inCentea

TECNOLOGIA DE GESTÃO

CERBERUS

Salvaguarda da Informação de Negócio

A REALIDADE EM QUE VIVEMOS É, CADA VEZ MAIS DIGITAL, COLOCANDO NOVOS DESAFIOS E ORIGINANDO NOVOS RISCOS NOS PROCESSOS DAS ORGANIZAÇÕES. Qualquer entidade que queira competir no mercado e vencer na era da informação digital precisa de garantir a Confidencialidade, Integridade, Disponibilidade e a Resiliência permanente dos seus ativos de informação, bem como, cumprir os requisitos legais e regulamentares afetos ao seu setor de atividade.

O aumento exponencial de vulnerabilidades e ameaças internas e externas expõe, diariamente, os sistemas de informação das organizações a riscos de violação e divulgação de informação sensível podendo originar efeitos adversos a nível financeiro, imagem e de competitividade perante as partes interessadas.

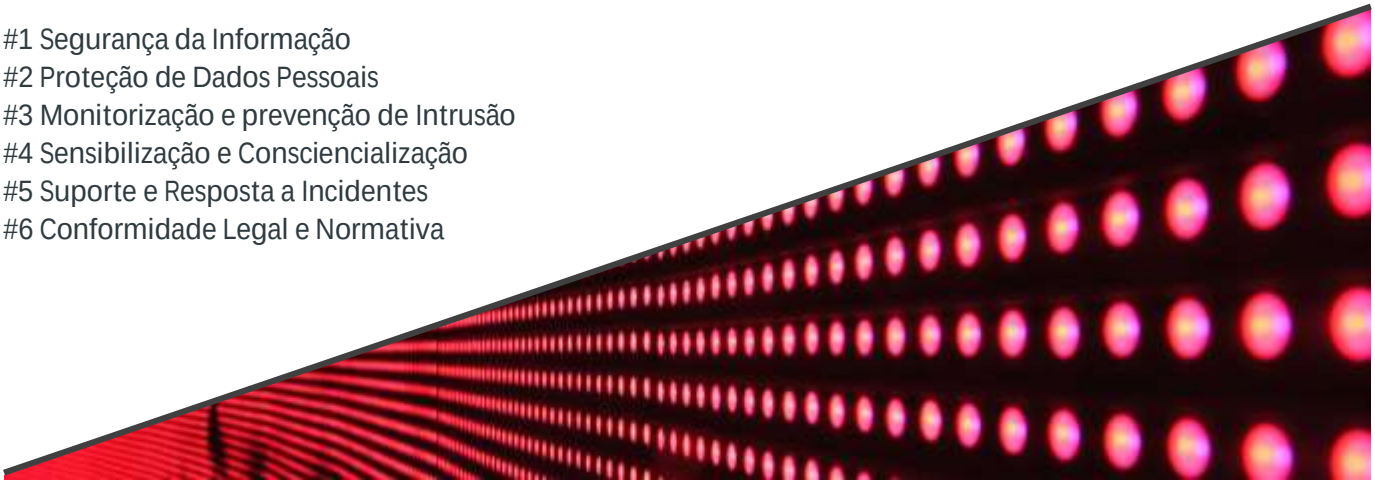
Todos os dias há organizações que veem os seus processos de negócio afetados a nível da divulgação de segredos comerciais, disrupção operacional (*ransomware*), coimas e ações legais, perda de confiança dos consumidores e investigação dos reguladores devido a ações de atores maliciosos externos e internos à própria Organização.

Só através de uma monitorização e correlação de vulnerabilidades e ameaças, de forma contínua aos ativos de informação da Organização, é possível promover uma defesa eficaz contra o cibercrime e outras ameaças de segurança, expondo os pontos fortes, pontos fracos, ameaças e oportunidades de melhoria que devem ser concretizadas, com o objetivo de tornar mais resiliente e robusta a infraestrutura que dá suporte a todas as direções do seu negócio e garantindo maior confiança às partes interessadas.

