EIOPA-BoS-20/600

Linji gwida dwar is-sigurtà u l-governanza tat-teknoloġija tal-informazzjoni u tal-komunikazzjoni

EIOPA – Westhafen Tower, Westhafenplatz 1 - 60327 Frankfurt – Il-Ġermanja - Tel. + 49 69-951119-20;
Faks. + 49 69-951119-19; posta elettronika: info@eiopa.europa.eu sit: www.eiopa.europa.eu

Werrej

Sfond

1. Skont l-Artikolu 16 tar-Regolament (UE) Nru 1094/2010, l-EIOPA tista' toħroġ linji gwida u rakkomandazzjonijiet indirizzati lill-awtoritajiet kompetenti u lill-istituzzjonijiet finanzjarji bil-għan li jiġu stabbiliti prattiki superviżorji konsistenti, effiċjenti u effettivi u tiġi żgurata l-applikazzjoni komuni, uniformi u konsistenti tad-dritt tal-Unjoni.

2. Skont l-Artikolu 16(3) ta' dan ir-Regolament, l-awtoritajiet kompetenti u l-istituzzjonijiet finanzjarji huma meħtieġa jagħmlu kull sforz sabiex jikkonformaw ma' dawn il-Linji gwida u r-rakkomandazzjonijiet.

3. L-EIOPA identifikat il-ħtieġa li tiġi żviluppata gwida speċifika dwar is-sigurtà u l-governanza tat-teknoloġija tal-informazzjoni u tal-komunikazzjoni (ICT) fir-rigward tal-Artikoli 41 u 44 tad-Direttiva 2009/138/KE fil-kuntest tal-analiżi mwettqa biex tingħata tweġiba għall-Pjan ta' Azzjoni tal-FinTech tal-Kummissjoni Ewropea (COM(2018)0109 finali), il-Pjan ta' Konverġenza Superviżorja tal-EIOPA 2018-2019[1] u wara interazzjonijiet ma' bosta partijiet interessati oħra[2].

4. Kif irrappurtat fil-Parir Konġunt tal-Awtoritajiet Superviżorji Ewropej lill-Kummissjoni Ewropea, il-Linji Gwida tal-EIOPA dwar is-sistema ta' governanza "*ma jirriflettux b'mod xieraq l-importanza tal-attenzjoni għall-ġestjoni tar-riskju tal-ICT (inklużi r-riskji ċibernetiċi)*". Ma hemm l-ebda gwida rigward l-elementi vitali li ġeneralment huma rikonoxxuti bħala parti mis-sigurtà u l-governanza xierqa tal-ICT".

5. L-analiżi tas-sitwazzjoni (leġiżlattiva) attwali fl-UE għall-Parir Konġunt imsemmi hawn fuq uriet li maġġoranza tal-Istati Membri tal-UE għandhom regoli nazzjonali definiti għas-sigurtà u l-governanza tal-ICT. Għalkemm ir-rekwiżiti huma simili, il-qafas regolatorju għadu frammentat. Barra minn hekk, stħarriġ dwar il-prattiki superviżorji attwali żvela varjetà wiesgħa ta' prattiki - minn "l-ebda superviżjoni speċifika" għal "superviżjoni b'saħħitha" (inklużi "spezzjonijiet mhux fuq il-post" u "spezzjonijiet fuq il-post").

6. Barra minn hekk, qed tiżdied il-kumplessità tal-ICT u qed tiżdied ukoll il-frekwenza tal-inċidenti relatati mal-ICT (inklużi l-inċidenti ċibernetiċi), bħal ma huwa l-impatt detrimentali ta' dawn l-inċidenti fuq il-funzjonament operazzjonali tal-impriżi. Għal din ir-raġuni, il-ġestjoni tar-riskju tal-ICT u tas-sigurtà huwa fundamentali għal impriża biex tikseb l-objettivi strateġiċi, korporattivi, operazzjonali u ta' reputazzjoni tagħha.

7. Barra minn hekk, fis-settur tal-assigurazzjoni, inklużi l-mudelli tan-negozju kemm tradizzjonali kif ukoll innovattiv, hemm dipendenza dejjem akbar fuq l-ICT fil-provvista tas-servizzi tal-assigurazzjoni u fil-funzjonament operazzjonali normali tal-impriżi, eż. id-diġitalizzazzjoni tas-settur tal-assigurazzjoni (InsurTech, IoT, eċċ.) kif ukoll l-interkonnessjoni permezz ta' kanali tat-telekomunikazzjonijiet (l-internet, il-konnessjonijiet mobbli u mingħajr fili u n-netwerks fuq żona wiesgħa). Dan jagħmel l-operazzjonijiet tal-impriżi vulnerabbli għal inċidenti tas-sigurtà inklużi l-attakki ċibernetiċi. Għaldaqstant huwa importanti li jiġi żgurat li l-impriżi

[1] https://www.eiopa.europa.eu/supervisory-convergence-plans-and-reports_en

[2] Ir-rapport ippubblikat mill-EIOPA bħala tweġiba għall-Pjan ta' Azzjoni tal-FinTech tal-Kummissjoni Ewropea jista' jinkiseb hawnhekk.

jkunu mħejjija b'mod adegwat biex jiġġestixxu r-riskji tal-ICT u tas-sigurtà tagħhom.

8. Barra minn hekk, filwaqt li jirrikonoxxu l-ħtieġa li l-impriżi jkunu mħejjija għal riskju ċibernetiku[3] u għal qafas sod tas-sigurtà ċibernetika, dawn il-Linji gwida jkopru wkoll is-sigurtà ċibernetika bħala parti mill-miżuri ta' sigurtà tal-informazzjoni tal-impriża. Filwaqt li dawn il-Linji gwida jirrikonoxxu li s-sigurtà ċibernetika għandha tkun indirizzata bħala parti mill-ġestjoni globali tar-riskju tal-ICT u tas-sigurtà ta' impriża, huwa importanti li jiġi nnutat li l-attakki ċibernetiċi għandhom xi karatteristiċi speċifiċi, li għandhom jiġu kkunsidrati biex jiġi żgurat li l-miżuri tas-sigurtà tal-informazzjoni jimmitigaw b'mod adegwat ir-riskju ċibernetiku:

   a) l-attakki ċibernetiċi spiss huma aktar diffiċli biex jiġu ġestiti (jiġifieri biex ikun hemm identifikazzjoni, protezzjoni, detezzjoni, reazzjoni għal u rkupru sħiħ minnhom) mill-biċċa l-kbira tas-sorsi l-oħra tar-riskju tal-ICT u tas-sigurtà kif ukoll huwa diffiċli jiġi ddeterminat il-limitu tal-ħsarat;

   b) xi attakki ċibernetiċi jistgħu jagħmlu ineffettivi l-ġestjoni komuni tar-riskju u l-arranġamenti tal-kontinwità tan-negozju, kif ukoll il-proċeduri ta' rkupru minn diżastru, peress li jistgħu jxerrdu l-malware f'sistemi ta' backup sabiex jagħmluhom mhux disponibbli jew biex iħassru d-*data* ta' backup;

   c) il-fornituri tas-servizzi, is-sensara, l-aġenti (ta' ġestjoni) u l-intermedjarji jistgħu jsiru kanali għall-propagazzjoni tal-attakki ċibernetiċi. It-theddid sieket kontaġġjuż jista' juża l-interkonnettività permezz ta' konnessjonijiet tat-telekomunikazzjoni ta' partijiet terzi biex jivvjaġġa lejn is-sistema tal-ICT tal-impriża. Għaldaqstant, impriża interkonnessa li jkollha rilevanza baxxa individwali tista' ssir vulnerabbli u sors ta' propagazzjoni tar-riskju u tista' tirriżulta f'impatt sistemiku. Meta wieħed josserva l-prinċipju tal-ħolqa l-aktar dgħajfa, is-sigurtà ċibernetika ma għandhiex tkun biss ta' tħassib għall-parteċipanti ewlenin fis-suq jew għall-fornituri tas-servizzi kritiċi.

9. L-objettiv ta' dawn il-Linji gwida huwa li:

   a) jipprovdu kjarifika u trasparenza lill-parteċipanti fis-suq dwar l-informazzjoni minima mistennija u l-kapaċitajiet tas-sigurtà ċibernetika, jiġifieri l-linja bażi tas-sigurtà;

   b) jevitaw arbitraġġ regolatorju potenzjali;

   c) irawmu konverġenza superviżorja rigward l-aspettattivi u l-proċessi applikabbli relatati mas-sigurtà u l-governanza tal-ICT bħala element ewlieni għall-ġestjoni xierqa tar-riskju tal-ICT u tas-sigurtà.

