KATALÓG SLUŽIEB 2024

NAKIB

E-LEARNINGOVÉ SLUŽBY

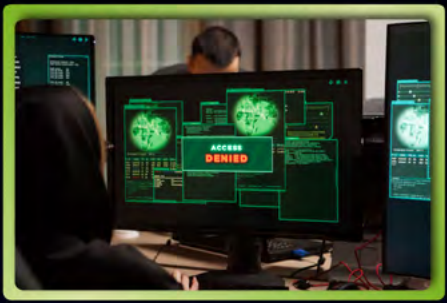
NÁRODNÁ AKADÉMIA PRE KYBERNETICKÚ
A INFORMAČNÚ BEZPEČNOSŤ

NAKIB.SK

NAKIB

E-LEARNINGOVÉ SLUŽBY

Základy informačnej bezpečnosti



Základy kyber bezpečnosti

Základy biznis kontinuity

Základy ochrany osobných údajov

Základy TISAX

TISAX Pokročilí

DORA

NAKIB.SK

EFEKTÍVNE VZDELÁVANIE FORMOU E-LEARNINGOVEJ SLUŽBY

Čo je?

E-learningový softvér Základy informačnej bezpečnosti je online kurz, ktorý sa zameriava na edukáciu o základných princípoch informačnej bezpečnosti. Kurz môže obsahovať rôzne témy, ako napríklad: Identifikácia a hodnotenie rizík: Naučíte sa, ako identifikovať a hodnotiť rôzne typy informačných bezpečnostných rizík. Ochrana dát: Naučíte sa, ako chrániť citlivé dáta pred neoprávneným prístupom, použitím, zverejnením, zmenou alebo zničením. Riadenie prístupov: Naučíte sa, ako definovať a implementovať politiky riadenia prístupov k informáciám a systémom. Bezpečnosť sietí a zariadení: Naučíte sa, ako chrániť počítačové siete a zariadenia pred kybernetickými útokmi. Zálohovanie a obnova dát: Naučíte sa, ako zálohovať a obnovovať dáta v prípade incidentu informačnej bezpečnosti. Zákony a regulácie: Naučíte sa o relevantných zákonoch a reguláciách týkajúcich sa informačnej bezpečnosti.

Prečo?

Zavedenie e-learningového softvéru Základy informačnej bezpečnosti prináša viacero benefitov: Zvýšenie povedomia: Zvýšenie povedomia o informačnej bezpečnosti medzi zamestnancami a zníženie rizika kybernetických incidentov.Zníženie rizík: Zvýšenie informovanosti o rôznych typoch informačných bezpečnostných rizík a naučenie sa, ako ich predchádzať a riešiť. Zlepšenie súladu: Zabezpečenie súladu s relevantnými zákonmi a reguláciami týkajúcimi sa informačnej bezpečnosti. Zníženie nákladov: Predchádzanie kybernetickým incidentom a minimalizácia ich dopadu môže priniesť značné úspory nákladov. Zvýšenie produktivity: Zvýšenie produktivity zamestnancov znížením prestojov súvisiacich s kybernetickými incidentmi.

Pre koho?

E-learningový softvér Základy informačnej bezpečnosti je určený pre:
Zamestnancov: Všetci zamestnanci by mali mať základné znalosti o informačnej bezpečnosti, aby sa vedeli chrániť pred kybernetickými hrozbami. Manažérov: Manažéri musia mať hlbšie znalosti o informačnej bezpečnosti, aby mohli efektívne riadiť riziká a chrániť firemné dáta. Študentov: Študenti, ktorí sa chcú venovať kariére v oblasti informačnej bezpečnosti, si v tomto kurze môžu vybudovať základné znalosti. Každý, kto sa chce dozvedieť viac o informačnej bezpečnosti.

Prínosy?

Implementácia e-learningového softvéru Základy informačnej bezpečnosti prináša nasledovné prínosy: Zvýšenie povedomia o informačnej bezpečnosti: Softvér umožňuje komplexnú edukáciu o rôznych aspektoch informačnej bezpečnosti a zvyšuje povedomie o kybernetických hrozbách. Zjednodušenie riadenia informačnej bezpečnosti: Softvér uľahčuje implementáciu a udržiavanie politík a procesov informačnej bezpečnosti. Zníženie rizík: Zvýšenie znalostí a zručností v oblasti informačnej bezpečnosti môže znížiť riziko kybernetických incidentov. Zlepšenie reputácie: Preukázanie záväzku k informačnej bezpečnosti posilňuje dôveru partnerov a zákazníkov. Zvýšenie konkurencieschopnosti: Dobre informovaní a edukovaní zamestnanci v oblasti informačnej bezpečnosti sú cenným prínosom pre každú firmu.

