps and overlaps in standardisation[[88]](#footnote-88) pela ENISA, a Agência Europeia para a Segurança Cibernética[[89]](#footnote-89) : *"Cybersecurity" refere-se à segurança do ciberespaço, onde o ciberespaço se refere a um conjunto de ligações e relações entre objectos acessíveis através de uma rede geral de telecomunicações e a um conjunto de objectos cujas interfaces permitem o seu controlo remoto, acesso remoto a dados, ou a sua ligação a acções de gestão dentro do ciberespaço. A cibersegurança incluirá o paradigma "CIA" da tríade de relações e objectos no ciberespaço, e será alargada para assegurar a protecção da privacidade das entidades (pessoas singulares e colectivas) e a resiliência [recuperação de um ataque]".*
* A Directiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de Julho de 2016, relativa a medidas destinadas a assegurar um elevado nível comum de segurança das redes e sistemas de informação em toda a União, declara[[90]](#footnote-90) no n.º 2 do artigo 4.º que *"segurança das redes e sistemas de informação significa a capacidade de as redes e sistemas de informação resistirem, com um determinado nível de confiança, a qualquer acção que comprometa a disponibilidade, autenticidade, integridade ou confidencialidade dos dados armazenados ou transmitidos ou processados ou dos serviços conexos oferecidos por essas redes e sistemas de informação, ou acessíveis através deles".*
* risco também pode ser definido como o potencial para uma ameaça se tornar real e explorar a vulnerabilidade de um activo. De acordo com o Artigo 4 (9) do NIS, um risco é *"qualquer circunstância ou evento razoavelmente identificável que possa ter um impacto negativo na segurança das redes e dos sistemas de informação".* No ciberespaço, os utilizadores, assim como os sistemas e aplicações informáticas estão em risco, assim como outros elementos das TIC.
* Um bem é qualquer coisa que tenha um certo valor para uma pessoa, organização ou estado. Um bem pode ser uma coisa tangível (edifício, sistema informático, redes, energia, bens, etc.) ou intangível (informação, conhecimento, dados, programas, etc.) do ponto de vista do direito civil.
* Contudo, um bem pode também ser uma qualidade (por exemplo, disponibilidade e funcionalidade do sistema e dos dados, etc.) ou um bom nome, reputação, etc. As pessoas (utilizadores, administradores, etc.) e os seus conhecimentos e experiência são também uma mais-valia do ponto de vista da ciber-segurança.
* Vulnerabilidade refere-se à fraqueza de um bem, software, segurança, que é explorado por uma ou mais ameaças. A vulnerabilidade, bem como uma ameaça, pode ser causada por uma série de factores fundamentados no comportamento humano, falha técnica, e possivelmente força maior.

**PALAVRAS-CHAVE A LEMBRAR** 

* ciber-segurança
* CIA
* risco
* activo
* vulnerabilidade
* ciberataque
* Ameaça cibernética

**PERGUNTAS DE VERIFICAÇÃO DE CONHECIMENTOS**  

* que é a tríade da CIA?
* Como é possível definir ciber-segurança?
* Em que elementos consiste a ciber-segurança?
* que é que o termo "bem" cobre?
* Como é possível definir vulnerabilidade?

## Equipas CERT/CSIRT

A Internet conheceu um desenvolvimento e uma comercialização em massa no século XXI. O número de utilizadores, o número de sistemas informáticos ligados à rede global e também o número de serviços críticos em funcionamento aumentou drasticamente, tanto da esfera comercial (por exemplo, bancos electrónicos, lojas electrónicas, leilões electrónicos) como da esfera estatal (por exemplo, administração de serviços de informação estatal e auto-governo, registos). Os incidentes de segurança, ciberataques e crimes cometidos através das tecnologias de informação e comunicação no mundo real e virtual estão a tornar-se cada vez mais graves, e os seus impactos e consequências estão a deteriorar-se.

Uma diferença significativa deste cibercrime de outros tipos de crime é a sua elevada latência, elevado nível de tolerância pela sociedade (incluindo a indiferença do utilizador), o anonimato do perpetrador e a sua identificação frequentemente difícil. Existe uma necessidade crescente de racionalizar a defesa contra estes ataques, em particular para melhorar o ambiente e os meios de localizar o perpetrador, para unificar e formalizar os procedimentos, e para educar os utilizadores a identificar, lidar com e, idealmente, prevenir ameaças e situações de risco. Para este fim, está a ser construída a infra-estrutura das equipas de segurança da CERT e CSIRT.

## História

O primeiro incidente de segurança que afectou negativamente o funcionamento da então Internet ao desligar aproximadamente 10% de todos os dispositivos ligados chama-se o verme Moriss. O verme foi lançado na Internet em 1988 por Robert Morris, um estudante da Universidade de Cornell, nos Estados Unidos. Este incidente iniciou uma era de criação e propagação de vírus informáticos, worms, cavalos de Tróia e outros "vermes electrónicos" semelhantes, referidos colectivamente como *malware*. E foi esta experiência que deu início à discussão sobre a segurança das redes e serviços no final dos anos 80, a fim de formular subsequentemente os princípios básicos de defesa, prevenção e protecção da transmissão de dados sensíveis.

Em resposta ao verme Moriss, a primeira equipa CERT foi formada na Carnegie Mellon University (CMU), nos EUA. Esta primeira CERT ad-hoc foi concebida para examinar o verme Moriss, encontrar uma defesa eficaz, e propor uma solução para a situação difícil. No final, o resultado mais valioso do trabalho da equipa foi descobrir que o mais importante era estar preparado com antecedência para uma quebra de segurança e lançar um plano de defesa e recuperação pré-definido e testado no momento do problema, e não apenas começar a examinar o que precisa de ser feito e quais as medidas a tomar. O resultado do trabalho desta primeira CERT iniciou assim a era da construção de uma infra-estrutura global de equipas deste tipo.

A Carnegie Mellon University registou a abreviatura CERT como marca registada, e embora não se oponha à sua utilização por outras organizações neste contexto (uma organização que deseje utilizar a abreviatura em nome da sua equipa deve solicitar autorização para utilizar a abreviatura e normalmente recebê-la), esta foi a razão do surgimento e introdução do segundo conceito de CSIRT.

## Equipas CERT e CSIRT

CERT (Equipa de Resposta a Emergências Informáticas) e CSIRT (Equipa de Resposta a Incidentes de Segurança Informática). Embora cada um destes acrónimos tenha um significado ligeiramente diferente e principalmente uma génese histórica ligeiramente diferente, ambos os acrónimos podem hoje em dia ser entendidos como o mesmo tipo de equipa - uma equipa que está no seu âmbito de actividade claramente definido responsável por lidar com incidentes de segurança e (ciber)ameaças, do ponto de vista dos utilizadores ou outras equipas, o local a que se podem dirigir com o incidente de segurança detectado, com um pedido de cooperação, troca de informações, assistência, etc.

As equipas CERT/CSIRT são criadas a nível de organizações individuais que medeiam o funcionamento da Internet (ISP - Internet Service Providers), bem como organizações que utilizam o ambiente da Internet para o seu negócio principal (tais como empresas de TI, fornecedores de conteúdos, bancos).

**O dever básico de cada equipa do CSIRT é responder a uma ameaça e cooperar na resolução de incidentes.** Uma equipa CSIRT aborda geralmente um problema que ocorre no seu âmbito de actividade (por exemplo, a sua própria infra-estrutura de rede), ou seja, onde tem possibilidades reais de intervir.

Um CERT/CSIRT de uma determinada rede (organização) é geralmente um ponto de contacto a que os utilizadores podem recorrer com um problema de segurança identificado (ou apenas um problema suspeito) que diz respeito a uma rede informática ou a um dos serviços operados. Uma equipa profissional CERT/CSIRT deve rever cada relatório (incluindo um potencial) incidente de segurança recebido e, se possível, remediar o problema.

Não é nada de revolucionário que não exista na prática, cada grande organização, fornecedor de Internet ou fornecedor de serviços dirige uma equipa de segurança. **A diferença entre uma equipa de segurança regular e uma equipa CERT/CSIRT está principalmente no envolvimento na** infra-estrutura de segurança global**, na** partilha de informação dentro desta infra-estrutura **e na observância** dos procedimentos formais estabelecidos.

A existência de pelo menos uma equipa oficial CERT/CSIRT é desejável em cada rede operada, especialmente nas grandes redes (de trânsito, regionais, universitárias), ou seja, ao nível dos grandes ISP, mas também ao nível dos bancos ou prestadores de serviços.

As **equipas de topo** globais dentro de cada Estado têm um **papel** significativo e **específico** - as chamadas equipas **nacionais** e **governamentais**, às quais será dedicado um subcapítulo separado.

Globalmente, as equipas CERT/CSIRT existentes podem ser vistas como uma infra-estrutura que trata de problemas de segurança na Internet. No trabalho, uma equipa CERT/CSIRT baseia-se principalmente na sua experiência, procedimentos pré-preparados e comprovados e na cooperação e troca de informação com outras equipas CERT/CSIRT.

**O requisito básico de uma comunidade é que a equipa CERT/CSIRT declare publicamente as suas** informações de contacto **e as suas** regras de actividade:

* que é o seu operador,
* que são os seus membros,
* a forma e quando é possível chegar à equipa,
* quais os serviços que oferece,
* âmbito de actividade (AS número[[91]](#footnote-91) , rede, domínios, serviços), em que a equipa está qualificada para actuar e de que forma, ou seja, definindo os seus poderes e responsabilidades. Com base no âmbito de actividade, a equipa é então contactada (por exemplo, pelos atacados) e aborda as questões (incidentes) a ela associadas.

O conceito de abordar um incidente de segurança pode ter diferentes especificidades dependendo das configurações da equipa e da sua política interna - pode ser uma simples eliminação de um ataque (destruição da origem do problema, por exemplo, desligando o sistema informático comprometido da rede), rastreando o atacante, retomada rápida do funcionamento do serviço/rede infectado, etc.

Dependendo das actividades da equipa na resolução de um incidente de segurança, as equipas podem ser descritas como internas (institucionais) ou de coordenação. O tipo interno da equipa tem normalmente a possibilidade de intervenção directa (desligar a fonte do problema, introduzir filtragem de tráfego na rede, etc.), o tipo de coordenação da equipa não tem a possibilidade de intervenção directa, as suas actividades centram-se na comunicação, cooperação e mediação de informação (são normalmente equipas nacionais, que serão discutidas a seguir).

No caso de abordar um incidente específico, os participantes tentam abordá-lo directamente na fonte, ou seja, com quem está mais próximo da fonte ou do destino do incidente e podem intervir da forma mais eficaz possível (administrador da rede ou dos serviços finais). A situação ideal ocorre quando a fonte e o alvo se encontram no âmbito de uma equipa CSIRT, porque é muito fácil e rápido encontrar um perito específico no local do problema. O perito pode então também abordar o problema de forma eficaz e as suas reacções são previsíveis, uma vez que publicou voluntariamente as suas regras do jogo. Este procedimento de comunicação é muito flexível, devido ao facto de a comunicação não passar por diferentes níveis. É rápido e preciso. Então a reacção pode ser a mesma. No entanto, se a vítima não conseguir encontrar uma contrapartida adequada (quer porque não existe, quer porque não dá qualquer informação útil sobre si própria, recusa-se a abordar o problema ou simplesmente não reage), uma "alavanca" seria apropriada. Isso pode ser normalmente, em certa medida, fornecido por equipas de topo - nacionais e governamentais.

## Como é formada uma equipa CERT/CSIRT

Uma organização que decida criar uma equipa CERT/CSIRT deve inicialmente definir de forma clara e compreensível o que pretende alcançar com a criação da equipa, que papel requer da equipa (ou seja, especifica o seu âmbito, poderes, responsabilidades e serviços operados) e deve também assegurá-lo de forma adequada na organização.

**Âmbito de** actividade

O âmbito da actividade é normalmente a área do ciberespaço em que a equipa está qualificada para actuar e sobre a qual tem os poderes e responsabilidades relevantes definidos pelo fundador. Com base no âmbito de actividade declarado, a equipa é então contactada, por exemplo, pelos atacados, e aborda problemas na esfera da sua influência. O âmbito de actividade de uma equipa pode ser definido como rede(s) específica(s), sistema(s) autónomo(s), domínio(s) de nome, mas há também equipas que listam a sua perícia, serviço específico, etc. como o âmbito de actividade.

**Serviços**

Para que uma equipa seja oficialmente designada por CERT/CSIRT, precisa de oferecer principalmente um serviço de resolução ou coordenação de incidentes de segurança dentro do seu âmbito definido, cumprindo assim a ideia de "resposta" utilizada nas siglas CERT/CSIRT, ou seja, esta equipa precisa de ser capaz de *responder* a um incidente de segurança. Contudo, a equipa pode oferecer uma série de outros serviços de muitas áreas, tais como formação, aviso de ataques actuais, vulnerabilidades de SO, auditorias de segurança, consultas SW, recomendações de regras básicas de segurança, desenvolvimento e operação de ferramentas de monitorização do tráfego de rede e serviços e muito mais.

**Membros da equipa**

A área que tem uma influência decisiva sobre a qualidade da equipa é o seu pessoal. Em cada rede operada, existe normalmente um departamento ou grupo de técnicos que são responsáveis pelo funcionamento e desenvolvimento da rede e serviços e que também se ocupam de aspectos de segurança (geralmente "pessoal informático", "pessoal de segurança", "administradores", etc.). Estas são geralmente as pessoas certas para integrar uma equipa CERT/CSIRT ou para serem designadas para a construir. Contudo, é aconselhável ter outros tipos de peritos na equipa (como um advogado, ou, no caso de equipas nacionais e governamentais, pode ser útil um oficial de ligação dos meios de comunicação social, um gestor, um sociólogo, etc.). Depende do foco, do ambiente, dos serviços oferecidos e do papel da equipa.

De um ponto de vista "externo", uma equipa torna-se uma equipa CERT/CSIRT quando é aceite como tal por outras equipas CERT/CSIRT globais existentes. O caminho para obter o estatuto de equipa CERT/CSIRT não é complicado, no início é suficiente para declarar claramente o seguinte

1. **Informações básicas de contacto** - nome da equipa, nome da organização que dirige a equipa, endereço(s) de correio electrónico da equipa onde os incidentes de segurança podem ser comunicados ou a equipa pode ser contactada, número(s) de telefone da equipa, endereço da sede, nomes dos membros da equipa, horários de trabalho para os quais a equipa pode ser contactada, etc.
2. **Âmbito de actividade da equipa** - define o que é da responsabilidade da equipa e qual é o seu papel. Isto, claro, depende da equipa que é. É possível criar equipas de aproximadamente os seguintes tipos:

* ***interno*** - serve e é responsável por uma rede específica (por exemplo, por uma gama específica de endereços IP, domínios), normalmente criada pelo operador de rede,
* ***coordenação*** - uma equipa cuja principal tarefa é coordenar a resolução de incidentes de segurança, não tem de os abordar de uma forma direccionada,
* ***fornecedor*** - uma equipa que se ocupa da resolução de incidentes de segurança que afectam um produto específico (SW),
* ***nacional, governamental*** - casos especiais baseados nos princípios das duas primeiras equipas mencionadas (interna e coordenação), o seu âmbito e papel dependem do fundador e muitas vezes também da legislação de um determinado país.

1. **Serviços oferecidos** - a equipa CERT/CSIRT deve fornecer pelo menos um serviço de resolução de incidentes de segurança.

Depois de uma equipa CSIRT/CERT recentemente estabelecida ter tratado dos passos acima referidos e estabelecido uma política básica de equipa para lidar com incidentes de segurança, que inclui a classificação da gravidade do incidente, regras de resposta ao incidente, contabilização dos membros da equipa, regras de comunicação com o autor do relatório do incidente de segurança, etc., está no bom caminho para ser aceite pelas equipas adjacentes. Uma parte natural e necessária é a necessidade de se familiarizar com as regras básicas acordadas pela comunidade CSIRT e de as seguir.

Logo no início da criação de uma equipa do tipo CERT/CSIRT é também a criação dos seus antecedentes técnicos e organizacionais, sem os quais nenhuma equipa pode funcionar eficazmente.

**O contexto técnico** significa, por exemplo, um instrumento de gestão eficaz dos relatórios de incidentes de segurança, que permite a monitorização de todo o seu ciclo de vida, ou seja, quando o relatório foi enviado, por quem, em que fases do incidente, porquê, como se processou, quem pediu a quem cooperar, qual a gravidade do incidente e que procedimentos de escalonamento lhe foram aplicados, etc. Para esta área, as equipas utilizam normalmente vários sistemas chamados de bilhética, por exemplo, RTIR[[92]](#footnote-92) , OTRS[[93]](#footnote-93) . Outras ajudas importantes no domínio das ferramentas técnicas são vários IDS (Intrusion Detection System), sistemas de auditorias de segurança de redes e equipamentos, sistemas de análise forense, monitorização do tráfego de rede (netflow), etc.

O **contexto organizacional** representa precisamente a mencionada "prontidão" para o problema, ou seja, a definição das regras básicas para o funcionamento da equipa, para que cada membro da equipa conheça o seu papel, deveres e responsabilidades, a política de resolução de incidentes de segurança, regras de comunicação, partilha e intercâmbio de informação, cooperação, etc. A base nesta área é geralmente uma ***gestão de incidentes*** bem gerida.

No momento em que a equipa recém-formada gere o acima exposto, ou seja, é capaz de se descrever a si própria e às suas actividades e de as levar a cabo. Pode participar na cooperação a nível nacional e internacional.

## Cooperação em infra-estruturas CERT/CSIRT

As equipas CERT/CSIRT são constituídas numa base voluntária, e é do seu interesse comunicar eficazmente entre si, trocar informações e conhecimentos importantes e cooperar. Por conseguinte, associam-se em organizações internacionais. Actualmente, as organizações mais conhecidas e activas que lidam com esta questão e criam um ambiente adequado para os objectivos acima referidos são as organizações internacionais **GÉANT**[[94]](#footnote-94) e **FIRST** (Forum for Incident Response and Security Teams)[[95]](#footnote-95) .

Ambas as organizações acima referidas iniciam e permitem reuniões regulares dos membros das equipas de segurança, troca de experiências e participam na definição das regras básicas de cooperação e comunicação entre as equipas CERT/CSIRT do mundo.

A organização europeia GÉANT gere várias actividades nas quais as equipas CERT/CSIRT mundiais podem participar se estiverem interessadas:

* **TF-CSIRT** (Task Force for CSIRT) é um grupo de trabalho que permite às equipas trabalharem em conjunto sob a forma de reuniões regulares de dois a três dias, que têm lugar 3 vezes por ano. (Esta reunião é geralmente organizada por uma equipa CERT/CSIRT.) Mais informações podem ser encontradas em: https://tf-csirt.org/.
* **Formação CSIRT** - utilizada para formar novos membros de equipas CSIRT/CERT, ou para aqueles que vão estabelecer uma equipa CERT/CSIRT. Realiza-se geralmente duas vezes por ano e os formadores são membros experientes de equipas CERT/CSIRT de renome e de outros peritos de segurança de topo. Mais informações podem ser encontradas em: [https:](https://tf-csirt.org/transits/)//tf-csirt.org/transits/.
* **Trusted Introducer**[[96]](#footnote-96) - um escritório cuja principal tarefa é criar confiança entre diferentes equipas CERT/CSIRT e ajudar na criação de novas equipas. Mais informações podem ser encontradas em: [https:](https://www.trusted-introducer.org/)//www.trusted-introducer.org/.

Para além da grande conferência anual realizada anualmente, FIRST organiza uma série de sessões de formação, cria directrizes e normas para o trabalho eficaz das equipas CERT/CSIRT e, naturalmente, coopera com a actividade TF-CSIRT.

