SIGURIA KIBERNETIKE DHE STANDARDI ISO 27701

Një projekt nga Agjencia Zvicerane për Zhvillim dhe Bashkëpunim SDC

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Agjencia Zvicerane për Zhvillim dhe Bashkëpunim SDC

Në partneritet me:

MINISTRIA E EKONOMISË, KULTURËS DHE INOVACIONIT

Zbatuar nga:

HELVETAS

PARTNERËT SHQIPËRI PËR NDRYSHIM DHE ZHVILLIM

Ky dokument është prodhuar nga RisiAlbania. Risi është një projekt punësimi për të rinjtë i Agjencisë Zvicerane për Zhvillim dhe Bashkëpunim SDC, i zbatuar nga Helvetas dhe Partnerët Shqipëri për Ndryshim dhe Zhvillim. Pikëpamjet dhe konkluzionet e përfshira këtu nuk pasqyrojnë domosdoshmërisht ato të Qeverisë Zvicerane, as të Agjencisë Zvicerane për Zhvillim dhe Bashkëpunim SDC.

SIGURIA KIBERNETIKE DHE STANDARDI ISO 27701

UDHËZUES

Përgatitur nga:

NIALL CONDON
Konsulent i Pavarur

Helvetas dhe Partnerët Shqipëri për Ndryshim dhe Zhvillim zbatojnë projektin inovativ të punësimit për të rinjtë, i mbështetur nga Agjencia Zvicerane për Zhvillim dhe Bashkëpunim (SDC), RisiAlbania; në bashkëpunim me Ministrinë e Ekonomisë, Kulturës dhe Inovacionit.

RisiAlbania mbështet krijimin e vendeve cilësore të punës në sektorin lokal të TIK-ut. Projekti synon të transformojë sektorin e TIK-ut në Shqipëri nëpërmjet promovimit të transformimit digjital, përmirësimit të sigurisë kibernetike dhe adoptimit të standardeve përkatëse ndërkombëtare. Kjo do të çonte në krijimin e një tregu pune më konkurrues për të rinjtë. Gjithashtu, kjo përpjekje synon kalimin nga shërbimet bazë në oferta me vlerë të lartë si Transferimi i Teknologjisë së Informacionit (ITO), siguria kibernetike dhe zgjidhjet digjitale, duke forcuar kështu sektorët kyç si tregtia elektronike, financat dhe turizmi.

TABELA E PËRMBAJTJES

PJESA 1 - BAZAT

Çfarë është Siguria Kibernetike?

Siguria kibernetike është praktika e mbrojtjes së kompjuterëve, rrjeteve dhe të dhënave nga aksesi, vjedhja, dëmtimi dhe ndërprerja e paautorizuar. Masat e sigurisë kibernetike përfshijnë nivele të shumta mbrojtjeje (shih diagramin më poshtë) të konceptuara me qëllim mbrojtjen e informacionit digjital nga sulmet kibernetike ose kërcënime të tjera si fatkeqësitë natyrore.

Në vitin 2024, Shqipëria miratoi ligjin e ri për sigurinë kibernetike (Ligji nr. 25/2024 për Sigurinë Kibernetike) me qëllim forcimin e infrastrukturës së saj kombëtare të sigurisë kibernetike. Zbatimi i ligjit mbikëqyret nga **Autoriteti Kombëtar për Sigurinë Kibernetike (AKSK).** Ligji parashikon respektimin e tij nga organizatat që administrojnë dhe përpunojnë sasi të konsiderueshme të informacionit digjital, duke përfshirë organizatat publike dhe private që administrojnë infrastrukturën kritike në sektorët e energjitikës, transportit, në sektorin bankar dhe atë shëndetësor.

LLOJET E ZAKONSHME TË KËRCËNIMEVE TË SIGURISË KIBERNETIKE

Phishing

Praktika e dërgimit të emaileve mashtruese për të vjedhur të dhëna të ndjeshme si numrat e kartave të kreditit dhe informacioni për kredencialet e sigurisë.