EFEKTÍVNE VZDELÁVANIE FORMOU E-LEARNINGOVEJ SLUŽBY

Čo je?

E-learningový softvér Základy kybernetickej bezpečnosti je online kurz, ktorý sa zameriava na edukáciu o základných princípoch kybernetickej bezpečnosti. Kurz môže obsahovať rôzne témy, ako napríklad:
Typy kybernetických hrozieb: Naučíte sa o rôznych typoch kybernetických hrozieb, ako sú malware, phishing, DDoS útoky a sociálne inžinierstvo. Ochrana zariadení: Naučíte sa, ako chrániť počítače, smartfóny a iné zariadenia pred kybernetickými útokmi. Bezpečnosť sietí: Naučíte sa, ako chrániť počítačové siete pred neoprávneným prístupom a útokmi. Bezpečnostné správanie: Naučíte sa o dôležitých bezpečnostných návykoch, ako je silné heslo a obozretnosť pri používaní online služieb. Zákon a regulácie: Naučíte sa o relevantných zákonoch a reguláciách týkajúcich sa kybernetickej bezpečnosti.

Prečo?

Zavedenie e-learningového softvéru Základy kybernetickej bezpečnosti prináša viacero benefitov:
Zvýšenie povedomia: Zvýšenie povedomia o kybernetických hrozbách medzi zamestnancami a zníženie rizika kybernetických incidentov. Zníženie rizík: Zvýšenie informovanosti o rôznych typoch kybernetických hrozieb a naučenie sa, ako ich predchádzať a riešiť. Zlepšenie súladu: Zabezpečenie súladu s relevantnými zákonmi a reguláciami týkajúcimi sa kybernetickej bezpečnosti. Zníženie nákladov: Predchádzanie kybernetickým incidentom a minimalizácia ich dopadu môže priniesť značné úspory nákladov. Zvýšenie produktivity: Zvýšenie produktivity zamestnancov znížením prestojov súvisiacich s kybernetickými incidentmi.

Pre koho?

E-learningový softvér Základy kybernetickej bezpečnosti je určený pre:
Zamestnancov: Všetci zamestnanci by mali mať základné znalosti o kybernetickej bezpečnosti, aby sa vedeli chrániť pred kybernetickými hrozbami. Manažérov: Manažéri musia mať hlbšie znalosti o kybernetickej bezpečnosti, aby mohli efektívne riadiť riziká a chrániť firemné dáta. Študentov: Študenti, ktorí sa chcú venovať kariére v oblasti kybernetickej bezpečnosti, si v tomto kurze môžu vybudovať základné znalosti. Každý, kto sa chce dozvedieť viac o kybernetickej bezpečnosti.

Prínosy?

Implementácia e-learningového softvéru Základy kybernetickej bezpečnosti prináša nasledovné prínosy:
Zvýšenie povedomia o kybernetickej bezpečnosti: Softvér umožňuje komplexnú edukáciu o rôznych aspektoch kybernetickej bezpečnosti a zvyšuje povedomie o kybernetických hrozbách. Zjednodušenie riadenia kybernetickej bezpečnosti: Softvér uľahčuje implementáciu a udržiavanie politík a procesov kybernetickej bezpečnosti. Zníženie rizík: Zvýšenie znalostí a zručností v oblasti kybernetickej bezpečnosti môže znížiť riziko kybernetických incidentov. Zlepšenie reputácie: Preukázanie záväzku k kybernetickej bezpečnosti posilňuje dôveru partnerov a zákazníkov. Zvýšenie konkurencieschopnosti: Dobre informovaní a edukovaní zamestnanci v oblasti kybernetickej bezpečnosti sú cenným prínosom pre každú firmu.

EFEKTÍVNE VZDELÁVANIE FORMOU E-LEARNINGOVEJ SLUŽBY

Čo je?

