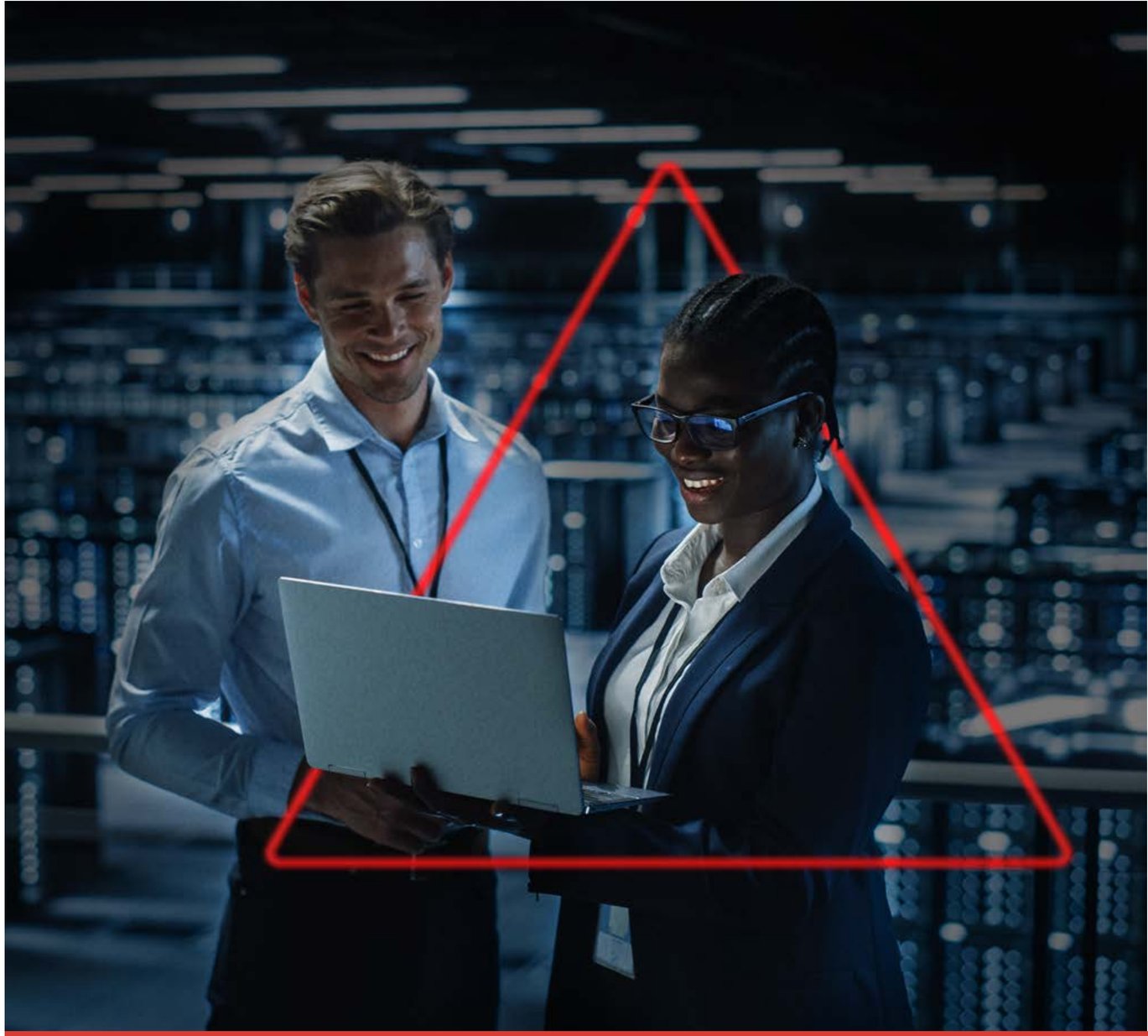
ALERTA
SECURITY

SERVIÇO DE GESTÃO DE RISCOS CIBERNÉTICOS - sGRC

Saiba como decidir qual solução de GRC é ideal para sua empresa



ALERTA
SECURITY

ÍNDICE

INTRODUÇÃO

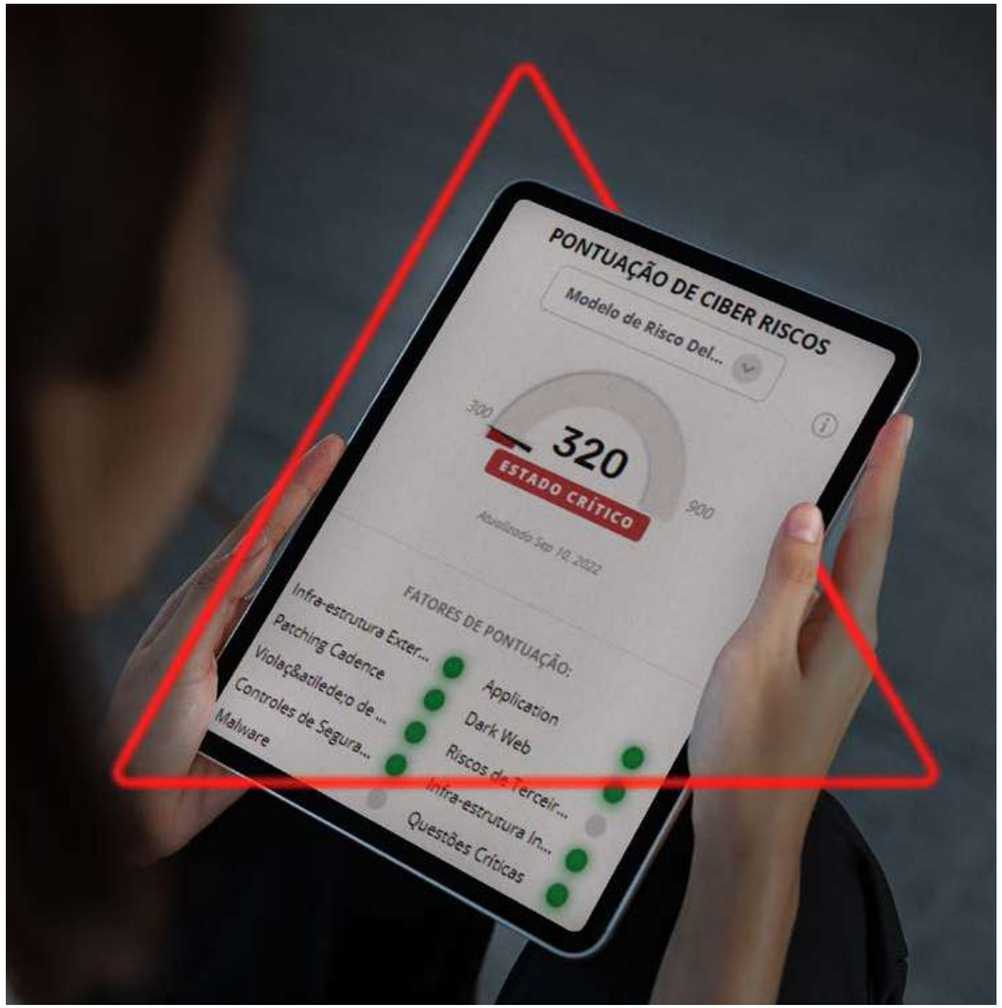
Organizações de todos os tamanhos precisam estar cientes de seu **risco cibernético**.

Uma grande organização precisa conhecer as vulnerabilidades, não apenas em seus próprios sistemas e processos de gerenciamento, mas também em toda a cadeia de fornecedores e terceiros.

À medida que as organizações crescem, aumenta também a necessidade de implementar **plataformas integradas de gerenciamento de riscos cibernéticos** que possam fazer um balanço adequado das vulnerabilidades ocultas.

Você é capaz de responder a todas estas perguntas:

- O software do endpoint está totalmente configurado e atualizado?
- O acesso de usuários aos sistemas requer dupla autenticação?
- As redes estão devidamente segmentadas e protegidas?
- Qual é o nível de acesso de terceiros às redes da empresa?
- Quais são as minhas maiores falhas na defesa cibernética?
- Estou atuando em conformidade com as normas ou frameworks de mercado?



VOLTAR AO ÍNDICE

Nosso gerenciamento de risco cibernético não é apenas uma catalogação de vulnerabilidades e outras fraquezas. Mas sim, uma cadeia de processos que também leva em conta a probabilidade de pontos fracos serem exploradose também quais seriam as consequências resultantes.

Esses riscos e seus custos precisam ser quantificados, como um valor que represente a expectativa de perda, o que é útil para estruturar discussões financeiras de segurança com a liderança e os membros do conselho.

No gerenciamento de riscos cibernéticos da **Alerta Security** são feitas diversas avaliações para identificar os mais importantes, elaborar planos para mitigá-los, além de monitorar e gerenciar outros riscos que não podem ser corrigidos imediatamente.

Nosso serviço integrado de **Gerenciamento de Riscos Cibernéticos** não apenas dará a sua organização uma **visão de seus próprios riscos**, mas também gerará uma **classificação de segurança** muito precisa.