Ransomware

Një lloj programi keqdashës i krijuar për të zhvatur para duke bllokuar aksesin në skedarë ose në sistemin përkatës kompjuterik derisa të paguhet një shpërblesë.

Malware

Një lloj programi i krijuar për të fituar akses të paautorizuar ose për të shkaktuar dëme në një kompjuter.

Çfarë është ISO 27001?

ISO 27001 është një standard ndërkombëtar për **menaxhimin e sigurisë së informacionit.** Standardi shërben si një kornizë për ngritjen dhe zbatimin e atyre që quhen **sisteme të menaxhimit të sigurisë së informacionit (SMSI)** për t'u mbrojtur kundër sulmeve kibernetike.

SMSI-të janë grupe politikash, procedurash dhe kontrollesh të krijuara nga organizatat **për të mbrojtur informacionin e tyre** (p.sh. informacionin e klientëve, të dhënat financiare, pronën intelektuale) nga qasja e paautorizuar; **për të identifikuar rreziqet e mundshme** për sigurinë e informacionit; **për të krijuar besimin** te klientët dhe për të lehtësuar **qasjen në tregje të reja** ku siguria e informacionit është një ndër kërkesat bazë; dhe **për të garantuar respektimin** e kërkesave ligjore si ligji shqiptar për sigurinë kibernetike dhe Rregullorja GDPR e BE-së (për më shumë shih informacionin më poshtë).

Çfarë janë ISO 27701 & GDPR?

ISO 27701 është një zgjerim i ISO 27001 i fokusuar te privatësia, duke synuar garantimin e privatësisë së atij që quhet **informacion i identifikueshëm personal (PII)** - çdo informacion i lidhur me një individ të caktuar që mund të përdoret për të zbuluar identitetin e atij individi. Këtu përfshihen informacione të tilla si numri i sigurimeve shoqërore, emri i plotë, adresa e emailit apo numri i telefonit.

Ndërkohë që ISO 27001 i orienton organizatat përmes procesit të krijimit të një sistemi solid të sigurisë së informacionit, ISO 27701 e çon këtë një hap më tej duke garantuar përfshirjen në këtë sistem të masave të forta për privatësinë e informacionit. Organizatat tashmë të certifikuara me standardin ISO 27001 do ta kenë relativisht të thjeshtë përmbushjen e kërkesave të ISO 27701 (shih faqen tjetër për më shumë detaje dhe udhëzime në lidhje me procesin e certifikimit).

ISO 27701 u krijua për të ndihmuar organizatat në punën për përmbushjen e kërkesave të legjislacionit të BE-së për **Rregulloren e Përgjithshme për Mbrojtjen e të Dhënave (GDPR)**, e cila u miratua në vitin 2018 për të rregulluar mënyrën se si i trajtojnë organizatat të dhënat personale të qytetarëve të BE-së. GDPR **mbron të dhënat personale** duke kërkuar që organizatat t'i trajtojnë këto të dhëna në mënyrë të përgjegjshme dhe të sigurt dhe u siguron **individëve të drejtën për të hyrë** tek të dhënat e tyre dhe për të **kufizuar mënyrën e përdorimit të të dhënave të tyre.** ISO 27701 ofron një bazë të fortë për pajtueshmërinë me GDPR-në, duke mbuluar shumë, por jo të gjitha, masat teknike dhe organizative të kërkuara nga GDPR-ja.

