POLITIKA BEZBEDNOSTI INFORMACIJA

Politika bezbednosti informacija utvrđuje opšte principe na kojima su zasnovani i propisani organizacioni zahtevi koji su neophodni da bi se obezbedila i, tokom vremena, sačuvala bezbednost informacija.

Predgovor

Pod "bezbednošću informacija" se podrazumevaju uslovi u kojima je neka organizacija u stanju da ostvaruje i, tokom vremena, sačuva odgovarajući nivo poverljivosti, integriteta i raspoloživosti informacija u skladu sa zahtevima koje propisuju:

a) Važeći zakonski propisi (naročito propisi o zaštiti privatnosti i intelektualne svojine);

b) Eventualni dodatni zahtevi koje samostalno utvrdi preduzeće Palladio Group.

"Poverljivost" označava svojstvo informacije da ne bude dostupna neovlašćenim subjektima; "integritet" informcije označava njeno svojstvo da ne može biti menjana ili izbrisana, osim od strane subjekata koji su za to ovlašćeni; "raspoloživost" je svojstvo informacije da, na zahtev ovlašćenog subjekta, bude dostupna u previđenom vremenu.

Opšte informacije

Palladio Group ima potrebu da, u okviru svojih poslovnih aktivnosti, pristupa i na različite načine obrađuje informacije koje se mogu odnositi na: projekte Klijenata, lične podatke o zaposlenima i saradnicima, administrativne i računovodstvene podatke proizvedene i čuvane u cilju ispunjavanja zakonskih obaveza.

U vezi sa tim, Direkcija preduzeća Palladio Group smatra da usvajanje organizacionog modela zasnovanog na bezbednosti informacija predstavlja neophodnu strateško odluku koja će Organizaciji omogućiti da:

a) proizvodi, koristi i na pravilan način čuva informacije koje su joj neophodne za ispunjavanje zakonskih i ugovornih obaveza;

b) na efikasan način koristi raspoložive resurse, uz odgovarajuću klasifikaciju kritičnosti informacija;

c) gradi i vremenom čuva poverenje "stakeholder"-a Palladio Group u pogedu pouzdanosti da će to preduzeće sačuvati informacije koje kreira i koristi.

PRINCIPI

Bezbednost informacija je strateška odluka

Svest o značaju pravilnog kreiranja, korišćenja i čuvanja informacija treba da postane deo svakodnevnih aktivnosti na svim nivoima. Ideal kome treba težiti je da svi procesi donošenja odluka i svi izvršni procesi u preduzeću Palladio Group koji podrazumevaju kreiranje, pristup i obradu informacija, budu strukturirani tako da garantuju bezbednost informacija.

Bezbednost informacija se zasniva na sagledavanju rizika

Da bi se omogućila bezbednost informacija ne postoji "magični recept" niti "najbolja praksa" koja važi za sve situacije: način na koji Preduzeće postupa da bi sačuvalo bezbednost informacija je usko povezan sa pretnjama i mogućnostima kojima Organizacija pretpostavlja da bi mogla biti izložena. Pristup *razmišljanja na bazi rizika* (*risk-based thinking*) je instrument koji pomaže da se identifikuju različite pretnje i mogućnosti, kao i da im se pravilno odredi prioritet: taj instrument bi, stoga, trebalo da postane sastavni deo svakodnevnog rada svih subjekata kojima je povereno da učestvuju u procesima odlučivanja u okviru Palladio Group.

Bezbednost informacija počinje od poštovanja pravila

Da bi se garantovala bezbednost informacija, od presudnog značaja je posvećivanje posebne pažnje poznavanju i poštovanju primenljivih zakonskih propisa i ugovornih obaveza. Ako, po pravilu, odluke o bezbednosti informacija treba donositi u skladu sa pristupom "baziranom na riziku", odnosno na osnovu procene troškova i benefita, zakonske i ugovorne obaveze treba uvek smatrati "čistim rizikom", tj. isključivo kao izvor pretnji (vezanih za nepoštovanje zakonske regulative ili ugovornih odredbi) a nikako kao mogućnosti. Organizacija se, stoga, mora angažovati na svim nivoima kako bi identifikovala, razumela i poštovala zakonske i ugovorne obaveze o bezbednosti informacija.

Posebno je potrebno da, na svim nivoima Organizacije, postoji svest o tome da je organizacioni model koji Palladio Group primenjuje za bezbednost informacija definisan i implementiran u skladu sa standardom UNI CEI ISO/IEC 27001:2014. Stoga je neophodno da razni organizacioni nivoi budu upoznati sa zahtevima koje propisuje taj standard, kao i sa značajem poštovanja tih zahteva.

Bezbednost informacija zahteva rad na ostvarivanju ciljeva

Da bi se moglo imati poverenja da će bezbednost informacija biti ostvarena i sačuvana u vremenu, treba utvrditi plan koji podrazumeva postavljanje odgovarajućih ciljeva na raznim organizacionim nivoima.

Ako je definisanje specifičnih sadržaja tih ciljeva prepušteno različitim nivoima Uprave, po pravilu je neophodno da ti ciljevi budu:

a) Izraženi merljivim vrednostima, u meri u kojoj je to izvodljivo;
b) Kompatibilni sa, i primereni resursima kojima raspolaže Organizacija;
c) Dopunjeni odgovarajućim vremenskim rokovima, bez kojih se cilj ne može smatrati pravim;
d) Periodično kontrolisani.

Bezbednost informacija podraumeva kontinuirano poboljšanje

Kontekst u kojem posluje Organizacija (tržište, društvo, potrebe i očekivanja klijenata...) se stalno menja. U takvim uslovima nemoguće je da bilo koja organizacija uspe da preživi ako periodično ne preispituje svoje vrednosti i svoju praksu, kako bi se uverila da su i dalje adekvatni za suočavanje sa promenama koje se neizbežno dešavaju.

Generalni Direktor

Dr. Mauro Marchi