Rok 2026: Kybernetická bezpečnosť pod tlakom termínov (bezpečnostné opatrenia, incidenty a audity)

JUDr. Ing. Miroslav Chlipala, PhD., LL.M.

AICH
ADVOKÁTI CHLIPALA

2014 - 2025 právnická firma roka

RANKED IN Chambers Europe 2021 - 2025

Miroslav Chlipala

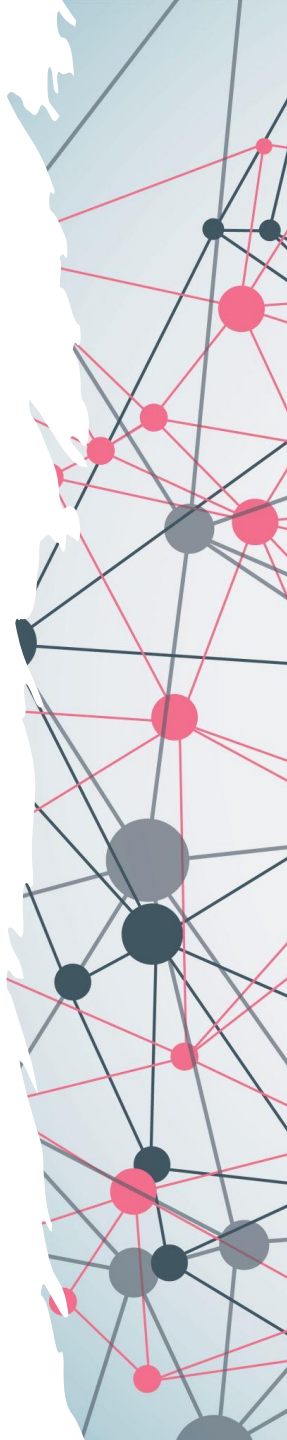
- Advokát s 23-ročnou praxou so zameraním na IT právo a moderné technológie
- Člen Asociácie kybernetickej bezpečnosti
- Spoluautor Komentára k zákonu o kybernetickej bezpečnosti
- Certifikovaný tútor Rady Európy pre vzdelávanie advokátov, sudcov a prokurátorov
- Člen Stálej komisie pre etiku a reguláciu umelej inteligencie pri MIRRI SR

ESET Security Days 2026

„Robíme v kybernetickej bezpečnosti dosť?“ Odpoveď býva zvyčajne rovnaká – kým incident nepríde, málokto si uvedomí, že rozhodujúce je príprava v súlade s legislatívnymi požiadavkami. Rok 2026 prináša nové povinnosti a termíny, ktoré budú mať zásadný vplyv na fungovanie PZS a ich dodávateľske reťazce.

V mojom vystúpení preto ukážem, **ktoré termíny podľa zákona č. 69/2018 Z.z. a jeho vyhlášok v roku 2026 nemožno ignorovať**. Predstavím **novú vyhlášku o bezpečnostných opatreniach**, ako aj **vyhlášku o hlásení incidentov**. Pozrieme sa aj na **novú metodiku NBÚ pre analýzu rizík**. Špeciálnu pozornosť venujem **pripravovanej vyhláške o auditoch**, ktorá prinesie **nové pravidlá periodicity samohodnotení a auditov** – s dopadom na **PZS a PKZS**.

Cieľom môjho príspevku je poskytnúť jasný prehľad toho, čo sa mení, ktoré povinnosti treba splniť v konkrétnych termínoch a ako sa na rok 2026 pripraviť tak, aby bola organizácia nielen v súlade so zákonom, ale najmä odolnejšia voči reálnym rizikám.



Termíny

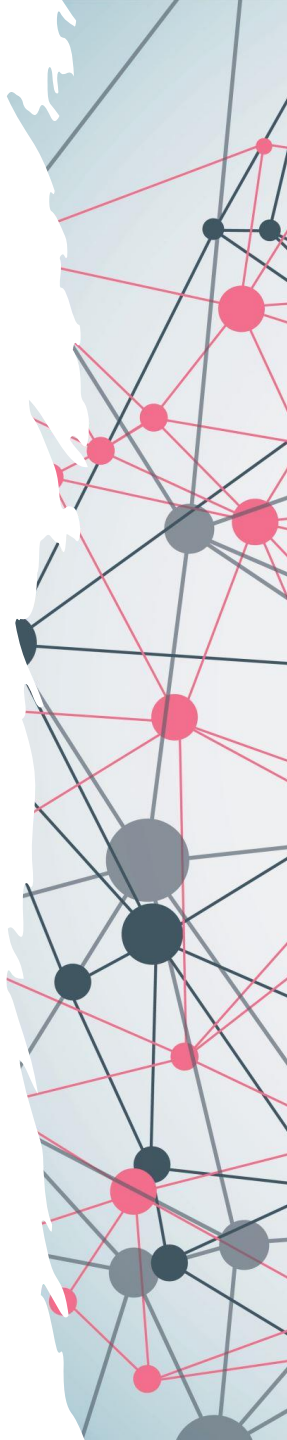
ktoré podľa zákona č. 69/2018 Z.z. a jeho vyhlášok **v roku 2026 nemožno ignorovať**

