REPUBLIKA E SHQIPËRISË
"PORTI DETAR" SH.A SARANDË

"TERMAT E REFERENCËS DHE SPECIFIKIMET TEKNIKE"

"Krijim i kapaciteteve kibernetike dhe digjitalizimi në Portin Detar Sarandë".

Hyrje

Qellimi i kesaj procedure eshte modernizimi i strukturave informatike te Portit te Sarandes. Nepermjet zhvillimit te 2 softwareve te dedikuar per ofrimin e nje sherbimi cilesor, bashkekohore dhe te sigurt per vizitoret e Portit (udhetare, turiste) te cilet jane gjithnje e me te medhenj ne numer nga viti ne vit si edhe per vete Portin e Sarandes si nje strukture e rendesie te vecante.

Projekti konsiston ne realizimin e:

- Sigurise Kibernetike nepermjet proceseve te Auditimit dhe Riskasestment
- PentTest per certifikimin e sigurise Kibernetike
- Keshillimit dhe realizimit te infrastruktures perkates
- Zhvillimi i politikave te Sigurise Kibernetike
- Ndergjegjesimi i punonjesve nepermjet Trajnimit te personelit
- Sugjerime per permiresimin e infrastruktures dhe politikave
- Audit i te gjithe struktures dhe sigurise Kibernetike
- Ndertimin e nje infopoint digjital ne hyrje te portit
- Realizimin e Software per informacionin e nevojshem mbi Oraret nisjes dhe mberritjes se Trageteve sipas modelit te aeroportit

Permbajtja

1. HYRJE

1.1 PERFITUESI / AUTORITETI KONTRAKTOR

Porti Detar Sarande

1.2 SITUATA AKTUALE NE INSTITUCION

Porti Detar Sarande ka një infrastrukturë network, rrjet fizik, ëireless, sisteme informatike, aplikacione të implementuara në datacenter, nëpërmjet të cilave ofrohen shërbimet e teknologjisë së informacionit dhe komunikimit në funksion të ushtrimit të misionit dhe funksioneve në Institucion.

Aplikimi i Teknologjisë së Informacionit dhe Komunikimit, përgatitja, instalimi dhe mirëmbajtja e sistemeve informatike rregullohet nga një bashkësi standardesh teknike të cilat ulin rrezikun dhe minimizojnë probabilitetin e gabimeve për instalimin dhe përdorimin e sistemeve informatike.

Situata aktuale rajonale dhe globale ka bërë të mundur rritjen eksponenciale të sulmeve kibernetike nga aktorë të jashtëm. Incidentet e zhvilluara së fundmi drejt shërbimeve qeveritare dhe institucioneve të sigurisë vërtetojnë veprimtarinë e adresuar në vend dhe gjithashtu dikton domosdoshmërinë për mbrojtjen dhe rritjen e sigurisë në Institucion.

Aktualisht në APS lind domosdoshmëria për implementimin e masave të sigurisë kibernetike dhe zhvillimit të sistemeve software për automatizimin e proceseve të punës në institucion dhe krijimin e mundësisë së shërimeve të ndryshme informuese për vizitorët. Si rrjedhojë, është e nevojshme realizimi i një kontrolli dhe një analizë rreziku të specializuar në lidhje me sistemet elektronike në përdorim të Institucionit si dhe dëmeve që do vinin nga humbja apo kompromet imi i sistemeve te informacionit. Për të bërë të mundur rritjen e sigurisë, uljen e gjurmës së sipërfaqes së sulmit si dhe parandalimin e sulmeve kibernetike kërkohet të zhvillohen politika të sigurisë kibernetike, teste sigurie ndaj infrastrukturës teknologjike të APS në formë të plotë me qëllim evidentimin e problematikave dhe riparimin apo sigurimin e tyre në të ardhmen, trajnimin / ndërgjegjësimin kibernetik të përdoruesve të këtyre sistemeve, implementimi i pajisjeve hardware dhe software me qëllim rritjen e sigurisë kibernetike në institucion etj.

1.3 QELLIMI DHE OBJEKTIVAT E PROCEDURES

Qellimi i ketij projekti eshte te implementoje standarde kombetare dhe nderkombetare te sigurise kibernetike si dhe zhvillimin e dy software-ve ne sherbim te vizitoreve portit Sarande.