E-learningový softvér Základy ochrany osobných údajov je online kurz, ktorý sa zameriava na edukáciu o základných princípoch ochrany osobných údajov v súlade s GDPR (General Data Protection Regulation). Kurz môže obsahovať rôzne témy, ako napríklad: Definícia a typy osobných údajov: Naučíte sa, aké informácie sa považujú za osobné údaje a aké sú rôzne typy osobných údajov. Princípy ochrany osobných údajov: Naučíte sa o základných princípoch ochrany osobných údajov, ako je zákonnosť, spravodlivosť a transparentnosť. Práva dotknutých osôb: Naučíte sa o právach dotknutých osôb, ako je právo na prístup k informáciám, právo na opravu a právo na výmaz. Povinnosti prevádzkovateľov a sprostredkovateľov: Naučíte sa o povinnostiach prevádzkovateľov a sprostredkovateľov osobných údajov, ako je vedenie záznamov o spracovateľských aktivitách a implementácia technických a organizačných opatrení na ochranu osobných údajov.
Sankcie za porušenie GDPR: Naučíte sa o sankciách za porušenie GDPR.

Prečo?

Zavedenie e-learningového softvéru Základy ochrany osobných údajov prináša viacero benefitov:
Zvýšenie povedomia: Zvýšenie povedomia o GDPR a ochrane osobných údajov medzi zamestnancami a zníženie rizika porušenia GDPR. Zníženie rizík: Zvýšenie informovanosti o rôznych aspektoch ochrany osobných údajov a naučenie sa, ako dodržiavať GDPR. Zlepšenie súladu: Zabezpečenie súladu s GDPR a minimalizácia rizika sankcií. Zníženie nákladov: Predchádzanie porušeniam GDPR a minimalizácia ich dopadu môže priniesť značné úspory nákladov. Zvýšenie reputácie: Preukázanie záväzku k ochrane osobných údajov posilňuje dôveru partnerov a zákazníkov.

Pre koho?

E-learningový softvér Základy ochrany osobných údajov je určený pre:
Zamestnancov: Všetci zamestnanci by mali mať základné znalosti o GDPR a ochrane osobných údajov, aby sa vedeli správať zodpovedne s citlivými informáciami. Manažérov: Manažéri musia mať hlbšie znalosti o GDPR a ochrane osobných údajov, aby mohli efektívne riadiť riziká a chrániť firemné dáta. Študentov: Študenti, ktorí sa chcú venovať kariére v oblasti ochrany osobných údajov, si v tomto kurze môžu vybudovať základné znalosti. Každý, kto sa chce dozvedieť viac o GDPR a ochrane osobných údajov.

Prínosy?

Implementácia e-learningového softvéru Základy ochrany osobných údajov prináša nasledovné prínosy:
Zvýšenie povedomia o GDPR a ochrane osobných údajov: Softvér umožňuje komplexnú edukáciu o rôznych aspektoch GDPR a ochrany osobných údajov a zvyšuje povedomie o relevantných pravidlách a povinnostiach. Zjednodušenie dodržiavania GDPR: Softvér uľahčuje implementáciu a udržiavanie politík a procesov potrebných pre súlad s GDPR. Zníženie rizík porušenia GDPR: Zvýšenie znalostí a zručností v oblasti ochrany osobných údajov môže znížiť riziko porušenia GDPR. Zlepšenie reputácie: Preukázanie záväzku k ochrane osobných údajov posilňuje dôveru partnerov a zákazníkov.Zvýšenie konkurencieschopnosti: Dobre informovaní a edukovaní zamestnanci.

EFEKTÍVNE VZDELÁVANIE FORMOU E-LEARNINGOVEJ SLUŽBY

Čo je?

E-learningový softvér Základy biznis kontinuity je online kurz, ktorý sa zameriava na edukáciu o základných princípoch riadenia kontinuity biznisu (BCMS). Kurz môže obsahovať rôzne témy, ako napríklad: Identifikácia a hodnotenie rizík: Naučíte sa, ako identifikovať a hodnotiť rôzne typy rizík, ktoré by mohli narušiť prevádzku organizácie. Plánovanie kontinuity: Naučíte sa, ako definovať plány kontinuity pre rôzne typy krízových scenárov. Implementácia a testovanie: Naučíte sa, ako implementovať a testovať plány kontinuity. Monitorovanie a reporting: Naučíte sa, ako monitorovať a reportovať o stave kontinuity biznisu.

Prečo?