[3] Għal definizzjoni tar-riskju ċibernetiku jekk jogħġbok irreferi għall-FSB Cyber Lexicon, tat-12 ta' Novembru 2018, https://www.fsb.org/wp-content/uploads/P121118-1.pdf

Linji gwida dwar is-sigurtà u l-governanza tat-teknoloġija tal-informazzjoni u tal-komunikazzjoni

Introduzzjoni

1. F'konformità mal-Artikolu 16 tar-Regolament (UE) Nru 1094/2010[4] l-EIOPA toħroġ dawn il-Linji gwida indirizzati lill-awtoritajiet superviżorji biex tipprovdi gwida dwar kif l-impriżi tal-assigurazzjoni u tar-riassigurazzjoni (kollettivament "impriżi") għandhom japplikaw ir-rekwiżiti ta' governanza previsti fid-Direttiva 2009/138/KE[5] ("Id-Direttiva tas-Solvibbiltà II") u fir-Regolament ta' Delega tal-Kummissjoni (UE) Nru 2015/35[6] ("Regolament ta' Delega") fil-kuntest tas-sigurtà u l-governanza tat-teknoloġija tal-informazzjoni u tal-komunikazzjoni("ICT"). Għal dan il-għan, dawn il-Linji gwida jibnu fuq id-dispożizzjonijiet dwar il-governanza pprovduti mill-Artikoli 41, 44, 46, 47, 132 u 246 tad-Direttiva tas-Solvibbiltà II u l-Artikoli 258 sa 260, 266, 268 sa 271 u 274 tar-Regolament Delegat. Barra minn hekk, dawn il-Linji gwida jibnu wkoll fuq il-gwida pprovduta mil-Linji gwida tal-EIOPA dwar is-sistema ta' governanza (EIOPA-BoS-14/253)[7] u mil-Linji gwida tal-EIOPA dwar l-esternalizzazzjoni lill-forniturituri tas-servizzi tal-cloud (EIOPA-BoS-19/270)[8].

2. Il-Linji Gwida japplikaw kemm għall-impriżi individwali kif ukoll, *mutatis mutandis* fil-livell ta' grupp[9].

3. L-awtoritajiet kompetenti għandhom, meta jkunu konformi jew meta qed jissorveljaw il-konformità ma' dawn il-Linji gwida, jikkunsidraw il-prinċipju tal-proporzjonalità[10], li għandu jiżgura li l-arranġamenti ta' governanza, inklużi dawk relatati mas-sigurtà u l-governanza tal-ICT jkunu proporzjonati man-natura, l-iskala u l-kumplessità tar-riskji korrispondenti li l-impriżi jiffaċċjaw jew jistgħu jiffaċċjaw.

4. Dawn il-Linji gwida għandhom jinqraw flimkien u mingħajr preġudizzju mad-Direttiva tas-Solvibbiltà II, ir-Regolament ta' Delega, il-Linji gwida tal-EIOPA dwar is-sistema ta' governanza u l-Linji gwida tal-EIOPA dwar l-esternalizzazzjoni lill-forniturituri tas-servizzi tal-cloud. Dawn il-Linji gwida huma maħsuba biex ikunu newtrali fit-teknoloġija u l-metodoloġija.

Definizzjonijiet

5. Jekk ma jkunux definiti f'dawn il-Linji Gwida, it-termini għandhom it-tifsira definita fid-Direttiva tas-Solvibbiltà II.

6. Għall-finijiet ta' dawn il-linji gwida, għandhom japplikaw id-definizzjonijiet li ġejjin:

---

[4] Ir-Regolament (UE) Nru 1094/2010 tal-Parlament Ewropew u tal-Kunsill tal-24 ta' Novembru 2010 li jistabbilixxi Awtorità Superviżorja Ewropea (Awtorità Ewropea tal-Assigurazzjoni u l-Pensjonijiet tax-Xogħol), u li jemenda d-Deċiżjoni Nru 716/2009/KE u li jħassar id-Deċiżjoni tal-Kummissjoni 2009/79/KE (ĠU L 331, 15.12.2010, p. 48).

[5] Id-Direttiva 2009/138/KE tal-Parlament Ewropew u tal-Kunsill tal-25 ta' Novembru 2009 dwar il-bidu u l-eżerċizzju tan-negozju tal-Assigurazzjoni u tar-Riassigurazzjoni (Solvibbiltà II), (ĠU L 335, 17.12.2019, p. 1).

[6] Ir-Regolament ta' Delega tal-Kummissjoni (UE) 2015/35 tal-10 ta' Ottubru 2014 li jissupplimenta d-Direttiva 2009/138/KE tal-Parlament Ewropew u tal-Kunsill dwar il-bidu u l-eżerċizzju tan-negozju tal-Assigurazzjoni u r-Riassigurazzjoni (Solvibbiltà II) (ĠU L 12, 17.1.2015, p. 1)

[7] https://www.eiopa.europa.eu/content/guidelines-system-governance_en?source=search

[8] https://www.eiopa.europa.eu/content/eiopa-consults-guidelines-outsourcing-cloud-service-providers_en?source=search

[9] L-Artikolu 212(1) tad-Direttiva 2009/138/KE.

[10] L-Artikolu 29(3) tad-Direttiva 2009/138/KE.

Sid tal-assi	Persuna jew entità bir-responsabbiltà u l-awtorità għal assi tal-informazzjoni u tal-ICT.
Disponibbiltà	Il-karatteristika li tkun aċċessibbli u tkun tista' tiġi użata fuq talba (il-puntwalità) minn entità awtorizzata.
Kunfidenzjalità	Il-karatteristika li l-informazzjoni ma ssirx disponibbli jew ma tiġix żvelata lil individwi, entitajiet, proċessi jew sistemi mhux awtorazzati.
Attakk ċibernetiku	Kwalunkwe tip ta' hacking li jwassal għal tentattiv offensiv / malizzjuż biex jeqred, jesponi, jibdel, iħassar, jisraq jew jikseb aċċess mhux awtorizzat għal jew jagħmel użu mhux awtorizzat ta' assi tal-informazzjoni li jkollu fil-mira sistemi tal-ICT.
Sigurtà ċibernetika	Il-preservazzjoni tal-kunfidenzjalità, l-integrità u d-disponibbiltà ta' informazzjoni u/jew sistemi ta' informazzjoni permezz tal-mezz ċibernetiku.
Assi tal-ICT	Assi jew ta' software jew ta' hardware li jinstab fl-ambjent tan-negozju.
Proġetti tal-ICT	Kwalunkwe proġett, jew parti minnu, fejn is-sistemi u s-servizzi tal-ICT jinbidlu, jiġu sostitwiti jew jiġu implimentati.
Riskju tal-ICT u tas-sigurtà	Bħala subkomponent tar-riskju operazzjonali; ir-riskju ta' telf minħabba l-ksur tal-kunfidenzjalità, in-nuqqas ta' integrità ta' sistemi u *data*, l-inadegwatezza jew in-nuqqas ta' disponibbiltà ta' sistemi u *data* jew in-nuqqas ta' kapaċità għall-bdil tal-ICT fi żmien u bi spejjeż raġonevoli meta r-rekwiżiti tal-ambjent jew tan-negozju jinbidlu (jiġifieri l-aġilità). Dan jinkludi r-riskji ċibernetiċi kif ukoll ir-riskji tas-sigurtà tal-informazzjoni li jirriżultaw minn proċessi interni inadegwati jew li fallew jew minn avvenimenti esterni inklużi attakki ċibernetiċi jew sigurtà fiżika inadegwata.
Sigurtà tal-informazzjoni	Il-preservazzjoni tal-kunfidenzjalità, tal-integrità u d-disponibbiltà tal-informazzjoni u/jew ta' sistemi tal-informazzjoni. Barra minn hekk, karatteristiċi oħra, bħall-awtentiċità, ir-responsabbiltà, in-nuqqas ta' rifjut u l-affidabbiltà wkoll jistgħu jkunu involuti.

Servizzi tal-ICT	Is-servizzi pprovduti permezz ta' sistemi tal-ICT u ta' forniturи tas-servizzi lil utent intern jew estern wieħed jew aktar.
Sistemi tal-ICT	Sett ta' applikazzjonijiet, servizzi, assi tat-teknoloġija tal-informazzjoni, assi tal-ICT jew komponenti oħra għat-trattament tal-informazzjoni, li jinkludi l-ambjent operazzjonali.
Assi ta' informazzjoni	Ġabra ta' informazzjoni, tanġibbli jew mhux tanġibbli, li tajjeb li tiġi protetta.
Integrità	Karatteristika ta' eżattezza u kompletezza.
Inċident operazzjonali jew tas-sigurtà	Avveniment singulari jew sensiela ta' avvenimenti marbuta mhux ippjanati li għandhom jew x'aktarx li jkollhom impatt negattiv fuq l-integrità, id-disponibbiltà u l-kunfidenzjalità tas-sistemi u s-servizzi tal-ICT.
Fornitur tas-servizzi	Tfisser entità ta' parti terza li tkun qed twettaq proċess, servizz jew attività, jew partijiet minnhom, taħt arranġament ta' esternalizzazzjoni.
L-Ittestjar tal-Penetrazzjoni Mmexxija mit-Theddid	Tentattiv ikkontrollat biex tiġi kompromessa r-reżiljenza ċibernetika ta' entità bis-simulazzjoni ta' tattiki, tekniki u proċeduri ta' atturi ta' theddid fil-ħajja reali. Din hija bbażata fuq l-intelliġenza dwar it-theddid immirat u tiffoka fuq in-nies, il-proċessi u t-teknoloġija ta' entità, b'għarfien minimu minn qabel u b'impatt fuq l-operazzjonijiet.
Vulnerabbiltà	Dgħjufija, suxxettibbiltà jew difett ta' assi jew kontroll li jistgħu jiġu sfruttati minn theddida waħda jew aktar.