Operatori ekonomik duhet te arrije keto objektiva:

- Zhvillimin e politikave te sigurise kibernetike per institucionin.
- Zhvillimin e nje metodologjie per vleresimin e riskut kibernetik.
- Trajnimin mbi sigurine kibernetike per personlein e institucionit.
- Percaktimin e pikave te dobeta te sistemeve te institucionit nepermjet testimeve te sigurise per aplikacionet web.
- Perpilimin e raportit te auditimit kibernetik mbi masat organizative dhe teknike te institucionit.
- Implementimin e nje serveri kryesor i cili do sherbeje si “domain controller” dhe server hostimi per aplikacionet web
- Implementimin e nje storage ku do te ruhen te dhenat qe perpunohen ne institucion
- Implementimin e zgjidhjeve te sigurise per mbrojtjen e informacionit dhe te sistemeve te institucionit
- Zhvillimin e software-ve per vizitoret e portit, me saktesisht Infopoint dhe Oraret

2. METODOLOGJIA E ZHVILLIMIT TE PROCEDURES

2.1 FAZA I – IMPLEMENTIMI I SERVERIT QENDROR, STORAGE, FIREWALL, ANTIVIRUS DHE POSTA ELEKTRONIKE

Faza e pare e projektit parashikon furnizimin dhe instalimin e pajisjeve hardware dhe software te listuara si me poshte:

2.1.1 Instalimi i serverit qendror i cili do te sherbeje si domain controller per rrjetin e brendshem te APS. Gjithashtu ne kete server do te behet dhe hostimi i software-ve Infopoint dhe Oraret. Ne domain controller do te konfigurohen perdoruesit (users) sipas struktures organizative te APS si dhe do te aplikohen

politika ne grup (GPO) per ceshtje te sigurise dhe te proceseve te punes te institucionit.

2.1.2 Instalimi i Storage i cili do te sherbeje si repository ku do te ruhen imazhet e kompjuterave te institucionit ne menyre te automatizuar te pakten nje here ne muaj. Gjithashtu ne Storage do te krijohet dhe nje skedar rrjeti i aksesueshem nga perdoruesit e institucionit ku secili prej tyre do te kete skedarin personal si dhe te drejtat per te aksesuar skedaret e perbashket.

2.1.3 Inplementimi i pajisjes se mbrojtjes perimetrale do te behet nepermjet pajisjes hardware dhe licenses perkatese sikurse percaktuar ne specifikimet teknike ne piken 5.3 te ketij dokumenti.

2.1.4 Implementimi i antivirusit qendror do te behet duke u konfiguruar ne serverin kryesor dhe duke shtuar pikat fundore per t'u monitoruar nga kjo console.

2.1.5 Sherbimi i postes elektronike duhet zhvilluar ne menyre qe adresat aktuale te perdoruesve te institucionit te mos ndryshojne, port e kalojne ne nje nga ofruesit e cloud email me qellim rritjen e sigurise te postes elektronike.

2.2 FAZA II – ZHVILLIMI I SOFTWARE PER INFOPOINT

2.2.1 Faza e dyte e projektit konsiston ne zhvillimin e aplikacionit Infopoint i cili do te sherbeje ne formen e nje platforme interactive per turistet te cilet do te kene mundesine ta aksesojne kete platforme nepermjet nje monitori touchscreen te vendosur ne terminalin e mberritjeve. Ne platforme do te jete e mundur vizualizimi i pikave turistike per t'u vizituar ne qytetin e Sarandes, aksesimi i informacioneve mbi sherbimet e hotelerise dhe restoranteve ne qytet, informacione mbi transportin publik, si dhe informacione te ndryshme te cilat do te sherbejne per permiresimin e experiences turistike te bizitoreve te qytetit te Sarandes.

2.3 FAZA III – ZHVILLIMI I SOFTWARE PER ORARET

2.3.1 Faza e trete e projektit parashikon zhvillimin e aplikacionit per oraret e lundrimeve ne portin e Sarandes. Ky aplikacion do te beje te mundur shfaqen e orareve te nisjes dhe mberritjes per udhetuesit, si dhe ofron mundesine e

menaxhimit ne forme te automatizuar per ndryshimet e mundshme ne orare apo njoftimet per udhetuesit. Gjithashtu ky aplikacion duhet te monitorohet edhe nga sektori i policies kufitare brenda portit Sarande me qellim permiresimin e procesit te kontrolleve te udhetareve.