Bezpečnostné opatrenia

Bezpečnostné opatrenia

: **Minimálne** bezpečnostné opatrenia

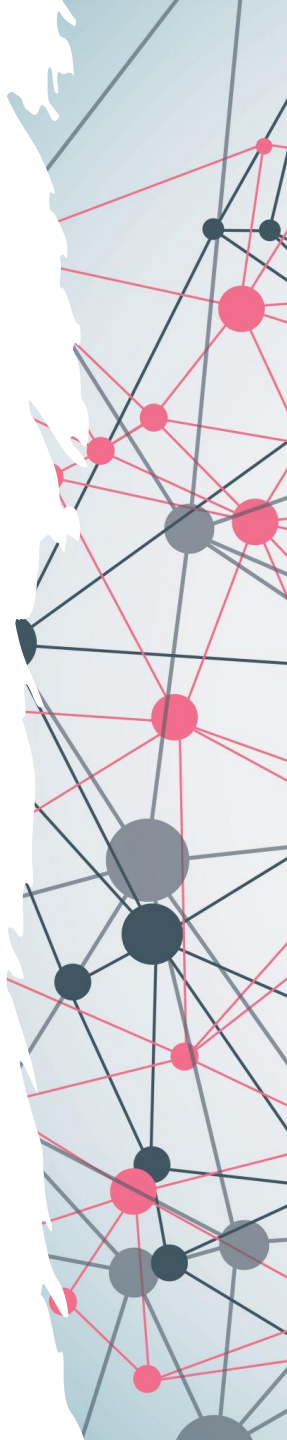
: **„Ďalšie“** bezpečnostné opatrenia



Minimálne bezpečnostné opatrenia

§ 20 ods. 4 ZoKB

: 9 opatrení

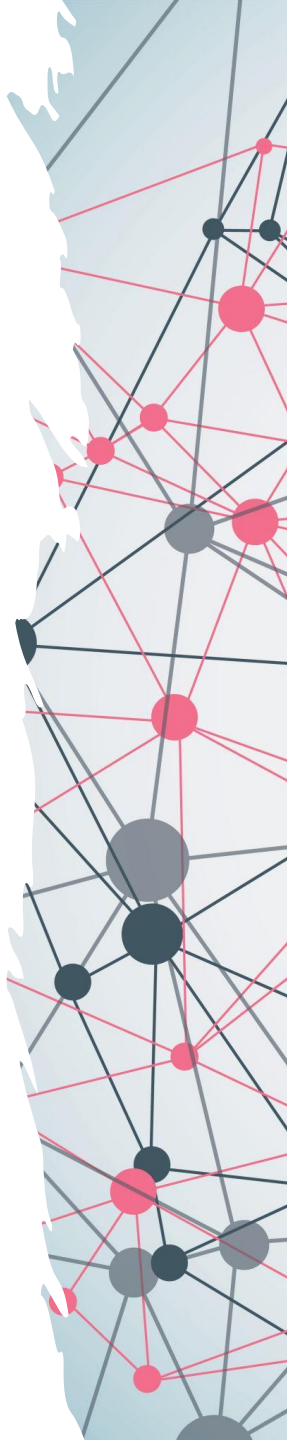


„Ďalšie“ bezpečnostné opatrenia

:Sektorové bezpečnostné opatrenia,
(ak existujú)

:Všeobecné bezpečnostné opatrenia

(ak **neexistujú** sektorové bezpečnostné opatrenia)



Všeobecné bezpečnostné opatrenia

§ 20 ods. 2 ZoKB

: 18 opatrení

§ 3 ods. 2 v spojení s **Prílohou č. 1** vyhlášky č. 227/2025 Z.z. o bezpečnostných opatreniach

: 151 položiek

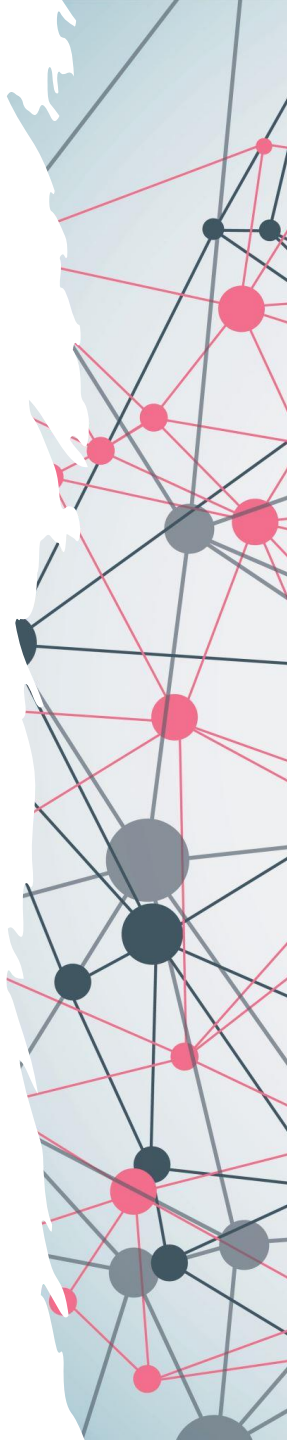
Sektorové bezpečnostné opatrenia

: DORA

Nariadenie 2022/2554 o digitálnej prevádzkovej odolnosti finančného sektora

Sektorové bezpečnostné opatrenia

: Atómový zákon



Sektorové bezpečnostné opatrenia

: Zákon č. 95/2019 Z. z.

o informačných technológiách

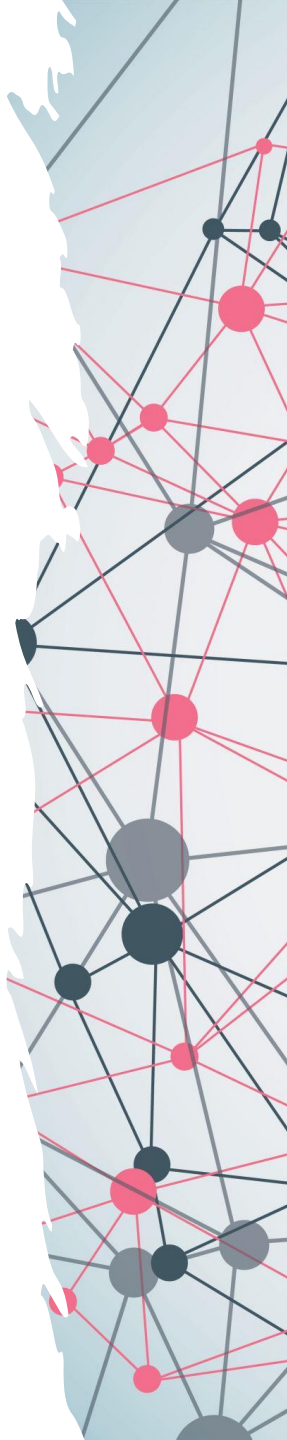
vo verejnej správe

: **Vyhláška č. 179/2020 Z.z.** ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy

Bezpečnostné opatrenia
podľa osobitného predpisu

: Vykonávacie nariadenie Komisie (EÚ) 2024/2690 pre **digitálnych sektor**

: ZoKB nedefinuje vzťah BO podľa osobitného predpisu k všeobecným BO a k sektorovým BO



Termíny

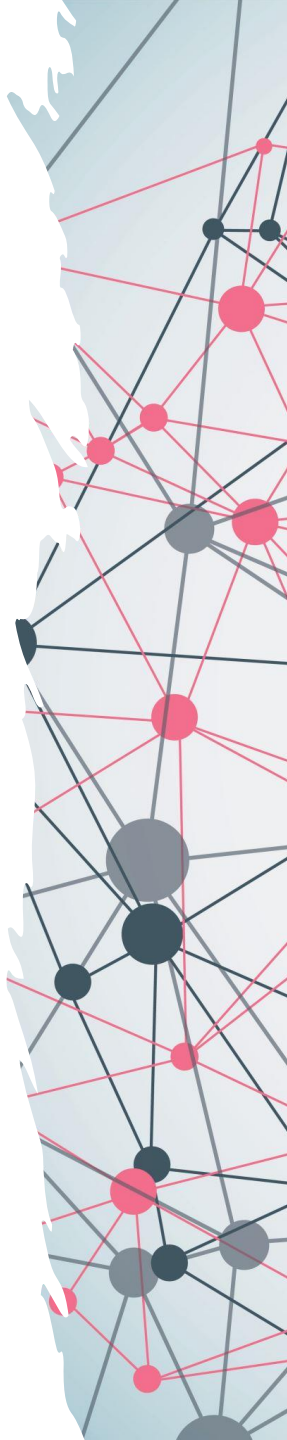
Zákon o kybernetickej bezpečnosti

Zákon o kybernetickej bezpečnosti

Oznamovacia povinnosť

: **60 dní** oznámiť začatie činnosti PZS

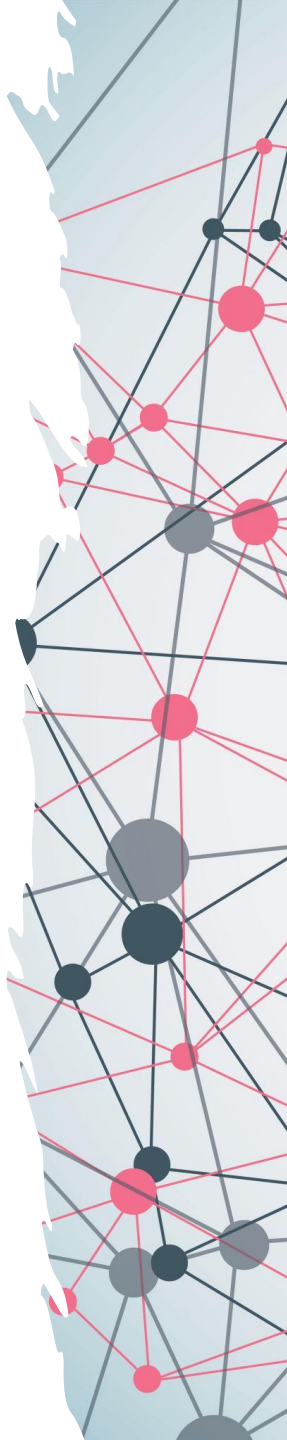
: **14/30 dní** oznámiť zmeny zapísaných údajov



Zákon o kybernetickej bezpečnosti

: Práva a povinnosti PZS

vznikajú **dňom uvedeným v oznámení** o zápise do registra

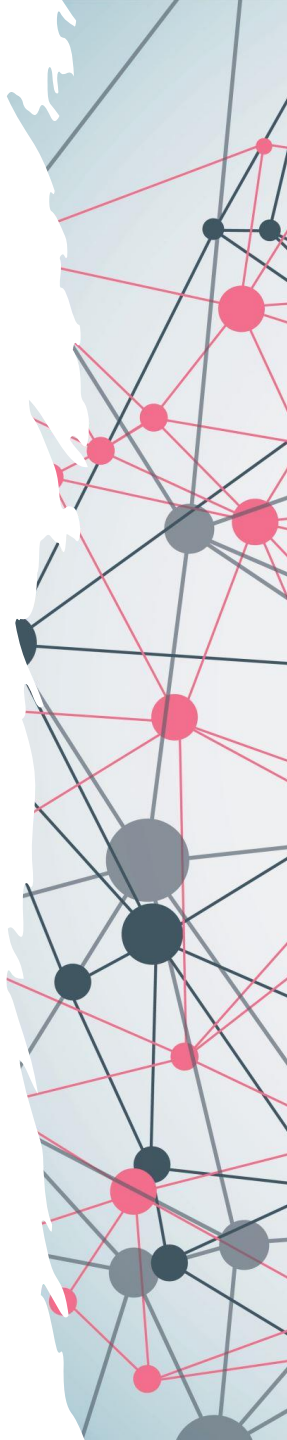


Zákon o kybernetickej bezpečnosti

Bezpečnostné opatrenia

: PZS je povinný do **12 mesiacov odo dňa zápisu do registra**

... prijať a vykonávať všeobecné bezpečnostné opatrenia



Zákon o kybernetickej bezpečnosti

: Povinnosti podľa § 19 ods. 6

(riešiť KBI, hlásiť závažný KBI, zabezpečiť dôkaz, oznámiť TČ, včasné informovanie štatutára)