7. Dawn il-Linji gwida għandhom japplikaw mill-1 ta' Lulju 2021.

Linja Gwida 1 – Proporzjonalità

8. L-impriżi għandhom japplikaw dawn il-Linji gwida b'mod li jkun proporzjonat man-natura, l-iskala u l-kumplessità tar-riskji inerenti fin-negozju tagħhom.

Linja gwida 2 – L-ICT fi ħdan is-sistema ta' governanza

9. Il-korp amministrattiv, maniġerjali jew superviżorju (AMSB) għandu jiżgura li s-sistema ta' governanza tal-impriżi, b'mod partikolari s-sistema tal-ġestjoni tar-riskju u tal-kontroll intern, tiġġestixxi b'mod adegwat ir-riskji tal-ICT u tas-sigurtà tal-impriżi.

10. L-AMSB għandu jiżgura li l-kwantità u l-ħiliet tal-persunal tal-impriżi jkunu adegwati biex jappoġġaw il-ħtiġijiet operazzjonali tal-ICT tagħhom u l-proċessi ta' ġestjoni tar-riskji tal-ICT u tas-sigurtà tagħhom fuq bażi kontinwa u biex tiġi żgurata l-implimentazzjoni tal-istrateġija tal-ICT tagħhom. Barra minn hekk, il-persunal għandu jirċievi taħriġ adegwat dwar ir-riskji tal-ICT u tas-sigurtà, inkluża s-sigurtà tal-informazzjoni, fuq bażi regolari, kif stabbilit fil-Linja gwida 13.

11. L-AMSB għandu jiżgura li r-riżorsi allokati huma xierqa biex jissodisfaw ir-rekwiżiti hawn fuq imsemmija.

Linja gwida 3 - L-istrateġija tal-ICT

12. L-AMSB għandu r-responsabbiltà ġenerali fit-twaqqif u l-approvazzjoni tal-istrateġija miktuba tal-ICT tal-impriżi bħala parti minn u li tkun allinjata mal-istrateġija kummerċjali ġenerali tagħhom, kif ukoll fis-sorveljanza tal-komunikazzjoni u l-implimentazzjoni tagħha.

13. L-istrateġija tal-ICT għandha tiddefinixxi tal-anqas:

    a) kif l-ICT tal-impriżi għandha tevolvi biex b'mod effettiv tappoġġa u timplimenta l-istrateġija tan-negozju tagħhom, inklużi l-evoluzzjoni tal-istruttura organizzazzjonali, il-mudelli tan-negozju, is-sistema tal-ICT u d-dipendenzi ewlenin ma' fornituri tas-servizzi;

    b) l-evoluzzjoni tal-arkitettura tal-ICT, inklużi d-dipendenzi tal-fornitur tas-servizz; u

    c) objettivi ċari dwar is-sigurtà tal-informazzjoni, li jiffukaw fuq is-sistemi u s-servizzi tal-ICT, il-persunal u l-proċessi.

14. L-impriżi għandhom jiżguraw li l-istrateġija tal-ICT tiġi implimentata, adottata u kkomunikata lill-persunal u l-fornituri tas-servizzi rilevanti kollha, kif applikabbli u rilevanti, u fil-ħin.

15. L-impriżi għandhom jistabbilixxu proċess biex jimmonitorjaw u jkejlu l-effettività tal-implimentazzjoni tal-istrateġija tal-ICT. Dan il-proċess għandu jiġi rivedut u aġġornat fuq bażi regolari.

Linja gwida 4 – Ir-riskji tal-ICT u tas-sigurtà fi ħdan is-sistema tal-ġestjoni tar-riskju

16. L-AMSB għandu r-responsabbiltà ġenerali li jistabbilixxi sistema effettiva għall-ġestjoni tar-riskji tal-ICT u tas-sigurtà bħala parti mis-sistema ġenerali tal-ġestjoni tar-riskju tal-impriża. Dan jinkludi d-determinazzjoni tat-tolleranza tar-riskju għal dawk ir-riskji, skont l-istrateġija tar-riskju tal-impriża, u rapport bil-miktub regolari dwar ir-riżultat tal-proċess tal-ġestjoni tar-riskju indirizzat lill-AMSB.

17. Bħala parti mis-sistema ġenerali tal-ġestjoni tar-riskju tagħhom, l-impriżi għandhom fir-rigward tar-riskji tal-ICT u tas-sigurtà (filwaqt li jiddefinixxu r-rekwiżiti tal-protezzjoni tal-ICT kif deskritt hawn taħt) jikkunsidraw tal-anqas dan li ġej:

    a) l-impriżi għandhom jistabbilixxu u b'mod regolari jaġġornaw l-immappjar tal-proċessi u l-attivitajiet tan-negozju, il-funzjonijiet tan-negozju, ir-rwoli u l-assi tagħhom (eż. l-assi tal-informazzjoni u l-assi tal-ICT) sabiex jidentifikaw l-importanza tagħhom u l-interdipendenzi tagħhom għar-riskji tal-ICT u tas-sigurtà;

b) l-impriżi għandhom jidentifikaw u jkejlu r-riskji rilevanti kollha tal-ICT u tas-sigurtà li huma esposti għalihom u jikklassifikaw il-proċessi u l-attivitajiet tan-negozju, il-funzjonijiet tan-negozju, ir-rwoli u l-assi identifikati (eż. l-assi tal-informazzjoni u l-assi tal-ICT) f'termini ta' kritikalità. L-impriżi għandhom jivvalutaw ukoll ir-rekwiżiti tal-protezzjoni, tal-anqas, tal-kunfidenzjalità, l-integrità u d-disponibbiltà ta' dawk il-proċessi u l-attivitajiet tan-negozju, il-funzjonijiet tan-negozju, ir-rwoli u l-assi tagħhom (eż. l-assi tal-informazzjoni u l-assi tal-ICT). Għandhom jiġu identifikati s-sidien tal-assi, li huma responsabbli għall-klassifikazzjoni tal-assi;

c) il-metodi użati biex tiġi ddeterminata l-kritikalità kif ukoll il-livell ta' protezzjoni meħtieġa, b'mod partikolari fir-rigward tal-objettivi ta' protezzjoni tal-integrità, id-disponibbiltà u l-kunfidenzjalità, għandhom jiżguraw li r-rekwiżiti ta' protezzjoni li jirriżultaw jkunu konsistenti u komprensivi;

d) il-kejl tar-riskji tal-ICT u tas-sigurtà għandu jitwettaq abbażi tal-kriterji definiti tar-riskju tal-ICT u tas-sigurtà filwaqt li jikkunsidra l-kritikalità tal-proċessi u l-attivitajiet tan-negozju, il-funzjonijiet tan-negozju, ir-rwoli u l-assi tagħhom (eż. l-assi tal-informazzjoni u l-assi tal-ICT), il-livell tal-vulnerabbiltajiet magħrufa u l-inċidenti preċedenti li kellhom impatt fuq l-impriża;

e) il-valutazzjoni tar-riskji tal-ICT u tas-sigurtà għandha titwettaq u tiġi ddokumentata b'mod regolari. Din il-valutazzjoni għandha titwettaq ukoll qabel kwalunkwe bidla maġġuri fl-infrastruttura, fil-proċessi jew fil-proċeduri li jaffettwaw il-proċessi u l-attivitajiet tan-negozju, il-funzjonijiet tan-negozju, ir-rwoli u l-assi (eż. l-assi tal-informazzjoni u l-assi tal-ICT);

f) abbażi tal-valutazzjoni tar-riskju tagħhom, l-impriżi għandhom, tal-inqas, jiddefinixxu u jimplimentaw miżuri għall-ġestjoni tar-riskji tal-ICT u tas-sigurtà identifikati u jipproteġu l-assi tal-informazzjoni skont il-klassifikazzjoni tagħhom. Dan għandu jinkludi d-definizzjoni tal-miżuri għall-ġestjoni tar-riskji residwi li jkun fadal.

18. Ir-riżultati tal-proċess tal-ġestjoni tar-riskju tal-ICT u tas-sigurtà għandhom jiġu approvati mill-AMSB u jiġu inklużi fil-proċess tal-ġestjoni tar-riskju operazzjonali bħala parti mill-ġestjoni tar-riskju ġenerali tal-impriżi.

Linja gwida 5 - Verifika

19. Il-governanza, is-sistemi u l-proċessi tal-impriżi għar-riskji tal-ICT u tas-sigurtà tagħhom għandhom jiġu vverifikati fuq bażi perjodika f'konformità mal-pjan tal-verifika[11] tal-impriżi minn awdituri b'għarfien, ħiliet u kompetenza esperta suffiċjenti fir-riskji tal-ICT u tas-sigurtà sabiex jipprovdu assigurazzjoni indipendenti tal-effettività tagħhom lill-AMSB. Il-frekwenza u l-attenzjoni ta' tali verifiki għandhom ikunu proporzjonati mar-riskji rilevanti tal-ICT u tas-sigurtà.