Dentro da infra-estrutura global das equipas CERT/CSIRT, GÉANT e FIRST actuam como uma espécie de "garantia" de que a equipa que afirma ser uma equipa CERT/CSIRT é realmente assim, e que o padrão de conduta declarado é verdadeiro. Cada nova equipa que queira aderir à infra-estrutura de segurança passa por um processo de entrada que verifica que a equipa cumpre os padrões da comunidade, é transparente, e não há razões de força maior para a aceitar. No caso da infra-estrutura europeia (plataforma TF-CSIRT), este processo de entrada é fornecido pelo Introdutor de Confiança e é efectivamente solicitado pela nova equipa para se registar na lista de equipas e obter o estatuto de ***membro da lista.****[[97]](#footnote-97)*

Entre as equipas existentes, deve haver também pelo menos duas equipas (os chamados patrocinadores) que irão apoiar uma nova equipa, e nenhuma equipa já estabelecida pode objectar à sua aceitação. Se tudo correr bem, a informação sobre a nova equipa é armazenada numa lista mantida pela TI (e parte dela é publicada), a equipa recebe o estatuto ***listado***, e a comunidade dá as boas-vindas ao novo membro.

No caso do FIRST, o procedimento de entrada é muito semelhante, terminando apenas não pela concessão do estatuto, mas pela obtenção da ***qualidade de membro.***

Ambos os processos têm uma coisa em comum - trata-se de determinar e divulgar a quantidade máxima de informação sobre uma dada equipa, descrever a sua conduta e perceber a questão da resolução de incidentes de segurança de modo a que corresponda às exigências da comunidade.

No caso do Introdutor de Confiança, é possível alcançar outros estatutos, mais significativos, nomeadamente os estatutos ***acreditados*** e ***certificados.*** As diferenças são as seguintes:

* Uma equipa com o estatuto alcançado forneceu informações básicas sobre si própria, declarou o desejo de se comportar como uma equipa CSIRT e a comunidade aceitou-o.
* Uma equipa com o estatuto ***acreditado*** declara à comunidade o nível exigido dos seus procedimentos e está empenhada em aderir a políticas de TI comuns.
* Uma equipa com o estatuto de ***certificada*** provou então o seu "nível de maturidade" (maturidade) no âmbito do processo de certificação.

Ser uma equipa ***acreditada*** ou ***certificada*** requer um esforço contínuo para manter o estatuto da equipa. Parte deste esforço é também a obrigação de manter a informação da equipa actualizada na lista da TI. Se a equipa não o fizer a longo prazo, pode perder o seu estatuto e, na pior das hipóteses, ser expulsa pela comunidade. Esta obrigação aplica-se também às equipas ***listadas***, as quais, se não passarem no processo de acreditação no prazo de três anos após a obtenção do estatuto listado, devem renovar o seu estatuto listado, demonstrando o apoio de outras equipas (ou seja, um processo de re-listagem). Este mecanismo assegura um elevado grau de actualidade da informação da lista de TI e, por conseguinte, a sua credibilidade.

Outra organização activa no domínio da segurança é a **ENISA** (Agência Europeia para a Segurança das Redes e da Informação, http://www.enisa.europa.eu/). Trabalha em estreita colaboração com os Estados-Membros da UE e o sector privado e abrange uma série de actividades, incluindo exercícios pan-europeus de cibersegurança, o desenvolvimento de estratégias nacionais de cibersegurança, a cooperação entre equipas CERT/CSIRT e o desenvolvimento de capacidades, abordando questões de protecção de dados e trabalhando em conjunto para criar e implementar legislação em matérias relacionadas com a Segurança da Informação em Rede (SRI).

As três organizações mencionadas têm mais uma função comum - reúnem o know-how de toda a comunidade e permitem a sua partilha (através da formulação dos chamados documentos de melhores práticas, instruções, recomendações).

## Hierarquia das equipas CERT/CSIRT?

**As equipas CERT/CSIRT não têm uma hierarquia oficial** que torne uma equipa superior a outra. Todas as equipas são iguais em termos de funcionamento, comunicação, cooperação e troca de informação e não estão limitadas nestas áreas. A existência das chamadas equipas nacionais e governamentais de topo sugere de certa forma que existe uma hierarquia entre as equipas, embora não seja esse o caso. A única "hierarquia", mas seria mais apropriado dizer "maior capacidade de acção", dá à equipa de topo a legislação do país, que regula os seus poderes (por exemplo, na área da resposta necessária às ameaças de segurança dos operadores de rede e serviços, etc.).

No mundo das equipas CERT/CSIRT, a vontade de partilhar informações importantes sobre um incidente e ameaças é fundamental. Para tal, é essencial que as equipas confiem umas nas outras e também que os utilizadores confiem nas suas equipas. Ganhar a confiança dos utilizadores e da comunidade é uma tarefa a longo prazo. As equipas devem mostrar as suas qualidades em todos os aspectos do seu funcionamento e construir credibilidade gradualmente - não só com a capacidade de ajudar, mas também com a capacidade de assegurar a confidencialidade e o tratamento justo dos dados partilhados, transparência de conduta, etc.

## Equipas nacionais e governamentais CERT/CSIRT

As equipas nacionais e governamentais são uma forma especial de equipas CERT/CSIRT. Tratam as outras equipas CERT/CSIRT como iguais, mas o seu papel em todo o sistema é diferente.

**O CERT/CSIRT nacional** actua como uma espécie de último recurso onde é possível pedir intercessão, assistência e intervenção. O seu objectivo é (dentro do estado ou área onde opera) mediar o contacto entre uma vítima e um perpetrador do problema e ajudar a resolver o problema com sucesso. As equipas nacionais (geralmente) não controlam as infra-estruturas físicas, pelo que não têm (ao contrário das equipas internas/institucionais) a oportunidade de intervir directamente. O seu papel consiste em mediar o contacto, ou em coordenar (daí que este tipo de equipa se chame equipa de coordenação) o procedimento de resolução de problemas individuais no caso de o problema ser mais extenso e a sua solução exigir a cooperação de várias componentes.

A partir do princípio do funcionamento de toda a estrutura, os incidentes que passam pelo sistema do CSIRT nacional são normalmente apenas uma fracção do número total. A maioria dos incidentes são resolvidos através de comunicação directa, sem necessidade de escalonamento e mediação. A equipa nacional recebe assim, na sua maioria, incidentes que não podem ser resolvidos de outra forma (os responsáveis recusam-se a resolvê-los; não é fácil identificar quem é responsável pela sua resolução), problemas muito graves ou recorrentes, ou problemas que podem ter um impacto geral, etc.

O CERT/CSIRT nacional tem geralmente formação e cooperação na sua descrição de funções. É ao mesmo tempo uma consciencialização em relação ao público e uma operação dentro da infra-estrutura da Internet. O objectivo é apoiar a criação de equipas adicionais CERT/CSIRT no país, a sua introdução na cena internacional e o apoio na implementação de procedimentos e métodos padrão. Tudo isto aumenta significativamente a transparência do ambiente e dá às vítimas uma oportunidade de procurar reparação eficaz.

Uma **CERT/CSIRT** governamental concentra-se geralmente na área da administração estatal e auto-governo e na resolução de incidentes que ameaçam a segurança do Estado e dos seus serviços. Uma CERT/CSIRT governamental pode tomar a forma de uma equipa interna com a possibilidade de intervenção directa no caso de um problema. A sua existência é geralmente apoiada por legislação.

No entanto, o acima exposto não é dogma, e a situação varia de país para país. Há países onde apenas a equipa nacional trabalha (e também serve como equipa governamental); há países onde a equipa governamental trabalha (e desempenha o papel da equipa nacional); há países onde ambos existem; há países onde não existe nenhum deles e o papel da equipa de topo é substituído por uma das equipas existentes, etc.

## Situação na República Checa e no mundo

Actualmente, cerca de 380 equipas de segurança CERT/CSIRT são oficialmente constituídas em todo o mundo, que são membros do FIRST ou da plataforma europeia TF-CSIRT (ou de ambos).

Na República Checa, 39 equipas de segurança do tipo CERT/CSIRT são actualmente oficialmente estabelecidas e reconhecidas pelo Introdutor de Confiança, o que torna a República Checa quase uma "superpotência" mundial, com apenas a França, a Alemanha e o Reino Unido a competir em números. Evidentemente, não se trata de quantidade, mas sobretudo de qualidade.

A primeira equipa de segurança CERT/CSIRT que foi estabelecida na República Checa é a equipa de segurança **CESNET-CERTS** [(](https://csirt.cesnet.cz/)https://csirt.cesnet.cz/). Foi oficialmente constituída em 2003, e em Janeiro de 2004 foi oficialmente reconhecida pela infra-estrutura internacional e pelo Introdutor de Confiança. É operada pela associação CESNET[[98]](#footnote-98) e é responsável por abordar e coordenar a resolução de incidentes de segurança na infra-estrutura electrónica CESNET. Entre outras coisas, trata do desenvolvimento de ferramentas de segurança e também fornece serviços educativos para os utilizadores na sua esfera de influência.

Outras equipas foram fundadas na associação CZ.NIC (CZ.NIC-CSIRT) em 2008, na Universidade Masaryk em Brno (CSIRT-MU) em 2009, na empresa Active24 (equipa Active24-CSIRT) em 2012 e no âmbito de um projecto apoiado pelo Ministério do Interior da República Checa equipa CSIRT.CZ (desde 2011 National CSIRT CR).

Podemos observar um grande boom no campo da construção de equipas de segurança CERT/CSIRT na República Checa, especialmente desde 2013, quando a República Checa enfrentou uma série de ataques DDoS a serviços públicos na Internet. Este evento iniciou subsequentemente a criação do projecto Fenix [(https://fe.nix.cz/](https://fe.nix.cz/)) no terreno do centro de peering checo NIX.CZ.

O objectivo deste projecto é permitir a disponibilidade de serviços Internet dentro das entidades envolvidas nesta actividade no caso de um ataque do DoS. O projecto Fenix definiu uma série de regras técnicas e organizacionais que os interessados em aderir ao projecto devem cumprir, e uma delas é também uma equipa CERT/CSIRT oficialmente constituída. Este foi um impulso para muitas organizações formalizarem as suas equipas de segurança numa equipa CERT/CSIRT e integrá-las na infra-estrutura internacional.

Outro impulso motivador que levou à constituição de novas equipas é a adopção e subsequente eficácia da lei sobre ciber-segurança. Muitas organizações compreenderam que a segurança vale a pena e que a criação de uma CERT/CSIRT traz benefícios.

A infra-estrutura actual das equipas CERT/CSIRT na República Checa, com 39 equipas, é constituída por uma equipa nacional e governamental, existem equipas a nível de grandes ISP, várias equipas no sector académico, equipas na indústria bancária, empresas de TI, registadores de domínios e, por último mas não menos importante, no terreno do centro de peering checo NIX.CZ, no terreno da associação CZ.NIC. Em conjunto, esta é uma infra-estrutura muito diversificada e, como resultado, robusta e viável, que inclui a experiência de várias indústrias.

**A lista actual das equipas checas CERT/CSIRT pode ser encontrada em:** <https://tiw.trusted-introducer.org/directory/country_LICSA.html>

## CSIRT Nacional da República Checa

Em Dezembro de 2010, a República Checa também estabeleceu oficialmente o CSIRT Nacional da República Checa. A Associação CZ.NIC e o Ministério do Interior assinaram (a 16 de Dezembro de 2010) um Memorando segundo o qual o administrador do domínio nacional checo da Associação CZ.NIC assumiu a agenda da equipa CSIRT.CZ e desde Janeiro de 2011 tem vindo a operá-la como o CSIRT Nacional da CR.

A prática CSIRT.CZ (http://www.csirt.cz/) foi estabelecida no âmbito de uma subvenção do Ministério do Interior da República Checa "*Cyber threats and Czech Republic's security interests*" (o código de identificação do projecto é VD20072010B013) e foi construída pela CESNET. Esta prática foi referida como um modelo e foi construída para verificar o estado das infra-estruturas de segurança na República Checa e para verificar a viabilidade da construção de uma hierarquia distribuída para uma solução sistemática e abrangente das questões de segurança nas redes informáticas checas através de equipas CSIRT. O funcionamento desta equipa foi oficialmente lançado a 3 de Abril de 2008. Em Maio do mesmo ano, foi apresentada a outras equipas europeias CERT/CSIRT na reunião da comunidade TF-CSIRT (que teve lugar em Oslo, Noruega) como uma prática do CSIRT com o papel de "*último recurso"* para a República Checa e, como tal, foi aceite pela comunidade.

A prática do CSIRT.CZ lançou as bases para o desenvolvimento futuro do nível superior da infra-estrutura CERT/CSIRT na República Checa, especialmente na área da cooperação. Ao mesmo tempo, verificou e confirmou a presunção de que as equipas de topo CERT/CSIRT na República Checa fazem sentido.

O CSIRT Nacional da República Checa executa também outras tarefas do CS.

## CERT do Governo da República Checa

Em 19 de Outubro de 2011, o Governo da República Checa adoptou a Resolução n.º 781 sobre a criação da Autoridade Nacional de Segurança (*Národní bezpečnostní úřad* - NBU) como guardiã das questões de cibersegurança na República Checa e, ao mesmo tempo, a autoridade nacional nesta área. Desde o início da sua nomeação, a NBU tem-se concentrado em três tarefas - redigir a lei sobre cibersegurança, construir o NCKB (*Národní centrum kybernetické bezpečnosti* - National Cyber Security Centre) e construir o CERT do Governo da República Checa.

O Governo CERT da República Checa, a equipa GovCERT.CZ, foi incorporada na comunidade internacional em 2012, tornando a República Checa num dos países que tem uma equipa nacional e governamental CERT/CSIRT.

A competência do GovCERT.CZ inclui redes de administração estatal, auto-governo e infra-estruturas críticas da República Checa. A equipa também se concentra no desenvolvimento e operação de serviços de segurança, educação e também está envolvida na cooperação nacional e internacional.

O CERT do Governo da República Checa também desempenha outras tarefas.

## Qual a equipa CERT/CSIRT a contactar?

O título deste subcapítulo é também um lamento frequente de um utilizador da Internet que se meteu em problemas (por exemplo, alguém o atacou, roubou a sua identidade, invadiu um perfil do Facebook ou uma conta de e-mail, ou testemunhou a propagação de pornografia infantil). O que deve um tal utilizador fazer? Contactar a Polícia da República Checa? Ou o fornecedor de serviços de Internet, por exemplo o seu helpdesk? Ou contactar a Agência Nacional de Cibersegurança e Segurança da Informação quando esta é responsável pela ciber-segurança? A linha directa do [National Safer Internet Center](http://www.ncbi.cz/)? Ou alguma equipa do CSIRT quando ainda se fala neles? Mas qual delas?

**O processo de comunicação e resolução de incidentes de segurança** (ou por outras palavras "quem contactar se eu quiser comunicar ou resolver um incidente de segurança") **pode ser visto de duas perspectivas.** Da perspectiva dos técnicos (administradores de redes e serviços, membros de equipas de segurança) e da perspectiva dos utilizadores.

Para os técnicos (administradores de redes e serviços, membros de equipas de segurança), a resposta à pergunta "quem contactar efectivamente com um pedido de acção" é bastante clara, mas isto deve-se ao exercício, à experiência e sobretudo a um conhecimento muito bom do ambiente da Internet e dos seus princípios básicos, bem como ao conhecimento de onde se encontram disponíveis informações de contacto para redes individuais existentes, serviços, domínios, etc.

Para os membros das equipas CERT/CSIRT, as fontes básicas de informação de contacto são as bases de dados RIR, a base de dados dos operadores de domínio de primeiro nível e os catálogos das equipas CERT/CSIRT.

**O RIR** (Registo Regional da Internet) detém e disponibiliza informação sobre a quem foi atribuído um bloco de endereços IP. O mundo está dividido em regiões e cada RIR (actualmente RIPE, ARIN, APNIC, LACNIC, AFRINIC) atribui endereços IP para a sua região. A região da Europa, Médio Oriente e Ásia é administrada pela RIPE NCC [(](https://www.ripe.net/)https://www.ripe.net/). Os RIRs operam bases de dados acessíveis ao público que contêm dados sobre redes Internet atribuídas e os seus administradores. Estas bases de dados permitem-lhe encontrar informações sobre quais as organizações e quais os administradores responsáveis por endereços IP específicos.

Outra fonte de informação útil são os dados sobre domínios operados e disponibilizados pelos administradores de domínios de topo; para o domínio TLD . cz, é a associação CZ.NIC.

E depois há a área das equipas CERT/CSIRT, que normalmente definem o seu âmbito utilizando identificadores da Internet, domínios de nomes, ou apenas verbalmente. Devido ao seu número, à forma como definem o seu âmbito e especialmente às diferenças no seu nível, nem sempre é fácil encontrar uma equipa que seja capaz de ajudar. Para facilitar a orientação entre equipas, foram criados alguns tipos de "catálogos", que são tratados pelo FIRST e pelo Trusted Introducer. Estes catálogos contêm informações básicas sobre CERT/CSIRTs, contactos, o seu alcance, etc.

O processo de notificação e resolução de incidentes de segurança (**tratamento de incidentes**) não é um processo exacto, pelo contrário, e muito depende da experiência e por vezes da criatividade da pessoa que executa este processo. A troca de informação entre equipas realiza-se normalmente de forma rápida e eficiente, embora mesmo isto muitas vezes não garanta uma solução rápida para o problema, porque toda a infra-estrutura é ainda relativamente "escassa", e infelizmente deve notar-se que o nível das equipas é diferente.

**O estado óptimo da infra-estrutura seria se cada endereço IP estivesse no âmbito de uma equipa oficial do CSIRT.** Esta não é, contudo, de longe, a situação da infra-estrutura do CERT/CSIRT.

Do ponto de vista de um utilizador normal, a situação é muito pouco clara e, na realidade, confusa. Então, o que deve um utilizador fazer se for detectado um incidente de segurança e quem deve contactar? É difícil para o utilizador querer orientar-se nas questões das equipas CERT/CSIRT, ser capaz de encontrar a correcta, estudar a sua política de comunicação de incidentes de segurança e tomar medidas. Um utilizador deve primeiro contactar o administrador da sua rede ou serviços (se tiver alguém assim), ou deve cooperar com o fornecedor de serviços da Internet, ou seja, com o helpdesk do seu ISP ou com o seu apoio ao utilizador. Por parte do ISP ou do fornecedor de serviços, deve haver um ponto de entrada (contacto) claramente descrito, que os utilizadores podem e devem contactar se forem alvo de um ataque, detectar um incidente de segurança, ou sentir que algo não está bem. É por isso que o ambiente dos ISPs é uma das áreas mais importantes onde uma equipa oficial CERT/CSIRT deve ser constituída e fornecer serviços de segurança aos utilizadores da sua rede.

É claro que pode haver situações em que tanto um técnico como um utilizador fazem tudo bem, e a solução para o problema ainda não está à vista. Uma pessoa ou equipa não reage ao problema relatado, ou mesmo recusa-se a resolvê-lo (dizendo que não é o seu problema, ou que não é tão grave), etc. Este é o momento em que ou entra a Polícia da República Checa (o utilizador pode contactá-la com a apresentação de uma queixa criminal), ou entra uma equipa de topo (nacional ou governamental) que o utilizador pode contactar como último recurso a partir do qual se pode esperar ajuda e resposta.

Existe uma cooperação muito estreita e troca de informações e dados relevantes entre a **equipa nacional e a equipa governamental**, e portanto a transferência do problema relatado para ser tratado de uma equipa para outra ou directamente para a solução.

Em geral, a equipa nacional e governamental deve ser um lugar para fornecedores de redes, prestadores de serviços (e, se necessário, utilizadores) onde, em caso de problemas, ambiguidades, etc., é possível pedir ajuda e consulta, por exemplo, encontrar uma contraparte adequada para a comunicação (equipa estrangeira CERT/CSIRT), mediação de comunicação (sim, por vezes a "alavanca" da equipa de topo é útil, a contraparte está então mais disposta), e uma fonte de know-how e informação.

**Em geral, contudo, seria desejável que os administradores de redes e serviços e os membros das equipas de segurança dominassem e aplicassem os princípios do processo de tratamento de incidentes e maximizassem a comunicação directamente** (não através de equipas de topo). Isto torna o processo de tratamento de incidentes rápido e eficiente, e outras fases intermédias podem introduzir atrasos desagradáveis e, infelizmente, distorções. Mas, como já foi mencionado, depende da gravidade da situação e do problema a ser tratado.

**Os CERT/CSIRTs e as suas infra-estruturas não são geralmente omnipotentes e não garantem a segurança "em poucas palavras".**

A sua existência é apenas um dos pequenos blocos no campo da construção da segurança na Internet, no qual todos os intervenientes desempenham um papel importante, ou seja, administradores de redes, gestores de serviços, gestores que decidem sobre os antecedentes para uma segurança eficaz de redes e serviços, ISPs, operadores de serviços críticos, forças de segurança, estado, e por último, mas não menos importante, nós, utilizadores.