A solução **CERBERUS** é gerida por uma equipa multidisciplinar de consultores certificados em *Lead Auditor* ISO/IEC:27001, *Certified Information Privacy Technologist* (CIPT) e em outras certificações técnicas reconhecias internacionalmente; o prestador de serviço é certificado na norma ISO/IEC: 27001 (Segurança da Informação) e ISO/IEC: 20000 (Gestão de Serviços) desde 2012, entre outras normas.

SERVIÇOS PRESTADOS

#1 Segurança da Informação
#2 Proteção de Dados Pessoais
#3 Monitorização e prevenção de Intrusão
#4 Sensibilização e Consciencialização
#5 Suporte e Resposta a Incidentes
#6 Conformidade Legal e Normativa



inCentea

TECNOLOGIA DE GESTÃO

Segurança da Informação - Chief Information Security Officer

- Produção e manutenção da Política e do Plano de Segurança;
- Assegurar que a confidencialidade, integridade e disponibilidade dos recursos da infraestrutura de TI vão ao encontro dos níveis de serviço da Organização;
- Participar na resolução e avaliação dos incidentes de segurança.
- Ação de formação anual em cibersegurança e segurança da informação para todos os colaboradores com acesso a sistemas de informação;
- Responder às questões da Organização em matérias que envolvam a segurança da informação;
- Assegurar que os departamentos internos da Organização adotam e estão conformes as melhores práticas e standards de segurança da informação;
- Avaliar o impacto de segurança da informação na gestão de alterações;
- Assegurar que todos os controlos e procedimentos de segurança são regularmente revistos e auditados;
- Assessor da Organização para a segurança da informação;
- Assegurar o comprometimento de todas as partes interessadas da Organização em relação à Política de Segurançada informação;
- Participar nas reuniões do *Change Advisory Board* (CAB) quando necessário;
- Elaboração de relatório anual sobre o estado de conformidade da Organização perante o processo de Gestão de Segurança da Informação;

Proteção de Dados Pessoais - Data Protection Officer

- Realização de avaliações de impacto sobre a proteção de dados, quando um certo tipo de tratamento, - em particular - que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares;
- Resposta às questões do responsável pelo tratamento dos dados em matérias que envolvam a proteção dos dados pessoais das partes interessadas;
- Elo entre o responsável pelo tratamento e a autoridade de controlo;
- Assessor da Organização para a privacidade;
- Elaboração de relatório anual sobre o estado de conformidade da organização perante o REGULAMENTO (UE) 2016/679;
- Produção de documentação necessária obrigatória ao cumprimento do REGULAMENTO (UE) 2016/679 por parte do responsável pelo tratamento dos dados.

Monitorização e prevenção de intrusão - Cyber Security Analyst

- Execução de testes de vulnerabilidades sobre a infraestrutura da Organização.
- Vigilância das aplicações da organização face a vulnerabilidades e *malware*.
- Monitorização e correlação de vulnerabilidades e ameaças de forma contínua sobre os ativos de informação da Organização.
- Alertas e notificações sempre que o risco associado assim o justificar.
- Avaliação da exposição ao risco tendo por base normativos ou regulamentos de proteção de dados.
- Deteção de intrusões e de eventos de segurança na rede corporativa

Bónus

- Ação de formação anual em cibersegurança e proteção de dados pessoais para todos os colaboradores que tratem informação.
- Entrega de relatório presencial trimestral.
- Suporte remoto ilimitado em relação a questões de privacidade e segurança da informação.
- Estabelecer, implementar, manter e melhorar de forma contínua um sistema de gestão de segurança da informação de acordo com os requisitos da norma ISO/IEC 27001:2013 a equipa de Security Manager da inCentea prepara a sua Organização para que a possa certificar na norma de segurança da informação por excelência, adquirindo assim, reconhecimento, reputação e vantagem de negócio face à concorrência.