Linja gwida 6 – Il-politika u l-miżuri tas-sigurtà tal-informazzjoni

20. L-impriżi għandhom jistabbilixxu politika ta' sigurtà tal-informazzjoni bil-miktub approvata mill-AMSB li għandha tiddefinixxi l-prinċipji u r-regoli ta' livell għoli għall-protezzjoni tal-kunfidenzjalità, l-integrità u d-disponibbiltà tal-informazzjoni tal-impriżi sabiex tappoġġa l-implimentazzjoni tal-istrateġija tal-ICT.

21. Il-politika għandha tinkludi deskrizzjoni tar-rwoli u r-responsabbiltajiet ewlenin għall-ġestjoni tas-sigurtà tal-informazzjoni, u għandha tistabbilixxi r-rekwiżiti għall-

[11] L-Artikolu 271 tar-Regolament ta' Delega.

persunal, il-proċessi u t-teknoloġija fir-rigward tas-sigurtà tal-informazzjoni, filwaqt li tirrikonoxxi li l-persunal fil-livelli kollha jkollu responsabbiltajiet biex jiżgura s-sigurtà tal-informazzjoni tal-impriżi.

22. Il-politika għandha tiġi kkomunikata fi ħdan l-impriża u għandha tapplika għall-persunal kollu. Fejn applikabbli u rilevanti, il-politika tas-sigurtà tal-informazzjoni jew partijiet minnha għandhom ukoll jiġu kkomunikati u applikati lill-fornituri tas-servizzi.

23. Abbażi tal-politika, l-impriżi għandhom jistabbilixxu u jimplimentaw proċeduri ta' sigurtà tal-informazzjoni u miżuri ta' sigurtà tal-informazzjoni aktar speċifiċi biex, *inter alia*, jimmitigaw ir-riskji tal-ICT u tas-sigurtà li jkunu esposti għalihom. Dawn il-proċeduri u l-miżuri ta' sigurtà tal-informazzjoni għandhom jinkludu kull proċess deskritt f'dawn il-Linji gwida, kif applikabbli.

Linja gwida 7 – Il-funzjoni tas-sigurtà tal-informazzjoni

24. L-impriżi għandhom jistabbilixxu, fis-sistema ta' governanza tagħhom u skont il-prinċipju tal-proporzjonalità, funzjoni tas-sigurtà tal-informazzjoni, bir-responsabbiltajiet assenjati lil persuna nominata. L-impriża għandha tiżgura l-indipendenza u l-oġġettività tal-funzjoni ta' sigurtà tal-informazzjoni billi b'mod xieraq tisseparaha mill-proċessi tal-iżvilupp u tal-operazzjonijiet tal-ICT. Il-funzjoni għandha tirrapporta lill-AMSB.

25. Il-kompiti tal-funzjoni tas-sigurtà tal-informazzjoni qegħdin tipikament biex:

    a) jagħtu appoġġ lill-AMSB meta dan jiddefinixxi u jżomm il-politika tas-sigurtà tal-informazzjoni għall-impriżi u jikkontrolla l-użu tagħha;

    b) jirrapportaw u jagħtu pariri lill-AMSB b'mod regolari u fuq bażi ad hoc dwar l-istatus tas-sigurtà tal-informazzjoni u l-iżviluppi tagħha;

    c) jimmonitorjaw u jirrevedu l-implimentazzjoni tal-miżuri tas-sigurtà tal-informazzjoni;

    d) jiżguraw li r-rekwiżiti tas-sigurtà tal-informazzjoni jiġu osservati meta jintużaw il-fornituri tas-servizzi;

    e) jiżguraw li l-impjegati u l-fornituri tas-servizzi kollha li jkollhom aċċess għall-informazzjoni u s-sistemi jkunu infurmati b'mod adegwat dwar il-politika tas-sigurtà tal-informazzjoni, pereżempju permezz ta' taħriġ dwar is-sigurtà tal-informazzjoni u sessjonijiet ta' sensibilizzazzjoni;

    f) jikkoordinaw l-eżaminazzjoni ta' inċident operazzjonali jew ta' sigurtà u jirrapportaw dawk rilevanti lill-AMSB.

Linja gwida 8 – Sigurtà loġika

26. L-impriżi għandhom jiddefinixxu, jiddokumentaw u jimplimentaw proċeduri għall-kontroll ta' aċċess loġiku jew sigurtà loġika (il-ġestjoni tal-identità u tal-aċċess) f'konformità mar-rekwiżiti ta' protezzjoni, kif definit fil-Linja gwida 4. Dawn il-proċeduri għandhom jiġu implimentati, infurzati, immonitorjati u perjodikament riveduti, u għandhom jinkludu wkoll kontrolli għall-monitoraġġ ta' anomaliji. Dawn il-proċeduri għandhom, bħala minimu, jimplimentaw l-elementi li ġejjin, fejn it-terminu "utent" jinkludi wkoll l-utenti tekniċi:

    a) il-ħtieġa ta' tagħrif, l-inqas privileġġ u s-segregazzjoni ta' dmirijiet: l-impriżi għandhom jiġġestixxu d-drittijiet ta' aċċess, inkluż l-aċċess mill-bogħod għal assi ta' informazzjoni u sistemi ta' appoġġ tagħhom fuq il-bażi ta' "ħtieġa ta'

tagħrif". L-utenti għandhom jingħataw id-drittijiet minimi ta' aċċess li jkunu strettament meħtieġa biex iwettqu dmirijiethom (il-prinċipju ta' "l-inqas privileġġ"), jiġifieri biex jiġi evitat aċċess mhux ġustifikat għal *data* jew li l-allokazzjoni ta' kombinazzjonijiet ta' drittijiet ta' aċċess jistgħu jintużaw biex jiġu evitati l-kontrolli (il-prinċipju ta' "segregazzjoni tad-dmirijiet");

b) ir-responsabbiltà tal-utent: l-impriżi għandhom jillimitaw, kemm jista' jkun, l-użu ta' kontijiet tal-utent ġeneriċi u kondiviżi u jiżguraw li l-utenti jkunu jistgħu jiġu identifikati u ttraċċati lura għal persuna fiżika responsabbli jew kompitu awtorizzat għall-azzjonijiet imwettqa fis-sistemi tal-ICT il-ħin kollu;

c) id-drittijiet ta' aċċess privileġġjat: l-impriżi għandhom jimplimentaw kontrolli b'saħħithom fuq l-aċċess privileġġjat għal sistema billi b'mod strett jillimitaw u jissorveljaw mill-qrib il-kontijiet b'aċċess elevat għas-sistema (eż. il-kontijiet ta' amministratur).

d) l-aċċess mill-bogħod: sabiex tiġi żgurata l-komunikazzjoni sikura u jitnaqqas ir-riskju, l-aċċess amministrattiv mill-bogħod għal sistemi tal-ICT kritiċi għandu jingħata biss abbażi ta' ħtieġa ta' tagħrif u meta jintużaw soluzzjonijiet ta' awtentikazzjoni b'saħħithom;

e) ir-reġistrazzjoni ta' attivitajiet tal-utenti: l-attivitajiet tal-utenti għandhom ikunu rreġistrati u mmonitorjati b'mod proporzjonat għar-riskju, li jinkludu, bħala minimu, l-attivitajiet tal-utenti privileġġjati. Ir-reġistri ta' aċċess għandhom jinżammu sikuri biex jiġu evitati l-modifika jew it-tħassir mhux awtorizzat u jinżammu għal perjodu li jkun proporzjonali mal-kritikalità tal-funzjonijiet ta' negozju, il-proċessi ta' appoġġ u l-assi ta' informazzjoni identifikati, mingħajr preġudizzju għar-rekwiżiti ta' żamma stipulati fil-liġi tal-UE u dik nazzjonali. L-impriżi għandhom jużaw din l-informazzjoni biex jiffaċilitaw l-identifikazzjoni u l-investigazzjoni ta' attivitajiet anomali li jkunu ġew identifikati fil-forniment tas-servizzi;

f) il-ġestjoni tal-aċċess: id-drittijiet tal-aċċess għandhom jingħataw, jitneħħew u jiġu modifikati fil-ħin, skont rutini predefiniti għall-approvazzjoni fejn ikun involut is-sid tal-assi tal-informazzjoni applikabbli. F'każ li ma jkunx għad hemm il-ħtieġa ta' aċċess, id-drittijiet tal-aċċess għandhom jiġu revokati b'mod immedjat;

g) il-valutazzjoni tal-aċċess: id-drittijiet tal-aċċess għandhom jiġu riveduti perjodikament biex ikun żgurat li l-utenti ma jkollhomx privileġġi eċċessivi u li d-drittijiet tal-aċċess jiġu rtirati/mneħħija meta ma jkunx għad hemm il-ħtieġa;

h) l-għoti, il-modifika, ir-revoka tad-drittijiet tal-aċċess għandhom jiġu ddokumentati b'mod li jiffaċilita l-komprensjoni u l-analiżi; u

i) Il-metodi ta' awtentikazzjoni: l-impriżi għandhom jinfurzaw il-metodi ta' awtentikazzjoni li jkunu robusti biżżejjed biex jiżguraw b'mod adegwat u effettiv li jkun hemm konformità mal-politiki u l-proċeduri ta' kontroll tal-aċċess. Il-metodi ta' awtentikazzjoni għandhom ikunu proporzjonati mal-kritikalità tas-sistemi tal-ICT, l-informazzjoni jew il-proċess li jkun hemm aċċess għalihom. Dan għandu, bħala minimu, jinkludi passwords sikuri jew metodi ta' awtentikazzjoni aktar b'saħħithom (bħal awtentikazzjoni b'żewġ fatturi), abbażi tar-riskju rilevanti.