**A lista actual das equipas CSIRT/CERT pode ser encontrada em:**

[https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map.](https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map)

**RESUMO / PRINCIPAIS RESULTADOS DO CAPÍTULO** 

* A diferença entre uma equipa de segurança regular e uma equipa CERT/CSIRT está principalmente no envolvimento na infra-estrutura de segurança global, na partilha de informação dentro desta infra-estrutura e na observância dos procedimentos formais estabelecidos.
* requisito básico de uma comunidade é que a equipa CERT/CSIRT declare publicamente as suas informações de contacto e as suas regras de actividade:
  + que é o seu operador,
  + que são os seus membros,
  + a forma e quando é possível chegar à equipa,
  + quais os serviços que oferece,
  + âmbito de actividade (AS número[[99]](#footnote-99) , rede, domínios, serviços), em que a equipa está qualificada para actuar e de que forma, ou seja, definindo os seus poderes e responsabilidades. Com base no âmbito de actividade, a equipa é então contactada (por exemplo, pelos atacados) e aborda as questões (incidentes) a ela associadas.
* Âmbito de actividade da equipa - define o que é da responsabilidade da equipa e qual é o seu papel. Isto, claro, depende da equipa que é. É possível criar equipas de aproximadamente os seguintes tipos:
  + interno - serve e é responsável por uma rede específica (por exemplo, por uma gama específica de endereços IP, domínios), normalmente criada pelo operador de rede,
  + coordenação - uma equipa cuja principal tarefa é coordenar a resolução de incidentes de segurança, não tem de os abordar de uma forma direccionada,
  + fornecedor - uma equipa que se ocupa da resolução de incidentes de segurança que afectam um produto específico (SW),
  + nacional, governamental - casos especiais baseados nos princípios das duas primeiras equipas mencionadas (interna e de coordenação), o seu âmbito e papel dependem do fundador e muitas vezes também da legislação de um determinado país.
* As equipas CERT/CSIRT não têm uma hierarquia oficial que tornaria uma equipa superior a outra. Todas as equipas são iguais em termos de funcionamento, comunicação, cooperação e troca de informação e não estão limitadas nestas áreas.
* CERT/CSIRT nacional actua como uma espécie de último recurso - a última instância onde é possível pedir intercessão, assistência e intervenção.
* Uma CERT/CSIRT governamental concentra-se geralmente na área da administração estatal e auto-governo e na resolução de incidentes que ameaçam a segurança do Estado e dos seus serviços. Uma CERT/CSIRT governamental pode tomar a forma de uma equipa interna com a possibilidade de intervenção directa no caso de um problema. A sua existência é geralmente apoiada por legislação.

**PALAVRAS-CHAVE A LEMBRAR** 

* Equipa CSIRT
* Equipa CERT
* Tratamento de incidentes
* Hierarquia das equipas
* Âmbito de actividade

**PERGUNTAS DE VERIFICAÇÃO DE CONHECIMENTOS**  

* que é uma equipa CSIRT/CERT?
* Como é criada e estabelecida uma equipa CSIRT/CERT?
* Em que se concentra a equipa nacional do CSIRT?
* Em que se concentra a equipa do CSIRT do governo?
* Quais são os requisitos básicos da comunidade para uma equipa CERT/CSIRT?

## Quadro legislativo do CSIRT/CERT

A 6 de Julho de 2016, a Directiva (UE) 2016/1148 do Parlamento Europeu e do Conselho de 6 de Julho de 2016 relativa a medidas para um elevado nível comum de segurança das redes e sistemas de informação em toda a União (a Directiva SRI) foi adoptada pelo Parlamento Europeu.

A Directiva NIS prevê medidas legais para aumentar o nível global de segurança cibernética na UE, garantindo

* A preparação dos Estados-Membros, exigindo-lhes que estejam devidamente equipados. Por exemplo, com uma Equipa de Resposta a Incidentes de Segurança Informática (CSIRT) e uma autoridade nacional competente em matéria de NIS,
* cooperação entre todos os Estados-membros, através da criação de um Grupo de Cooperação para apoiar e facilitar a cooperação estratégica e o intercâmbio de informações entre os Estados-membros.
* uma cultura de segurança através de sectores vitais para a nossa economia e sociedade e que, além disso, dependem fortemente das TIC, tais como energia, transportes, água, banca, infra-estruturas do mercado financeiro, cuidados de saúde e infra-estruturas digitais.

As empresas identificadas pelos Estados-membros como operadores de serviços essenciais nos sectores acima referidos terão de tomar as medidas de segurança adequadas e notificar as autoridades nacionais competentes de incidentes graves. Os principais fornecedores de serviços digitais, tais como motores de busca, serviços de computação em nuvem e mercados em linha, terão de cumprir os requisitos de segurança e notificação ao abrigo da nova directiva.

Com base nos progressos significativos realizados no âmbito do Fórum Europeu dos Estados-Membros para promover debates e intercâmbios sobre boas práticas políticas, incluindo o desenvolvimento de princípios para a cooperação europeia em matéria de cibercrise, deverá ser criado um Grupo de Cooperação, composto por representantes dos Estados-Membros, da Comissão e da Agência da União Europeia para a Segurança das Redes e da Informação ("ENISA"), para apoiar e facilitar a cooperação estratégica entre os Estados-Membros em matéria de segurança das redes e dos sistemas de informação. Para que esse grupo seja eficaz e inclusivo, é essencial que todos os Estados-Membros tenham capacidades mínimas e uma estratégia que garanta um elevado nível de segurança das redes e dos sistemas de informação no seu território. Além disso, os requisitos de segurança e notificação devem aplicar-se aos operadores de serviços essenciais e aos fornecedores de serviços digitais para promover uma cultura de gestão de riscos e assegurar que os incidentes mais graves sejam comunicados.

As capacidades existentes não são suficientes para garantir um elevado nível de segurança das redes e dos sistemas de informação dentro da União. Os Estados-Membros têm níveis de preparação muito diferentes, o que levou a abordagens fragmentadas em toda a União. Isto resulta num nível desigual de protecção dos consumidores e das empresas, e compromete o nível global de segurança das redes e dos sistemas de informação no seio da União. A falta de requisitos comuns aos operadores de serviços essenciais e aos fornecedores de serviços digitais, por sua vez, torna impossível a criação de um mecanismo global e eficaz de cooperação a nível da União. As universidades e os centros de investigação têm um papel decisivo a desempenhar no fomento da investigação, desenvolvimento e inovação nestas áreas.

A Directiva da UE sobre Segurança das Redes e da Informação (Directiva NIS) visa criar uma Rede CSIRT "para contribuir para o desenvolvimento da confiança entre os Estados-Membros e para promover uma cooperação operacional rápida e eficaz". A directiva estabelece que cada Estado-membro designará um ou mais CSIRT que deverão cumprir os requisitos estabelecidos no ponto (1) do Anexo I (requisitos) da directiva, abrangendo pelo menos os sectores referidos no Anexo II e os serviços referidos no Anexo III, responsáveis pela gestão de riscos e incidentes, de acordo com um processo bem definido.

A Directiva SRI visa criar uma Rede CSIRT "para contribuir para o desenvolvimento da confiança entre os Estados-Membros e para promover uma cooperação operacional rápida e eficaz". A Directiva estabelece que cada Estado-Membro designará um ou mais CSIRT que devem cumprir um conjunto de requisitos de alto nível definidos. [[100]](#footnote-100)

De acordo com o Artigo 9 dos Estados NEI:

*"Cada Estado-membro designará um ou mais CSIRT que deverão cumprir os requisitos estabelecidos no ponto 1 do Anexo I, abrangendo pelo menos os sectores referidos no Anexo II e os serviços referidos no Anexo III, responsáveis pela gestão dos riscos e incidentes, de acordo com um processo bem definido. Pode ser estabelecido um CSIRT no âmbito de uma autoridade competente".*

E a NISD continua a afirmar isso:

* + - * *O CSIRTS tem recursos adequados para desempenhar eficazmente as suas tarefas*
      * *Os Estados-Membros devem assegurar a cooperação eficaz, eficiente e segura dos seus CSIRT*
      * *Os Estados-Membros assegurarão que os seus CSIRT tenham acesso a uma infra-estrutura de comunicação e informação adequada, segura e resiliente a nível nacional*
      * *Os Estados-membros informarão a Comissão sobre o mandato, bem como sobre os principais elementos do processo de tratamento dos incidentes, dos seus CSIRT*
      * *Os Estados-Membros podem solicitar a assistência da ENISA no desenvolvimento de CSIRTs nacionais [[101]](#footnote-101)*

O Anexo I do NISD é rotulado como *REQUISITOS E TAREFAS DE EQUIPAS DE RESPONSABILIDADE INCIDENTES DE SEGURANÇA COMPUTENTE (CSIRTs)* e é aqui citado na íntegra devido à sua grande relevância para a comunidade nacional/governamental CSIRT dentro da UE:

*(1) Requisitos para CSIRTs:*

*(a) Os CSIRT devem assegurar um elevado nível de disponibilidade dos seus serviços de comunicações, evitando pontos únicos de falha, e devem dispor de vários meios para serem contactados e para contactarem outras pessoas em qualquer altura. Além disso, os canais de comunicação devem ser claramente especificados e bem conhecidos do círculo eleitoral e dos parceiros de cooperação.*

*(b) As instalações do CSIRT e os sistemas de informação de apoio devem ser localizados em locais seguros.*

*(c) Continuidade de negócios:*

*(i) Os CSIRT devem estar equipados com um sistema adequado de gestão e encaminhamento dos pedidos, a fim de facilitar as transferências.*

*(ii) Os CSIRT devem ser dotados de pessoal adequado para assegurar a disponibilidade a todo o momento.*

*(iii) Os CSIRTs devem contar com uma infra-estrutura cuja continuidade seja assegurada. Para o efeito, devem estar disponíveis sistemas redundantes e espaço de trabalho de reserva.*

*(d) Os CSIRT terão a possibilidade de participar, onde o desejarem, em redes de cooperação internacional.*

*(2) As tarefas dos CSIRTs:*

*(a) As tarefas dos CSIRT devem incluir pelo menos o seguinte:*

*(i) monitorização de incidentes a nível nacional;*

*(ii) fornecer alertas, alertas, anúncios e divulgação de informação aos intervenientes relevantes sobre riscos e incidentes;*

*(iii) resposta a incidentes;*

*(iv) fornecendo uma análise dinâmica do risco e dos incidentes e uma consciência situacional;*

*(v) Participação na rede CSIRTs.*

*(b) Os CSIRT devem estabelecer relações de cooperação com o sector privado.*

*(c) Para facilitar a cooperação, os CSIRT devem promover a adopção e utilização de práticas comuns ou normalizadas:*

*(i) procedimentos de incidentes e de gestão de riscos;*

*(ii) esquemas de classificação de incidentes, riscos e informações.*



## República Checa

O quadro legislativo das equipas CSIRT/CERT na República Checa é parcialmente estabelecido pela Lei de Segurança Cibernética. Esta lei estabelece as condições para a existência da equipa nacional e governamental CSIRT/CERT, mas por outro lado não restringe a criação e existência de outras equipas CSIRT/CERT.

Com base na Lei de Cibersegurança, duas equipas CERT/CSIRT, **nomeadamente nacionais e governamentais**, **estão obrigatoriamente estabelecidas na República Checa.** Cada uma destas equipas tem os direitos e obrigações especificados por lei (Secção 17 e seguintes do AoCS).

As equipas cujo âmbito é definido pela Lei de Segurança Cibernética são obrigadas a respeitar os limites estabelecidos por esta lei.

## CERT Nacional

A equipa nacional da CERT é definida na Secção 17 do AoCS. Também se afirma que:

**(1) A CERT nacional assegura, na medida estipulada por este acto, a partilha de informação a nível nacional e internacional no domínio da ciber-segurança.**

**(2)O operador da CERT nacional**

* 1. **recebe notificações de contactos das autoridades e pessoas referidas na Secção 3 (a), (b) e (h) e regista e armazena estes dados,**
  2. **recebe relatórios de incidentes de ciber-segurança das autoridades e pessoas referidas na Secção 3 (b) e (h) e regista, armazena e protege estes dados,**
  3. **avalia os incidentes de cibersegurança no caso dos organismos e pessoas referidos na Secção 3 (b) e (h),**
  4. **fornece aos organismos e pessoas referidos na Secção 3 (a), (b) e (h) apoio metodológico, assistência e cooperação em caso de incidente de ciber-segurança,**
  5. **actua como ponto de contacto para os organismos e pessoas referidos na Secção 3 (a), (b) e (h),**
  6. **avalia as vulnerabilidades no campo da ciber-segurança,**
  7. **transmite ao Gabinete dados sobre incidentes de ciber-segurança comunicados nos termos da Secção 8 (3), sem declarar o notificador,**
  8. **transmite os dados nos termos do artigo 16 (5) e (6) mediante pedido ao Instituto,**
  9. **actuar como CSIRT em conformidade com a legislação pertinente da União Europeia**[[102]](#footnote-102) **,**
  10. **informar a autoridade competente de outro Estado-Membro, sem revelar a identidade do notificador, de um incidente de cibersegurança com impacto significativo na continuidade do serviço básico ou digital nesse Estado-Membro, informando simultaneamente o Gabinete e mantendo os interesses comerciais e de segurança do notificador,**
  11. **cooperar com CSIRTs de outros Estados Membros; e**
  12. **recebe relatórios sobre incidentes de cibersegurança das autoridades e pessoas não enumeradas na Secção 3, e se as suas capacidades o permitirem, processa-os e presta apoio metodológico, assistência e cooperação às autoridades ou pessoas afectadas por um incidente de ciber-segurança.**

**(3) O operador de uma CERT nacional pode, em nome do seu próprio nome e sob a sua própria responsabilidade, exercer também outras actividades económicas no domínio da ciber-segurança não reguladas pela presente Lei, desde que essa actividade não interfira com o cumprimento das obrigações referidas no n.º 2.**

**(4) O operador do CERT nacional deve, no cumprimento das obrigações referidas no n.º 2, coordenar as suas actividades com o Gabinete.**

**(5) O operador de uma CERT nacional deve agir de forma imparcial no cumprimento das obrigações previstas no parágrafo 2.**

*Esta disposição define a instituição do organismo de controlo nacional para o qual é utilizada a abreviatura legislativa CERT nacional e define as suas actividades. O acto assume que a CERT nacional será normalmente dirigida por uma pessoa de direito privado, que celebrará um contrato público com o NBU, e servirá em particular como ponto de contacto e coordenação conjunta para pessoas obrigadas ao abrigo do direito privado. Os fornecedores de serviços de comunicações electrónicas, entidades que fornecem redes de comunicações electrónicas e entidades que fornecem redes significativas implementarão a sua obrigação legal de notificação para o local de trabalho de supervisão nacional.*

*O modelo de desempenho padrão de direito privado das funções da CERT nacional facilita a comunicação entre a CERT nacional e os devedores que a utilizam como ponto de contacto. Estas pessoas serão também, por regra, de natureza de direito privado. A CERT nacional também poderá participar em redes internacionais de organismos de controlo nacionais privados semelhantes e beneficiar do conhecimento que é informalmente partilhado no seio destas redes.*

*Dado o significado e a finalidade do acto, o presumível carácter de direito privado da CERT nacional é também apropriado porque o operador da CERT nacional pode, se for uma pessoa de direito privado, tomar iniciativas com base numa autorização tácita, ou seja, qualquer actividade de direito privado não violará as obrigações legais. O operador da CERT nacional poderá assim, por exemplo, prestar assistência metodológica e informativa a entidades fora do âmbito pessoal do acto, ou seja, a pessoas fora da definição de categorias individuais de devedores que demonstrem interesse no mesmo. A CERT nacional poderá desenvolver as suas próprias actividades educativas, editoriais, de investigação ou desenvolvimento, etc. A condição que limita as actividades da CERT nacional realizadas por iniciativa para alcançar o objectivo deste acto é a sua indiscutível conformidade com o cumprimento das obrigações legalmente especificadas no acto.*

Relativamente à Secção 17 (2) (a), (b), (d) e (e)

*Os prestadores de serviços digitais são adicionados às entidades com as quais o operador nacional CERT comunica e coopera.*

Relativamente à Secção 17 (2) (c)

*Os prestadores de serviços digitais são adicionados às entidades com as quais o operador nacional CERT coopera, neste caso para as quais avalia incidentes de ciber-segurança. Esta disposição está em guarda inversa à disposição que obriga os prestadores de serviços digitais a comunicar incidentes de cibersegurança ao operador nacional CERT.*

Relativamente à Secção 17 (2) (g)

*Trata-se de um ajustamento linguístico das disposições e da relação explícita da obrigação de fornecer informações a incidentes comunicados por entidades obrigadas.*

Relativamente à Secção 17 (2) (h)

*A redacção da disposição é clarificada e a restrição das situações em que a CERT nacional transmite os dados de contacto dos devedores ao Gabinete é suprimida.*

Relativamente à Secção 17 (2) (i) a (l)

*A CERT (Equipa Nacional de Resposta a Emergências Informáticas) adquire novas competências e obrigações relacionadas ao abrigo da directiva nesta disposição. Esta disposição está estreitamente ligada à Secção 8, que, entre outras coisas, regula a comunicação de incidentes de cibersegurança que tenham afectado o sistema de informação de um fornecedor de serviços digitais. A este respeito, o CERT nacional é determinado, entre outros, como um dos CSIRT (Computer Security Incident Response Team) na República Checa; o CERT governamental (National Cyber Security Centre, que faz parte da NSA) é o segundo CSIRT na acepção da directiva sobre incidentes contra a segurança de redes e sistemas de informação dos provedores de serviços básicos designados.*

*As equipas CSIRT devem cumprir os requisitos do Anexo I da directiva, o que é cumprido no caso de uma CERT nacional operada pela CZ.NIC pelos requisitos para o operador da CERT nacional estabelecidos na Secção 18 da Lei e pelo conteúdo do contrato público que a NBU celebrou com ela nos termos da Secção 19. Este contrato nos termos do n.º 1 da presente disposição destina-se a assegurar o cumprimento das actividades nos termos da Secção 17, ou seja, também os novos requisitos decorrentes da directiva.*

*Especificamente, o acto corresponde às tarefas do CSIRT ao abrigo da directiva, como se segue:*

*CERT nacional: recebe relatórios sobre incidentes de ciber-segurança, avalia-os, fornece apoio metodológico, assistência e cooperação às entidades envolvidas, actua como ponto de contacto, avalia vulnerabilidades no domínio da ciber-segurança, transmite dados sobre incidentes à ANS, actua como CSIRT ao abrigo da directiva, coopera com outros CSIRT, comunica com as autoridades competentes de outros Estados-Membros e, por último mas não menos importante, recebe relatórios voluntários de incidentes de ciber-segurança. Com isto cumpre os requisitos do Apêndice I da Directiva:*

* *Controlo de incidentes a nível nacional - Secção 17 (2) (b), (c), (l)*
* *Emissão de alertas e alertas precoces, notificação e divulgação de informação sobre riscos e incidentes aos intervenientes relevantes - Secção 17 (2) (d), (e), (g), (j)*
* *Resposta a incidentes - Secção 17 (2) (c), (d)*
* *Fornecimento de análise dinâmica de riscos e incidentes e visão geral da situação - Secção 17 (2) (f)*
* *Participação na rede CSIRT - ao critério do operador nacional CERT, ver mais comentários sobre a Secção 20.*

A obrigação de criar pelo menos uma equipa de segurança CSIRT responsável pela gestão de risco e resolução de incidentes de acordo com procedimentos bem definidos e cumprindo os requisitos das equipas de segurança CSIRT decorre do n.º 1 do artigo 9.

A Directiva SRI estipula que esta equipa obrigatória deve abranger pelo menos os sectores enumerados no Apêndice II (tipos de entidades) e os serviços enumerados no Apêndice III (tipos de serviços digitais).