Bizneset shqiptare, pavarësisht nga madhësia apo industria përkatëse, që mbledhin dhe përpunojnë të dhëna personale të qytetarëve të BE-së si rezultat i shitjes së mallrave apo shërbimeve në BE, duhet të respektojnë kërkesat e GDPR-së. Mosrespektimi mund të çojë në ndalimin ose kufizimin e aktivitetit për përpunimin e të dhënave, në verifikimin e detyrueshëm të trajtimit të të dhënave ose, në skenarin më të keq, në gjoba deri në 4% të xhiros. Paisja me certifikimin ISO 27701 kontribuon ndjeshëm për garantimin që bizneset shqiptare i përmbushin kërkesat e GDPR-së dhe që mund të kryejnë aktivitet tregtar në BE me siguri të plotë. Edhe respektimi i GDPR-së është vendimtar për procesin e anëtarësimit të Shqipërisë në BE.

SHEMBUJ TË NIVELEVE TË SIGURISË KIBERNETIKE

SIGURIA E PAJISJEVE TË PËRDORUESVE FUNDORË

Sigurimi i pajisjeve individuale si kompjuterët, telefonat inteligjentë dhe tabletët; përfshin programet kompjuterike kundër viruseve, programet anti-malware.

Siguria e të Dhënave

Mbron të dhënat nga aksesi i paautorizuar; përfshin kodimin, maskimin e të dhënave dhe zgjidhjet e sigurta të ruajtjes së të dhënave.

SIGURIA E RRJETIT

Mbron integritetin, konfidencialitetin dhe disponueshmërinë e rrjetit dhe të të dhënave; përfshin firewalls, sistemet e zbulimit të ndërhyrjeve dhe protokollet e sigurta të rrjetit.

SIGURIA FIZIKE

Sigurimi i aksesit fizik në kompjuterë, serverë dhe pajisje të tjera. Në këto masa përfshihen dyert e kyçura, rojet e sigurisë dhe kamerat vëzhguese.

PJESA 2 – REALIZIMI

Çfarë më nevojitet për t'u certifikuar me standardin ISO27701 dhe kush mund të më ndihmojë për këtë?

Një gjë e rëndësishme që duhet kuptuar këtu është se, për shkak se ISO 27701 është një zgjerim i ISO 27001, një organizatë duhet së pari të certifikohet me standardin ISO 27001 përpara se të marrë në konsideratë certifikimin me standardin ISO 27701. Organizatat zakonisht aplikojnë për të dy standardet njëkohësisht - ky është procesi i paraqitur në diagramin më poshtë.

1

VENDOSNI NËSE KËRKOHET CERTIFIKIMI.

ÇFARË nënkupton kjo?

Pikë së pari, në mënyrë që organizata të kuptojë nëse i nevojitet certifikimi ISO 27001-27701 apo jo, ajo duhet t'i japë përgjigje disa pyetjeve të thjeshta:

- A duhet të respektoj ligjin e Shqipërisë për sigurinë kibernetike të vitit 2024? Me fjalë të tjera, a menaxhon organizata ime ndonjë infrastrukturë kritike të theksuar në këtë legjislacion?
- A duhet të respektoj kërkesat e GDPR-së? Me fjalë të tjera, a mbledh dhe përpunon aktualisht organizata ime apo planifikon të mbledhë dhe të përpunojë informacionin personal të qytetarëve të BE-së?

KUSH mund të më mbështesë?

Autoriteti Kombëtar për Sigurinë Kibernetike (AKSK) mund të ofrojë udhëzime në lidhje me organizatat që duhet të respektojnë ligjin e 2024 për sigurinë kibernetike dhe GDPR-në.

2

PLOTËSONI VLERËSIMIN DHE PLANIN FILLESTAR

ÇFARË nënkupton kjo?

Pas përcaktimit të nevojës dhe kërkesës për marrjen e certifikimit, hapi tjetër është kryerja e analizës së mangësive për të identifikuar dhe dokumentuar kontrollet ekzistuese të sigurisë së informacionit dhe privatësisë të organizatës suaj dhe për të nxjerrë në pah mangësitë mbi bazën e standardeve ISO 27001 dhe ISO 27701.

Analiza e mangësive do të përdoret për të përgatitur një plan projekti që përshkruan burimet, afatet kohore dhe detyrat për zbatimin e ISO 27001 dhe ISO 27701.