2.4 FAZA IV – IMPLEMENTIMI I SOFTWARE PER SIGURINE KIBERNETIKE

2.4.1 Gjate fazes kater te projektit kerkohet te kryhet implementimi i zgjidhjes se sigurise te qenderzuar. Kjo zgjidhje ne forme software duhet te instalohet dhe te menaxhohet nga server kryesor dhe duhet te ofroje mundesine e monitorimit te sigurise te te gjitha pajisjeve ne rrjetin e brendshem dhe te aplikacioneve te hostuara ne server. Gjithashtu, duhet mundesuar aftesia per gjenerimin e raporteve te situates kibernetike ne institucion, aftesia per te parandaluar dhe per t'ju pergjigjur incidenteve kibernetike, aftesia e kthimit te te dhenave ne rast sulmesh te suksesshme me ransomware. Software per sigurine kibernetike duhet te mundesoje aftesine per te implementuar mbrojtjen nga humbja e te dhenave (Data Loss Protection). Te gjitha opsionet e mesiperme duhet te ofrohen nepermjet nje agjenti unik per cdo pajisje fundore dhe te menaxhohen nga nje console e vetme me nderfaqe web.

2.5 FAZA V – ZHVILLIMI I POLITIKAVE TE SIGURISE KIBERNETIKE, VLERESIMIT TE RISKUT, TESTIMEVE TE SIGURISE PER FAQEN WEB DHE SOFTWARE INFOPOINT & ORARET, TRAJNIMI I PERSONELIT

Ne fazen e peste parashikohen te zhvillohen proceset si me poshte:

2.5.1 Zhvillimi i politikave te sigurise ku duhet te parashikohen dokumentacion I tille qe te siguroje plotesimin e masave administrative dhe teknike te sigurise kiebrnetike. Politikat e sigurise duhet te permbajne dokumentacion mbi procedurat e punes per trajtimin e konfigurimeve dhe mirembajtjes se sistemeve, procedurat e ruajtjes se te dhenave, proderuat e punes me sistemet per perdoruesit, dhe procedurat per ruajtjen e informacionit.

2.5.2 Zhvillimin e raportit te vleresimit te riskut ku te behet I mundur identifikimi I aseteve qe kane nevoje per mbrojtje kibernetike, identifikimin e rreziqeve dhe

dobesive, vleresimi i nivelit te rriskut, percaktimi i impaktit ne rastin e risqeve te detektuara, proceset e pranimit dhe reduktimit te riskut dhe kontrollet e pershtatshme per t'u implementuar me qellim zvogelimin e riskut.

2.5.3 Zhvillimi I testimeve te sigurise se aplikacioneve web ku te perfshihen ne nje raport te permbledhur pika si mbledhja e informacionit; menaxhimi I konfigurimeve; testimi I menaxhimit te identitetit; testimi I autentifikimit; testimi I proceseve te autorizimit; testimi I menaxhimit te sesioneve; testimi I validimit te inputeve; testimi I logjikes se funksionimit; testimi I nderfaqes se perdoruesve dhe testimi API.

2.6 FAZA VI – ZHVILLIMI I AUDITIMIT TE MASAVE TE SIGURISE KIBERNETIKE

2.6.1 Faza e fundit e projektit parashikon zhvillimin e auditimit te kontrolleve teknike dhe administrative te sigurise kibernetike te institucionit. Ne raportin e auditit duhet te perfshihen identifikimi i kontrolleve te parashikuara ne piken 5.13 te ketij dokumenti dhe sugjerimet per implementime ne te ardhmen. Raporti I auditimit duhet te perpilohet nga nje specialist I certifikuar per auditime te sigurise kibernetike.

3. SUPOZIME DHE RISQE

3.1.1 SUPOZIME

Gjate zhvillimit te projektit OE duhet te siguroje mbarevajtjen e funksionalitetit te sistemeve dhe te rrjetit kompjuterik ne menyre qe puna e perditshme e institucionit me sistemet te mos nderpritet.

3.1.2 RISQE

Aplikimi i teknikave testuese paraqet rrezikshmëri në vazhdimësinë e sistemeve. Gjatë aplikimeve të testimeve përdoren SW dhe teknika informatike që mund të kompromet ojnë sistemet ekzistuese. Është përgjegjësi e OE të ruajë konsistencën e sistemeve duke aplikuar në mënyrë të sigurt SW dhe teknikat përkatëse.

4. DETYRIMET E PALEVE

4.1.1 DETYRIMET E OPERATORIT EKONOMIK

OE duhet të plotësojë të gjithë kushtet teknike dhe organizative të përshkruar në këtë dokument. Operatori ekonomik është përgjegjës për pajisjen me sistemet HW dhe SW si dhe mënyrën e përdorimit të tyre për realizimin e kontratës

4.1.2 DETYRIMET E AUTORITETIT KONTRAKTOR

Për zhvillimin e projektit APS do të vendosë në dispozicion stafin teknik të saj si dhe informacionet e nevojshme për zhvillimin zerave te punes sipas preventivit.