Zavedenie e-learningového softvéru Základy biznis kontinuity prináša viacero benefitov:
Zvýšená odolnosť: Zvýšenie odolnosti organizácie voči neočakávaným udalostiam a minimalizácia ich dopadu na prevádzku. Rýchle obnovenie prevádzky: Zrýchlenie obnovenia prevádzky v prípade krízy a minimalizácia prestojov. Zníženie strát: Zníženie finančných a reputačných strát súvisiacich s krízovými situáciami.
Zlepšenie dodržiavania regulácií: Zabezpečenie súladu s regulačnými požiadavkami na riadenie kontinuity biznisu. Zvýšenie informovanosti: Zvýšenie informovanosti manažmentu a zamestnancov o rizikách a plánoch kontinuity.

Pre koho?

E-learningový softvér Základy biznis kontinuity je určený pre:
Manažérov a vedúcich pracovníkov: Zodpovedných za riadenie kontinuity biznisu v rámci svojej organizačnej jednotky. IT profesionálov: Ktorí sa podieľajú na implementácii a údržbe softvéru BCMS.
Audítorov: Ktorí sa venujú auditu riadenia kontinuity biznisu. Konzultantov: Ktorí poskytujú poradenstvo v oblasti riadenia kontinuity biznisu. Každý, kto sa chce dozvedieť viac o riadení kontinuity biznisu.

Prínosy?

Implementácia e-learningového softvéru Základy biznis kontinuity prináša nasledovné prínosy:
Zvýšená odolnosť voči krízovým situáciám: Softvér umožňuje komplexnú identifikáciu a hodnotenie rizík, definovanie a implementáciu plánov kontinuity a efektívne riadenie krízových situácií.
Rýchle obnovenie prevádzky: Automatizácia procesov a centralizované uchovávanie informácií v softvéri umožňuje rýchle a efektívne obnovenie prevádzky po kríze.
Zníženie strát: Predchádzanie krízovým situáciám a minimalizácia ich dopadu môže priniesť značné úspory nákladov a minimalizovať reputačné straty. Zlepšenie informovanosti a koordinácie: Softvér umožňuje efektívnu komunikáciu a koordináciu rôznych tímov v rámci krízovej situácie. Zvýšenie konkurencieschopnosti: Preukázanie záväzku k riadeniu kontinuity biznisu posilňuje dôveru partnerov a zákazníkov a môže zlepšiť konkurencieschopnosť na trhu.

EFEKTÍVNE VZDELÁVANIE DORA FORMOU E-LEARNINGOVEJ SLUŽBY

Čo je?

Regulácia DORA (Digital Operational Resilience Act) je komplexný proces posudzovania súladu informačného systému a kybernetickej odolnosti organizácie s požiadavkami nariadenia DORA. Audit zahŕňa:
Analýzu rizík: Identifikácia a hodnotenie rôznych typov rizík prevádzkových výpadkov a kybernetických hrozieb v súlade s definíciou DORA. Posúdenie riadenia kybernetickej odolnosti: Hodnotenie existujúcich procesov a opatrení riadenia kybernetickej odolnosti v organizácii a ich súladu s požiadavkami DORA. Testovanie odolnosti: Simulácia rôznych scenárov prevádzkových výpadkov a kybernetických útokov s cieľom otestovať odolnosť informačného systému a reakcie organizácie. Vypracovanie správy: Zhrnutie zistení auditu a odporúčaní na zlepšenie kybernetickej odolnosti v súlade s nariadením DORA.

Prečo?

Vzdelávanie štandardu DORA prináša viacero benefitov:
Zvýšenie súladu: Zabezpečenie súladu s požiadavkami nariadenia DORA, čím sa minimalizuje riziko sankcií a administratívnych pokút. Zníženie rizík: Zvýšenie kybernetickej odolnosti a zníženie rizika prevádzkových výpadkov a kybernetických incidentov. Zlepšenie kontinuity prevádzky: Implementácia odporúčaní z auditu môže posilniť kontinuitu prevádzky a minimalizovať dopady výpadkov a incidentov. Zvýšenie konkurencieschopnosti: Dobre chránený informačný systém a vysoká kybernetická odolnosť môže priniesť organizácii konkurenčnú výhodu.

Pre koho?