KUSH mund të më mbështesë?

Ekspertët lokalë të sigurisë dhe privatësisë mund të mbështesin ekipin tuaj të brendshëm të TI-së për të kryer këtë analizë të mangësive.

Infosecurity https://infosecurity.al/ është një ofrues shërbimi lokal me ekspertizë në fushën e sigurisë kibernetike dhe për kryerjen e analizave të mangësive bazuar në ISO 27001/27701, si dhe për planifikimin e projekteve.
FISA Academy https://www.fisa.pro/ ofron trajnime profesionale dhe certifikime ndërkombëtare në fushën e sigurisë kibernetike, teknologjisë së informacionit dhe standardeve ISO, të përshtatura për profesionistë dhe organizata. Përmes kurseve praktike, platformave online dhe konsulencës teknike, akademia mbështet zhvillimin e aftësive digjitale dhe përputhshmërinë me standardet globale. Gjithashtu, vepron si urë lidhëse mes tregut të punës dhe talenteve në sektorin TIK, duke nxitur punësimin dhe ngritjen profesionale

KRIJONI SISTEME PËR MENAXHIMIN E SIGURISË DHE PRIVATËSISË SË TË DHËNAVE.

3

ÇFARË nënkupton kjo?

Zhvilloni dhe vini në funksionim kontrollet teknike dhe organizative[1] të nevojshme për të dy standardet.

Ndërgjegjësoni dhe informoni punonjësit në lidhje me sigurinë dhe privatësinë e informacionit përmes seancave të vazhdueshme të trajnimit dhe edukimit, duke patur si objektiv përfundimtar krijimin e kulturës së fortë për sigurinë e informacionit dhe privatësinë brenda organizatës.

KUSH mund të më mbështesë?

Përsëri, këtu duhet të shfrytëzohet një ofrues shërbimi lokal si InfoSecurity për të mbështetur procesin e ndërtimit të aftësisë së organizatës suaj për të respektuar sigurinë e të dhënave dhe kontrollet e privatësisë të kërkuara nga të dy standardet.

KRYENI AUDITIMIN DHE CERTIFIKOHUNI.

4

ÇFARË nënkupton kjo?

Kryeni një auditim të brendshëm para-vlerësues për të identifikuar çdo mangësi të mbetur për të dy standardet.