Për sa i përket vlerësimit të kuadrit rregullator të TIK brenda institucionit, APS do të vendosë në dispozicion të gjithë dokumentacionin dhe rregulloret që disiplinojnë aktivitetin e strukturës përkatëse brenda institucionit. Për plotësimin e pyetësorëve të sigurisë APS do të vendosë në dispozicion punonjësit sipas sektorëve për të plotësuar formularët me asistencën e stafit përgjegjës të operatorit ekonomik.

5. SPECIFIKIMET TEKNIKE TE PROJEKTIT

5.1 SPECIFIKIMET TEKNIKE TE SERVERIT QENDROR

KARAKTERISTIKA MINIMALE TEKNIKE	
Form Factor	Rack, Min 1U, Aksesore te perfshire.
Procesori	Procesore multi-core, Minimumi 2 Core.
Ram	Min 24GB Serveri duhet te suportoje module RAM ECC
Kontrolleri RAID	Kontroller i afte te suportoje min. RAID 0,1
Storage I brendshem	Minimumi. 2HDD hot pluggable min 1Tb 3.5”
Kontrollori Ethernet	Minimumi 2 dalje 1 GB,
Ushqimi dhe ftohje	Blloqet e ushqimit dhe ftohjes duhet te jene hot pluggable
Sistemet	Serveri duhet te suportoje sistemet Windows dhe Linux

	Duhet te suportoje platformat e virtualizimit HyperV dhe VMware License per Windows Server 2016 Standard
Garancia	1 vit

5.2 SPECIFIKIMET TEKNIKE TE STORAGE

KARAKTERISTIKA MINIMALE TEKNIKE	
Formati	2U. Aksesoret e montimit
Memoria	Duhet ofroje min.1GB DDR4 memorie ne total
Protokollet e rrjetit	Te suportoje protokollet e rrjetit: SMB, AFP, NFS, FTP, WebDAV, CalDAV, iSCSI, Telnet, SSH, SNMP, VPN (PPTP, OpenVPN™, L2TP)
Portat	Minimumi 2 porta USB 3.0, Min 1. Gigabit Lan interface(RJ-45)
Disqet dhe RAID	-Duhet te ofrohet me min. 2 HDD 1TB te perfshire nga Vendori. -Raid 0, 1,5,6 dhe 10
Kapaciteti dhe zgjerimi	Te jete I zgjerueshem deri ne 60TB ose me shume.
Nderfaqe per konfigurim dhe menaxhim	-Duhet te ofroje nderfaqe web (GUI) Nderfaqja e menaxhimit duhet te ofroje monitorim te performances kohe reale
Aksesore	Te gjitha kabllot e ushqimit dhe te rrjetit te jene te perfshira.
Garancia	2 vjet nga prodhuesi

5.3 SPECIFIKIMET TEKNIKE TE FIREWALL-IT

KARAKTERISTIKA MINIMALE TEKNIKE	
Pajisja	Next generation firewall
Montimi	Në rack, 1U

Vecoritë e mbrojtjes	Pajisja duhet të ofrojë një sistem te besueshem sigurie, duke perfshire minimalisht mbrojtje NGFW, antivirus, IPS, Kontroll te Aplikacioneve, filtrim URL, Anti-bot, Anti-Spam etj.
Komponentët fizike	Min 5 porta 10/100/1000 Base-T RJ45 1 portë konsole RJ45 Min 1 port USB 2.0
Kapaciteti	Throughput i VPN: min 4.4 Gbps
	Throughput i IPS: min 1 Gbps
	Throughput i Firewall: min 7.5 Mpps
	Throughtput i FW te gjenerates se re: min 800 Mbps
	Thorughtput Threat Prevention/Protection: min 600 Mbps
	Sesione të njekohesishme: min 700 000
	Sesione të reja: min 35,000 sesione/sec
Njësi Ushqimi	100–240V AC, 50/60 Hz
Specifikime mbi sigurinë	Të suportojë efikasitet të lartë dhe sandbox Të ofrojë detektim, gjurmim, analizim dhe bllokim të sulmeve të vazhdueshem malware Të ofrojë parandalim të avancuar të kercenimeve dhe uljen e kercenimeve të njohura dhe atyre të panjohura Te suportoje multi-factor authentification
Manaxhimi	Pajisja duhet te ofroje manaxhim te qenderzuar te politikave te sigurise (mund te jete pajisje fizike-hardware ose software) Të mundësojë dhe ofrojë gjenerimin e raporteve në lidhje me incidentet Të ofrojë monitorim të rrjetit dhe të performancës së sigurisë
Licensimi dhe suporti	Pajisja duhet të ofrohet me abonim minimalisht 1 vit në shërbimet e mbrojtjes për paketat: Intrusion Prevention System (IPS) Advanced Malware Protection Kontroll te Aplikacioneve