O apêndice I da Directiva NIS define as tarefas e requisitos para os CSIRTs. Estas tarefas e responsabilidades de acordo com o Apêndice I da Directiva SRI incluem:

1. **Requisitos para CSIRTs**

* Os CSIRTs assegurarão que não haja pontos únicos de falha nos seus serviços de comunicação, para que estes serviços estejam amplamente disponíveis e tenham várias formas de contactar outros e que permitam contactá-los em qualquer altura. Além disso, os canais de comunicação devem ser claramente especificados e bem conhecidos dos parceiros e entidades colaboradoras no âmbito das equipas.
* As práticas do CSIRT e os seus sistemas de informação de apoio estão localizados num local seguro.
* Continuidade da actividade:
  + Os CSIRTs estão equipados com sistemas adequados de gestão de requisitos e encaminhamento para facilitar a entrega,
  + Os CSIRT são dotados de pessoal adequado para que estejam disponíveis a todo o momento,
  + Os CSIRTs devem trabalhar com infra-estruturas cuja continuidade seja garantida. Os sistemas e postos de trabalho de apoio devem estar disponíveis para este fim.
* Os CSIRTs devem poder participar em redes de cooperação internacional se desejarem fazer parte delas.

1. **Tarefas dos CSIRTs**

* As tarefas dos CSIRTs incluem, pelo menos:
  + - monitorização de incidentes a nível nacional,
    - emitir alertas e alertas precoces, notificar e divulgar informações sobre riscos e incidentes aos intervenientes relevantes,
    - resposta a incidentes,
    - fornecendo uma análise dinâmica dos riscos e incidentes e uma visão geral da situação,
    - participação na rede CSIRT.
  + Os CSIRTs estabelecerão uma cooperação com o sector privado.
  + A fim de facilitar a cooperação, os CSIRTs promovem a adopção e utilização de procedimentos comuns ou normalizados nas áreas de:
    - gestão de incidentes e riscos,
    - classificação de incidentes, riscos e informação.

A Associação CZ.NIC opera a **equipa nacional CSIRT da República Checa - CSIRT.CZ** (para mais detalhes ver https://csirt.cz/).

**Relativamente aos parágrafos (1), (2) e (4)**

De acordo com a Lei de Segurança Cibernética, o operador da CERT nacional:

* **recebe notificações de dados de contacto** das autoridades e pessoas referidas na Secção 3 (a), (b) e (h) do AoCS e regista e armazena esses dados,
* **recebe relatórios de incidentes de ciber-segurança** das autoridades e pessoas referidas na Secção 3 (b) e (h) do AoCS e regista, armazena e protege estes dados,
* **avalia os incidentes de cibersegurança** nos organismos e pessoas referidos na Secção 3 (b) e (h) do AoCS,
* **fornece aos organismos e pessoas** referidos na Secção 3 (a), (b) e (h) do AoCS **apoio metodológico, assistência e cooperação em caso de incidente de ciber-segurança,**
* âmbito de actividade da equipa CSIRT.CZ é toda a gama de endereços da República Checa. CSIRT.CZ pode ser contactado para ajuda por todos os administradores da rede que necessitem de assistência para resolver um incidente que exija coordenação da solução ou que suspeitem que o incidente possa ter um impacto a nível nacional. Mais informações e instruções sobre a comunicação de incidentes podem ser encontradas [aqui](https://www.csirt.cz/page/2632/kdy-nas-kontaktovat/)[[103]](#footnote-103) . **A equipa CSIRT.CZ não tem poderes executivos** e, na resolução de incidentes, actua como um coordenador que também pode prestar assistência metodológica na resolução dos mesmos.[[104]](#footnote-104)
* **actua como ponto de contacto** para os organismos e pessoas referidos na Secção 3 (a), (b) e (h) do AoCS,
* **avalia as vulnerabilidades** no campo da ciber-segurança,
* **transmite ao NUKIB dados sobre incidentes de ciber-segurança** comunicados nos termos da Secção 8 (3) do AoCS, sem declarar o notificador,
* **transmite dados** nos termos da secção 16 (5) e (6) do AoCS **a pedido da NUKIB,**
* **actuar como CSIRT em conformidade com a Directiva NIS**,
* **informar a autoridade competente de outro Estado-Membro,** sem revelar a identidade do notificador**, de um incidente de cibersegurança com impacto significativo** na continuidade do serviço básico ou digital nesse Estado-Membro, informando simultaneamente o Gabinete e mantendo os interesses comerciais e de segurança do notificador,
* **cooperar com CSIRTs de outros Estados Membros**,
* **recebe relatórios sobre incidentes de cibersegurança de outras pessoas** não referidas na Secção 3 do AoCS, e se as suas capacidades o permitirem, processa-os e presta apoio metodológico, assistência e cooperação às autoridades ou pessoas afectadas por um incidente de cibersegurança.

Nos termos da Secção 17 (4) do AoCS, a **Associação CZ.NIC é obrigada a coordenar as actividades da equipa nacional do CSIRT com as actividades do NÚKIB**.

Para além das obrigações explicitamente estabelecidas na Lei de Segurança Cibernética, o CSIRT nacional impôs a si próprio outras tarefas[[105]](#footnote-105) , incluindo

* **Informação sobre uma infecção no domínio .CZ**
  + Para efeitos de monitorização central e tratamento de ameaças no domínio de segunda ordem, o CSIRT.CZ desenvolveu um rastreador de código aberto: [Gestor de Domínio Malicioso](https://gitlab.labs.nic.cz/labs/mdm).
  + A aplicação serve como ponto central para recolher e analisar informação sobre URLs maliciosos no domínio .CZ.
* pedido apoia o histórico de ameaças no domínio e o contacto directo com o seu titular. Os titulares do domínio são contactados a partir do endereço dedicado malware@nic.cz.
* **Scanner Web**
  + Para o sector não lucrativo e público, é principalmente fornecido um serviço gratuito de testes de penetração de websites. Os testes consistem em testes automáticos e manuais destinados a encontrar vulnerabilidades de segurança na aplicação. Cada constatação de segurança é identificada por um nível estimado de risco potencial e contém uma descrição de recomendações para a sua possível correcção.
  + Para mais pormenores, ver https://www.skenerwebu.cz.
* **Educação e palestras**
  + Em cooperação com a Academia CZ.NIC, os cursos [Segurança Informática na Prática](https://akademie.nic.cz/akademie/course/79/detail/) e [Fundamentos da Operação da Equipa CSIRT](https://akademie.nic.cz/akademie/course/115/detail/) são implementados regularmente. O CSIRT.CZ também implementa cursos especializados para forças de segurança, instituições estatais e educacionais ou palestras ad hoc.
* **Assistência na criação de uma equipa CERT/CSIRT**
* **Grupos de trabalho**
  + A equipa CSIRT.CZ organiza reuniões regulares das equipas de segurança e dos membros da comunidade de segurança na República Checa.
* **Testes de stress** 
  + Após os ataques DDoS de 2013, que se concentraram em serviços importantes na República Checa, os Laboratórios CZ.NIC prepararam [**testes de stress**](https://www.csirt.cz/page/3722/zatezove-testy/) que atingiram a mesma e maior intensidade que os mencionados ataques DDoS. Em cooperação com o CSIRT.CZ, este serviço é fornecido gratuitamente a todas as partes interessadas que preencham as condições de entrada.
* **Sistema de Detecção de Intrusão**
  + Em cooperação com a Associação [CESNET](http://www.cesnet.cz/), CSIRT.CZ opera um sistema que detecta comportamentos suspeitos de sistemas ligados à Internet.
  + Em caso de registo de tentativas suspeitas de ligação a partir de endereços IP específicos, os administradores responsáveis são imediatamente informados sobre tal evento (através do endereço de correio electrónico ids@csirt.cz).
* **Funcionamento de honeypots**
  + Como parte da investigação sobre segurança, o CSIRT.CZ, em cooperação com os Laboratórios CZ.NIC, opera uma série de honeypots. No âmbito do projecto Honeynet, é possível encontrar uma visualização dos ataques em tempo real em https://honeymap.cz. As amostras de malware recentemente detectadas são analisadas.
* **PROKI**
  + Envio de informações sobre incidentes de segurança que têm origem na gama de endereços IP checos.

**Relativamente aos parágrafos (3) e (5)**

A disposição da Secção 17 (2) do AoCS permite à Associação CZ.NIC realizar outras actividades económicas no domínio da ciber-segurança em seu próprio nome e sob a sua própria responsabilidade, o que não é regulado directamente pela Lei da Ciber-segurança. Contudo, existe uma condição de que esta actividade económica adicional não interfira com o desempenho das tarefas do CSIRT nacional.

A Associação CZ.NIC é obrigada a agir imparcialmente no cumprimento das obrigações da equipa nacional CSIRT.

De acordo com as disposições da Secção 18 do AoCS, só essa entidade jurídica pode tornar-se o operador de uma CERT nacional

* 1. **que satisfaça as condições estabelecidas no parágrafo 2 e**
  2. **com o qual o Instituto celebrou um contrato público nos termos da Secção 19.**

**(2)O operador de uma CERT nacional só pode ser uma entidade jurídica que**

* 1. **não actua ou não actuou contra os interesses da República Checa no sentido da lei que regula a protecção de informações classificadas,**
  2. **opera ou gere sistemas ou serviços de informação e redes de comunicações electrónicas**[[106]](#footnote-106) **ou participa no seu funcionamento e gestão há pelo menos 5 anos,**
  3. **tem pré-requisitos técnicos no domínio da ciber-segurança,**
  4. **é membro de uma organização supranacional que opera no domínio da ciber-segurança,**
  5. **não tem nenhum atraso registado no registo fiscal dos organismos da Administração Financeira da República Checa ou dos organismos da Administração Aduaneira da República Checa ou nos prémios da segurança social e nos prémios do seguro de saúde público,**
  6. **não foi condenado por uma infracção penal referida na Secção 7 da Lei sobre Responsabilidade Penal de Pessoas Colectivas e Procedimentos Contra elas,**
  7. **não é uma pessoa estrangeira ao abrigo de outro acto legislativo e**
  8. **não foi estabelecido ou criado com o único objectivo de obter lucro; isto não afecta a possibilidade de o operador da CERT nacional proceder em conformidade com a Secção 17 (3).**

**(3) O requerente prova o preenchimento das condições mediante a apresentação de**

* 1. **uma declaração sob juramento no caso do n.º 2, alíneas a) a d), g) e h), e**
  2. **confirmação do organismo da Administração Financeira da República Checa e da Administração Aduaneira da República Checa, no caso do parágrafo 2 (e).**

**(4) Do conteúdo da declaração juramentada de acordo com o parágrafo 3 (a), deve ficar claro que o requerente preenche os requisitos pertinentes. A confirmação, nos termos do parágrafo 3 (b), de que o requerente não tem nenhum atraso registado no registo fiscal dos organismos da Administração Financeira da República Checa ou dos organismos da Administração Aduaneira da República Checa ou nos prémios da segurança social e dos seguros de saúde públicos, não pode ter mais de 30 dias. A fim de demonstrar a condição referida no parágrafo 2 (f), o Instituto solicitará um extracto do registo criminal, em conformidade com outro regulamento legal**[[107]](#footnote-107) **.**

**(5) O operador da CERT nacional realiza actividades nos termos do artigo 17 (2) (a) a (c), (e) e (g) a (l) gratuitamente. O operador da CERT nacional é obrigado a incorrer nos custos necessários para o correcto e eficiente desempenho das actividades referidas no n.º 2 do artigo 17º.**

**(6) O Instituto publicará no seu sítio web dados sobre o operador do CERT nacional, nomeadamente o seu nome ou firma, endereço da sede social, número de identificação da entidade, identificador da caixa de dados e endereço do seu sítio web.**

*Esta disposição estabelece as condições gerais para a selecção do operador CERT nacional. Ao mesmo tempo, o método para estabelecer a sua obrigação de operar um CERT nacional é regulado sob a forma de um contrato de direito público celebrado com a NBU. A utilização do instituto de um contrato público corresponde à presunção de que o operador do CERT nacional será uma pessoa de direito privado. Embora as obrigações do operador nacional do CERT para realizar as actividades especificadas nesta lei sejam principalmente de natureza privada, em relação aos prestadores de serviços de comunicações electrónicas, entidades que fornecem redes de comunicações electrónicas e entidades que fornecem redes significativas, o operador nacional do CERT actuará como uma entidade através da qual estes obrigacionistas desempenham algumas das suas obrigações legais, tipicamente a obrigação de comunicar detalhes de contacto e, no caso de entidades que fornecem redes significativas, também a obrigação de comunicar a ocorrência de incidentes de ciber-segurança.*

*Dado que a CERT nacional é uma organização de grande importância para o sistema de ciber-segurança da República Checa, o seu operador é obrigado a ter a sua sede social na República Checa. No que diz respeito à exposição da CERT nacional à segurança, não é portanto possível perceber este requisito como discriminatório contra pessoas estabelecidas noutros estados da União Europeia. Integridade, uma estrutura de propriedade transparente e a ausência das devidas obrigações financeiras para com o Estado são as condições formais padrão exigidas em caso de cooperação entre o Estado e uma pessoa regida pelo direito privado. O acto também formula as condições materiais para o desempenho da função do operador nacional da CERT, exigindo que o operador nacional da CERT demonstre as competências factuais, a experiência e as capacidades técnicas para desempenhar as actividades que lhe são impostas por este acto, bem como a capacidade de trabalhar em cooperação com entidades estrangeiras que operam no domínio da ciber-segurança. O acto exige ainda que o operador de uma CERT nacional execute actividades que lhe são confiadas imparcialmente por este acto, independentemente da sua possível relação contratual ou outra com os devedores.*

Relativamente à Secção 18 (5)

*Esta disposição responde ao alargamento das competências do operador CERT nacional na Secção 17 e alarga adequadamente a gama de actividades que o operador CERT nacional realiza gratuitamente.*

Relativamente à Secção 18 (5)

*Ajustamento técnico legislativo devido ao alargamento das competências do operador nacional do CERT. A fim de assegurar o cumprimento coerente das obrigações decorrentes da Directiva e subsequentemente da Lei de Segurança Cibernética, a obrigação da CERT nacional é de gastar fundos adequados para assegurar o exercício das competências.*

**Re parágrafos (1) e (2)**

**O operador da equipa nacional CERT é a associação CZ.NIC.**

As disposições da Secção 18 do AoCS definem as condições em que uma entidade pode tornar-se o operador da CERT nacional.

O operador do CERT nacional só pode ser uma **entidade jurídica**[[108]](#footnote-108) **, com a qual a NUKIB** (ou anteriormente NBU) celebrou **um contrato de direito público**[[109]](#footnote-109) (de acordo com a secção 19 do AoCS), e **que preenche as seguintes condições**:

1. **não actua ou não actuou contra os interesses da República Checa** no sentido da lei que regula a protecção de informações classificadas,

De acordo com a Secção 2 (b) da Lei sobre a Protecção da Informação Classificada e sobre a Competência em matéria de Segurança é *"do interesse da República Checa preservar a sua constitucionalidade, soberania e integridade territorial, assegurar a ordem e segurança interna, obrigações internacionais e defesa, proteger a economia e proteger a vida ou saúde dos indivíduos".*

1. **opera ou gere sistemas ou serviços de informação e redes de comunicações electrónicas** ou participa no seu funcionamento e gestão **há pelo menos 5 anos,**
2. **tem pré-requisitos técnicos no domínio da ciber-segurança,**
3. **é membro de uma organização supranacional que opera no domínio da ciber-segurança,**

O requisito de operar um dos sistemas referidos em (c), a existência de pré-requisitos técnicos no domínio da ciber-segurança e a adesão a uma organização multinacional que opera no domínio da ciber-segurança dá ao Estado uma garantia de que a pessoa esteve envolvida na ciber-segurança, na resolução de incidentes, etc. É essencialmente uma demonstração da capacidade factual, experiência e capacidade técnica para realizar as actividades que lhe são impostas pelo AoCS.

1. **não tem nenhum atraso registado no** registo fiscal dos organismos da Administração Financeira da República Checa ou dos organismos da Administração Aduaneira da República Checa **ou nos prémios da segurança social e nos prémios do seguro de saúde público,**
2. **não foi condenado por uma infracção penal** referida na Secção 7 da Lei sobre Responsabilidade Penal de Pessoas Colectivas e Procedimentos Contra elas,

A ausência das devidas obrigações financeiras para com o Estado, bem como a prova de integridade, é uma condição padrão para a celebração de um contrato no caso de cooperação entre o Estado e uma pessoa de direito privado.

A Lei sobre a Ciber-segurança na Secção 18 (2) (f) faz uma imprecisão factual causada pela alteração à Lei n.º 418/2011 Sb., sobre a Responsabilidade Criminal das Pessoas Colectivas e Procedimentos contra elas. Nesta lei, a Secção 7 definiu originalmente as infracções penais que uma pessoa colectiva pode cometer. Na actual regulamentação jurídica efectiva, a Secção 7 contém uma definição negativa de infracções penais.

A disposição da Secção 7 da ACLLE (Act on Criminal Liability of Legal Entities) (em vigor desde 1st de Dezembro de 2016) estipula que uma pessoa colectiva pode ser criminalmente responsável pela prática de todas as infracções penais, com a excepção das infracções penais exaustivamente enumeradas nesta disposição.

Para além da definição do âmbito das infracções penais, a questão da imputabilidade também deve ser abordada no caso da responsabilidade penal das pessoas colectivas. Embora uma pessoa colectiva seja uma construção fictícia, a lei geralmente reconhece, em relação às pessoas colectivas, a sua capacidade de agir legalmente (e portanto ilegalmente), inclusive atribuindo-lhes culpa. A culpa como condição de responsabilidade criminal é imputada a uma pessoa colectiva se as circunstâncias tiverem surgido nos termos da Secção 8 (2) da Lei sobre Responsabilidade Penal das Pessoas Colectivas.

Nos termos da Secção 8 (1) da ACLLE, uma infracção penal cometida por uma pessoa colectiva significa um acto ilegal cometido no seu interesse ou no âmbito das suas actividades, se se tratar de um acto de

1. um órgão estatutário ou um membro de um órgão estatutário, ou outra pessoa em posição de direcção no seio de uma pessoa colectiva que esteja autorizada a agir em nome ou por conta de uma pessoa colectiva,
2. uma pessoa numa posição de gestão dentro de uma pessoa colectiva que exerce actividades de gestão ou controlo sobre essa pessoa colectiva, mesmo que não seja a pessoa referida em (a),
3. uma pessoa que exerça influência decisiva sobre a gestão dessa pessoa colectiva, se a sua conduta for pelo menos uma das condições para a ocorrência de uma responsabilidade penal da pessoa colectiva, ou
4. um empregado ou pessoa em posição semelhante (doravante referido como "empregado") no desempenho das suas funções, mesmo que não seja a pessoa referida nas alíneas (a) a (c),

se as acções da pessoa acima mencionada puderem ser atribuídas à pessoa colectiva de acordo com a Secção 8 (2) da ACLLE.

1. **não é uma pessoa estrangeira** ao abrigo de outra regulamentação legal,

De acordo com a Secção 3024 do Código Civil, uma pessoa estrangeira é uma pessoa singular com residência ou uma pessoa colectiva com sede social fora do território da República Checa.

Devido à importância da equipa nacional CERT no domínio da ciber-segurança na República Checa, é necessário que o operador desta equipa esteja sediado na República Checa. Esta exigência não pode ser entendida como discriminação contra outras pessoas estabelecidas noutro Estado Membro da União.

1. **não tenha sido estabelecido ou criado com o único objectivo de obter lucro;** isto não afecta a possibilidade do operador da CERT nacional proceder em conformidade com a Secção 17 (3) do AoCS.

**Relativamente aos parágrafos (3) e (4)**

Uma entidade jurídica que pretenda tornar-se o operador de uma CERT nacional deve provar o preenchimento das condições, apresentando uma declaração sob juramento [no caso da Secção 18 (2) (a) a (d), (g), (h) do AoCS] e a confirmação do órgão da Administração Financeira da República Checa e da Administração Aduaneira da República Checa [no caso da Secção 18 (2) (e) do AoCS].