27. L-aċċess elettroniku permezz ta' applikazzjonijiet għad-*data* u s-sistemi tal-ICT għandu jkun limitat għal minimu meħtieġ biex jiġi pprovdut is-servizz rilevanti.

Linja gwida 9 – Sigurtà fiżika

28. Il-miżuri ta' sigurtà fiżiċi tal-impriżi (eż. il-protezzjoni kontra l-qtugħ ta' dawl, in-nirien, l-ilma u l-aċċess fiżiku mhux awtorizzat) għandhom ikunu definiti, iddokumentati u implimentati biex jipproteġu l-bini, iċ-ċentri tad-*data* u ż-żoni sensittivi tagħhom minn aċċess mhux awtorizzat u minn perikli ambjentali.

29. L-aċċess fiżiku għas-sistemi tal-ICT għandu jingħata biss lil individwi awtorizzati. L-awtorizzazzjoni għandha tkun assenjata f'konformità mal-kompiti u r-responsabbiltajiet tal-individwi, u tkun limitata għal individwi li jiġu mħarrġa u mmonitorjati kif xieraq. L-aċċess fiżiku għandu jiġi rivedut b'mod regolari biex ikun żgurat li d-drittijiet ta' aċċess bla bżonn jiġu irtirati/imneħħija b'mod immedjat.

30. Miżuri adegwati għall-protezzjoni minn perikli ambjentali għandhom ikunu proporzjonati mal-importanza tal-bini u ma' kemm ikunu kritiċi l-operazzjonijiet jew is-sistemi tal-ICT li jinsabu f'dan il-bini.

Linja gwida 10 – Is-sigurtà tal-operazzjonijiet tal-ICT

31. L-impriżi għandhom jimplimentaw proċeduri biex jiżguraw il-kunfidenzjalità, l-integrità u d-disponibbiltà tas-sistemi tal-ICT u tas-servizzi tal-ICT sabiex rispettivament jimminimizzaw l-impatt ta' kwistjonijiet ta' sigurtà fuq il-forniment ta' servizzi tal-ICT. B'mod xieraq, dawn il-proċeduri għandhom jinkludu l-miżuri li ġejjin:

    a) l-identifikazzjoni tal-vulnerabbiltajiet potenzjali li għandhom jiġu evalwati u rrimedjati billi jiġi żgurat li s-sistemi tal-ICT ikunu aġġornati, inkluż is-software ipprovdut mill-impriżi lill-utenti interni u esterni tagħhom, billi jintuża software korrettiv tas-sigurtà kritika, inklużi l-aġġornamenti ta' definizzjonijiet tal-antivirus jew billi jiġu implimentati kontrolli ta' kumpens;

    b) l-implimentazzjoni ta' linji bażi ta' konfigurazzjoni sikura għall-komponenti kritiċi kollha bħas-sistemi operattivi, il-bażijiet tad-*data*, ir-routers jew is-swiċis;

    c) l-implimentazzjoni ta' segmentazzjoni tan-netwerk, sistemi ta' prevenzjoni ta' telf ta' *data* u l-kriptaġġ tat-traffiku tan-netwerk (f'konformità mal-klassifikazzjoni tal-assi tal-informazzjoni);

    d) l-implimentazzjoni ta' protezzjoni tal-punti aħħarin inklużi s-servers, l-istazzjonijiet tax-xogħol u l-apparat mobbli. L-impriżi għandhom jevalwaw jekk punt aħħari jissodisfax l-istandards tas-sigurtà definiti minnhom qabel ma jingħata aċċess għan-netwerk korporattiv;

    e) l-iżgurar li l-mekkaniżmi ta' kontroll tal-integrità jkunu fis-seħħ biex tiġi vverifikata l-integrità tas-sistemi tal-ICT;

    f) il-kriptaġġ tad-*data* wieqfa u fi tranżitu (f'konformità mal-klassifikazzjoni tal-assi tal-informazzjoni).

Linja gwida 11 – Il-monitoraġġ tas-sigurtà

32. L-impriżi għandhom jistabbilixxu u jimplimentaw proċeduri u proċessi biex b'mod kontinwu jimmonitorjaw l-attivitajiet li jħallu impatt fuq is-sigurtà tal-informazzjoni tal-impriżi. Il-monitoraġġ għandu jkopri tal-anqas:

    a) il-fatturi interni u esterni, inklużi l-funzjonijiet amministrattivi tan-negozju u tal-ICT;

b) it-tranżazzjonijiet minn fornituri tas-servizzi, entitajiet oħra u l-utenti interni; u

c) it-theddid intern u estern potenzjali.

33. Abbażi tal-monitoraġġ, l-impriżi għandhom jimplimentaw kapaċitajiet xierqa u effettivi għad-detezzjoni, ir-rappurtar u r-reazzjoni għal attivitajiet u theddid anomali, bħall-intrużjoni fiżika jew loġika, il-ksur tal-kunfidenzjalità, l-integrità u d-disponibbiltà tal-assi tal-informazzjoni, il-kodiċi malizzjuż u l-vulnerabbiltajiet magħrufa pubblikament għas-software u l-hardware.

34. Ir-rappurtar mill-monitoraġġ tas-sigurtà għandu jgħin lill-impriżi biex jifhmu n-natura kemm ta' inċidenti operazzjonali jew tas-sigurtà, biex jidentifikaw ix-xejriet u biex jagħtu appoġġ lill-investigazzjonijiet interni tal-impriżi u jippermettulhom jieħdu d-deċiżjonijiet xierqa.

Linja gwida 12 – Ir-rieżamijiet, il-valutazzjoni u l-ittestjar tas-sigurtà tal-informazzjoni

35. L-impriżi għandhom iwettqu varjetà ta' rieżamijiet, valutazzjonijiet u ttestjar differenti tas-sigurtà tal-informazzjoni, sabiex tiġi żgurata l-identifikazzjoni effettiva tal-vulnerabbiltajiet fis-sistemi u s-servizzi tal-ICT tagħhom. Pereżempju, l-impriżi jistgħu jwettqu analiżi tan-nuqqasijiet meta mqabbla mal-istandards tas-sigurtà tal-informazzjoni, ir-rieżamijiet tal-konformità, il-verifiki interni u esterni tas-sistemi tal-informazzjoni, jew ir-rieżamijiet tas-sigurtà fiżika.

36. L-impriżi għandhom jistabbilixxu u jimplimentaw qafas tal-ittestjar tas-sigurtà tal-informazzjoni li jivvalida r-robustezza u l-effettività tal-miżuri ta' sigurtà tal-informazzjoni u jiżguraw li dan il-qafas jikkunsidra t-theddid u l-vulnerabbiltajiet identifikati permezz tal-monitoraġġ tat-theddid u l-proċess tal-valutazzjoni tar-riskji tal-ICT u tas-sigurtà.

37. L-ittestjar għandu jsir b'mod sikur u minn persuni indipendenti li jwettqu t-testijiet li jkollhom l-għarfien, il-ħiliet u l-kompetenza esperta sufiċjenti fl-ittestjar tal-miżuri tas-sigurtà tal-informazzjoni.

38. L-impriżi għandhom iwettqu testijiet fuq bażi regolari. Il-kamp ta' applikazzjoni, il-frekwenza u l-metodu tal-ittestjar (bħall-ittestjar tal-penetrazzjoni, inkluż l-ittestjar tal-penetrazzjoni mmexxija mit-theddid) għandhom ikunu proporzjonati mal-livell ta' riskju identifikat. L-ittestjar ta' sistemi tal-ICT kritiċi u l-iskannjar tal-vulnerabbiltà għandhom jitwettqu kull sena.

39. L-impriżi għandhom jiżguraw li t-testijiet tal-miżuri ta' sigurtà jitwettqu f'każ ta' bidliet fl-infrastruttura, fil-proċessi jew fil-proċeduri u jekk isiru bidliet minħabba inċidenti operazzjonali kbar jew ta' sigurtà jew minħabba r-rilaxx ta' applikazzjonijiet kritiċi ġodda jew mibdula b'mod sinifikanti. L-impriżi għandhom jimmonitorjaw u jevalwaw ir-riżultati tat-testijiet tas-sigurtà, u jaġġornaw il-miżuri ta' sigurtà tagħhom kif xieraq mingħajr dewmien żejjed fil-każ ta' sistemi tal-ICT kritiċi.