	DNS dhe Video Filtering Filtrim i URL Anti-Spam Të ofrojë përditësime, përmirësime, update etj
Garancia	1 vit

5.4 SPECIFIKIMET TEKNIKE TE ANTIVIRUSIT

5.5 SPECIFIKIMET TEKNIKE TE POSTES ELEKTRONIKE

KARAKTERISTIKA MINIMALE TEKNIKE	
Tipi	Llogari per posten elektronike per 20 perdorues duke perdorur domain-in e sakte portidetarsarande.com
Madhesia e ruajtjes se te dhenave	Te mundesoje kapacitet per ruajtjen e te dhenave per cdo perdorues ne madhesine jo me pak se 30GB. Te mundesoje ndarjen e dokumentave midis dy ose me shume llogarive ne te njejten hapesire virtuale. Te mundesoje konfigurimin e privilegjeve per cdo perdorues ne dokumenta specifike.
Kalendari	Te ofroje mundesine per te menaxhuar takime ne menyre te automatizuar duke integruar kalendarin me llogarine e postes elektronike
Dokumentat	Te ofroje mundeine per te punuar ne menyre online dokumenta ne formatin word, excel dhe powerpoint. Punimi, ruajtja e ndryshimeve, historiku i ndryshimeve etj. te jene ne kohe reale nepermjet aplikacionit web.
Menaxhimi fundor i sigurise	Te mundesoje siguri ne menaxhimin e pikave fundore (endpoints) duke perdorur verifikim me dy faktore (two-factor authentication) ose single sign-on. Te mundesoje menaxhimin e mesazheve ne chat real-time duke i konfiguruar per kohen e ruajtjes, aksesimin etj.
Afati i sherbimit/licencimit	1 Vit

5.6 SPECIFIKIMET TEKNIKE TE SOFTWARE PER SIGURINE KIBERNETIKE

KARAKTERISTIKA MINIMALE TEKNIKE	
Tipi	Platforme e qenderzuar e sigurise kibernetike. Proaktive, Aktive dhe Reaktive
Struktura	Nje platforme e vetme menaxhimi e cila siguron zgjidhje per sigurine kibernetike dhe backup. Kapacitet per 20+ perdorues
Aftesi identifikimi	Te ofroje mundesi per zbulim automatik pajisjeve te reja. Te ofroje mundesi per vleresim te cenueshmerise. Te shfaqe harte/skeme te mbrojtjes se te dhenave.
Aftesi mbrojtje	Te ofroje mundesi per instalimin e agjentit ne largesi (remote). Te ofroje mundesi per zgjidhje «backup &disaster recovery ». Te ofroje mundesi per menaxhm te unifikuar te politikave te sigurise.
Aftesi zbulimi	Te kontrolloje gjendjen funksionale te hard drive. Te ofroje mbrojtje nga “malware” dhe ‘’exploit’’. Te ofroje mundesi per menaxhimi nga paneli qendror dhe te gjeneroje raporte.
Aftesi per tu pergjigjur	Te vendose ne karantine materialet e klasifikuara si te demshme/keqberese. Te ofroje mundesi shpetimi per «bootable media”. Menaxhim te patch-eve te integruar me backup.
Afesi per kthimin/rigjenerimin e te dhenave	Te perfshije mundesine e “Backup & Disaster Recovery” Te ofroje mundesine e sigurimit te te dhenave ne backup. Te ofroje mundesi menaxhimi remote.
Siguria	Zgjidhja te ofrohet nga nje prodhues/brand i njohur ne perputhshmeri me standartet nderkombetare ISO 27001, NIST, GDPR
Afati i sherbimit/licencimit	1 Vit