Nós gerenciamos totalmente sua classificação de risco cibernético e os fatores que afetam seu perfil de risco usando a **Plataforma FortifyData**. Isso garante que sua classificação de risco seja precisa, livre de atribuições incorretas e falsos positivos, além de obter um plano de fortalecimento de defesa, mitigando todos os riscos detectados.

A abordagem abrangente do FortifyData vai além das metodologias tradicionais e oferece flexibilidade para gerenciar suas classificações de segurança com acesso total para classificar seus sistemas, ajustar a probabilidade e o impacto das ameaças.

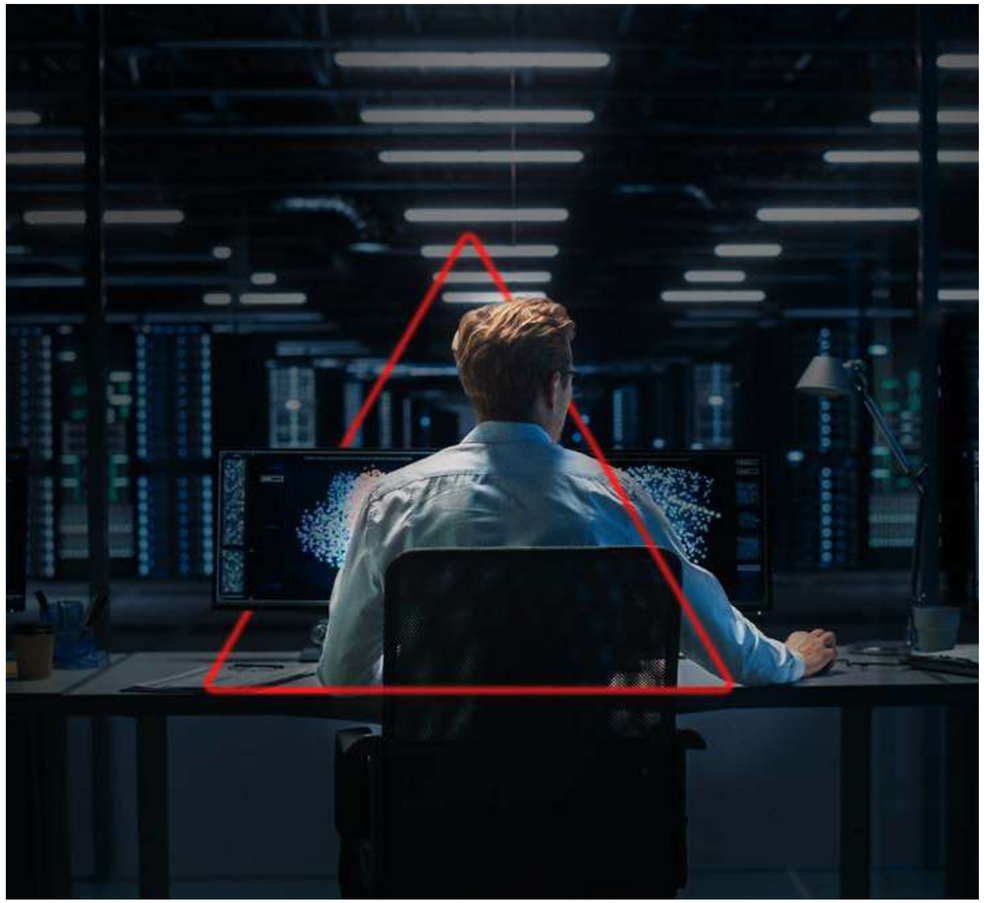
Isso permite que você apresente uma visão precisa de exposição ao risco cibernético para todos os interessados, como conselho diretivo e clientes.

VOLTAR AO ÍNDICE

O QUE É O SGRC DA ALERTA SECURITY?

O serviço de Gerenciamento de Riscos Cibernéticos da Alerta Security aponta os pontos de risco ou falhas e também fornece apoio constante no fortalecimento dos mecanismos de defesa cibernética.

O objetivo é obter proximidade com as principais normas do mercado de defesa cibernética.



VOLTAR AO ÍNDICE

MONITORAMENTO CONTÍNUO DE RISCOS

A Alerta Security fez uma parceria com a maior plataforma de gerenciamento de riscos cibernéticos, a FortifyData.

FortifyASM é o recurso de **gerenciamento de superfície de ataque.**

ASM é uma função crítica para que as organizações descubram e verifiquem continuamente ativos expostos à rede pública ou privada. A verificação é feita em ativos externos, redes internas, serviços em nuvem e na superfície de ataque externo de terceiros.