Vzdelávanie DORA je určený pre:
Finančné inštitúcie: Banky, poisťovne, investičné firmy a iné subjekty podliehajúce nariadeniu DORA. Poskytovateľov kritickej infraštruktúry: Prevádzkovatelia energetických sietí, telekomunikácií, dopravy a iných kritických sektorov definovaných v DORA.Organizácie, ktoré chcú zlepšiť kybernetickú odolnosť: Audit môže identifikovať oblasti, v ktorých je možné zlepšiť kybernetickú odolnosť a súlad s požiadavkami DORA. Organizácie, ktoré sa chystajú na certifikáciu kybernetickej odolnosti: Audit môže pomôcť organizácii pripraviť sa na certifikáciu podľa medzinárodných štandardov s ohľadom na špecifiká DORA.

Prínosy?

Vzdelávanie štandardu DORA prináša nasledovné prínosy:
Zvýšenie povedomia o rizikách prevádzkových výpadkov a kybernetických hrozieb: Audit sa zameriava na špecifické hrozby a riziká definované v DORA, čím zvyšuje povedomie manažmentu a zamestnancov v daných oblastiach. Zlepšenie procesov a opatrení riadenia kybernetickej odolnosti: Audit identifikuje oblasti, v ktorých je nutné implementovať alebo upraviť procesy a opatrenia riadenia kybernetickej odolnosti tak, aby spĺňali požiadavky DORA. Zníženie rizika prevádzkových výpadkov a kybernetických incidentov: Včasná identifikácia a náprava zraniteľností a slabín v kybernetickej odolnosti znižuje riziko a dopady výpadkov a incidentov.

EFEKTÍVNE VZDELÁVANIE ZÁKLADY TISAX® FORMOU E-LEARNINGOVEJ SLUŽBY

Čo je?

E-learningový softvér Základy TISAX je online kurz, ktorý sa zameriava na edukáciu o základných princípoch informačnej bezpečnosti v automobilovom priemysle podľa požiadaviek TISAX (Trusted Information Security Assessment Exchange). Kurz môže obsahovať rôzne témy, ako napríklad:
Základné pojmy TISAX: Naučíte sa o histórii a cieľoch TISAX, rôznych úrovniach auditu a relevantných dokumentoch. Požiadavky na informačnú bezpečnosť: Naučíte sa o požiadavkách TISAX na riadenie rizík, ochranu dát, riadenie prístupov, bezpečnosť sietí a zariadení, incident response a kontinuitu biznisu. Proces auditu TISAX: Naučíte sa o priebehu auditu TISAX, príprave na audit a nápravných opatreniach. Praktické tipy: Naučíte sa o praktických tipoch a nástrojoch na implementáciu požiadaviek TISAX.

Prečo?

Zavedenie e-learningového softvéru Základy TISAX prináša viacero benefitov:
Zvýšenie povedomia o TISAX: Zvýšenie povedomia o požiadavkách TISAX medzi zamestnancami a dodávateľmi v automobilovom priemysle. Zlepšenie súladu: Zabezpečenie súladu s požiadavkami TISAX a zníženie rizika neúspešného auditu. Zníženie rizík: Zvýšenie informačnej bezpečnosti a zníženie rizika kybernetických incidentov. Zlepšenie reputácie: Preukázanie záväzku k informačnej bezpečnosti posilňuje dôveru partnerov a zákazníkov. Zvýšenie konkurencieschopnosti: Dodržiavanie požiadaviek TISAX môže zlepšiť konkurencieschopnosť na trhu automobilového priemyslu.

Pre koho?

E-learningový softvér Základy TISAX je určený pre:
Zamestnancov: Všetci zamestnanci v automobilovom priemysle by mali mať základné znalosti o TISAX a požiadavkách na informačnú bezpečnosť. Manažérov: Manažéri musia mať hlbšie znalosti o TISAX a požiadavkách na informačnú bezpečnosť, aby mohli efektívne riadiť riziká a chrániť firemné dáta.
Dodávateľov: Dodávatelia v automobilovom priemysle musia spĺňať požiadavky TISAX, aby mohli spolupracovať s výrobcami automobilov. Audítorov: Audítori TISAX musia mať hlboké znalosti o požiadavkách TISAX a procese auditu. Každý, kto sa chce dozvedieť viac o TISAX a informačnej bezpečnosti v automobilovom priemysle.

Prínosy?