Linja gwida 13 – It-taħriġ u s-sensibilizzazzjoni dwar is-sigurtà tal-informazzjoni

40. L-impriżi għandhom jistabbilixxu programmi ta' taħriġ dwar is-sigurtà tal-informazzjoni għall-persunal kollu, inkluż l-AMSB, sabiex jiġi żgurat li dawn jiġu mħarrġa biex iwettqu d-dmirijiet u r-responsabbiltajiet tagħhom biex jonqos l-iżball

uman, is-serq, il-frodi, l-użu ħażin jew it-telf. L-impriżi għandhom jiżguraw li l-programm ta' taħriġ jipprovdi t-taħriġ għall-persunal kollu fuq bażi regolari.

41. L-impriżi għandhom jistabbilixxu u jimplimentaw programmi ta' sensibilizzazzjoni dwar is-sigurtà perjodiċi biex jedukaw lill-persunal tagħhom, inkluż l-AMSB, dwar kif jindirizzaw ir-riskji relatati mas-sigurtà tal-informazzjoni.

Linja gwida 14 - Il-ġestjoni tal-operazzjonijiet tal-ICT

42. L-impriżi għandhom jiġġestixxu l-operazzjonijiet tal-ICT tagħhom abbażi tal-istrateġija tal-ICT. Id-dokumenti għandhom jiddefinixxu kif l-impriżi joperaw, jimmonitorjaw u jikkontrollaw is-sistemi tal-ICT u s-servizzi tal-ICT, inkluż id-dokumentazzjoni tal-proċessi, il-proċeduri u l-operazzjonijiet kritiċi tal-ICT.

43. L-impriżi għandhom jimplimentaw proċeduri ta' reġistrazzjoni u monitoraġġ għal operazzjonijiet kritiċi tal-ICT biex ikunu jistgħu jiġu identifikati, analizzati u kkoreġuti l-iżbalji.

44. L-impriżi għandhom iżommu inventarju aġġornat tal-assi tal-ICT tagħhom. L-inventarju tal-assi tal-ICT għandu jkun dettaljat biżżejjed biex jippermetti l-identifikazzjoni fil-pront ta' assi tal-ICT, is-sit tiegħu, il-klassifikazzjoni tas-sigurtà u s-sjieda.

45. L-impriżi għandhom jimmonitorjaw u jiġġestixxu ċ-ċikli tal-ħajja tal-assi tal-ICT biex jiżguraw li jkomplu jissodisfaw u jappoġġaw ir-rekwiżiti tan-negozju u tal-ġestjoni tar-riskju. L-impriżi għandhom jimmonitorjaw li l-assi tal-ICT ikunu appoġġati mill-bejjiegħa tagħhom jew mill-iżviluppaturi interni u li s-software korrettiv u l-aġġornamenti rilevanti kollha jkunu applikati abbażi ta' proċess dokumentat. Ir-riskji li jirriżultaw minn assi tal-ICT skaduti jew mhux appoġġati għandhom jiġu vvalutati u mmitigati. L-assi tal-ICT dekummissjonati għandhom jiġu pproċessati u mormija b'mod sikur.

46. L-impriżi għandhom jimplimentaw proċessi tal-ippjanar u ta' monitoraġġ tal-prestazzjoni u tal-kapaċità biex fi żmien adegwat jipprevjenu, jidentifikaw u jirrispondu għal kwistjonijiet importanti ta' prestazzjoni tas-sistemi tal-ICT u tan-nuqqasijiet fil-kapaċità tal-ICT.

47. L-impriżi għandhom jiddefinixxu u jimplimentaw proċeduri ta' backup u ta' rkupru tas-sistemi tad-*data* u tal-ICT biex jiżguraw li dawn ikunu jistgħu jiġu rkuprati kif meħtieġ. Il-kamp ta' applikazzjoni u l-frekwenza tal-backups għandhom jiġu stabbiliti skont ir-rekwiżiti ta' rkupru tan-negozju u l-kritikalità tas-sistemi tad-*data* u tal-ICT, li jiġu evalwati skont il-valutazzjoni tar-riskju mwettqa. L-ittestjar tal-proċeduri ta' backup u ta' rkupru għandu jitwettaq fuq bażi regolari.

48. L-impriżi għandhom jiżguraw li l-backups tas-sistemi tad-*data* u tal-ICT jinħażnu f'post wieħed jew aktar barra mis-sit primarju, li jkunu sikuri u mbiegħda biżżejjed mis-sit primarju sabiex jiġi evitat li jkunu esposti għall-istess riskji.

Linja gwida 15 - Il-ġestjoni ta' inċidenti u problemi tal-ICT

49. L-impriżi għandhom jistabbilixxu u jimplimentaw proċess ta' ġestjoni ta' inċidenti u problemi biex jimmonitorjaw u jirreġistraw inċidenti operazzjonali u ta' sigurtà u biex jippermettu lill-impriżi jkomplu jew jerġgħu jibdew il-funzjonijiet u l-proċessi tan-negozju kritiċi meta jkun hemm tfixkil.

50. L-impriżi għandhom jiddeterminaw il-kriterji u l-limiti xierqa għall-klassifikazzjoni ta' avveniment bħala inċident operazzjonali jew ta' sigurtà, kif ukoll indikaturi ta'

twissija bikrija li għandhom iservu ta' twissija għad-detezzjoni bikrija ta' dawn l-inċidenti.

51. Sabiex jiġi minimizzat l-impatt tal-avvenimenti avversi u jkun jista' jsir irkupru f'waqtu, l-impriżi għandhom jistabbilixxu proċessi u strutturi organizzazzjonali xierqa biex jiżguraw monitoraġġ, indirizzar u segwitu konsistenti u integrati ta' inċidenti operazzjonali u ta' sigurtà sabiex jiżguraw li l-kawżi ewlenin jiġu identifikati, trattati, u jittieħdu azzjonijiet/miżuri korrettivi biex tiġi evitata l-okkorrenza ripetuta tal-inċident. Il-proċess ta' ġestjoni ta' inċidenti u ta' problemi għandu, tal-anqas, jistabbilixxi:

    a) il-proċeduri biex jiġu identifikati, ittraċċati, irreġistrati, ikkategorizzati u kklassifikati inċidenti skont prijorità definita mill-impriża u bbażata fuq il-kritikalità tan-negozju u l-ftehimiet tas-servizzi;

    b) ir-rwoli u r-responsabbiltajiet għal xenarji ta' inċidenti differenti (eż. l-iżbalji, il-funzjonament ħażin, l-attakki ċibernetiċi);

    c) proċedura ta' ġestjoni ta' problemi biex tiġi identifikata, analizzata u solvuta l-kawża ewlenija wara inċident wieħed jew aktar; impriża għandha tanalizza inċidenti operazzjonali jew ta' sigurtà li jkunu ġew identifikati jew li seħħew fi u/jew barra l-organizzazzjoni, u għandha tqis it-tagħlimiet ewlenin meħuda minn dawn l-analiżijiet u taġġorna l-miżuri ta' sigurtà kif xieraq;

    d) pjanijiet ta' komunikazzjoni interna effettivi, inklużi proċeduri ta' notifiki u ta' eskalazzjoni ta' inċidenti — li jkopru wkoll ilmenti ta' klijenti relatati mas-sigurtà — biex jiġi żgurat li:

        i. inċidenti b'impatt potenzjalment qawwi fuq sistemi tal-ICT u servizzi tal-ICT kritiċi jiġu rrapportati lill-maniġment superjuri rilevanti;

        ii. l-AMSB jiġi infurmat fuq bażi ad hoc f'każ ta' inċidenti sinifikanti u, tal-anqas, infurmat dwar l-impatt, ir-reazzjoni u l-kontrolli addizzjonali li għandhom jiġu definiti bħala riżultat tal-inċidenti.

    e) il-proċeduri ta' reazzjoni għall-inċidenti biex jitnaqqas l-impatt relatat mal-inċidenti u biex jiġi żgurat li s-servizz isir operazzjonali u sikur fi żmien adegwat;

    f) pjanijiet ta' komunikazzjoni esterna speċifiċi għal funzjonijiet u proċessi tan-negozju kritiċi sabiex:

        i. jikkollaboraw mal-partijiet ikkonċernati rilevanti biex jirrispondu b'mod effettiv għall-inċident u jirkupraw minnu;

        ii. jipprovdu informazzjoni f'waqtha, li tinkludi r-rappurtar tal-inċidenti, lil partijiet esterni (eż. il-klijenti, parteċipanti oħra fis-suq, l-awtoritajiet (superviżorji) rilevanti, kif xieraq u f'konformità mar-regolament applikabbli).

Linja gwida 16 - Il-ġestjoni tal-proġett tal-ICT

52. L-impriżi għandhom jimplimentaw metodoloġija ta' proġett tal-ICT (inklużi l-konsiderazzjonijiet tar-rekwiżiti ta' sigurtà indipendenti) bi proċess ta' governanza adegwat u tmexxija fl-implimentazzjoni ta' proġett biex b'mod effettiv tiġi appoġġata l-implimentazzjoni tal-istrateġija tal-ICT permezz ta' proġetti tal-ICT.