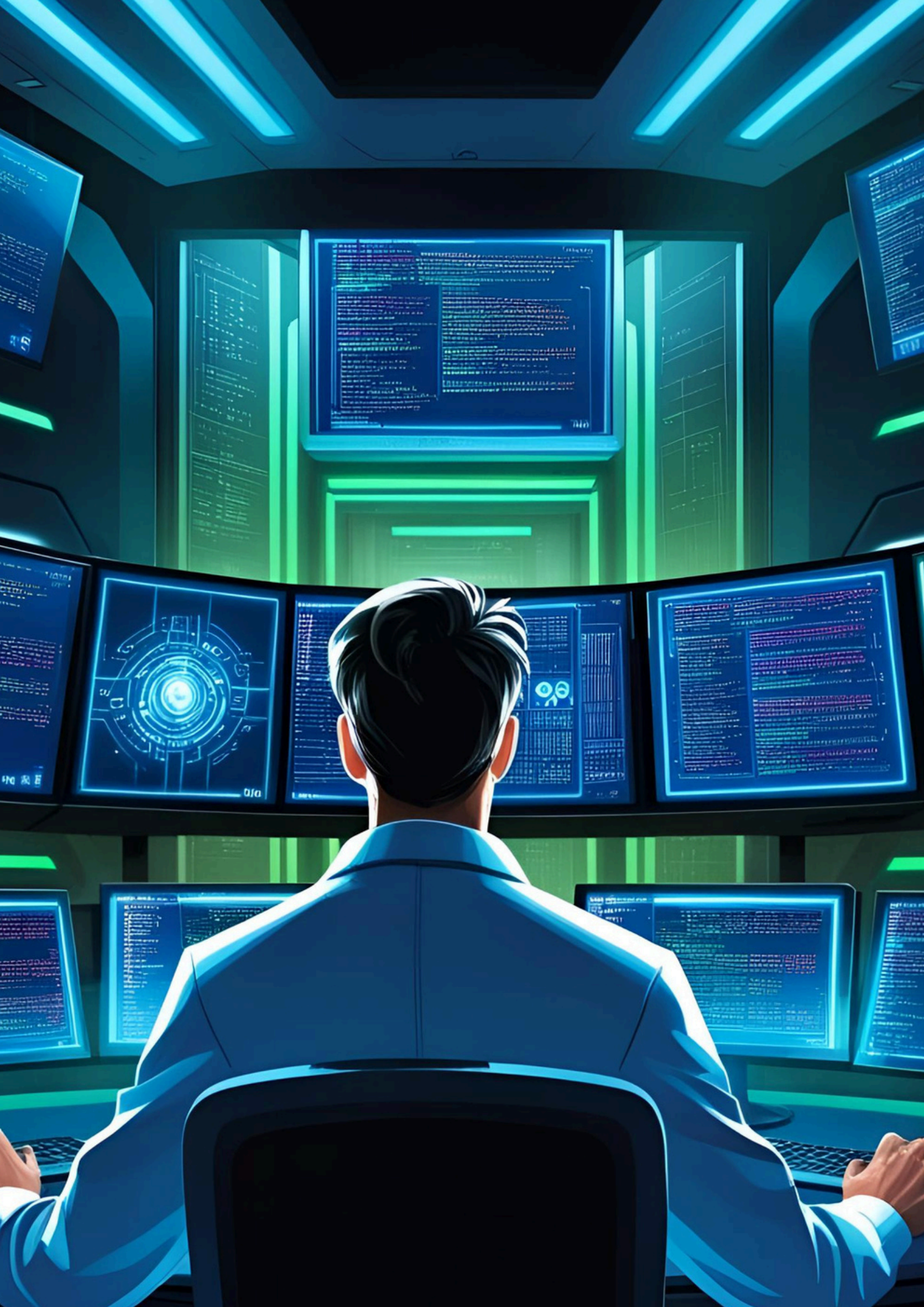
Kryeni auditimin e certifikimit formal nga një organizëm certifikues i akreditуar për të dy standardet.

Certifikata jepët vetëm nëse auditimi rezulton i suksesshëm.

KUSH mund të më mbështesë?

Axe Register (https://www.axe-register.com/) është i vetmi organ certifikues i akreditуar vendas i autorizuar për të kryer auditimet e standardeve ISO 27001 dhe ISO 27701 dhe për të lëshuar certifikimin. Edhe audituesit e akreditуar ndërkombëtarë janë një alternativë, megjithëse më të kushtueshëm.

SHËNIM [1]: Kontrollet teknike përfshijnë kontrollin e aksesit (menaxhimi i aksesit të përdoruesit, duke përfshirë mekanizmat e konfirmimit dhe autorizimit); kodimi për të parandaluar aksesin e paautorizuar dhe për të siguruar privatësinë e të dhënave; siguria e rrjetit (p.sh. firewalls) dhe siguria e paisjeve të përdoruesve fundorë (p.sh. programi antivirus në kompjuter). Kontrolli organizativ përfshin politikat dhe procedurat e sigurisë së informacionit dhe privatësisë, të tilla si politikat e ruajtjes dhe depozitimit të të dhënave; procedurat për menaxhimin e riskut dhe incidenteve për zbulimin, raportimin dhe reagimin ndaj incidenteve të sigurisë së informacionit.



Rr. Ismail Qemali,
P18, H.3, Apt. 15
Tirana, Albania

+355 (0) 422 48 527

info@risialbania.al