5.7 SPECIFIKIMET TEKNIKE TE SOFTWAREINFOPOINT

KARAKTERISTIKA MINIMALE TEKNIKE	
Tipi	Aplikacion I bazuar ne web
Gjuha e programimit	PHP
Baza e te dhenave	Databaza duhet te shkruhet ne MySQL dhe duhet te ofroje mundesine per te ruajtur informacion per cdo pike turistike si: - Vendndoshjen - Pershkrimin - Imazhe - Vleresimet e vizitoreve
Back-end Framework	Sistemi duhet te kete nje back-end te mundesuar nga Laravel, e cila duhet te pergjigjet per ; - Autentifikimin e perdoruesve - Menaxhimin e databazes - Procesimin e te dhenave lidhur me informacionin mbi pikat turistike
Nderfaqja	Sistemi duhet te kete nje nderfaqje user-friendly duke lejuar administratoret te menaxhojne pikat turistike duke perfshire; - Shtimin e pikave te reja turistike - Perditesimin e pikave turistike ekzistuese - Shfaqjen e informacionit per cdo pike turistike
Te dhenat e hostimit te software-it	- Web server me sherbimin Nginx ose Apache - Gjuhe programimi PHP version 8.1 ose me lart per te siguruar mirefunksionimin e sistemit - Te pakten 50GB hapesire per ruajtjen e datazaes ose te cdo imazhi qe mund te ngarkohet ne sistem

5.7.1 SPECIFIKIMET TEKNIKE PER MONITORIN PER INFOPOINT

KARAKTERISTIKA MINIMALE TEKNIKE

Back light	Direct type LED
Size (diagonal)	≥65"
Resolution	≥3840x2160 4K UHD
Brightness	370 candela per m2
Contrast ratio	1,200:1 ose me mire
Contrast ratio (dynamic)	4,000:1 ose me mire
Viewing angle	178° ose me mire
Response time	8ms ose me mire
Life	≥ 50,000 hours
Speaker count	2
Watts per speaker	≥ 15W
Surface hardness	7H ose me mire
Glass	Anti Glare + Anti Finger Print
Touch Interactivity	FInger & Passive Infrared Pen me detektim automatik
Included in the box/configuration.	European standard power cord（3m), USB cable HDMI cable (5m) 2x Writing Pen Remote control Battery Pen holder Quick start guide
Connections	Inputs 3 x HDMI 2.0, 1 x VGA, 1 x DisplayPort, 1 x Audio 3.5mm, (4) USB2, 1 x USB 3.0 (1)RJ45 Outputs 1 x HDMI 2.0, 1 x S/PDIF, 1 x Audio 3.5mm, 1 RJ 45 Control 5 x USB-A interactive, 1 x RS232
Opeartion System	≥ Android 8.0 ose ekuivalent
Power supply	100-240V~ 50/60Hz
RAM	≥3GB

Storage	≥16GB
Physical Specifications Flat Panel	1.6 m x 1 m x 0.1 m ose me e vogel Te gjithe aksesoret e montimit te perfshira.
Kushtet e operimit	20% - 80% lageshti deri ne 40 grade Celcius

5.8 SPECIFIKIMET TEKNIKE TE SOFTWARE PER ORARET

KARAKTERISTIKA MINIMALE TEKNIKE	
Tipi	Aplikacion i bazuar ne web
Gjuha e programimit	PHP
Baza e te dhenave	Databaza duhet te shkruhet ne MySQL dhe duhet te ofroje mundesine per ruajtur informacion per cdo mjet lundrues si: - Oraret e nisjeve dhe mberritjeve - Prejardhjen dhe destinacionit per cdo mjet lundrues - Informacione shtese
Back-end Framework	Sistemi duhet te kete nje back-end te mundesuar nga Laravel, e cila duhet te pergjigjet per ; - Autentifikimin e perdoruesve - Menaxhimin e databazes - Procesimin e te dhenave lidhur me mjetet lundruese
Nderfaqja	Sistemi duhet te kete nje nderfaqje user-friendly duke lejuar administratoret te menaxhojne pikat turistike duke perfshire; - Ndryshimet ne oraret e mjeteve lundruese - Informacione lajmeruese per udhetaret sipas situates - Shfaqjen e informacioneve te ndryshme ndihmese
Te dhenat e hostimit te software-it	- Web server me sherbimin Nginx ose Apache - Gjuhe programimi PHP version 8.1 ose me lart per te siguruar mirefunksionimin e sistemit - Te pakten 50GB hapesire per ruajtjen e datazaes ose te cdo imazhi qe mund te ngarkohet ne sistem