**O conteúdo da declaração ajuramentada deve indicar claramente que o requerente preenche os requisitos pertinentes. A confirmação** de que o requerente não tem nenhum atraso registado no registo fiscal dos organismos da Administração Financeira da República Checa ou dos organismos da Administração Aduaneira da República Checa ou nos prémios da segurança social e de seguro de saúde público, **não pode ter mais de 30 dias.**

A fim de **provar o facto de uma pessoa colectiva não ter sido condenada por uma infracção penal, NUKIB solicitará um extracto do Registo Criminal.**

**Relativamente ao parágrafo (5)**

O operador da CERT nacional **realiza gratuitamente as actividades especificadas na Secção 17 (2) do AoCS.** As excepções à condição de gratuidade são apenas as seguintes actividades:

* **fornece aos organismos e pessoas** referidos na Secção 3 (a), (b) e (h) do AoCS **apoio metodológico, assistência e cooperação em caso de incidente de ciber-segurança,**
* **avalia as vulnerabilidades** no campo da ciber-segurança.

O operador da CERT nacional é obrigado a incorrer nos custos necessários para o desempenho adequado e eficiente das actividades referidas no nº 2 da Secção 17 do AoCS.

**Relativamente ao parágrafo (6)**

Devido à possibilidade de contactar o operador da equipa nacional CERT, os dados sobre este operador são publicados no website da NÚKIB. São publicadas as seguintes informações: nome ou razão social, endereço da sede social, número de identificação da entidade, identificador da caixa de dados e endereço do seu sítio web.

## CERT do Governo

CERT do Governo, como parte do Gabinete,

* 1. **recebe notificações de contactos das autoridades e pessoas referidas na secção 3 (c) a (g),**
  2. **recebe relatórios de incidentes de cibersegurança das autoridades e das pessoas referidas na Secção 3 (c) a (g),**
  3. **avalia dados sobre eventos de cibersegurança e incidentes de cibersegurança da infra-estrutura de informação crítica, do sistema básico de informação de serviços, dos sistemas de informação significativos e de outros sistemas de informação da administração pública,**
  4. **fornece aos organismos e pessoas referidas na Secção 3 (c) a (g) apoio metodológico e assistência,**
  5. **presta cooperação aos organismos e pessoas referidos na Secção 3 (c) a (g) em caso de incidente de ciber-segurança e evento de ciber-segurança,**
  6. **recebe sugestões e dados dos organismos e pessoas referidos na Secção 3 e de outros organismos e pessoas e avalia essas sugestões e dados,**
  7. **recebe dados do operador da CERT nacional e avalia esses dados,**
  8. **recebe dados de autoridades que actuam no domínio da ciber-segurança no estrangeiro e avalia esses dados,**
  9. **nos termos da Secção 9 (4), fornece ao operador do CERT nacional, aos organismos que actuam no domínio da ciber-segurança no estrangeiro e a outras pessoas que operam no domínio da ciber-segurança, os dados do registo de incidentes,**
  10. **avalia as vulnerabilidades no campo da ciber-segurança,**
  11. **informa a autoridade competente de outro Estado-Membro, sem revelar a identidade do notificador, de um incidente de ciber-segurança que tenha um impacto significativo na continuidade dos serviços básicos nesse Estado-Membro ou que afecte a prestação de serviços digitais nesse Estado-Membro, mantendo simultaneamente os interesses comerciais e de segurança do notificador,**
  12. **recebe relatórios de um incidente de cibersegurança das autoridades e pessoas não referidas na Secção 3; a CERT governamental processa os relatórios e, se as suas capacidades o permitirem e se for um incidente de cibersegurança com impacto significativo, fornece apoio metodológico, assistência e cooperação às autoridades ou pessoas afectadas pelo incidente de cibersegurança,**
  13. **actuar como CSIRT em conformidade com a legislação pertinente da União Europeia**[[110]](#footnote-110) **e**
  14. **coopera com CSIRTs de outros Estados Membros.**

*O CERT governamental faz parte do NBU, ou Centro Nacional para a Ciber-segurança, que é uma unidade organizacional do NBU, que assegura as suas actividades. O CERT governamental é concebido como um departamento público central e um "ponto de contacto único" público para a área da ciber-segurança. As suas actividades incluem a recepção de dados de contacto de devedores seleccionados, a recepção de informações sobre a situação de cibersegurança, em particular a recepção de relatórios obrigatórios e de iniciativa de incidentes de cibersegurança e outros dados sobre a situação de cibersegurança de autoridades públicas nacionais e estrangeiras e entidades cooperantes e a sua avaliação. O CERT governamental também presta cooperação a tipos seleccionados de obrigados em caso de incidente de cibersegurança, assegura a cooperação com outros organismos e entidades que asseguram a cibersegurança na República Checa e nos Estados cooperantes ou aliados, e também realiza avaliações de vulnerabilidade de cibersegurança.*

Relativamente à Secção 20 (a), (b), (d) e (e)

*Entre as entidades com as quais o CERT governamental comunica e coopera, são acrescentadas novas entidades obrigatórias - operadores de serviços básicos e administradores e operadores de sistemas de informação de serviços básicos.*

Relativamente à Secção 20 (c)

*Os sistemas de informação para os quais a CERT governamental avalia os dados sobre eventos de cibersegurança e incidentes de cibersegurança são complementados por sistemas de informação de cujo funcionamento depende a prestação de serviços básicos.*

Relativamente à Secção 20 (i)

*Adaptação técnica legislativa resultante da necessidade de acrescentar novas cartas a esta disposição.*

Relativamente à Secção 20 (j) e (k) a (n)

*O CERT governamental adquire novas competências e obrigações relacionadas ao abrigo da directiva nesta disposição. Esta disposição está estreitamente ligada à Secção 8, que regula a comunicação de incidentes de cibersegurança.*

*De acordo com a lei, emendada por esta proposta, o CERT governamental: recebe relatórios sobre incidentes de ciber-segurança, avalia-os, fornece apoio metodológico, assistência e cooperação às entidades envolvidas, actua como ponto de contacto, avalia vulnerabilidades no domínio da ciber-segurança, transmite dados sobre incidentes à ANS, actua como CSIRT ao abrigo da directiva, coopera com outros CSIRT, comunica com as autoridades competentes de outros Estados Membros e, por último mas não menos importante, recebe relatórios voluntários de incidentes de ciber-segurança.*

*Com isto cumpre os requisitos do Apêndice I da Directiva:*

* *Monitorização de incidentes a nível nacional - Secção 20 (b), (c), (f), (g), (l).*
* *Emissão de alertas e alertas precoces, notificação e divulgação de informação sobre riscos e incidentes aos intervenientes relevantes - Secção 20 (d), (e), (i), (n).*
* *Resposta a incidentes - Secção 20 (d), (e).*
* *Fornecer uma análise dinâmica dos riscos e incidentes e uma visão geral da situação - Secção 20 (j).*
* *Participação na rede CSIRT - Secção 20 (m).*

*Ao cumprir o papel do CSIRT, a CERT governamental, que faz parte da NBU, também cumprirá os requisitos da Directiva para a participação da equipa CSIRT na rede CSIRT nos termos do Artigo 12 da Directiva. A participação de representantes da CERT nacional será deixada à sua discrição.*

*O artigo 9º da Directiva estipula que cada Estado-membro criará um ou mais CSIRT, mas não contempla que os representantes de todos os CSIRT de um Estado-membro devem ser obrigados a participar nos trabalhos do CSIRT. A participação plena de pelo menos uma equipa CSIRT é assim suficiente, o que será cumprido pelos representantes da CERT governamental. A disposição regula o procedimento da CERT governamental no caso do incidente de ciber-segurança relatado ter um impacto significativo na continuidade da prestação de serviços básicos, ou o impacto na prestação de serviços digitais noutro Estado Membro da União Europeia. Nesse caso, em conformidade com o n.º 5 do artigo 14º, e por conseguinte com o n.º 6 do artigo 16º da Directiva, é consagrado o poder de uma CERT governamental de informar as autoridades competentes de outros Estados-Membros sobre o incidente.*

*O artigo 20º da directiva prevê uma situação em que uma entidade que não tenha sido designada como operador de serviços básicos e não seja um fornecedor de serviços digitais detecta e procura abordar a segurança dos seus sistemas de informação. Neste caso, pode voluntariamente comunicar o incidente de ciber-segurança ao CERT governamental e trabalhar com o CERT para resolver a situação. Neste caso, a CERT governamental processará o relatório e, se as suas capacidades o permitirem e se for um incidente de ciber-segurança com um impacto significativo, fornecê-lo-á tão adequadamente como quando um incidente de ciber-segurança lhe é comunicado pelo fornecedor de serviços básicos.*

Com base na Lei de Cibersegurança, duas equipas CERT/CSIRT, **nomeadamente nacionais e governamentais**, **estão obrigatoriamente estabelecidas na República Checa.**

O operador da CERT nacional é uma entidade jurídica com a qual a NUKIB (antiga NBU) celebrou um contrato de direito público (ver secção 19 do AoCS).

O Governo CERT (**GovCERT.CZ** - ver https://www.govcert.cz/) é estabelecido de acordo com a lei como parte da Agência Nacional de Cibersegurança e Segurança da Informação (anteriormente sob a responsabilidade do NBU).

De acordo com a Lei da Ciber-segurança, o CERT governamental:

* **recebe notificações de dados de contacto** das autoridades e pessoas referidas na Secção 3 (c) a (g) do AoCS,
* **recebe relatórios de incidentes de cibersegurança** das autoridades e pessoas referidas na Secção 3 (c) a (g) do AoCS,
* **avalia dados** sobre **eventos de** cibersegurança e **incidentes de** cibersegurança da infra-estrutura de informação crítica, do sistema básico de informação de serviços, de sistemas de informação significativos e de outros sistemas de informação da administração pública,
* fornece **aos organismos e pessoas** referidas na Secção 3 (c) a (g) do AoCS **apoio metodológico e assistência,**
* **presta cooperação** aos organismos e pessoas referidos na Secção 3 (c) a (g) do AoCS **em caso de incidente de ciber-segurança e evento de ciber-segurança,**
  + A resolução de incidentes de segurança é uma das principais actividades da equipa governamental. Ao comunicar um incidente de cibersegurança, a equipa governamental do GovCERT.CZ está pronta a ajudar os especialistas em TI de um ponto de vista técnico, incluindo o aconselhamento para outras medidas preventivas. Caso se verifique que um dos incidentes visa mais do que uma entidade, a equipa governamental do GovCERT.CZ está pronta a coordenar um procedimento conjunto para a sua resolução. [[111]](#footnote-111)
* **recebe sugestões e dados** dos organismos e pessoas referidas na Secção 3 do AoCS e de outros organismos e pessoas e **avalia** essas sugestões e dados,
* **recebe dados do operador da CERT nacional** e avalia esses dados,
* **recebe dados de autoridades que actuam no domínio da ciber-segurança no estrangeiro** e avalia esses dados,
* **de acordo com os dados do registo de incidentes** (ver Secção 9 (4) do AoCS), fornece ao operador do CERT nacional, aos organismos que actuam no domínio da ciber-segurança no estrangeiro e a outras pessoas que operam no domínio da ciber-segurança os dados do registo de incidentes,
* **avalia as vulnerabilidades** no campo da ciber-segurança,
* **informa a autoridade competente de outro Estado-Membro, sem revelar a identidade do notificador, de um incidente de ciber-segurança que tenha um impacto significativo** na continuidade dos serviços básicos nesse Estado-Membro ou que afecte a prestação de serviços digitais nesse Estado-Membro, mantendo simultaneamente os interesses comerciais e de segurança do notificador,
* **recebe relatórios de um incidente de cibersegurança das autoridades e pessoas não referidas na Secção 3 do AoCS;** a CERT governamental processa os relatórios e, se as suas capacidades o permitirem e se for um incidente de cibersegurança com impacto significativo, fornece apoio metodológico, assistência e cooperação às autoridades ou pessoas afectadas pelo incidente de cibersegurança,
* **agir como um CSIRT em conformidade com o** artigo 9º da Directiva SRI,
* **coopera com CSIRTs de outros Estados Membros**.

Para além das obrigações explicitamente estabelecidas na Lei de Segurança Cibernética, o governo CSIRT impôs a si próprio outras tarefas[[112]](#footnote-112) , incluindo

* **Partilha de dados**

GovCERT.CZ obtém vários relatórios e dados relativos a sistemas de informação potencialmente infectados na República Checa em cooperação com várias organizações multinacionais que lidam com a ciber-segurança. Fornece esta informação a outras entidades como parte de actividades pró-activas. Os dados partilhados estão divididos nos seguintes projectos:

* + **BotnetFeed** - utilizando esta ferramenta, são processados dados sobre estações finais ligadas a redes botnet a partir de servidores C&C tomados a cargo. Para identificar um sistema informático potencialmente infectado, o gestor da gama IP recebe um endereço IP e informações sobre a rede de bots em que está integrado.
  + **IHAP** (Incident Handling Automation Project)**, MDM** (Malicious Domain Manager) - fragmentos de indicadores de compromisso (IoCs) de vários servidores são recolhidos no âmbito destes projectos. Os indicadores mais comuns incluem phishing, ataques de força bruta, alertas de ids, spam, tentativas de scan, vulnerabilidades de exploração, malware, e muitos outros tipos. Com base nestes dados, são preparados pequenos relatórios, que contêm sempre o endereço IP da máquina comprometida e um breve resumo do tipo de incidente.
  + **Shadowserver** - o projecto centra-se na procura contínua de informação relevante sobre vulnerabilidades no ciberespaço e a ocorrência destas vulnerabilidades em endereços IP específicos.
* **Implantação de Honeypots**
* **Teste de penetração**

Esta é uma tentativa legal de invadir os sistemas testados. O resultado é um relatório das vulnerabilidades de segurança do sujeito do teste, que é dirigido exclusivamente ao seu proprietário, que tomará as medidas de segurança adequadas com base no relatório.

Outra opção é realizar um scan de vulnerabilidade de acordo com o OWASP (Open Web Application Security Project).

* **Informação HUB**

No site govcert.cz é possível encontrar informações, pesquisas, análises e artigos relativos a ameaças e vulnerabilidades actuais relacionadas com sistemas na República Checa. Estes documentos são complementados por boletins mensais regulares que resumem os incidentes de segurança significativos na República Checa e no estrangeiro.

* **Actividades de educação e investigação**

**Laboratório forense e** laboratório **SCADA**

## Polónia

**CERT Polska** é uma Equipa de Resposta a Emergências Informáticas que opera dentro das estruturas de Naukowa i Akademicka Sieć Komputerowa (Scientific and Academic Computer Network ou NASK) - um instituto de investigação que conduz actividade científica, opera o registo nacional de domínios .pl e fornece serviços avançados de rede informática. CERT Polska é a primeira equipa polaca de resposta a emergências informáticas. Activa desde 1996 no ambiente das equipas de resposta, tornou-se uma entidade reconhecida e experiente no domínio da segurança informática. Desde o seu lançamento, o núcleo da actividade da equipa tem sido o tratamento de incidentes de segurança e a cooperação com unidades semelhantes em todo o mundo. Conduz também uma extensa I&D sobre temas de segurança.

Em 1997, a CERT Polska tornou-se membro do fórum internacional de equipas de resposta - FIRST, e desde 2000 que é membro do grupo de trabalho das equipas de resposta europeias - [TERENA](https://en.wikipedia.org/wiki/TERENA) TF-CSIRT e uma organização associada Trusted Introducer. Em 2005, por iniciativa da CERT Polska, foi criado um fórum de equipas de abuso polacas - FÓRUM DO Abuso, enquanto em 2010 a CERT Polska aderiu ao [Grupo de Trabalho Anti-Phishing](https://en.wikipedia.org/wiki/Anti-Phishing_Working_Group), uma associação de empresas e instituições que combatem activamente a criminalidade em linha.

As principais tarefas da CERT Polska incluem:

* registo e tratamento de incidentes de segurança de rede para a Polónia e o espaço de nome de domínio ".pl";
* prestação de serviços de vigilância e aviso aos utilizadores da Internet na Polónia;
* resposta activa em caso de ameaças directas aos utilizadores;
* cooperação com outras equipas CERT na Polónia e em todo o mundo;
* participação em projectos nacionais e internacionais relacionados com a segurança informática;
* actividade de investigação em relação a métodos de detecção de incidentes de segurança, análise de malware, sistemas de troca de informação sobre ameaças;
* desenvolvimento de ferramentas próprias para detecção, monitorização, análise e correlação de ameaças;
* publicação regular do Relatório CERT Polska sobre a segurança dos recursos em linha polacos;
* actividades de informação/educação destinadas a aumentar a sensibilização em relação à segurança informática;
* realizar análises e soluções de teste independentes relacionadas com a segurança informática.

Abaixo está a descrição completa da CERT Polska em conformidade com o RFC 2350 "Expectativas de Resposta a Incidentes de Segurança Informática":

Descrição CSIRT para CERT Polska

=================================

*1. Sobre este documento*

*1.1 Data da última actualização*

*Esta é a versão 2.0, publicada a 04 de Março de 2019.*

*1.2 Lista de Distribuição para Notificações*

*Actualmente a CERT Polska não utiliza nenhuma lista de distribuição*

*para notificar sobre alterações neste documento.*

*1.3 Locais onde este Documento pode ser encontrado*

*A versão actual deste documento de descrição CSIRT é*

*disponível no site CERT Polska WWW; o seu URL é*

*https://www.cert.pl/wp-content/uploads/2017/12/rfc2350.txt*

*Por favor, certifique-se de que está a utilizar a versão mais recente.*

*1.4 Autenticação do presente documento*

*Este documento foi assinado com o CERT Polska PGP*

*chave. As assinaturas também se encontram no nosso sítio Web, em baixo:*

*http://www.cert.pl/o-nas*

*2. Informação de contacto*

*2.1 Nome da equipa*

*CERT Polska*

*2.2 Morada*

*CERT Polska*

*NASK*

*ul. Kolska 12*

*01-045 Warszawa*

*Polónia*

*2.3 Fuso horário*

*Hora da Europa Central (GMT+0100, GMT+0200 a partir de Abril*

*até Outubro)*

*2.4 Número de telefone*

*+48 22 3808 274*

*2.5 Número de facsimile*

*+48 22 3808 399 (nota: isto é \*não\* um fax seguro)*

*2.6 Outras Telecomunicações*

*Nenhum disponível.*

*2.7 Endereço de correio electrónico*

*<cert@cert.pl> Este é um pseudónimo de correio que serve*

*o(s) humano(s) em serviço para a CERT Polska.*

*2.8 Chaves públicas e outras informações de encriptação*

*CERT Polska tem uma chave PGP, cujo KeyID é 969C0EB8 e*

*que impressão digital é*

*DC34 CB6E CD73 C0B1 DC8C 8AE7 FD58 C59E 969C 0EB8*

*A chave e as suas assinaturas podem ser encontradas no tamanho habitual*

*servidores de chaves públicas.*

*2.9 Outras informações*

*Informação geral sobre a CERT Polska, bem como links*

*a vários recursos de segurança recomendados, podem ser encontrados*

*em http://www.cert.pl/*

*A CERT Polska utiliza a seguinte página no Facebook para publicar*

*notícias sobre as actividades em curso http://www.facebook.com/CERT.Polska*

*CERT Polska publica mensagens curtas sobre eventos actuais para*

*as seguintes contas do twitter*

*http://www.twitter.com/cert\_polska*

*http://www.twitter.com/cert\_polska\_en*

*2.10 Pontos de Contacto do Cliente*

*O método preferido para contactar a CERT Polska é através*

*e-mail em <cert@cert.pl>; e-mail enviado para este endereço*

*será tratado pelo humano responsável. Encorajamos os nossos*

*clientes a utilizar a encriptação PGP ao enviar qualquer*

*informação sensível à CERT Polska.*

*Se não for possível (ou não for aconselhável para a segurança*

*razões) para utilizar o e-mail, o CERT Polska pode ser contactado por*

*telefonar durante o horário normal de expediente. Fora destas horas*

*as chamadas telefónicas recebidas são transmitidas a uma central telefónica de atendimento*