: Povinnosti uložené zo strany NBÚ

(prijať opatrenia na nápravu, informovať verejnosť, zákaz poskytovať službu)

: Povinnosť vykonať audit / samohodnotenie

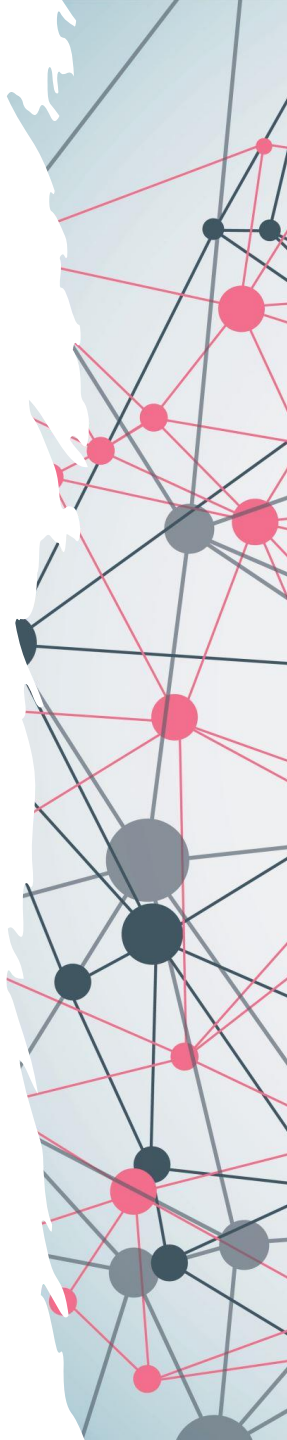
: Povinnosť súčinnosti a poskytnutia informácií