Essa inteligência identifica ativos conhecidos, desconhecidos e vulnerabilidades associadas a esses ativos. Nós efetuamos toda a classificação do risco por criticidade e tipo de dados sendo processados, transmitidos ou armazenados.

A plataforma FortifyData analisa e apresenta os ativos com base em uma visão priorizada para correção **com base na gravidade da vulnerabilidade.**

O FortifyASM é usado para **gerenciamento de riscos corporativos e gerenciamento de riscos de terceiros**. Compreender as vulnerabilidades da superfície de ataque externo dá às organizações a mesma inteligência de reconhecimento sobre vulnerabilidades exploráveis que os hackers podem ver.

COMITÊ DE SEGURANÇA

Nós, da Alerta Security, em conjunto com a sua organização, iremos estabelecer um **Comitê de Segurança** composto por diversas lideranças organizacionais, dentre elas:

- **Departamento Tecnologia;**
- **Departamento de Recursos Humanos;**
- **Departamento de Finanças;**
- **Demais departamentos operacionais.**

O Comitê de Segurança será responsável por passar informações relacionadas aos processos de negócio, participar de reuniões sobre gerenciamento de risco, analisar relatórios gerenciais de risco e apoiar em medidas mitigantes.

PRÉ-AUDITORIA EM NORMAS

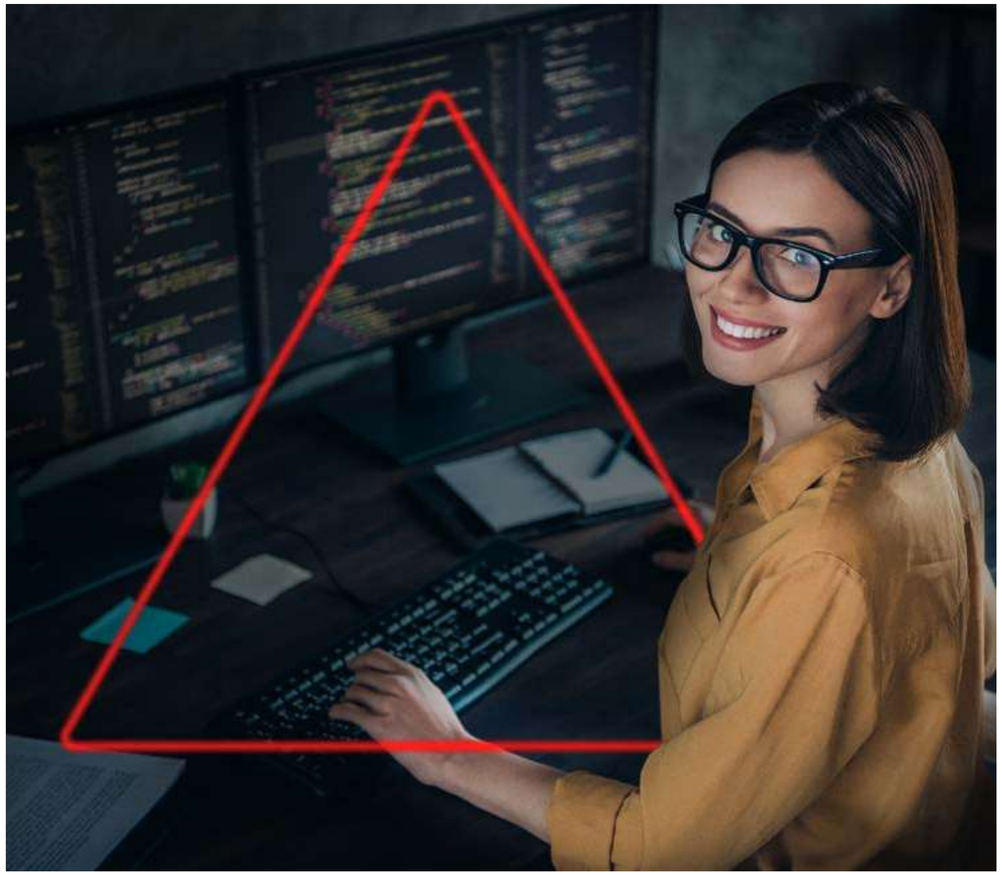
O primeiro passo é entender o quão distante a organização está das normas ou frameworks de mercado, que são um baseline importante nesse trabalho.