53. L-impriżi għandhom b'mod xieraq jimmonitorjaw u jimmitigaw ir-riskji li jirriżultaw mill-portafoll tal-proġetti tal-ICT, filwaqt li jikkunsidraw ukoll ir-riskji li jistgħu

jirriżultaw minn interdipendenzi bejn proġetti differenti u minn dipendenzi ta' proġetti multipli fuq l-istess riżorsi u/jew kompetenza esperta.

Linja gwida 17 - L-akkwist u l-iżvilupp ta' sistemi tal-ICT

54. L-impriżi għandhom jiżviluppaw u jimplimentaw proċess li jirregola l-akkwist, l-iżvilupp u l-manutenzjoni ta' sistemi tal-ICT sabiex jiżguraw li l-kunfidenzjalità, l-integrità, id-disponibbiltà tad-*data* li jkollha tiġi pproċessata jkunu sikuri b'mod komprensiv u jiġu ssodisfati r-rekwiżiti ta' protezzjoni definiti. Dan il-proċess għandu jitfassal billi jintuża approċċ ibbażat fuq ir-riskju.

55. L-impriżi għandhom jiżguraw li qabel ma jsiru l-akkwisti ta' sistemi jew l-attivitajiet ta' żvilupp, jiġu definiti b'mod ċar ir-rekwiżiti funzjonali u mhux funzjonali (inklużi r-rekwiżiti tas-sigurtà tal-informazzjoni), u l-objettivi tekniċi.

56. L-impriżi għandhom jiżguraw li jkun hemm fis-seħħ il-miżuri għall-prevenzjoni ta' alterazzjoni mhux intenzjonata jew ta' manipulazzjoni intenzjonata tas-sistemi tal-ICT matul l-iżvilupp.

57. L-impriżi għandu jkollhom metodoloġija stabbilita għall-ittestjar u l-approvazzjoni tas-sistemi tal-ICT, tas-servizzi tal-ICT u tal-miżuri ta' sigurtà tal-informazzjoni.

58. L-impriżi għandhom b'mod xieraq jittestjaw is-sistemi tal-ICT, is-servizzi tal-ICT u l-miżuri ta' sigurtà tal-informazzjoni biex jidentifikaw dgħufijiet, ksur u inċidenti relatati mas-sigurtà potenzjali.

59. L-impriżi għandhom jiżguraw is-segregazzjoni tal-ambjenti ta' produzzjoni minn ambjenti ta' żvilupp, ittestjar u oħrajn li ma jkunux ta' produzzjoni.

60. L-impriżi għandhom jimplimentaw miżuri biex jipproteġu l-integrità tal-kodiċi tas-sors (fejn disponibbli) tas-sistemi tal-ICT. Dawn għandhom jiddokumentaw ukoll l-iżvilupp, l-implimentazzjoni, l-operat, u/jew il-konfigurazzjoni tas-sistemi tal-ICT b'mod komprensiv biex titnaqqas kwalunkwe dipendenza mhux meħtieġa fuq l-esperti fis-suġġett.

61. Il-proċessi tal-impriżi għall-akkwist u l-iżvilupp ta' sistemi tal-ICT għandhom japplikaw ukoll għal sistemi tal-ICT żviluppati jew ġestiti minn utenti finali tal-funzjoni tan-negozju barra mill-organizzazzjoni tal-ICT (eż. l-applikazzjonijiet ġestiti min-negozju jew l-applikazzjonijiet tal-informatika tal-utent finali) permezz ta' approċċ ibbażat fuq ir-riskju. L-impriżi għandhom iżommu reġistru ta' dawn l-applikazzjonijiet li jappoġġaw il-funzjonijiet jew il-proċessi tan-negozju kritiċi.

Linja gwida 18 - Il-ġestjoni tat-tibdil fl-ICT

62. L-impriżi għandhom jistabbilixxu u jimplimentaw proċess ta' ġestjoni tat-tibdil fl-ICT biex jiżguraw li l-bidliet kollha fis-sistemi tal-ICT jiġu rreġistrati, ivvalutati, ittestjati, approvati, awtorizzati u implimentati b'mod ikkontrollat. Tibdil waqt bidliet urġenti jew ta' emerġenza fl-ICT għandu jkun traċċabbli u nnotifikat ex-post lis-sid tal-assi rilevanti għal analiżi ex-post.

63. L-impriżi għandhom jiddeterminaw jekk il-bidliet fl-ambjent operazzjonali eżistenti jħallux impatt fuq il-miżuri ta' sigurtà eżistenti jew jirrikjedux l-adozzjoni ta' miżuri addizzjonali għall-mitigazzjoni tar-riskji involuti. Dawn il-bidliet għandhom ikunu skont il-proċess tal-ġestjoni tat-tibdil formali tal-impriżi.

Linja gwida 19 – Il-ġestjoni tal-kontinwità tan-negozju

64. Bħala parti mill-politika ġenerali tal-kontinwità tan-negozju tal-impriżi, l-AMSB għandu r-responsabbiltà li jistabbilixxi u japprova l-politika tal-kontinwità tal-ICT

tal-impriżi. Il-politika tal-kontinwità tal-ICT għandha tiġi kkomunikata b'mod xieraq fi ħdan l-impriżi u għandha tapplika għall-persunal rilevanti kollu u, fejn rilevanti, għall-fornituri tas-servizzi.

Linja gwida 20 – L-analiżi tal-impatt fuq in-negozju

65. Bħala parti mill-ġestjoni soda tal-kontinwità tan-negozju, l-impriżi għandhom iwettqu analiżi tal-impatt fuq in-negozju biex jivvalutaw l-esponiment tal-impriżi għal tfixkil kbir fin-negozju u l-impatt potenzjali tiegħu, kemm b'mod kwantitattiv kif ukoll b'mod kwalitattiv, bl-użu ta' *data* interna u/jew esterna u bl-analiżi tax-xenarji. L-analiżi tal-impatt fuq in-negozju għandha tikkunsidra wkoll il-kritikalità tal-proċessi u l-attivitajiet tan-negozju identifikati u kklassifikati, il-funzjonijiet tan-negozju, ir-rwoli u l-assi (eż. l-assi tal-informazzjoni u l-assi tal-ICT), u l-interdipendenzi tagħhom f'konformità mal-Linja gwida 4.

66. L-impriżi għandhom jiżguraw li s-sistemi tal-ICT u s-servizzi tal-ICT tagħhom ikunu mfassla u allinjati mal-analiżi tal-impatt fuq in-negozju tagħhom, pereżempju billi jitwarrbu ċerti komponenti kritiċi biex jiġi evitat it-tfixkil ikkawżat minn avvenimenti li jkollhom impatt fuq dawk il-komponenti.

Linja gwida 21 – L-ippjanar tal-kontinwità tan-negozju

67. Il-Pjanijiet ġenerali tal-Kontinwità tan-Negozju (BCPs) tal-impriżi għandhom jikkunsidraw ir-riskji materjali li jistgħu jaffettwaw b'mod ħażin is-sistemi tal-ICT u s-servizzi tal-ICT. Il-pjanijiet għandhom jappoġġjaw objettivi biex jipproteġu u, jekk meħtieġ, jerġgħu jistabbilixxu l-kunfidenzjalità, l-integrità u d-disponibbiltà tal-proċessi u l-attivitajiet tan-negozju tal-impriżi, il-funzjonijiet tan-negozju, ir-rwoli u l-assi (eż. l-assi tal-informazzjoni u l-assi tal-ICT). L-impriżi għandhom jikkoordinaw ma' partijiet ikkonċernati interni u esterni rilevanti, kif xieraq, matul l-istabbiliment ta' dawn il-pjanijiet.

68. L-impriżi għandhom idaħħlu fis-seħħ il-BCPs biex jiżguraw li jkunu jistgħu jirreaġixxu b'mod xieraq għal xenarji ta' falliment potenzjali fi ħdan Objettiv ta' Żmien ta' Rkupru (il-ħin massimu li fih sistema jew proċess iridu jiġu rkuprati wara inċident) u Objettiv ta' Punt ta' Rkupru (il-perjodu ta' żmien massimu li matulu d-*data* tista' tintilef f'każ ta' inċident f'livell ta' servizz predefinit).

69. L-impriżi għandhom jikkunsidraw firxa ta' xenarji differenti fil-BCPs tagħhom, inklużi xenarji estremi iżda plawżibbli u xenarji ta' attakki ċibernetiċi, u jivvalutaw l-impatt potenzjali ta' tali xenarji. Abbażi ta' dawn ix-xenarji, l-impriżi għandhom jiddeskrivu kif jiġu żgurati kemm il-kontinwità tas-sistemi u s-servizzi tal-ICT, kif ukoll is-sigurtà tal-informazzjoni tal-impriżi.