*máquina. Todas as mensagens gravadas são verificadas o mais rápido possível.*

*CERT Polska funciona 24 horas por dia, todos os dias do ano.*

*Se possível, ao apresentar o seu relatório, utilize o formulário*

*mencionado na secção 6.*

*3. Carta*

*3.1 Declaração de Missão*

*A missão da CERT Polska é identificar, analisar e*

*mitigar as ameaças que visam os utilizadores polacos da Internet. Como um*

*parte essencial do sistema nacional de segurança cibernética, CERT*

*O Polska contribui para garantir a segurança cibernética no*

*a nível nacional.*

*3.2 Consituência*

*A consitituição da CERT Polska é definida no Artigo 26 (1) de*

*a Lei de 5 de Julho de 2018 sobre o sistema nacional de cibersegurança.*

*Todas as entidades jurídicas e pessoas singulares na Polónia, com o*

*excepções de:*

*- entidades subordinadas ou supervisionadas pelo Ministro de*

*Defesa Nacional, incluindo entidades cujos sistemas de TIC ou TIC*

*redes são cobertas por uma única lista de instalações,*

*instalações, dispositivos e serviços incluídos no crítico*

*inrastrutura a que se refere o artigo 5b, parágrafo 7,*

*parágrafo 1 da Lei de 26 de Abril de 2007 sobre a crise*

*gestão,*

*- empresas de importância significativa em termos de economia e*

*defesa, para quem a autoridade que organiza e supervisiona*

*a sua execução de tarefas para a defesa do Estado é*

*o Ministro da Defesa Nacional,*

*- entidades do sector das finanças públicas referidas no artigo 9º,*

*artigos 1, 8 e 9 da lei de 27 de Agosto de 2009 sobre o público*

*finanças, com excepção de: institutos de investigação, Gabinete de*

*Supervisão Técnica, Agência Polaca de Serviços de Navegação Aérea,*

*Centro Polaco para a Acreditação, Fundo Nacional para*

*Protecção ambiental e gestão da água e regional*

*fundos para a protecção ambiental e gestão da água,*

*- Banco Nacional da Polónia,*

*- Banco Nacional de Desenvolvimento,*

*- entidades do que as enumeradas nos itens 1 a 4 e no parágrafo 5, cujos*

*Os sistemas ou redes TIC são abrangidos por uma única lista de*

*instalações, dispositivos e serviços incluídos em*

*as infra-estruturas críticas referidas no artigo 5°-B,*

*parágrafo 7, parágrafo 1 da Lei de 26 de Abril de 2007 sobre*

*gestão de crises.*

*Note que QUALQUER incidente relativo a qualquer anfitrião, rede, legal*

*entidade ou pessoa singular na Polónia PODE ser comunicada à CERT*

*Polska. Relatos de incidentes para além do círculo eleitoral da CERT Polska*

*será encaminhado sem demora indevida para o CSIRT relevante,*

*de acordo com o artigo 26 (8) da Lei de 5 de Julho de 2018 sobre o*

*sistema nacional de ciber-segurança.*

*3.3 Patrocínio e/ou Afiliação*

*O CERT Polska é mantido financeiramente pela National Research*

*Instituto NASK, do qual faz formalmente parte.*

*A NASK recebe um subsídio de utilizador especificado da parte do*

*orçamento de estado atribuído ao ministro compenetrado para*

*digitalização para financiar as operações da CERT Polska.*

*3.4 Autoridade*

*A Lei de 5 de Julho de 2018 sobre o sistema nacional de cibersegurança*

*define competências e autoridade do "CSIRT NASK" - um papel*

*atribuída à NASK no sistema nacional de cibersegurança.*

*Partes desse papel, abordando especificamente operacionais*

*aspectos tais como:*

*- monitorização das ameaças à segurança cibernética a nível nacional,*

*- resposta ao incidente,*

*- partilha de informação,*

*- participação na Rede CSIRTs*

*são cumpridas pela CERT Polska.*

*4. Políticas*

*4.1 Tipos de Incidentes e Nível de Apoio*

*A CERT Polska está autorizada a dirigir-se a todos os tipos de*

*incidentes de segurança informática que ocorrem, ou ameaçam*

*ocorrem, na sua circunscrição eleitoral.*

*O nível de apoio dado pela CERT Polska variará*

*em função do tipo e da gravidade do incidente ou*

*o problema, o tipo de constituinte, o tamanho do utilizador*

*comunidade afectada, e a disponibilidade do CERT Polska's*

*recursos na altura, embora em todos os casos alguma resposta*

*irá bemade dentro de dois dias úteis.*

*Os incidentes serão prioritizados de acordo com as suas*

*aparente gravidade e extensão.*

*Incidentes críticos, significativos e substanciais, bem como*

*incidentes numa entidade pública (tal como definido no artigo 2º do*

*Lei de 5 de Julho sobre o sistema nacional de cibersegurança) são*

*coordenado pelos respectivos CSIRTs - incluindo a CERT Polska,*

*de acordo com a sua circunscrição eleitoral.*

*O tratamento de incidentes é da responsabilidade de entidades individuais.*

*Contudo, nos termos do artigo 26º da Lei de 5 de Julho sobre o*

*sistema de cibersegurança, em casos razoáveis, a pedido de*

*operador de serviços essenciais, fornecedores de serviços digitais, ou*

*entidades públicas, a CERT Polska pode prestar apoio em incidentes*

*manuseamento.*

*4.2 Cooperação, Interacção e Divulgação de Informação*

*CERT Polska troca todas as informações necessárias com*

*outras CSIRTs, outras entidades incluídas no nacional polaco*

*sistema de cibersegurança, bem como com as partes afectadas".*

*administradores. Não há dados pessoais nem dados gerais.*

*trocados, a menos que explicitamente autorizados.*

*Todos os dados sensíveis (tais como dados pessoais, sistema*

*configurações, vulnerabilidades conhecidas com as suas localizações)*

*são encriptados se tiverem de ser transmitidos em modo não seguro*

*ambiente, tal como indicado abaixo.*

*4.3 Comunicação e Autenticação*

*Tendo em conta os tipos de informação que a CERT Polska*

*acordos, os telefones serão considerados suficientemente*

*seguro para ser utilizado mesmo não encriptado. E-mail não encriptado*

*não será considerado particularmente seguro, mas será*

*suficiente para a transmissão de dados de baixa sensibilidade.*

*Se for necessário enviar dados altamente sensíveis por correio electrónico,*

*O PGP será utilizado. As transferências de ficheiros em rede serão consideradas*

*ser semelhante ao correio electrónico para estes fins: dados sensíveis*

*deve ser codificado para transmissão.*

*Onde é necessário estabelecer a confiança, por exemplo*

*antes de confiar na informação dada à CERT Polska, ou*

*antes de revelar informações confidenciais, a identidade*

*e a boa-fé da outra parte será verificada para*

*um nível razoável de confiança. Dentro da NASK, e com o conhecido*

*sites vizinhos, referências de pessoas de confiança conhecidas irão*

*é suficiente para identificar alguém. Caso contrário, apropriado*

*serão utilizados métodos, tais como a pesquisa dos membros do FIRST,*

*a utilização do WHOIS e de outros registos na Internet*

*informação, etc., juntamente com a chamada telefónica de retorno ou e-mail*

*mail-back para garantir que a parte não é um impostor.*

*O correio electrónico recebido cujos dados devem ser fidedignos será verificado*

*com o autor pessoalmente, ou por meio de digital*

*assinaturas (o PGP em particular é apoiado).*

*5. Serviços*

*5.1 Resposta ao incidente*

*O CERT Polska irá fornecer capacidades de resposta a incidentes em*

*as seguintes áreas:*

*5.1.1 Triagem de Incidentes*

*- Investigar se de facto ocorreu um incidente.*

*- Determinar a extensão do incidente.*

*5.1.2 Coordenação de Incidentes*

*- Determinação da causa inicial do incidente*

*(vulnerabilidade explorada)*

*- Facilitar o contacto com outros sítios que possam ser*

*envolvidos.*

*- Facilitar o contacto com a aplicação da lei apropriada*

*funcionários, se necessário.*

*- Fazer relatórios a outros CSIRTs*

*- Composição de anúncios aos utilizadores, se aplicável*

*5.1.3 Tratamento de incidentes*

*Em alguns casos, pode ser prestado apoio limitado em termos técnicos*

*tratamento de incidentes, incluindo malware e análise forense,*

*caça à ameaça, recolha de provas.*

*A extensão deste apoio dependerá do tipo e da severidade*

*do incidente, e o tipo de entidade afectada.*

*5.2 Serviços pró-activos*

*CERT Polska coordena e mantém os seguintes serviços*

*na medida do possível, em função dos seus recursos:*

*- Plataforma de partilha de informações de segurança de rede ("n6")*

*disponível a todos os administradores de rede:*

*https://n6.cert.pl/*

*- Serviços de informação através dos seguintes canais:*

*= sítio Web: https://www.cert.pl/*

*= sítio Web do Facebook: https://facebook.com/CERT.Polska*

*= twitter: https://twitter.com/CERT\_Polska (PL) e*

*https://twitter.com/CERT\_Polska\_en (EN)*

*- Serviços de formação e educação*

*CERT Polska organiza uma conferência anual sobre a SEGURANÇA*

*questões actuais de segurança importantes e abertas a todos*

*partes interessadas.*

*A CERT Polska contribui para as actividades da NASK na área*

*de sensibilização e educação sobre segurança cibernética.*

*5.3 Investigação e Desenvolvimento*

*A CERT Polska fornece ferramentas e instalações para monitorizar e*

*analisar as ameaças.*

*https://github.com/CERT-Polska*

*https://www.cert.pl/en/projekty/*

*6. Formulários de Comunicação de Incidentes*

*CERT Polska tinha criado um formulário local designado para*

*relatar incidentes à equipa. Encorajamos vivamente*

*qualquer pessoa que comunique um incidente para o preencher, embora*

*isto nunca é necessário. A versão actual do formulário*

*está disponível a partir de:*

*https://incydent.cert.pl/*

*7. Renúncias de responsabilidade*

*Enquanto todas as preacções serão tomadas na preparação de*

*informação, notificações e alertas, CERT Polska assume*

*nenhuma responsabilidade por erros ou omissões, ou por danos*

*resultantes da utilização da informação contida no seu interior.*

## Portugal

**RESUMO / PRINCIPAIS RESULTADOS DO CAPÍTULO** 

* A Directiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de Julho de 2016, relativa a medidas para um elevado nível comum de segurança das redes e sistemas de informação em toda a União (a Directiva NIS) foi adoptada pelo Parlamento Europeu.
* A Directiva NIS prevê medidas legais para aumentar o nível global de segurança cibernética na UE, garantindo
  + A preparação dos Estados-Membros, exigindo-lhes que estejam devidamente equipados. Por exemplo, com uma Equipa de Resposta a Incidentes de Segurança Informática (CSIRT) e uma autoridade nacional relevante em matéria de NIS,
  + cooperação entre todos os Estados-membros, através da criação de um Grupo de Cooperação para apoiar e facilitar a cooperação estratégica e o intercâmbio de informações entre os Estados-membros.
  + uma cultura de segurança através de sectores vitais para a nossa economia e sociedade e que, além disso, dependem fortemente das TIC, tais como energia, transportes, água, banca, infra-estruturas do mercado financeiro, cuidados de saúde e infra-estruturas digitais.
* Os Estados-Membros adoptaram abordagens diferentes na implementação dos SRI.
* O quadro legislativo das equipas CSIRT/CERT na República Checa é parcialmente estabelecido pela Lei de Segurança Cibernética. Esta lei estabelece as condições para a existência da equipa nacional e governamental CSIRT/CERT, mas por outro lado não restringe a criação e existência de outras equipas CSIRT/CERT.
  + Com base na Lei de Cibersegurança, duas equipas CERT/CSIRT, **nomeadamente nacionais e governamentais**, **estão obrigatoriamente estabelecidas na República Checa.** Cada uma destas equipas tem os direitos e obrigações especificados por lei (Secção 17 e seguintes do AoCS).
* O quadro legislativo das equipas CSIRT/CERT na Polónia

A Lei de 5 de Julho de 2018 sobre o sistema nacional de ciber-segurança distingue 3 CSIRTs nacionais:

* + CSIRT GOV - Equipa de Resposta a Incidentes de Segurança Informática a operar a nível nacional, liderada pelo Chefe da Agência de Segurança Interna
  + CSIRT MON - Equipa de Resposta a Incidentes de Segurança Informática a operar a nível nacional, liderada pelo Ministro da Defesa Nacional
  + CSIRT NASK - a Equipa de Resposta a Incidentes de Segurança Informática a operar a nível nacional, liderada pela Rede de Computadores Científicos e Académicos - Instituto Nacional de Investigação
  + Para além disso, a lei menciona os seguintes actores do sistema nacional de ciber-segurança:
    - operadores de serviços essenciais;
    - fornecedores de serviços digitais;
    - CSIRT MON;
    - CSIRT NASK;
    - CSIRT GOV;
    - equipas de ciber-segurança sectorial;
    - unidades do sector das finanças públicas, referidas no artigo 1º. 9 pontos 1-6, 8, 9, 11 e 12 da Lei de 27 de Agosto
    - 2009 sobre finanças públicas (Journal of Laws de 2017, item 2077 e de 2018, itens 62, 1000 e 1366);
    - institutos de investigação;
    - o Banco Nacional da Polónia;
    - Banco Gospodarstwa Krajowego;
    - o Gabinete de Inspecção Técnica;
    - Agência Polaca de Serviços de Navegação Aérea;
    - Centro Polaco de Acreditação;
    - O Fundo Nacional para a Protecção Ambiental e Gestão da Água e fundos provinciais para a protecção ambiental e gestão da água;
    - empresas comerciais que desempenham tarefas de utilidade pública na acepção da Arte. 1 cláusula 2 da Lei de 20 de Dezembro de 1996 sobre a gestão municipal (Journal of Laws de 2017, item 827 e JoL de 2018, item 1496);
    - entidades que prestam serviços de ciber-segurança;
    - autoridades competentes em matéria de ciber-segurança;
    - Ponto de contacto único para ciber-segurança;
    - o Plenipotenciário Governamental para a Ciber-segurança;
    - Colégio de Ciber-segurança.
* O quadro legislativo das equipas CSIRT/CERT em Portugal

**PALAVRAS-CHAVE A LEMBRAR** 

* ciber-segurança
* CSIRT/CERT
* Directiva SRI
* ENISA
* Circunscrição eleitoral
* CERT/CSIRT nacional e governamental
* Colaboração de equipa

**PERGUNTAS DE VERIFICAÇÃO DE CONHECIMENTOS**  

* Existe uma hierarquia entre as equipas CSIRT/CERT?
* Como é definido o âmbito de actividade de uma equipa CSIRT/CERT?
* Quem é a equipa do governo CSIRT/CERT?
* Quem é a equipa nacional CSIRT/CERT?
* Quais são as funções e tarefas de outras equipas CSIRT/CERT?
* Que tal o círculo eleitoral das equipas CSIRT/CERT no seu país?

## Conclusão

Vivemos numa época em que as tecnologias de informação e comunicação já estão indissociavelmente ligadas a todos os aspectos do nosso ser. Um certo paradoxo é que essencialmente não temos a oportunidade de evitar esta penetração e interacção mútua com as TIC, o que, ao mesmo tempo, nos torna mais vulneráveis.

medida que o volume de dados e informações armazenadas em cada FSI cresce, as questões da sua segurança efectiva, transferência ou eliminação são cada vez mais abordadas, não só com base num contrato celebrado entre o prestador de serviços e o utilizador final, mas também com base em legislação emergente.

Estados, organizações, mas também indivíduos estão cada vez mais conscientes de que a informação e os dados representam um potencial significativo, que é cada vez mais atacado por ciberataques, seja com o objectivo de roubo, dano, inacessibilidade ou eliminação de dados.

Se quisermos viver na sociedade actual e tirar partido dos seus benefícios, não é possível livrarmo-nos das TIC e definitivamente não faz sentido deixar de utilizar estas tecnologias. É necessário começar a aprender como utilizar estas tecnologias e serviços, como evitar ou pelo menos eliminar as consequências dos ciberataques.

Muitos eventos negativos podem ser evitados se indivíduos e organizações respeitarem pelo menos os princípios básicos da ciber-segurança.

No ciberespaço, como no mundo real, não existe um único tipo de segurança ou protecção que possa ser aplicado universalmente a todos. Se queremos abordar a segurança, precisamos de a abordar de forma abrangente, e precisamos de a adaptar a cada indivíduo.

As tecnologias de informação e comunicação são o campo mais dinâmico e massivamente desenvolvido. As áreas a que devemos prestar extrema atenção neste contexto são a segurança dos utilizadores e a educação.