5.9 KERKESAT TEKNIKE PER ZHVILLIMIN E VLERESIMIT TE RISKUT

KARAKTERISTIKA MINIMALE TEKNIKE	
Tipi	Zhvillimi i vleresimit te riskut sipas standardeve kombetare dhe nderkombetare
Pikat e raportit te vleresimit te riskut	- Identifikimi i aseteve qe kane nevoje per mbrojtje kibernetike - Identifikimi i rreziqeve dhe dobesive - Identifikimi i dobesive te shfrytezueshme - Vleresimi i nivelit te rrezikut nepermjet agjenteve te riskut - Percaktimi i impaktit ne punen rutine ne rastin e rrisqeve te detektuara - Zhvillimi i vleresimit te riskut per sigurine kibernetike te institucionit - Keshillim mbi pranimin e lejuar te riskut - Keshillim mbi kontrollet e pershtatshme per implementim

5.10 KERKESAT TEKNIKE PER ZHVILLIMIN E TRAJNIMIT PER SIGURINE KIBERNETIKE

KARAKTERISTIKA MINIMALE TEKNIKE	
Tipi	Zhvillimi i trajnimeve mbi sigurine kibernetike
Ndergjegjesim per perdoruesit fundor mbi sigurine kibernetike	- Sulmet “Phishing” - Ransomware - “Social Engineering” - Perdorimi i rrjeteve sociale - Perdorimi i email-it - Siguria e pajisjeve mobile - Pajisjet e levizshme - Fjalekalimet dhe autentifikimi

	- Siguria fizike - Parimet e punes ne distance - Rrjetet wi-fi publike - Siguria ne “Cloud”
Trajnim per personelin IT mbi sigurine kibernetike	- Siguria e sistemeve te operimit - Siguria e aplikacioneve web - Siguria e rrjeteve kompjuterike - Siguria e serverave - Siguria “cloud”

5.11 KERKESAT TEKNIKE PER ZHVILLIMIN E TESTIMEVE TE SIGURISE

KARAKTERISTIKA MINIMALE TEKNIKE	
Tipi	Zhvillimi i testimeve te sigurise per aplikacionet web
Pikat e raportit te testimit te aplikacioneve web	- Mbledhja e informacionit - Menaxhimi i konfigurimeve te aplikacionit web - Testimi i menaxhimit te identitetit - Testimi i autentifikimit - Testimi i proceseve te autorizimit - Testimi i menaxhimit te sesioneve - Testimi i validimit te inputeve - Testimi i logjikes se funksionimit - Testimi i nderfaqjes se perdoruesit - Testimi API

5.12 KERKESAT TEKNIKE PER ZHVILLIMIN E POLITIKAVE TE SIGURISE KIBERNETIKE

KARAKTERISTIKA MINIMALE TEKNIKE	
Tipi	Zhvillimi i politikave per sigurine kibernetike te institucionit
Politikat e konfigurimeve dhe mirembajtjes	- Politika mbi menaxhimin e ndryshimeve ne sistem - Politika mbi nxjerrjen jashte perdorimi te pajisjeve

	- Politika mbi pajisjet mobile (BYOD) - Politika mbi shperndarjen e rrjetit - Politika mbi aksesin ne distance - Politika mbi sigurine e sitcheve dhe routerave - Politika mbi sigurine e serverave - Politika mbi instalimin e software-ve - Politika mbi licensimin e software-ve - Politika mbi konfigurimin e llogarive te sistemit - Politika mbi menaxhimin e dobesive ne sistem - Politika mbi konfigurimet e rrjetave wireless - Politika mbi konfigurimin e workstations
Politikat mbi ruajtjen e te dhenave	- Politika per backup te te dhenave - Politika per klasifikimin e te dhenave - Politika per kriptimin e te dhenave
Politikat per perdoruesit	- Politika per pastrimin e hapesirave personale - Politika per perdoruesit fundor - Politika per trajnimin e perdoruesve fundor - Politika per perdorimin e email-it nga perdoruesit fundor - Politika per aksesimin ne distance nga perdoruesit fundor - Politika per krijimin dhe menaxhimin e profileve te perdoruesve - Politika per fjalekalimet e perdoruesve
Politika per ruajtjen e informacionit	- Politika per auditin e aktivitetit te perdoresve - Politika per standarded e ruajtjes se informacionit

5.13 KERKESAT TEKNIKE PER ZHVILLIMIN E AUDITIMIT TE SIGURISE KIBERNETIKE

KARAKTERISTIKA MINIMALE TEKNIKE

Tipi	Zhvillimi i auditit per sigurine kibernetike te institucionit
Pikat e auditit te sigurise kibernetike	- Kontroll mbi sistemet e operimit dhe perditesimet e nevojshme - Kontroll mbi protokollet e ISP se institucionit - Kontroll i aksesueshmerise se sistemit - Kontroll i software-ve te antivirusit dhe anti malware - Kontroll mbi sigurine e perdorimit te email-eve - Kontroll mbi sigurine e komunikimeve te jashtme dhe te brendeshme - Kontroll mbi politikat e humbjes se te dhenave - Rishikim i skemes te komunikimit te sigurte - Kontroll dhe permiresim i procesit te backup te te dhenave - Skanim i dobesive te brendeshme dhe te jashtme - Kontroll i siguracionit kibernetik

6. PLANI I ZHVILLIMIT

6.1 VENDI I ZHVILLIMIT TE PROCEDURES

Vendi I zhvillimit te kesaj procedure do te jete Porti Sarande, Sarande, Shqiperi.