Zákon o kybernetickej bezpečnosti

Bezpečnostná dokumentácia

: musí byť udržiavaná aktuálna

: trvalá povinnosť

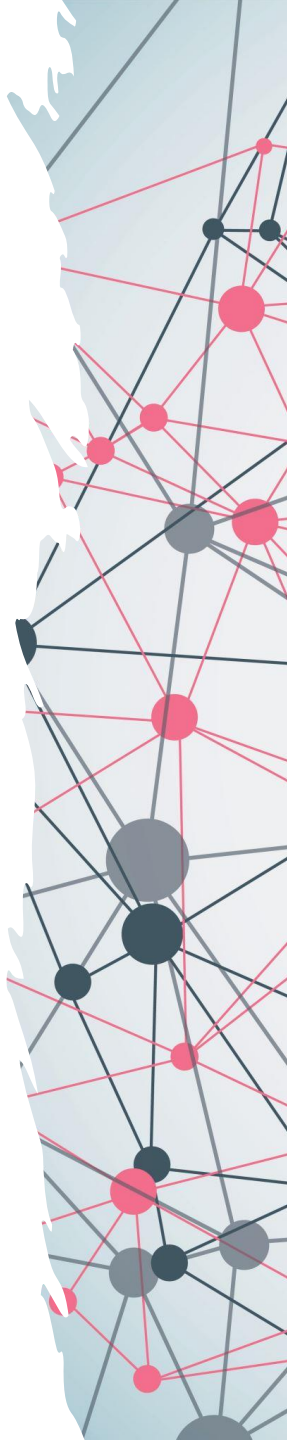


Zákon o kybernetickej bezpečnosti

31.12.2026

: NBÚ môže rozhodnúť o výmaze PZS / PKZS

: odporúčame podať „podnet“ PZS / PKZS na NBÚ



Zákon o kybernetickej bezpečnosti

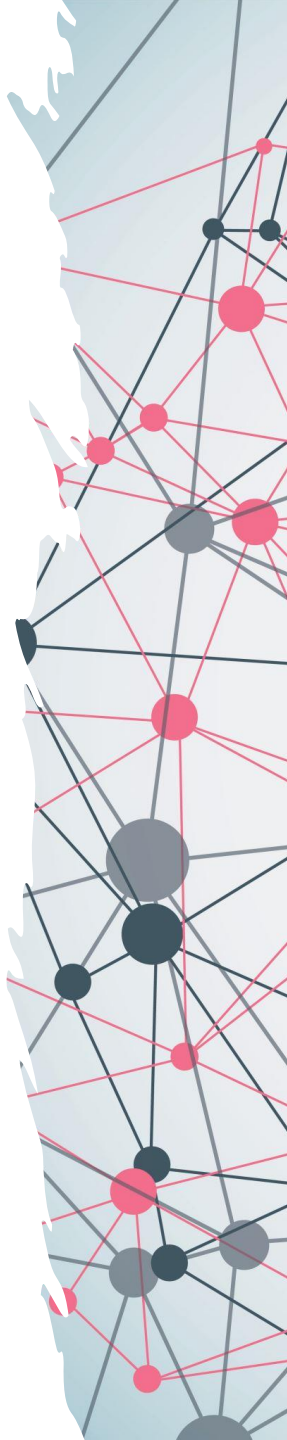
Kedykoľvek

: NBÚ môže vymazať PZS / PKZS

: odôvodnená žiadosť PZS / PKZS na NBÚ

: (alternatívne) „podnet“ na ústredný orgán

výmaz na základe oznámenia ústredného orgánu



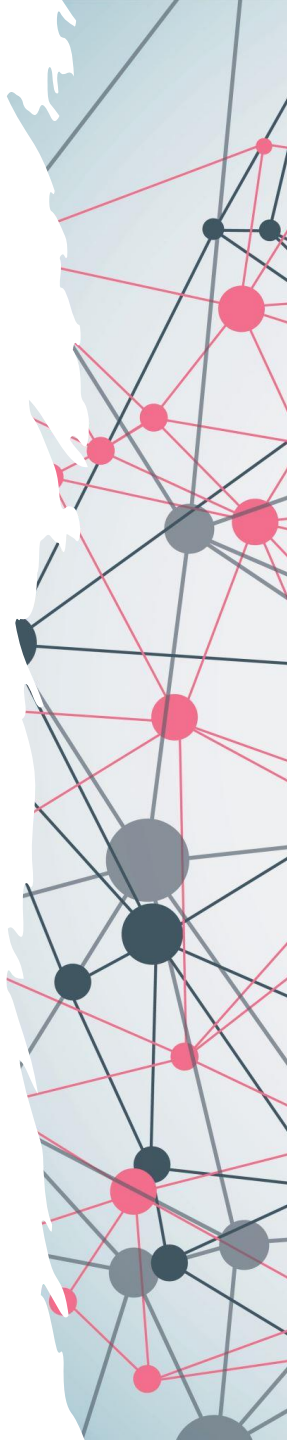
Termíny

Vyhláška
o bezpečnostných opatreniach

Vyhláška o bezpečnostných opatreniach

Vlastná bezpečnostná metodika pre analýzu rizík

: Mapovanie na úrovne rizika v súlade s Metodikou 2.0
(účinná od 01.09.2025)

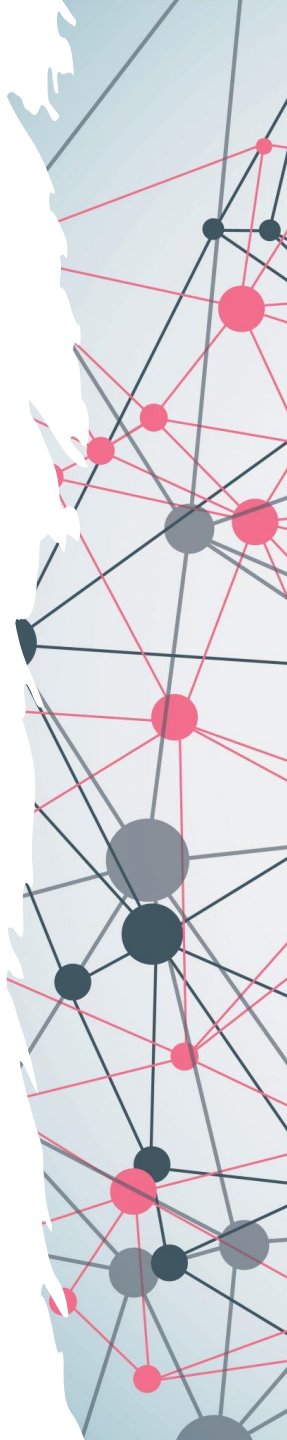


Vyhláška o bezpečnostných opatreniach

Preskúmavanie identifikovaných rizík

: Najmenej **raz ročne**

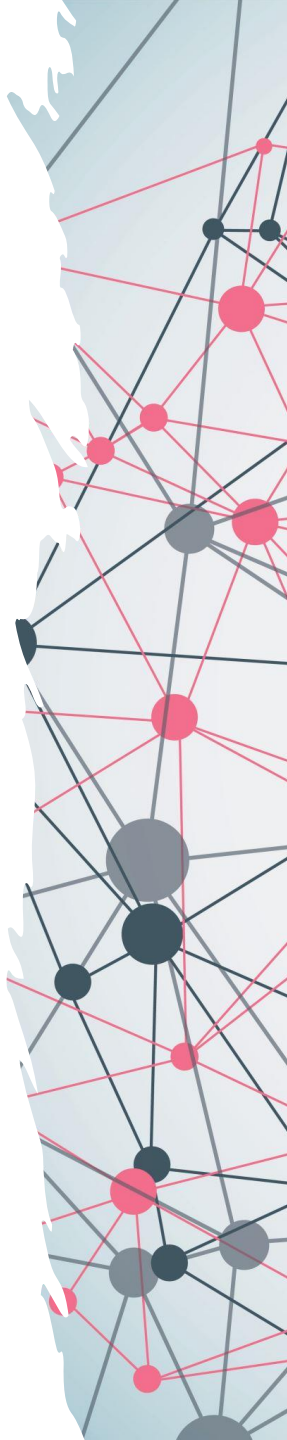
: Aktualizácia rizík (ak treba)
: Revízia prijatých bezpečnostných opatrení (ak treba)



Vyhláška o bezpečnostných opatreniach

Zmluvy s tretími stranami

: nesmú byť po 31.08.2025 predlžované,
ak nie sú v súlade s novými bezpečnostnými opatreniami