Linja gwida 22 – Pjanijiet ta' reazzjoni u ta' rkupru

70. Abbażi tal-analiżi tal-impatt fuq in-negozju u ta' xenarji plawżibbli l-impriżi għandhom jiżviluppaw pjanijiet ta' reazzjoni u ta' rkupru. Dawn il-pjanijiet għandhom jispeċifikaw il-kundizzjonijiet li jistgħu jeħtieġu l-attivazzjoni tal-pjan u tal-azzjonijiet li għandhom jittieħdu biex jiżguraw l-integrità, id-disponibbiltà, il-kontinwità u l-irkupru ta', mill-anqas, is-sistemi tal-ICT u s-servizzi tal-ICT kritiċi u d-*data* tal-impriżi. Il-pjanijiet ta' reazzjoni u ta' rkupru għandu jkollhom l-għan li jilħqu l-objettivi ta' rkupru tal-operazzjonijiet tal-impriżi.

71. Il-pjanijiet ta' reazzjoni u ta' rkupru għandhom iqisu l-għażliet ta' rkupru kemm fuq terminu qasir kif ukoll fuq terminu twil. Il-pjanijiet għandhom, tal-anqas:

a) jiffokaw fuq l-irkupru tal-operazzjonijiet tas-servizzi tal-ICT importanti, il-funzjonijiet tan-negozju, il-proċessi ta' appoġġ, l-assi tal-informazzjoni u l-interdipendenzi tagħhom biex jiġu evitati effetti negattivi fuq il-funzjonament tal-impriża;

b) ikunu ddokumentati u magħmula disponibbli għan-negozju u l-unitajiet ta' appoġġ u faċilment aċċessibbli f'każ ta' emerġenza, inkluża definizzjoni ċara tar-rwoli u r-responsabbiltajiet; u

c) jiġu kontinwament aġġornati f'konformità mat-tagħlimiet meħuda mill-inċidenti, it-testijiet, ir-riskji ġodda identifikati u t-theddid, u l-objettivi u l-prijoritajiet ta' rkupru mibdula.

72. Il-pjanijiet għandhom jikkunsidraw ukoll għażliet alternattivi fejn l-irkupru jista' ma jkunx prattiku fi żmien qasir minħabba l-ispejjeż, ir-riskji, il-loġistika jew ċirkostanzi mhux previsti.

73. Bħala parti mill-pjanijiet ta' reazzjoni u ta' rkupru, l-impriżi għandhom jikkunsidraw u jimplimentaw miżuri ta' kontinwità biex itaffu l-falliment tal-forniturі tas-servizzi, li huma ta' importanza ewlenija għall-kontinwità tas-servizz tal-ICT tal-impriżi (f'konformità mad-dispożizzjonijiet tal-Linji gwida tal-EIOPA dwar sistema ta' governanza u Linji gwida dwar l-esternalizzazzjoni lill-forniturі tas-servizzi tal-cloud).

Linja gwida 23 – L-ittestjar tal-pjanijiet

74. L-impriżi għandhom jittestjaw il-BCPs tagħhom, u jiżguraw li l-operazzjoni tal-proċessi u l-attivitajiet kritiċi tan-negozju tagħhom, il-funzjonijiet tan-negozju, ir-rwoli u l-assi (eż. l-assi tal-informazzjoni) u l-assi tal-ICT u l-interdipendenzi tagħhom (inklużi dawk ipprovduti mill-forniturі tas-servizzi) jiġu regolarment ittestjati abbażi tal-profil tar-riskju tal-impriżi.

75. Il-BCPs għandhom jiġu regolarment aġġornati, abbażi tar-riżultati tal-ittestjar, l-intelliġenza attwali dwar it-theddid u t-tagħlimiet meħuda mill-avvenimenti preċedenti. Kwalunkwe bidla rilevanti fl-objettivi ta' rkupru (inklużi l-Objettiv ta' Żmien ta' Rkupru u l-Objettiv ta' Punt ta' Rkupru) u/jew bidliet fil-proċessi u l-attivitajiet tan-negozju, il-funzjonijiet tan-negozju, ir-rwoli u l-assi (eż. l-assi tal-informazzjoni u l-assi tal-ICT) ukoll għandha tiġi inkluża.

76. L-ittestjar tal-BCP għandu juri li huma kapaċi jsostnu l-vijabbiltà tan-negozju sakemm jerġgħu jiġu stabbiliti l-operazzjonijiet kritiċi f'livell ta' servizz predefinit jew ta' tolleranza għall-impatt.

77. Ir-riżultati tat-test għandhom jiġu ddokumentati u kwalunkwe nuqqas identifikat li jirriżulta mit-testijiet għandu jiġi analizzat, indirizzat u rrappurtat lill-AMSB.

Linja gwida 24 - Il-komunikazzjoni f'sitwazzjoni ta' kriżi

78. F'każ ta' tfixkil jew emerġenza, u matul l-implimentazzjoni tal-BCPs, l-impriżi għandhom jiżguraw li jkollhom fis-seħħ miżuri effettivi ta' komunikazzjoni f'sitwazzjoni ta' kriżi sabiex il-partijiet ikkonċernati interni u esterni rilevanti kollha, inklużi l-awtoritajiet superviżorji rilevanti, meta jkun meħtieġ mir-regolamentazzjoni nazzjonali, kif ukoll il-forniturі tas-servizzi rilevanti, jiġu infurmati fil-ħin u b'mod xieraq.

Linja gwida 25 – L-esternalizzazzjoni ta' servizzi tal-ICT u ta' sistemi tal-ICT

79. Mingħajr preġudizzju għal-Linji gwida tal-EIOPA dwar l-esternalizzazzjoni lill-fornituri tas-servizzi tal-cloud, l-impriżi għandhom jiżguraw li fejn is-servizzi tal-ICT u s-sistemi tal-ICT jiġu esternalizzati, jiġu ssodisfati r-rekwiżiti rilevanti għas-servizz tal-ICT jew għas-sistema tal-ICT.

80. Fil-każ ta' esternalizzazzjoni ta' funzjonijiet kritiċi jew importanti, l-impriżi għandhom jiżguraw li l-obbligi kuntrattwali tal-fornitur tas-servizz (eż. kuntratt, ftehimiet ta' livell ta' servizz, dispożizzjonijiet ta' terminazzjoni fil-kuntratti rilevanti) jinkludu, tal-anqas, dan li ġej:

    a) objettivi u miżuri ta' sigurtà ta' informazzjoni xierqa u proporzjonati li jinkludu rekwiżiti bħal rekwiżiti minimi ta' sigurtà tal-informazzjoni, speċifikazzjonijiet taċ-ċiklu tal-ħajja tad-*data* tal-impriżi, drittijiet ta' verifika u ta' aċċess u kwalunkwe rekwiżit rigward il-post taċ-ċentri tad-*data* u rekwiżiti ta' kriptaġġ tad-*data*, sigurtà tan-netwerks u proċessi ta' monitoraġġ tas-sigurtà;

    b) ftehimiet fil-livell ta' servizz, biex tiġi żgurata l-kontinwità tas-servizzi tal-ICT u s-sistemi tal-ICT u miri ta' prestazzjoni f'ċirkostanzi normali kif ukoll dawk ipprovduti minn pjanijiet ta' kontinġenza f'każ ta' interruzzjoni tas-servizz; u

    c) proċeduri ta' ġestjoni ta' inċidenti operazzjonali u ta' sigurtà, inklużi eskalazzjoni u rapportar.

81. L-impriżi għandhom jimmonitorjaw u jfittxu l-assigurazzjoni dwar il-livell ta' konformità ta' dawn il-fornituri tas-servizzi mal-objettivi, il-miżuri u l-miri ta' prestazzjoni tas-sigurtà.

Regoli dwar il-konformità u r-rapportar

82. Dan id-dokument fih Linji Gwida maħruġa skont l-Artikolu 16 tar-Regolament (UE) Nru 1094/2010. Skont l-Artikolu 16(3) ta' dan ir-Regolament, l-awtoritajiet kompetenti u l-impriżi huma meħtieġa jagħmlu kull sforz sabiex jikkonformaw mal-linji gwida u mar-rakkomandazzjonijiet.

83. L-awtoritajiet kompetenti li jikkonformaw jew li għandhom il-ħsieb li jikkonformaw ma' dawn il-Linji gwida għandhom jinkorporawhom fil-qafas regolatorju jew superviżorju tagħhom b'mod xieraq.

84. L-awtoritajiet kompetenti jeħtieġ li jikkonfermaw lill-EIOPA jekk jikkonformawx jew għandhomx il-ħsieb li jikkonformaw ma' dawn il-Linji gwida, bir-raġunijiet għan-nuqqas ta' konformità, fi żmien xahrejn mill-ħruġ tal-verżjonijiet tradotti.

85. Fin-nuqqas ta' tweġiba sa din l-iskadenza, l-awtoritajiet kompetenti jitqiesu bħala mhux konformi mar-rapportar u jiġu rrapportati bħala tali.

Dispożizzjoni finali dwar ir-rieżami

86. Il-Linji gwida preżenti jiġu soġġetti għal rieżami mill-EIOPA.