COIG

DATA CENTER

Oferta Audytu Bezpieczeństwa Systemów Informatycznych

Zastosowanie ochrony informacji w organizacjach

Informacje o usłudze

made by COIG SA

Dlaczego audyt jest tak ważny?

W celu ochrony informacji zabezpieczenia zastosowane w organizacji muszą podlegac ciągłej analizie, w związku z potencjanym zagrożeniem, które może zagrozić:

01

Wyciekiem danych

02

Utratą lub modyfikacją

03

Przejęciem kontroli nad infrastrukturą

04

Wykorzystywaniem systemu oraz sieci w nieodpowiedni sposób np. do celów przestępczych

971

Ataktów na godzinę

w Polsce według szacunków przy użyciu złośliwego oprogramowania

DATA CENTER

Audyt polega na kontrolowaniu poziomu bezpieczeństwa IT

Polega na sprawdzeniu integralności, poufności oraz dostępności systemów informatycznych, kontroli ich awaryjności, weryfikacji wiarygodności przetwarzanych danych jak również na spełnianiu wymogów standardów bezpieczeństwa

Audyt obejmuje obszary organizacyjne oraz techniczne. W przeprowadzanym u klienta audycie stosujemy się do wytycznych określonych w Audit Guideline Międzynarodowego Stowarzyszenia Audytorów Systemów Informatycznych ISACA.

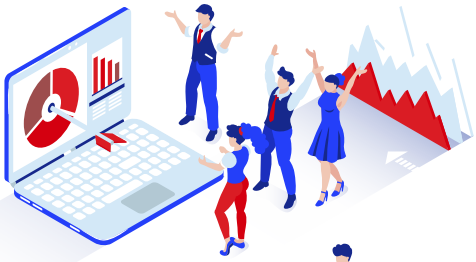
W zakresie organizacyjnym audyt obejmuje:

Procedury, politykę wewnętrzną organizacji oraz stosowanie się do zapisów zawartych w dokumentacji jak i w przepisach prawa.

Zakres działań audytu:

- przegląd polityki bezpieczeństwa firmy;
- analiza procedur bezpieczeństwa oraz ich zastosowanie w praktyce;
- weryfikacja poprawnego stosowania przepisów ochrony danych osobowych zgodnych z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO);
- weryfikacjęa zgodności z ustawą o krajowym systemie cyberbezpieczeństwa (dla podmiotów które jej podlegają;
- zarządzanie kopiami zapasowymi;
- administrowanie kontami i hasłami dostępowymi;
- zarządzanie rejestracją błędów.

DATA CENTER



Zabezpieczenia

W zakresie technicznym audyt **obejmuje techniczne zabezpieczenia wdrożone w organizacji:**

- techniczne zabezpieczenia komputerów oraz stacji roboczych;
- techniczne zabezpieczenia poczty elektronicznej;
- techniczne zabezpieczenia ochrony antywirusowej, antyspamowej;
- kontrolę mechanizmów logowania;
- kontrolę weryfikacji i konfiguracji oprogramowania.

COIG

10 kroków

do skutecznego audytu

Zmniejsz ryzyko wycieku danych

1. ocena dokumentacji dotyczącej systemu zarządzania bezpieczeństwem informacji pod kątem spełnienia wymogów normy PN-EN ISO/IEC 27001;
2. ocena poprawności wdrożonych procedur oraz przepisów ochrony danych osobowych zgodnych z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO),
3. ocena zgodności z ustawą o krajowym systemie cyberbezpieczeństwa
4. analiza podatności systemów teleinformatycznych;
5. przegląd oraz analiza słabych punktów systemów teleinformatycznych;
6. kontrola struktury sieci oraz wewnętrznych i zewnętrznych kanałów komunikacyjnych firmy ;
7. kontrola środowiska Wi-Fi;
8. kontrola bezpieczeństwa fizycznego obiektów;
9. ocena stanu technicznego infrastruktury;
10. stworzenie raportu zawierającego stwierdzone nieprawidłowości oraz wskazówki w zakresie rozwiązań zwiększających bezpieczeństwo.

...i gotowe

DATA
CENTER

Grzegorz Łunkiewicz

OPIEKUN PRODUKTU

grzegorz.lunkiewicz@coig.pl
32 757 44 44

COIG SA

Mikołowska 100
40-065 Katowice