Termíny

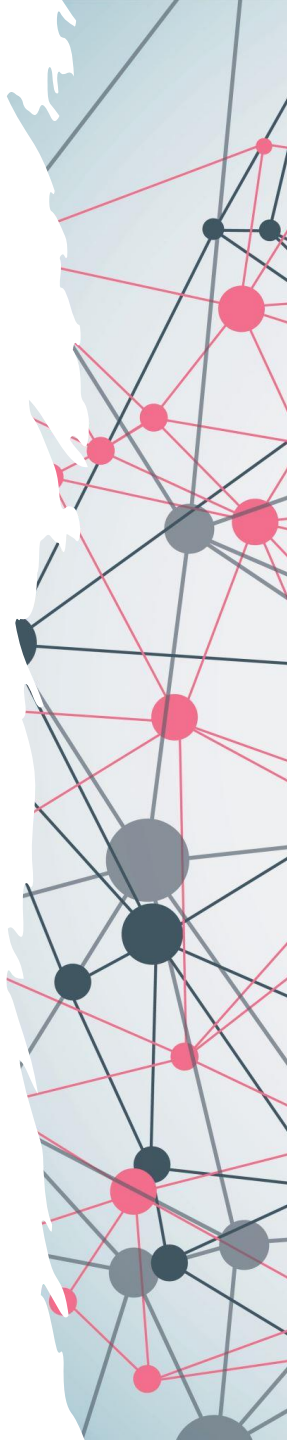
Vyhláška
o „hlásení incidentov“

Vyhláška o „hlásení incidentov“

Úplný výpadok alebo nedostupnosť činnosti
: PKZS >30 min., PZS >60 min.

Narušenie alebo obmedzenie činnosti
: PKZS >60 min., PZS >180 min.

(Identifikačné kritériá závažného narušenia fungovania Prevádzkovateľa základnej služby)



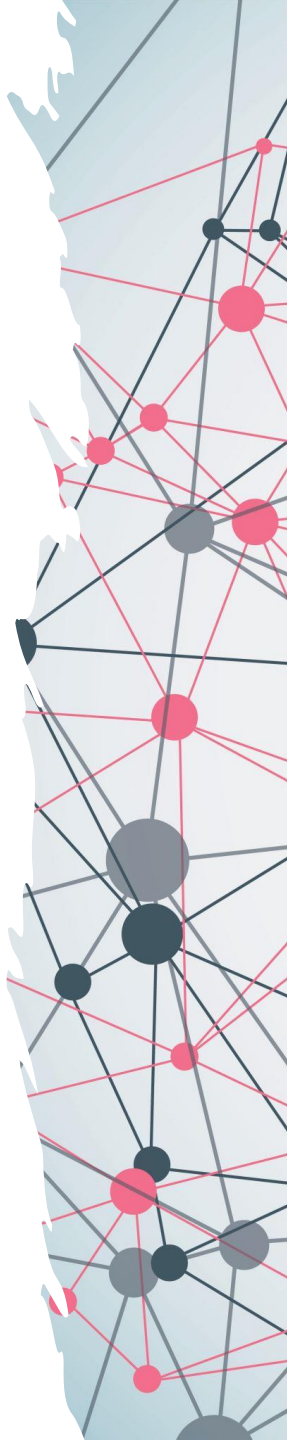
Hlásenie incidentov

Včasné varovanie
24 hodín
od zistenia

Oznámenie
72 hodín od
zistenia

Záverečná správa
1 mesiac
od Oznámenia

Aktualizovaná ZS
30 dní od
obnovenia
prevádzky



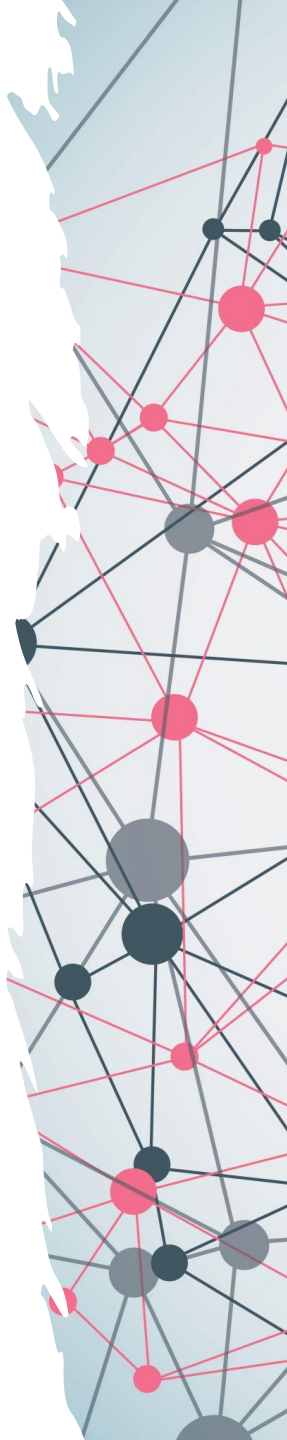
Termíny

Vyhláška
o audite „návrh novely“

Vyhláška o audite (návrh novely)

PKZS

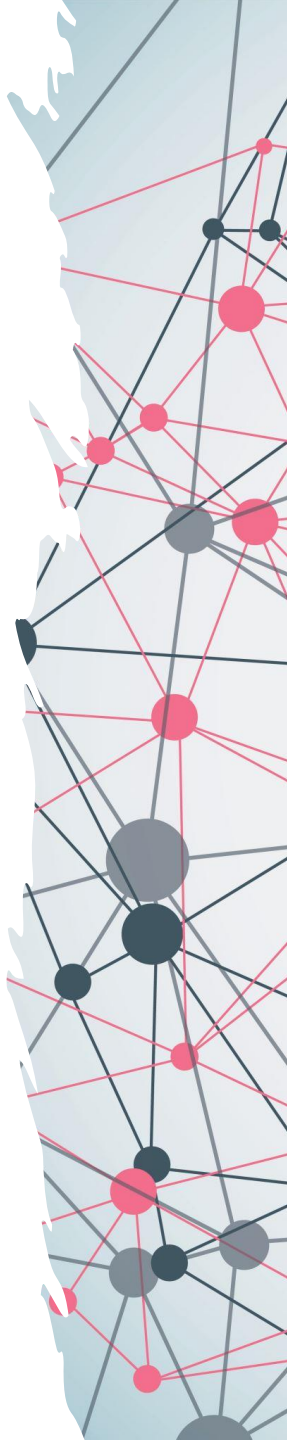
: audit musí byť vykonaný a ukončený najneskôr
do konca 3. kalendárneho roka
nasledujúceho po roku, v ktorom bol posledný audit ukončený