Implementácia e-learningového softvéru Základy TISAX prináša nasledovné prínosy:
Zvýšenie povedomia o TISAX a požiadavkách na informačnú bezpečnosť: Softvér umožňuje komplexnú edukáciu o rôznych aspektoch TISAX a informačnej bezpečnosti v automobilovom priemysle. Zjednodušenie implementácie TISAX: Softvér uľahčuje implementáciu a udržiavanie požiadaviek TISAX. Zníženie rizík kybernetických incidentov: Zvýšenie znalostí a zručností v oblasti informačnej bezpečnosti môže znížiť riziko kybernetických incidentov. Zlepšenie reputácie: Preukázanie záväzku k informačnej bezpečnosti a súladu s TISAX posilňuje dôveru partnerov a zákazníkov. Zvýšenie konkurencieschopnosti: Dobre informovaní a edukovaní zamestnanci a dodávatelia v oblasti TISAX a informačnej bezpečnosti sú cenným prínosom pre každú firmu v automobilovom priemysle.

EFEKTÍVNE VZDELÁVANIE TISAX® POKROČILÍ FORMOU E-LEARNINGOVEJ SLUŽBY

Čo je?

E-learningový softvér TISAX Pokročilí - Ochrana prototypov a GDPR je online kurz, ktorý sa zameriava na komplexnú edukáciu o pokročilých témach informačnej bezpečnosti v automobilovom priemysle v súlade s požiadavkami TISAX a GDPR. Kurz sa zameriava na dve kľúčové oblasti: Ochrana prototypov:
Dôvernosť prototypov: Naučíte sa o rôznych typoch prototypov a o tom, ako ich chrániť pred neoprávneným prístupom, použitím a zverejnením. Riadenie prístupov: Naučíte sa o definovaní a implementácii politík riadenia prístupov k prototypom. Technické riešenia: Naučíte sa o rôznych technických riešeniach na ochranu prototypov, ako sú šifrovanie, pseudonymizácia a watermarking.
Požiadavky GDPR: Naučíte sa o požiadavkách GDPR na spracovanie osobných údajov v kontexte TISAX.
Práva dotknutých osôb: Naučíte sa o právach dotknutých osôb, ako je právo na prístup k informáciám a právo na výmaz. Implementácia GDPR: Naučíte sa o tom, ako implementovať GDPR v praxi v kontexte TISAX.

Prečo?

Zavedenie e-learningového softvéru TISAX Pokročilí - Ochrana prototypov a GDPR prináša viacero benefitov: Zvýšenie povedomia o pokročilých témach informačnej bezpečnosti: Zvýšenie povedomia o dôležitosti ochrany prototypov a súladu s GDPR. Zlepšenie súladu: Zabezpečenie súladu s požiadavkami TISAX a GDPR a zníženie rizika sankcií. Zníženie rizík: Zvýšenie informačnej bezpečnosti a zníženie rizika kybernetických incidentov. Zlepšenie reputácie: Preukázanie záväzku k informačnej bezpečnosti a súladu s GDPR posilňuje dôveru partnerov a zákazníkov. Zvýšenie konkurencieschopnosti: Dobre informovaní a edukovaní zamestnanci v oblasti ochrany prototypov a GDPR sú cenným prínosom pre každú firmu v automobilovom priemysle.

Pre koho?

E-learningový softvér TISAX Pokročilí - Ochrana prototypov a GDPR je určený pre:
Manažérov: Manažéri musia mať hlbšie znalosti o ochrane prototypov a GDPR, aby mohli efektívne riadiť riziká a chrániť firemné dáta. Vývojárov: Vývojári prototypov musia mať znalosti o tom, ako chrániť prototypy pred neoprávneným prístupom a zneužitím. IT profesionálov: IT profesionáli musia mať znalosti o implementácii technických riešení na ochranu prototypov a o súlade s GDPR. Audítorov: Audítori TISAX a GDPR musia mať hlboké znalosti o požiadavkách TISAX a GDPR a o procese auditu. Každý, kto sa chce dozvedieť viac o ochrane prototypov a GDPR v kontexte TISAX.

Prínosy?

Implementácia e-learningového softvéru TISAX Pokročilí - Ochrana prototypov a GDPR prináša nasledovné prínosy:
Zvýšenie povedomia o ochrane prototypov a GDPR: Softvér umožňuje komplexnú edukáciu o rôznych aspektoch ochrany prototypov a GDPR. Zjednodušenie implementácie TISAX a GDPR: Softvér uľahčuje implementáciu a udržiavanie požiadaviek TISAX a GDPR. Zníženie rizík kybernetických incidentov: Zvýšenie znalostí a zručností v oblasti informačnej bezpečnosti a GDPR môže znížiť riziko kybernetických incidentov.