## Referências

1. *Relatório de Investigação de Violação de Dados de 2018. 11th Edição.* [online]. [cit. 28/07/2018]. Disponível em: [http:](http://www.documentwereld.nl/files/2018/Verizon-DBIR_2018-Main_report.pdf)//www.documentwereld.nl/files/2018/Verizon-DBIR\_2018-Main\_report.pdf
2. *Analýza rizik.* [online]. [cit. 01/07/2018]. Disponível em: [https:](https://www.vlastnicesta.cz/metody/analyza-rizik-risk/)//www.vlastnicesta.cz/metody/analyza-rizik-risk/
3. ANDRESS, Jason. *The Basics of Information Security*. 2ª Edição. Singresso. ISBN: 9780128007440
4. CASEY, Eoghan. *Provas digitais e crime informático: Forensic Science, Computers, and the Internet, Segunda Edição.* Londres: Academic Press, 2004, p. 9 e seguintes.
5. *Metodologia da tríade da CIA.* [em linha]. [cit. 10/07/2018]. Disponível em: [https:](https://en.wikipedia.org/wiki/Information_security#/media/File:CIAJMK1209.png)//en.wikipedia.org/wiki/Information\_security#/media/File:CIAJMK1209.png
6. *Guia de Tratamento de Incidentes de Segurança Informática* [online]. [cit. 13/08/2018], p. 6. Disponível a partir de: <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf>
7. *Ciber-segurança.* [em linha]. [cit. 06/07/2018]. Disponível em: [https:](https://en.oxforddictionaries.com/definition/cybersecurity)//en.oxforddictionaries.com/definition/cybersecurity
8. *Ciber-segurança.* [em linha]. [cit. 06/07/2018]. Disponível a partir de: <https://www.merriam-webster.com/dictionary/cybersecurity>
9. *Ameaça cibernética.* [online]. [cit. 06/07/2018]. Disponível em: [https:](https://en.oxforddictionaries.com/definition/cyberthreat)//en.oxforddictionaries.com/definition/cyberthreat
10. *Definição de Ciber-segurança - Lacunas e sobreposições na normalização*. [em linha]. [cit. 10/12/2017]. Disponível a partir de: <https://www.enisa.europa.eu/publications/definition-of-cybersecurity> p. 30
11. *Modelo de avaliação de maturidade ENISA CSIRT* [online], 2019. VERSÃO 2.0. Atenas, Grécia: Agência da União Europeia para a Segurança das Redes e da Informação (ENISA) [cit. 2021-03-16]. ISBN 978-92-9204-292-9. Disponível em: [https:](https://www.enisa.europa.eu/publications/study-on-csirt-maturity/at_download/fullReport)//www.enisa.europa.eu/publications/study-on-csirt-maturity/at\_download/fullReport, p. 6
12. EVANS, Donald, Philip, BOND e Arden BEMET. [*Normas de Categorização de Segurança da Informação Federal e Sistemas de Informação*](http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf)*.* Instituto Nacional de Padrões e Tecnologia, Centro de Recursos de Segurança Informática. [online]. [cit. 10/12/2017]. Disponível em: <https://csrc.nist.gov/csrc/media/publications/fips/199/final/documents/fips-pub-199-final.pdf>
13. FRANCISCO, Libor. *Bezpečnostní studia.* [online]. [cit. 10/07/2018]. Disponível a partir de: <https://moodle.unob.cz/pluginfile.php/35788/mod_page/content/23/Bezpe%C4%8Dnostn%C3%AD%20studia.pdf>
14. FRUHLINGER, Josh. *O que é o Stuxnet, quem o criou e como é que funciona?* [online]. [cit. 01/07/2018]. Disponível a partir de: <https://www.csoonline.com/article/3218104/malware/what-is-stuxnet-who-created-it-and-how-does-it-work.html>
15. HENDERSON, Anthony. *A Tríade da CIA: Confidencialidade, Integridade, disponibilidade.* [em linha]. [cit. 13/01/2018]. Disponível em: [http:](http://panmore.com/the-cia-triad-confidentiality-integrity-availability)//panmore.com/the-cia-triad-confidentiality-integrity-availability
16. *Hrozba.* [online]. [cit. 28/07/2018]. Disponível em: [http:](http://www.mvcr.cz/clanek/hrozba.aspx)//www.mvcr.cz/clanek/hrozba.aspx
17. HSU, D. Frank e D. MARINUCCI (eds.). *Avanços na segurança cibernética: tecnologia, operações, e experiências*. Nova Iorque: Fordham University Press, 2013. 272 p. ISBN 978-0-8232-4456-0. p. 41.
18. JIRÁSEK, Petr, Luděk NOVÁK e Josef PO`ÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. 3ª edição actualizada. Praga: AFCEA, 2015, p. 23. [online]. [cit. 10/07/2018]. Disponível em: <https://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/vykladovy-slovnik-kyberneticke-bezpecnosti---druhe-vydani/>
19. JIROVSKÝ, Václav. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praga: Grada Publishing, a. s., 2007. p. 21 et seq
20. KADLECOVÁ, Lucie. *Konceptuální a teoretické aspekty kybernetické bezpečnosti.* [online]. [cit. 21/07/2018]. Disponível a partir de: <https://is.muni.cz/el/1423/podzim2015/BSS469/um/Prezentace_FSS_Konceptualni_a_teoreticke_aspekty_KB.pdf>
21. KOLOUCH, Jan. *CyberCrime.* Praga: CZ.NIC, 2016.
22. *Kybernetická bezpečnost: Co s tím?* [online]. [cit. 29/06/2018]. Disponível a partir de:<http://www.businessinfo.cz/cs/clanky/kyberneticka-bezpecnost-co-s-tim-84467.html>
23. *Macronův volební štáb napadli hackeři, tvrdí japonská protivirová firma.* [online]. [cit. 29/06/2017]. Disponível em: [http:](http://zpravy.idnes.cz/macron-utok-hackeri-trend-micro-d3b-/zahranicni.aspx?c=A170425_071554_zahranicni_san)//zpravy.idnes.cz/macron-utok-hackeri-trend-micro-d3b-/zahranicni.aspx?c=A170425\_071554\_zahranicni\_san
24. MAREÍSIA, Miroslav. *Bezpečnost.* [online]. [cit. 10/07/2018]. Disponível em: [https:](https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=69511)//is.mendelu.cz/eknihovna/opory/zobraz\_cast.pl?cast=69511
25. MATUROVÁ, Jana a Miroslav VALTA. *Prevence rizik - provádění kontrol technického stavu technických zařízení.* [online]. [cit. 01/07/2018]. Disponível em: [https:](https://www.bozpinfo.cz/prevence-rizik-provadeni-kontrol-technickeho-stavu-technickych-zarizeni)//www.bozpinfo.cz/prevence-rizik-provadeni-kontrol-technickeho-stavu-technickych-zarizeni
26. *Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020.* [online]. [cit. 01/07/2018]. Disponível em: <https://www.govcert.cz/download/gov-cert/container-nodeid-998/nskb-150216-final.pdf> p. 5
27. *Parkerian Hexad*. [online]. [cit. 20/08/2016]. Disponível em: [https:](https://vputhuseeri.wordpress.com/2009/08/16/149/)//vputhuseeri.wordpress.com/2009/08/16/149/
28. PO`ÁR, Josef. Informační bezpečnost. Plzeň: Aleš Čeněk, 2005, p. 37.
29. PO`ÁR, Josef. *Vybrané hrozby informační bezpečnosti organizace.* [online]. [cit. 06/07/2018]. Disponível em: [https:](https://www.cybersecurity.cz/data/pozar2.pdf)//www.cybersecurity.cz/data/pozar2.pdf
30. PROSISE, Chris e Kevin MANDIVA. *Resposta a incidentes & forense informática, segunda edição.* Emeryville: McGraw-Hill, 2003, p. 13
31. Před čím chránit? - Bezpečnostní hrozby, události, incidenty. *[online]. [cit. 06/07/2018]. Disponível a partir de:* [*https://www.kybez.cz/bezpecnost/pred-cim-chranit*](https://www.kybez.cz/bezpecnost/pred-cim-chranit)
32. *Příchod hackerů: příběh Stuxnetu.* [online]. [cit. 01/07/2018]. Disponível em: [https:](https://www.root.cz/clanky/prichod-hackeru-pribeh-stuxnetu/)//www.root.cz/clanky/prichod-hackeru-pribeh-stuxnetu/
33. RAK, Roman. Homo sapiens versus segurança. ICT fórum/PERSONALIS 2006. [apresentado em 27/09/2006]. Praga (uma apresentação da conferência).
34. SCHNEIER, Bruce. [em linha]. [cit. 18/07/2018]. Disponível em: [https:](https://www.azquotes.com/quote/570039)//www.azquotes.com/quote/570039
35. SCHNEIER, Bruce. [em linha]. [cit. 18/07/2018]. Disponível em: [https:](https://www.azquotes.com/quote/570035)//www.azquotes.com/quote/570035
36. SCHNEIER, Bruce. [em linha]. [cit. 18/07/2018]. Disponível a partir de: <https://www.azquotes.com/quote/570047>
37. SCHNEIER, Bruce. [em linha]. [cit. 18/07/2018]. Disponível em: [https:](https://www.azquotes.com/quote/570040)//www.azquotes.com/quote/570040
38. *Směrnice NIS.* [em linha]. [cit. 01/07/2018]. Disponível em: [https:](https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016L1148&amp;amp;from=EN)//eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016L1148&from=EN
39. SVOBODA, Ivan. *Řešení kybernetické bezpečnosti.* Přednáška v rámci CRIF Academy. (23/ 09/2014)
40. SÁMAL, Pavel et al. *Trestní zákoník II. § 140 až 421. Komentář.* 2. Publicar. Praga: C. H. Beck, 2012, p. 2308
41. Século, Vladimír. *Kybernetická bezpečnost.* Plzeň: Aleš Čeněk, 2018. p. 20 et seq.
42. *Tajné sluzby: Kampaň, která měla ovlivnit prezidentské volby v USA, nařídil Putin.* [online]. [cit. 29/06/2017]. Disponível em: [http:](http://www.ceskatelevize.cz/ct24/svet/2005207-tajne-sluzby-kampan-ktera-mela-ovlivnit-prezidentske-volby-v-usa-naridil-putin)//www.ceskatelevize.cz/ct24/svet/2005207-tajne-sluzby-kampan-ktera-mela-ovlivnit-prezidentske-volby-v-usa-naridil-putin
43. *A amplitude completa dos serviços da CGI Cyber Security.* [online]. [cit. 10/07/2018]. Disponível a partir de: <https://mss.cgi.com/service-portfolio>
44. *Definições e Utilização do Protocolo de Semáforos (TLP).* [online]. [cit. 13/01/2018]. Disponível a partir de: [https:](https://www.us-cert.gov/tlp)//www.us-cert.gov/tlp
45. VALÁŠEK, Jarmil, František KOVÁŘÍK et al. *Krizové řízení při nevojenských krizových situacích*. Praga: Ministerstvo vnitra - generální ředitelství Hasičského záchranného sboru ČR, 2008. [online]. [cit. 01/07/2018]. Disponível a partir de: [http://www.hzscr.cz/soubor/modul-c-krizove-rizeni-pri-nevojenskych-krizovych-situacich-pdf.aspx](view-source:http://www.hzscr.cz/soubor/modul-c-krizove-rizeni-pri-nevojenskych-krizovych-situacich-pdf.aspx)
46. WAISOVÁ, sárka. *Bezpečnost: vývoj a proměny konceptu.* Plzeň: Aleš Čeněk, s.r.o., 2005. ISBN 80-86898-21-0
47. *WannaCry se neměl vůbec vůbec rozšířit. Stačilo, abychom pouzívali Windows Update.* [online]. [cit. 27/06/2017]. Disponível em: [https:](https://www.zive.cz/clanky/wannacry-se-nemel-vubec-rozsirit-stacilo-abychom-pouzivali-windows-update/sc-3-a-187740/default.aspx)//www.zive.cz/clanky/wannacry-se-nemel-vubec-rozsirit-stacilo-abychom-pouzivali-windows-update/sc-3-a-187740/default.aspx
48. WIENER, Norbert. *Kybernetika: neboli řízení a sdělování v živých organismech a strojích.* Praga: Státní nakladatelství technické literatury, 1960. 148 p.
49. *Základní pojmy.* [online]. [cit. 10/07/2018]. Disponível em: [https:](https://www.kybez.cz/bezpecnost/pojmoslovi)//www.kybez.cz/bezpecnost/pojmoslovi
50. ZEMAN, Petr et al. *Česká bezpečnostní terminologie: Výklad základních pojmů.* [online]. [cit. 10/07/2018]. Disponível em: [http:](http://www.defenceandstrategy.eu/filemanager/files/file.php?file=16048)//www.defenceandstrategy.eu/filemanager/files/file.php?file=16048. p. 13
51. *Zpráva o stavu kybernetické bezpečnosti za rok 2017.* [online]. [cit. 29/06/2018]. Disponível em[:https://nukib.cz/download/Zpravy-KB-vCR/Zprava-stavu-KB-2017-fin.pdf](https://nukib.cz/download/Zpravy-KB-vCR/Zprava-stavu-KB-2017-fin.pdf)

1. Ver informações sobre como influenciar as eleições presidenciais nos EUA (2016) e em França (2017). Para mais pormenores, ver, por exemplo

   # *Tajné sluzby: Kampaň, která měla ovlivnit prezidentské volby v USA, nařídil Putin.* [online]. [cit. 29/06/2017]. Disponível em: [http:](http://www.ceskatelevize.cz/ct24/svet/2005207-tajne-sluzby-kampan-ktera-mela-ovlivnit-prezidentske-volby-v-usa-naridil-putin)//www.ceskatelevize.cz/ct24/svet/2005207-tajne-sluzby-kampan-ktera-mela-ovlivnit-prezidentske-volby-v-usa-naridil-putin

   # *Macronův volební štáb napadli hackeři, tvrdí japonská protivirová firma.* [online]. [cit. 29/06/2017]. Disponível em: [http:](http://zpravy.idnes.cz/macron-utok-hackeri-trend-micro-d3b-/zahranicni.aspx?c=A170425_071554_zahranicni_san)//zpravy.idnes.cz/macron-utok-hackeri-trend-micro-d3b-/zahranicni.aspx?c=A170425\_071554\_zahranicni\_san

   [↑](#footnote-ref-1)
2. A seguir referidas como as TIC [↑](#footnote-ref-2)
3. # *WannaCry se neměl vůbec vůbec rozšířit. Stačilo, abychom pouzívali Windows Update.* [online]. [cit. 27/06/2017]. Disponível a partir de:<https://www.zive.cz/clanky/wannacry-se-nemel-vubec-rozsirit-stacilo-abychom-pouzivali-windows-update/sc-3-a-187740/default.aspx>

   [↑](#footnote-ref-3)
4. *Modelo de avaliação de maturidade ENISA CSIRT* [online], 2019. VERSÃO 2.0. Atenas, Grécia: Agência da União Europeia para a Segurança das Redes e da Informação (ENISA) [cit. 2021-03-16]. ISBN 978-92-9204-292-9. Disponível em: [https:](https://www.enisa.europa.eu/publications/study-on-csirt-maturity/at_download/fullReport)//www.enisa.europa.eu/publications/study-on-csirt-maturity/at\_download/fullReport, p. 6 [↑](#footnote-ref-4)
5. *Zpráva o stavu kybernetické bezpečnosti za rok 2017.* [online]. [cit. 29/06/2018]. Disponível em: <https://nukib.cz/download/Zpravy-KB-vCR/Zprava-stavu-KB-2017-fin.pdf> [↑](#footnote-ref-5)
6. # *Kybernetická bezpečnost: Co s tím?* [online]. [cit. 29/06/2018]. Disponível a partir de:<http://www.businessinfo.cz/cs/clanky/kyberneticka-bezpecnost-co-s-tim-84467.html>

   [↑](#footnote-ref-6)
7. No que diz respeito à interpretação do próprio termo, é necessário mencionar a relativa imprecisão da língua checa em comparação com o inglês, que normalmente utiliza dois termos para o termo checo "bezpečnost": **segurança** e **protecção**. O termo **segurança** é utilizado no sentido de protecção activa ou segurança activa, garantia ou protecção e o termo **segurança** é normalmente utilizado para expressar segurança passiva, prevenção de danos, características do estado ou propriedades de um determinado objecto. [↑](#footnote-ref-7)
8. # Ver, por exemplo, a Lei Constitucional nº 110/1998 Sb., sobre a Segurança da República Checa; Lei nº 240/2000 Sb., sobre gestão de crises e emendas a certas leis (Lei da Crise); Lei da Ciber-segurança, etc.

   [↑](#footnote-ref-8)
9. ZEMAN, Petr et al. *Česká bezpečnostní terminologie: Výklad základních pojmů.* [online]. [cit. 10/07/2018]. Disponível a partir de:<http://www.defenceandstrategy.eu/filemanager/files/file.php?file=16048>, p. 13 [↑](#footnote-ref-9)
10. PO`ÁR, Josef. Informační bezpečnost. Plzeň: Aleš Čeněk, 2005, p. 37. [↑](#footnote-ref-10)
11. JIRÁSEK, Petr, Luděk NOVÁK e Josef PO`ÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. 3ª edição actualizada em Praga: AFCEA, 2015, p. 23. [online]. [cit. 10/07/2018]. Disponível em: <https://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/vykladovy-slovnik-kyberneticke-bezpecnosti---druhe-vydani/> [↑](#footnote-ref-11)
12. Para mais detalhes, ver, por exemplo, MAREŠ, Miroslav. *Bezpečnost.* [online]. [cit. 10/07/2018]. Disponível em: [https:](https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=69511)//is.mendelu.cz/eknihovna/opory/zobraz\_cast.pl?cast=69511

    WAISOVÁ, sárka. *Bezpečnost: vývoj a proměny konceptu.* Plzeň: Aleš Čeněk, s.r.o., 2005. ISBN 80-86898-21-0

    FRANCISCO, Libor. *Bezpečnostní studia.* [online]. [cit. 10/07/2018]. Disponível a partir de: <https://moodle.unob.cz/pluginfile.php/35788/mod_page/content/23/Bezpe%C4%8Dnostn%C3%AD%20studia.pdf> [↑](#footnote-ref-12)
13. Ver WAISOVÁ, sárka. *Bezpečnost: vývoj a proměny konceptu.* Plzeň: Aleš Čeněk, 2005. 159 p. ISBN 80-86898-2-10 [↑](#footnote-ref-13)
14. *Ciber-segurança.* [em linha]. [cit. 06/07/2018]. Disponível a partir de: <https://www.merriam-webster.com/dictionary/cybersecurity> [↑](#footnote-ref-14)
15. *Ciber-segurança.* [em linha]. [cit. 06/07/2018]. Disponível em: [https:](https://en.oxforddictionaries.com/definition/cybersecurity)//en.oxforddictionaries.com/definition/cybersecurity [↑](#footnote-ref-15)
16. JIRÁSEK, Petr, Luděk NOVÁK e Josef PO`ÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. 3ª edição actualizada. Praga: AFCEA, 2015, p. 69. [online]. [cit. 10/07/2018]. Disponível em: [https:](https://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/vykladovy-slovnik-kyberneticke-bezpecnosti---druhe-vydani/)//www.govcert.cz/cs/informacni-servis/akce-a-udalosti/vykladovy-slovnik-kyberneticke-bezpecnosti---druhe-vydani/ [↑](#footnote-ref-16)
17. *Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020.* [online]. [cit. 01/07/2018]. Disponível em: <https://www.govcert.cz/download/gov-cert/container-nodeid-998/nskb-150216-final.pdf> p. 5 [↑](#footnote-ref-17)
18. As aplicações, contas de utilizadores, etc. também podem ser atacadas. Relativamente aos ataques, são descritos, por exemplo, alguns ataques individuais em: KOLOUCH, Jan. *CyberCrime.* Praga: CZ.NIC, 2016, p. 181 e seguintes. [↑](#footnote-ref-18)
19. # Para mais detalhes, ver por exemplo *Příchod hackerů: příběh Stuxnetu.* [online]. [cit. 01/07/2018]. Disponível em: <https://www.root.cz/clanky/prichod-hackeru-pribeh-stuxnetu/> ou FRUHLINGER, Josh. *O que é o Stuxnet, quem o criou e como é que funciona?* [online]. [cit. 01/07/2018]. Disponível a partir de: <https://www.csoonline.com/article/3218104/malware/what-is-stuxnet-who-created-it-and-how-does-it-work.html>

    [↑](#footnote-ref-19)
20. *Definição de Ciber-segurança - Lacunas e sobreposições na normalização*. [em linha]. [cit. 10/12/2017]. Disponível a partir de: <https://www.enisa.europa.eu/publications/definition-of-cybersecurity> p. 30 [↑](#footnote-ref-20)
21. A Agência da União Europeia para a Segurança das Redes e da Informação [↑](#footnote-ref-21)
22. A seguir referida como a **Directiva SRI** ou **SNI**. [em linha]. [cit. 01/07/2018]. Disponível a partir de: [https:](https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016L1148&amp;amp;from=EN)//eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016L1148&from=EN [↑](#footnote-ref-22)
23. Ver, por exemplo, HSU, D. Frank e D. MARINUCCI (eds.). *Avanços na ciber-segurança: tecnologia, operações e experiências*. Nova Iorque: Fordham University Press, 2013. 272 p. ISBN 978-0-8232-4456-0. p. 41.