Vyhláška o audite (návrh novely)

PZS

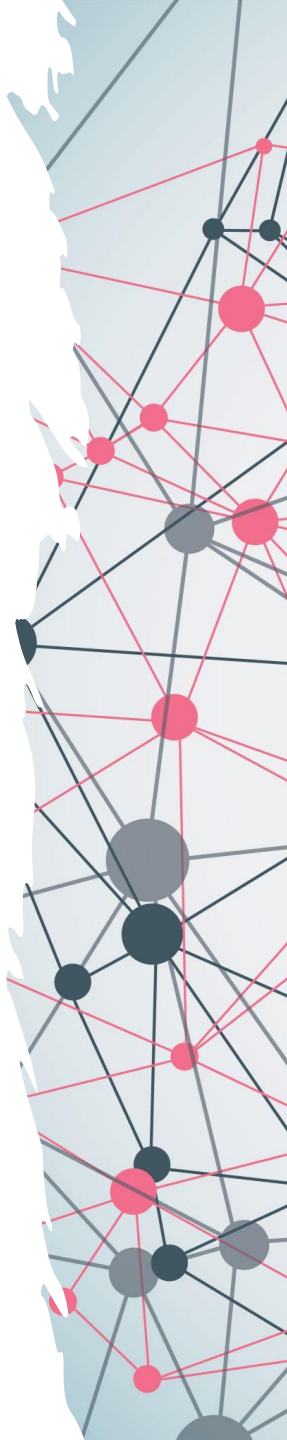
: audit musí byť vykonaný a ukončený najneskôr
do konca 5. kalendárneho roka
nasledujúceho po roku, v ktorom bol posledný audit ukončený



Vyhláška o audite (návrh novely)

PZS a samohodnotenie

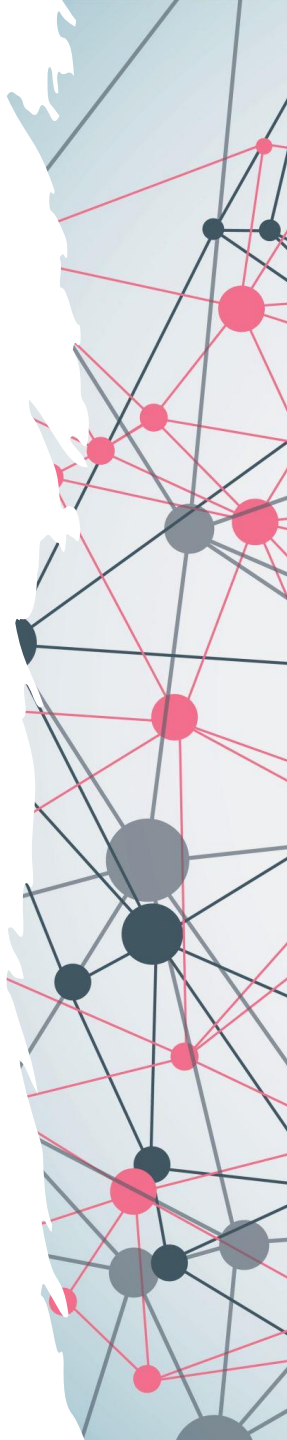
: vykonáva sa každé **2 roky**
: nevykonáva sa v roku, v ktorom prebieha audit
: správa sa predkladá do konca kalendárneho roka



Vyhláška o audite (návrh novely)

Trvanie a ukončenie auditu

: maximálne **12** po sebe nasledujúcich mesiacov
: **odovzdanie** záverečnej správy



Vyhláška o audite (návrh novely)