6.2 GRAFIKU I ZHVILLIMIT TE SHERBIMEVE

Data për fillimin e zbatimit të kontratës do të jetë menjëherë në datën e nënshkrimit dhe kohëzgjatja e implementimit të detyrave do të jetë 30 (tridhjete) dite nisur nga kjo datë. Tabela e mëposhtme paraqet kohën e zhvillimit të projektit. Në raste të veçanta, kjo periudhë mund të zgjatet me miratimin paraprak dhe pas kërkesës se justifikuar të Operatorit ekonomik jo më shumë se 1 (nje) javë nga afati maksimal i parashikuar. Kygrafik nuk do të konsiderohet në raste emergjencash reale dhe/ose sulmesh paralele nga palë e tretë gjatë kohës së implementimit te projektit.

?????????????

Faza	Emertimi I fazes	Java 1	Java 2	Java 3	Java 4
I	IMPLEMENTIMI I SERVERIT QENDROR, STORAGE, FIREWALL, ANTIVIRUS DHE POSTA ELEKTRONIKE				
II	ZHVILLIMI I SOFTWARE PER INFOPOINT				
III	ZHVILLIMI I SOFTWARE PER ORARET				
IV	IMPLEMENTIMI I SOFTWARE PER SIGURINE KIBERNETIKE				
V	ZHVILLIMI I POLITIKAVE TE SIGURISE KIBERNETIKE, VLERESIMIT TE RISKUT, TESTIMEVE TE SIGURISE PER FAQEN WEB DHE SOFTWARE INFOPOINT & ORARET, TRAJNIMI I PERSONELIT				
VI	ZHVILLIMI I AUDITIMIT TE MASAVE TE SIGURISE KIBERNETIKE				

7. SIGURIA E TE DHENAVE TE VENDOSURA NE DISPOZICION

Kontraktuesi merr përsipër ruajtjen dhe konfidencialitetin e të dhënave të vëna në dispozicion nga Autoriteti Portual Sarande me qëllim zbatimin e kontratës dhe arritjen e rezultateve dhe përmbushjen e detyrimeve që rrjedhin nga ajo. Raportet dhe të dhënat e mbledhura gjatë zhvillimit te projektit jane pronë ekskluzive e Autoriteti Portual Sarande. Operatori Ekonomik nuk mund ti publikojë, apo ti përdorë për asnjë lloj qëllimi qofshin ato dhe raste studimore, pa miratimin paraprak të AK.

Preventivi

Nr.	Zeri	Njesia	Sasia
1.	**Siguria Kibernetike dhe Infrastrukture**		
1.1.	**Vleresim Risku**	**Ore**	**40**
1.2.	**Zhvillim politikash per sigurine kibernetike**	**Ore**	**60**
1.3.	**Audit per sigurine kibernetike**	**Ore**	**60**
1.4.	**Testime sigurie ne faqen web**	**Ore**	**20**
1.5.	**Trajnim mbi sigurine kibernetike per perdoruesite sistemit**	**Ore**	**10**
1.6.	**Server Aplikacionesh**	**Cope**	**1**
1.7.	**Server Storage per te dhenat**	**Cope**	**1**
1.8.	**Pajisje per mbrojtje perimetrale + license 1vjecare (Firewall)**	**Cope**	**1**
1.9.	**Antivirus per pajisje fundore (1 vjecare)**	**Cope**	**20**
1.10.	**Software per monitorimin e sigurise kibernetike(1 vjecare)**	**Cope**	**20**
1.11.	**Llogari per posten elektronike (1 Vjecare)**	**Cope**	**20**
2.	**Infopoint**		
2.1.	**Interactive Board**	**Cop**	**1**
2.2.	**Software per infopoint**	**Ore**	**180**
2.3.	**Instalim**	**Ore**	**10**
3.	**Zhvillim Software per oraret**		
3.1.	**Zhvillimi I Softit**	**Ore**	**150**
3.2.	**Instalim**	**Ore**	**10**