    KADLECOVÁ, Lucie. *Konceptuální a teoretické aspekty kybernetické bezpečnosti.* [online]. [cit. 21/07/2018]. Disponível a partir de: <https://is.muni.cz/el/1423/podzim2015/BSS469/um/Prezentace_FSS_Konceptualni_a_teoreticke_aspekty_KB.pdf> [↑](#footnote-ref-23)
24. Para mais detalhes, ver, por exemplo, *Parkerian Hexad*. [online]. [cit. 20/08/2016]. Disponível a partir de: <https://vputhuseeri.wordpress.com/2009/08/16/149/> [↑](#footnote-ref-24)
25. Artigo 1(b) da Convenção sobre a Criminalidade Cibernética. *Convenção sobre a Criminalidade Cibernética.* [em linha]. [cit. 20/08/2016]. Disponível a partir de: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804931c0> [↑](#footnote-ref-25)
26. PO`ÁR, Josef. *Informační bezpečnost.* Plzeň: Aleš Čeněk, 2005, p. 25 [↑](#footnote-ref-26)
27. Para mais detalhes, ver WIENER, Norbert. *Kybernetika: neboli řízení a sdělování v živých organismech a strojích.* Praga: Státní nakladatelství technické literatury, 1960. 148 p., p. 32 et seq. [↑](#footnote-ref-27)
28. SÁMAL, Pavel et al. *Trestní zákoník II. § 140 až 421. Komentář.* 2. Publicar. Praga: C. H. Beck, 2012, p. 2308 [↑](#footnote-ref-28)
29. PO`ÁR, Josef. Informační *bezpečnost.* Plzeň: Aleš Čeněk, 2005, p. 25 [↑](#footnote-ref-29)
30. Para mais pormenores, ver: KOLOUCH, Jan. *CyberCrime.* Praga: CZ.NIC, 2016, p. 57 e seguintes. [↑](#footnote-ref-30)
31. Para mais detalhes, ver por exemplo EVANS, Donald, Philip, BOND e Arden BEMET. [*Normas para Categorização de Segurança de Sistemas Federais de Informação e Informação*](http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf)*.* Instituto Nacional de Padrões e Tecnologia, Centro de Recursos de Segurança Informática. [online]. [cit. 10/12/2017]. Disponível em: <https://csrc.nist.gov/csrc/media/publications/fips/199/final/documents/fips-pub-199-final.pdf>

    ANDRESS, Jason. *The Basics of Information Security*. 2ª Edição. Singresso. ISBN: 9780128007440

    HENDERSON, Anthony. *A Tríade da CIA: Confidencialidade, Integridade, disponibilidade.* [em linha]. [cit. 13/01/2018]. Disponível em: [http:](http://panmore.com/the-cia-triad-confidentiality-integrity-availability)//panmore.com/the-cia-triad-confidentiality-integrity-availability [↑](#footnote-ref-31)
32. Para mais detalhes, ver https://www.nbu.cz/cs/pravni-predpisy/zakon-c-412-2005/1122-uplne-zneni-zakona-c-412-2005/ [↑](#footnote-ref-32)
33. Ver também: SécULC, Vladimír. *Kybernetická bezpečnost.* Plzeň: Aleš Čeněk, 2018. p. 20 et seq. [↑](#footnote-ref-33)
34. Actualmente o Centro de Protecção de Infra-estruturas Nacionais - CPNI [↑](#footnote-ref-34)
35. Para mais detalhes, ver, por exemplo, *Definições e Utilização do Protocolo de Semáforo (TLP).* [online]. [cit. 13/01/2018]. Disponível a partir de: [https:](https://www.us-cert.gov/tlp)//www.us-cert.gov/tlp [↑](#footnote-ref-35)
36. *Definições e Utilização do Protocolo de Semáforos (TLP).* [online]. [cit. 13/01/2018]. Disponível a partir de: [https:](https://www.us-cert.gov/tlp)//www.us-cert.gov/tlp [↑](#footnote-ref-36)
37. Século, Vladimír. *Kybernetická bezpečnost.* Plzeň: Aleš Čeněk, 2018. p. 19 [↑](#footnote-ref-37)
38. A seguir referido como o Decreto sobre Ciber-segurança ou **DoCS**. [↑](#footnote-ref-38)
39. JIRÁSEK, Petr, Luděk NOVÁK e Josef PO`ÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. 3ª edição actualizada. Praga: AFCEA, 2015, p. 58. [online]. [cit. 10/07/2018]. Disponível em: [http:](http://afcea.cz/wp-content/uploads/2015/03/Slovnik_v303.pdf)//afcea.cz/wp-content/uploads/2015/03/Slovnik\_v303.pdf [↑](#footnote-ref-39)
40. Século, Vladimír. *Kybernetická bezpečnost.* Plzeň: Aleš Čeněk, 2018. p. 22 [↑](#footnote-ref-40)
41. JIRÁSEK, Petr, Luděk NOVÁK e Josef PO`ÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. 3ª edição actualizada. Praga: AFCEA, 2015, p. 43. [online]. [cit. 10/07/2018]. Disponível em: [http:](http://afcea.cz/wp-content/uploads/2015/03/Slovnik_v303.pdf)//afcea.cz/wp-content/uploads/2015/03/Slovnik\_v303.pdf [↑](#footnote-ref-41)
42. Ver, por exemplo, EVANS, Donald, Philip, BOND e Arden BEMET. [*Standards for Security Categorization of Federal Information and Information Systems*](http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf)*.* Instituto Nacional de Normas e Tecnologia, Centro de Recursos de Segurança Informática. [online]. [cit. 10/12/2017]. Disponível em: <https://csrc.nist.gov/csrc/media/publications/fips/199/final/documents/fips-pub-199-final.pdf> [↑](#footnote-ref-42)
43. Século, Vladimír. *Kybernetická bezpečnost.* Plzeň: Aleš Čeněk, 2018. p. 24 [↑](#footnote-ref-43)
44. *O Parkerian Hexad*. [online]. [cit. 20/08/2016]. Disponível em: [http:](http://cs.lewisu.edu/mathcs/msisprojects/papers/georgiependerbey.pdf)//cs.lewisu.edu/mathcs/msisprojects/papers/georgiependerbey.pdf [↑](#footnote-ref-44)
45. SCHNEIER, Bruce. [em linha]. [cit. 18/07/2018]. Disponível em: [https:](https://www.azquotes.com/quote/570039)//www.azquotes.com/quote/570039 [↑](#footnote-ref-45)
46. SCHNEIER, Bruce. [em linha]. [cit. 18/07/2018]. Disponível em: [https:](https://www.azquotes.com/quote/570035)//www.azquotes.com/quote/570035 [↑](#footnote-ref-46)
47. SCHNEIER, Bruce. [em linha]. [cit. 18/07/2018]. Disponível em: [https:](https://www.azquotes.com/quote/570040)//www.azquotes.com/quote/570040 [↑](#footnote-ref-47)
48. Um firewall é um sistema que contém regras que regem os fluxos de dados dentro das tecnologias de rede. [↑](#footnote-ref-48)
49. **IPS** (Sistema de Prevenção de Intrusão), um dispositivo que monitoriza a actividade indesejada (maliciosa) da rede e/ou actividade do sistema informático. A seguir referido como **IPS.**

    **IDS** (Intrusion Detection System) é um sistema concebido para detectar actividades invulgares que podem potencialmente levar a violações da segurança de redes informáticas, sistemas informáticos, aplicações, etc. A seguir designado por **IDS**. [↑](#footnote-ref-49)
50. Um honeypot é um sistema cujo objectivo é detectar malware ou outras actividades indesejadas, que são depois analisadas neste ambiente artificial. [↑](#footnote-ref-50)
51. SCHNEIER, Bruce. [em linha]. [cit. 18/07/2018]. Disponível a partir de: <https://www.azquotes.com/quote/570047> [↑](#footnote-ref-51)
52. O termo "utilizador" é aqui utilizado para expressar uma pessoa singular autorizada a utilizar elementos das TIC, sistemas e aplicações individuais. Deste ponto de vista, o utilizador significa tanto uma pessoa com direitos de administrador como um utilizador final. [↑](#footnote-ref-52)
53. O gráfico foi baseado no gráfico publicado em: *Metodologia da tríade da CIA.* [em linha]. [cit. 10/07/2018]. Disponível em: [https:](https://en.wikipedia.org/wiki/Information_security#/media/File:CIAJMK1209.png)//en.wikipedia.org/wiki/Information\_security#/media/File:CIAJMK1209.png [↑](#footnote-ref-53)
54. Para mais detalhes, ver SVOBODA, Ivan. *Řešení kybernetické bezpečnosti.* Přednáška v rámci CRIF Academy. (23/ 09/2014) [↑](#footnote-ref-54)
55. *Základní pojmy.* [online]. [cit. 10/07/2018]. Disponível em: [https:](https://www.kybez.cz/bezpecnost/pojmoslovi)//www.kybez.cz/bezpecnost/pojmoslovi [↑](#footnote-ref-55)
56. *A amplitude completa dos serviços da CGI Cyber Security.* [online]. [cit. 10/07/2018]. Disponível a partir de: <https://mss.cgi.com/service-portfolio> [↑](#footnote-ref-56)
57. *Relatório de Investigação de Violação de Dados de 2018. 11th Edição.* [online]. [cit. 28/07/2018]. Disponível em: [http:](http://www.documentwereld.nl/files/2018/Verizon-DBIR_2018-Main_report.pdf)//www.documentwereld.nl/files/2018/Verizon-DBIR\_2018-Main\_report.pdf [↑](#footnote-ref-57)
58. As técnicas e ferramentas são geralmente combinadas como parte de ataques individuais. [↑](#footnote-ref-58)
59. *Relatório de Investigação de Violação de Dados de 2018. 11th Edição.* [online]. [cit. 28/07/2018]. Disponível a partir de: <http://www.documentwereld.nl/files/2018/Verizon-DBIR_2018-Main_report.pdf> p. 7 [↑](#footnote-ref-59)
60. *Národní úřad pro kybernetickou a informační bezpečnost.* A seguir referido como **NUKIB** [↑](#footnote-ref-60)
61. *Zpráva o stavu kybernetické bezpečnosti za rok 2017.* [online]. [cit. 29/06/2018]. Disponível em: <https://nukib.cz/download/Zpravy-KB-vCR/Zprava-stavu-KB-2017-fin.pdf> [↑](#footnote-ref-61)
62. *Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020.* [online]. [cit. 01/07/2018]. Disponível em: [https:](https://www.govcert.cz/download/gov-cert/container-nodeid-998/nskb-150216-final.pdf)//www.govcert.cz/download/gov-cert/container-nodeid-998/nskb-150216-final.pdf [↑](#footnote-ref-62)
63. JIRÁSEK, Petr, Luděk NOVÁK e Josef PO`ÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. 3ª edição actualizada. Praga: AFCEA, 2015. p. 99. Disponível em: <https://nukib.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf> [↑](#footnote-ref-63)
64. VALÁŠEK, Jarmil, František KOVÁŘÍK et al. *Krizové řízení při nevojenských krizových situacích*. Praga: Ministerstvo vnitra - generální ředitelství Hasičského záchranného sboru ČR, 2008. [online]. [cit. 01/07/2018]. Disponível a partir de: [http://www.hzscr.cz/soubor/modul-c-krizove-rizeni-pri-nevojenskych-krizovych-situacich-pdf.aspx](view-source:http://www.hzscr.cz/soubor/modul-c-krizove-rizeni-pri-nevojenskych-krizovych-situacich-pdf.aspx)

    ISBN 978-80-86640-93-8 p. 73 [↑](#footnote-ref-64)
65. *Analýza rizik.* [online]. [cit. 01/07/2018]. Disponível em: [https:](https://www.vlastnicesta.cz/metody/analyza-rizik-risk/)//www.vlastnicesta.cz/metody/analyza-rizik-risk/ [↑](#footnote-ref-65)
66. Cf. JIRÁSEK, Petr, Luděk NOVÁK e Josef PO`ÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. 3ª edição actualizada. Praga: AFCEA, 2015. p. 29. Disponível em: <https://nukib.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf> [↑](#footnote-ref-66)
67. *Hrozba.* [online]. [cit. 28/07/2018]. Disponível em: [http:](http://www.mvcr.cz/clanek/hrozba.aspx)//www.mvcr.cz/clanek/hrozba.aspx [↑](#footnote-ref-67)
68. JIRÁSEK, Petr, Luděk NOVÁK e Josef PO`ÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. 3ª edição actualizada. Praga: AFCEA, 2015. p. 52. Disponível em: <https://nukib.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf> [↑](#footnote-ref-68)
69. Neste caso, há um problema com a tradução de alguns termos do inglês e vice-versa. Se quisermos traduzir consistentemente o termo ameaça à segurança da informação, então o equivalente checo correcto é, por exemplo, "hrozba pro bezpečnost informací; hrozba zabezpečení informací" etc. [↑](#footnote-ref-69)
70. Ibidem, p. 25. [↑](#footnote-ref-70)
71. Ibidem, p. 16, 81 a 87 [↑](#footnote-ref-71)
72. *Ameaça cibernética.* [online]. [cit. 06/07/2018]. Disponível em: [https:](https://en.oxforddictionaries.com/definition/cyberthreat)//en.oxforddictionaries.com/definition/cyberthreat [↑](#footnote-ref-72)
73. A alteração também significa o roubo de informação, a sua destruição, ou a frustração da sua utilização. [↑](#footnote-ref-73)
74. Cf. JIROVSKÝ, Václav. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praga: Grada Publishing, a. s., 2007. p. 21 et seq. [↑](#footnote-ref-74)
75. Estes ataques são, por exemplo, **DoS** - **Denial of Service**, **DDoS** - **Distributed Denial of Service**, etc. Para mais detalhes, ver KOLOUCH, Jan. *CyberCrime.* Praga: CZ.NIC, 2016, p. 295 e seguintes. [↑](#footnote-ref-75)
76. Por exemplo, um sistema cobrado será atacado e os seus serviços utilizados sem pagamento por serviços. [↑](#footnote-ref-76)
77. Para ciberataques individuais, ver por exemplo: KOLOUCH, Jan. *CyberCrime.* Praga: CZ.NIC, 2016, p. 181 e seguintes. [↑](#footnote-ref-77)
78. Para mais detalhes, ver, por exemplo, PO`ÁR, Josef. *Vybrané hrozby informační bezpečnosti organizace.* [online]. [cit. 06/07/2018]. Disponível em: [https:](https://www.cybersecurity.cz/data/pozar2.pdf)//www.cybersecurity.cz/data/pozar2.pdf [↑](#footnote-ref-78)
79. ### Před čím chránit? - Bezpečnostní hrozby, události, incidenty. [online]. [cit. 06/07/2018]. Disponível a partir de: <https://www.kybez.cz/bezpecnost/pred-cim-chranit>

    [↑](#footnote-ref-79)
80. PROSISE, Chris e Kevin MANDIVA. *Resposta a incidentes & forense informática, segunda edição.* Emeryville: McGraw-Hill, 2003, p. 13

    Ver também: CASEY, Eoghan. *Evidência Digital e Crime Informático: Forensic Science, Computers, and the Internet, Segunda Edição.* Londres: Academic Press, 2004, p. 9 e seguintes. [↑](#footnote-ref-80)
81. JIRÁSEK, Petr, Luděk NOVÁK e Josef PO`ÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. 3ª edição actualizada. Praga: AFCEA, 2015. p. 28. Disponível em: <https://nukib.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf> [↑](#footnote-ref-81)
82. *Guia de Tratamento de Incidentes de Segurança Informática* [online]. [cit. 13/08/2018]**, p. 6**. Disponível a partir de: <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf> [↑](#footnote-ref-82)
83. JIRÁSEK, Petr, Luděk NOVÁK e Josef PO`ÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. 3ª edição actualizada. Praga: AFCEA, 2015. p. 25. Disponível em: <https://nukib.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf> [↑](#footnote-ref-83)
84. *Guia de Tratamento de Incidentes de Segurança Informática* [online]. [cit. 17/02/2018], p. 6. Disponível em: <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf> [↑](#footnote-ref-84)
85. JIRÁSEK, Petr, Luděk NOVÁK e Josef PO`ÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. 3ª edição actualizada. Praga: AFCEA, 2015. p. 71. Disponível em: <https://nukib.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf> [↑](#footnote-ref-85)
86. A definição acima carece especialmente de uma definição de qualquer motivação do atacante que não seja a de... *causar danos ou ganhar para informações estrategicamente importantes*. Um exemplo não abrangido por esta definição pode ser os ataques motivados economicamente, que estão a crescer dramaticamente no presente. [↑](#footnote-ref-86)
87. É necessário distinguir o conceito de ciberataque do conceito de incidente de segurança, que representa uma violação da segurança SI/TI e das regras definidas para a sua protecção (política de segurança). [↑](#footnote-ref-87)
88. *Definição de Ciber-segurança - Lacunas e sobreposições na normalização*. [em linha]. [cit. 10/12/2017]. Disponível a partir de: <https://www.enisa.europa.eu/publications/definition-of-cybersecurity> p. 30 [↑](#footnote-ref-88)
89. A Agência da União Europeia para a Segurança das Redes e da Informação [↑](#footnote-ref-89)
90. A seguir referida como a **Directiva SRI** ou **SNI**. [em linha]. [cit. 01/07/2018]. Disponível a partir de: [https:](https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016L1148&amp;amp;from=EN)//eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016L1148&from=EN [↑](#footnote-ref-90)
91. **AS** - Sistema Autónomo. Um sistema autónomo é um conjunto de redes IP e encaminhadores sob gestão técnica comum, o que representa uma política comum de encaminhamento para a Internet. [↑](#footnote-ref-91)
92. **RTIR** - Request **Tracker** for Incident Response (**RTIR).** Para mais detalhes, ver, por exemplo: [http:](http://www.bestpractical.com/rtir/)//www.bestpractical.com/rtir/. [↑](#footnote-ref-92)
93. **OTRS** - **Sistema de** Pedido de Bilhetes de Código Aberto. Para mais detalhes, ver, por exemplo: [http:](http://www.otrs.org/)//www.otrs.org/. [↑](#footnote-ref-93)
94. A associação foi formada pela fusão da TERENA (Trans-European Research and Education Networking Association) e da DANTE. [↑](#footnote-ref-94)
95. Mais informação sobre o FIRST pode ser encontrada em: [https:](https://www.first.org)//www.first.org [↑](#footnote-ref-95)
96. A seguir também **TI**. [↑](#footnote-ref-96)
97. ***Listada -*** listagem da equipa na base de dados de todas as equipas registadas. [↑](#footnote-ref-97)
98. A Associação CESNET, z. S. P. O., é uma associação industrial de pessoas colectivas, fundada em 1996 por universidades e pela Academia de Ciências da República Checa. Opera a rede nacional de computadores de alta velocidade para a ciência, investigação, desenvolvimento e educação CESNET2. Para mais detalhes, ver: [http:](http://www.cesnet.cz/)//www.cesnet.cz/. [↑](#footnote-ref-98)
99. **AS** - Sistema Autónomo. Um sistema autónomo é um conjunto de redes IP e encaminhadores sob gestão técnica comum, o que representa uma política comum de encaminhamento para a Internet. [↑](#footnote-ref-99)
100. *Modelo de avaliação de maturidade ENISA CSIRT* [online], 2019. VERSÃO 2.0. Atenas, Grécia: Agência da União Europeia para a Segurança das Redes e da Informação (ENISA) [cit. 2021-03-16]. ISBN 978-92-9204-292-9. Disponível em: [https:](https://www.enisa.europa.eu/publications/study-on-csirt-maturity/at_download/fullReport)//www.enisa.europa.eu/publications/study-on-csirt-maturity/at\_download/fullReport, p. 5-6 [↑](#footnote-ref-100)
101. *Modelo de avaliação de maturidade ENISA CSIRT* [online], 2019. VERSÃO 2.0. Atenas, Grécia: Agência da União Europeia para a Segurança das Redes e da Informação (ENISA) [cit. 2021-03-16]. ISBN 978-92-9204-292-9. Disponível em: [https:](https://www.enisa.europa.eu/publications/study-on-csirt-maturity/at_download/fullReport)//www.enisa.europa.eu/publications/study-on-csirt-maturity/at\_download/fullReport, p. 11 [↑](#footnote-ref-101)
102. Artigo 9º do SNI [↑](#footnote-ref-102)
103. *Kdy nás kontaktovat.* [online]. [cit. 07/07/2018]. Disponível em: [https:](https://www.csirt.cz/page/2632/kdy-nas-kontaktovat/)//www.csirt.cz/page/2632/kdy-nas-kontaktovat/ [↑](#footnote-ref-103)
104. *Sluzby CSIRT.CZ.* [online]. [cit. 07/07/2018]. Disponível a partir de:<https://csirt.cz/page/2764/sluzby/> [↑](#footnote-ref-104)
105. Todas as tarefas são tiradas de: *Sluzby CSIRT.CZ.* [online]. [cit. 07/07/2018]. Disponível a partir de: <https://csirt.cz/page/2764/sluzby/> [↑](#footnote-ref-105)
106. Lei n.º 127/2005 Sb., sobre Comunicações Electrónicas e sobre a Alteração de Certas Leis Relacionadas (Lei das Comunicações Electrónicas), com as alterações que lhe foram introduzidas. [↑](#footnote-ref-106)
107. Lei n.º 269/1994 Sb., sobre o Registo Criminal, com as alterações que lhe foram introduzidas. [↑](#footnote-ref-107)
108. Nos termos da Secção 20 (1) do Código Civil (CC), uma pessoa colectiva significa ***"uma entidade organizada que a lei estipula ter personalidade jurídica ou cuja personalidade jurídica é reconhecida por lei".*** *Independentemente do objecto da sua actividade, uma pessoa colectiva pode ter direitos e obrigações que sejam compatíveis com a sua natureza jurídica".* O Estado é considerado uma entidade jurídica no domínio do direito privado. (Secção 21 do CC).

     **Uma entidade jurídica pode ser uma pessoa de direito privado ou público**, dependendo do interesse em que a entidade jurídica se encontra estabelecida (Secção 144 do CC). Do ponto de vista do direito civil, as sociedades (ver Secção 210 e seguintes do CC), as fundações (ver Secção 303 e seguintes do CC) e os institutos (ver Secção 402 e seguintes do CC) são entidades jurídicas. [↑](#footnote-ref-108)
109. A utilização do instituto de um contrato público de acordo com a Secção 160 e seguintes de SŘ corresponde à presunção de que o operador do CERT nacional será uma pessoa de direito privado. [↑](#footnote-ref-109)
110. Ver artigo 9º do SNI [↑](#footnote-ref-110)
111. *Poskytované sluzby.* [online]. [cit. 01/08/2018]. Disponível a partir de: [https:](https://www.govcert.cz/cs/vladni-cert/poskytovane-sluzby/)//www.govcert.cz/cs/vladni-cert/poskytovane-sluzby/ [↑](#footnote-ref-111)
112. Todas as tarefas são retiradas de: *Poskytované sluzby.* [online]. [cit. 07/07/2018]. Disponível a partir de: [https:](https://www.govcert.cz/cs/vladni-cert/poskytovane-sluzby/)//www.govcert.cz/cs/vladni-cert/poskytovane-sluzby/ [↑](#footnote-ref-112)