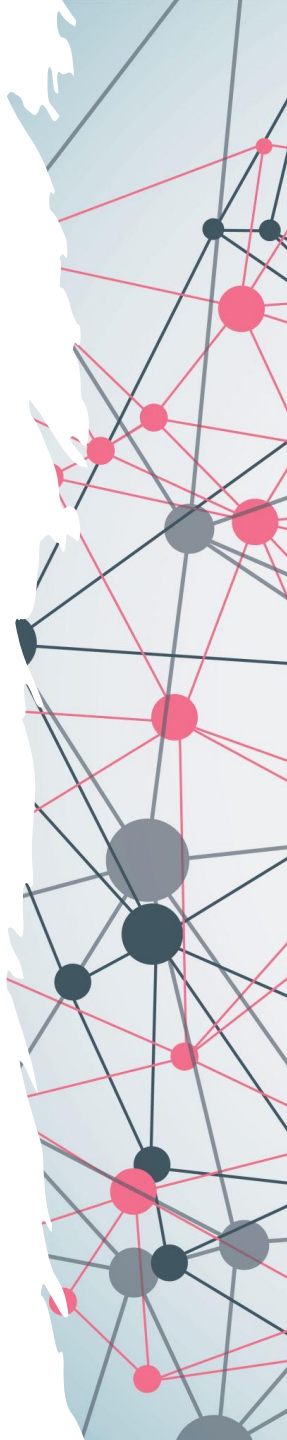
PKZS

16 mesiacov

: Kontrola plnenia nápravných opatrení

18 mesiacov

: Správa o plnení nápravných opatrení



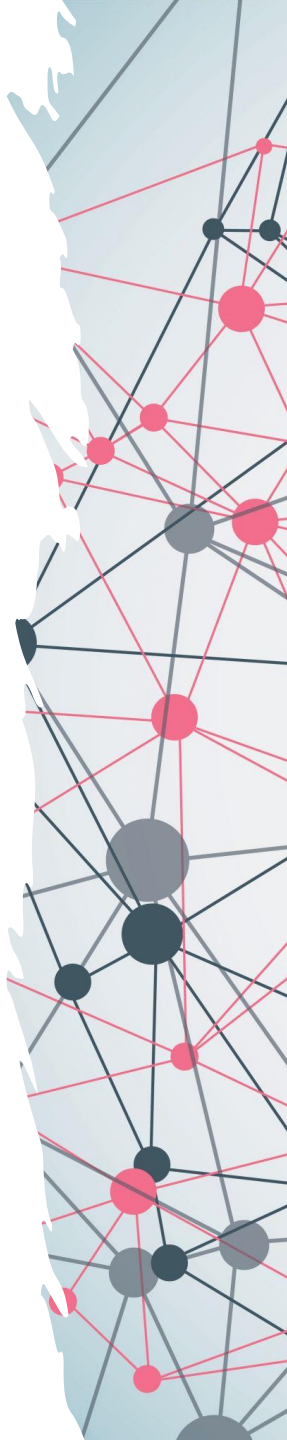
Termíny

Metodika 2.0

Metodika 2.0

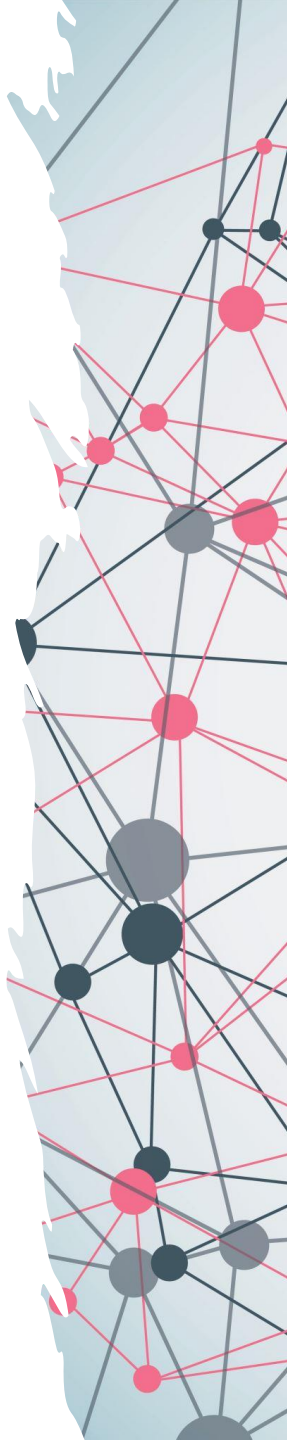
Pokiaľ má PZS implementovaný proces riadenia rizík
s vyššou úrovňou vyspelosti, rozdielny od tejto metodiky,
navrhne spôsob mapovania hodnôt z používanej metriky na požadovanú jednotnú metriku podľa tejto metodiky

(od 01.09.2025)



Metodika 2.0

Všetky akceptované riziká musia byť prehodnocované minimálne **raz ročne**



Vaše otázky...

JUDr. Ing. Miroslav Chlipala, PhD., LL.M.

Advokát s 23-ročnou praxou so zameraním na IT právo a moderné technológie (umelá inteligencia, elektronizácia a e-Government, cloudové služby, opensource, IoT, právne aspekty kybernetickej bezpečnosti, GDPR a ochrana osobných údajov) a duševné vlastníctvo. Vybudoval a vedie tím právnikov, ktorý predstavuje na Slovensku jedinečnú kombináciu pre oblasti IT právo a telekomunikácie, Duševné vlastníctvo a Compliance. V týchto kategóriách je advokátska kancelária pod jeho vedením dlhodobo oceňovaná v domácich a medzinárodných hodnoteniach.

Je certifikovaným tútorom Rady Európy pre vzdelávanie advokátov, sudcov a prokurátorov v programe HELP. **Je členom Stálej komisie pre etiku a reguláciu umelej inteligencie** pri MIRRI SR. Je riadnym členom Asociácie kybernetickej bezpečnosti. Pôsobil ako člen predsedníctva SAK a predsedom pracovnej skupiny pre elektronizáciu advokácie.

Mimo výkonu advokácie sa venuje teoreticko-odborným aspektom práva informačných technológií a ich dopadom na podnikateľskú sféru. **Aktívne sa zúčastňuje odborných konferencií a vedie workshopy a semináre**, kde prednáša aktuálne témy z oblasti práva a moderných technológií s dôrazom na ich biznis prepojenie. Opakovane prednáša na prestížnych podujatiach ako sú Slovenské dni práva SAK, alebo na najvýznamnejších slovenských odborných konferenciách z oblasti IT práva a z oblasti kybernetickej bezpečnosti, na ktorých sa podieľa aj ako predseda programového výboru.

Dlhodobom pôsobil ako pedagóg na Právnickej fakulte UK a následne na Fakulte práva PEVŠ. Je spoluzakladateľom predmetu Právo informačných a komunikačných technológií na FIIT STU. **Je aktívnym autorom mnohých odborných článkov a niekoľkých publikácii** z oblasti IT práva. Absolvoval niekoľko zahraničných pobytov a stáží (Hague Academy of International Law, University of Oslo, University of Zaragoza, University of Ljubljana, Jagiellonian University in Kraków).

Naše kontakty

Link na osobný linkedin:

https://www.linkedin.com/in/chlipala/

Link na náš firemný linkedin:

https://www.linkedin.com/company/advokati-chlipala

Link na našu webstránku:

https://www.AICH.sk/

Ďakujem za pozornosť

AICH
ADVOKÁTI CHLIPALA

2014 - 2025
právnická firma roka

RANKED IN
Chambers
Europe
2021 - 2025