Dentre algumas normas que podemos gerenciar estão:

- **ISO 27001**
- **CIS Controls V8**
- **PCI**

- **ISO 27001**
- **CIS Controls V8**
- **PCI**

O levantamento é feito como uma auditoria, através de questionários completos e coletas de evidências. As respostas obtidas determinarão um nível de risco inicial com prioridades definidas.

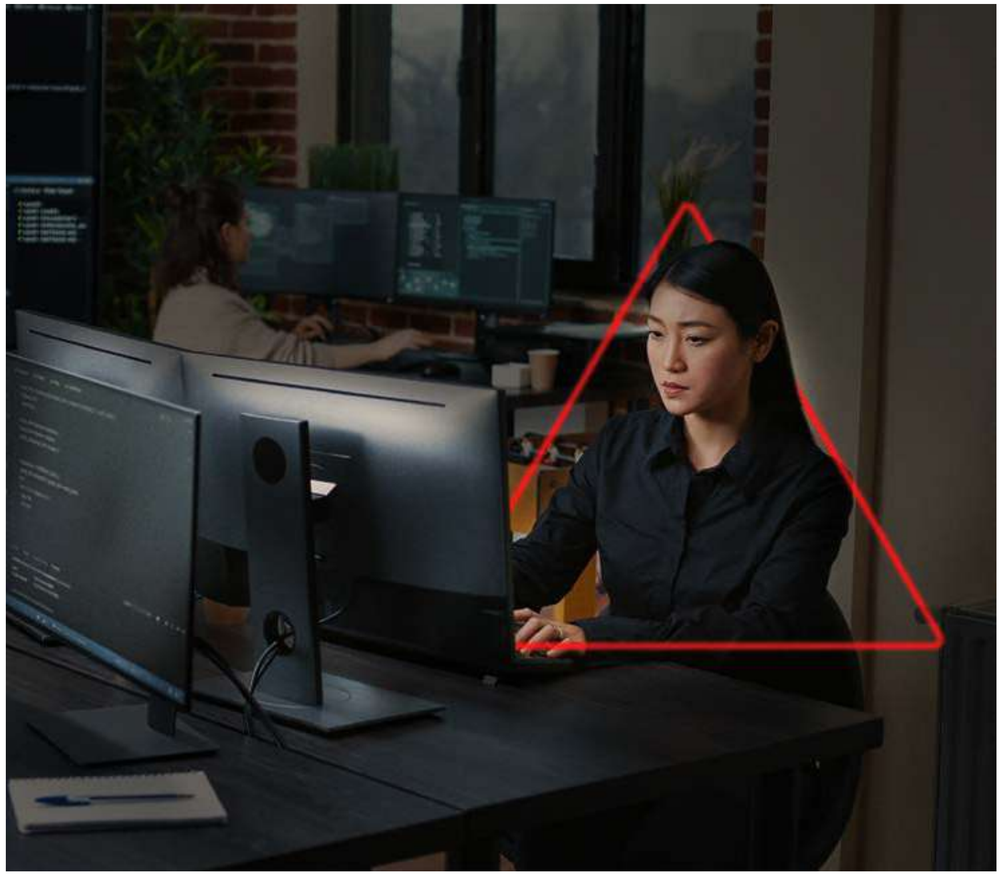


VOLTAR AO ÍNDICE

INVENTÁRIO E CLASSIFICAÇÃO DOS ATIVOS

Iremos inventariar os ativos de informação mais importantes e adicionaremos a classificação da criticidade em seu processo de negócio.

Iremos atribuir uma medida relativa de importância a cada ativo. Por exemplo, seus principais servidores de aplicação Web são mais importantes do que um desktop de endpoint que raramente é usado.



MONITORAMENTO DE DADOS VAZADOS PARA A DARK WEB

Os feeds de inteligência da FortifyData alertam nossos clientes quando os dados estão comprometidos, seja dentro de sua organização ou através de uma entidade terceirizada. Por meio da **varredura contínua de arquivos e bancos de dados** na dark/deep web nas mídias sociais, sites profundos não indexados e transitórios, alertamos você sobre registros da empresa expostos, incluindo informações vazadas, credenciais roubadas e documentos confidenciais.

VERIFICAÇÃO E AVALIAÇÃO DE VULNERABILIDADES EM SISTEMAS

Depois de catalogar seus ativos de informação, iniciaremos verificações de vulnerabilidades semanais para nos certificarmos de que todos os seus dispositivos e softwares estejam atualizados e, caso não estejam, daremos todo o apoio para que o problema seja resolvido.

Além disso, faremos a verificação da vulnerabilidade catalogada para constatar o que ainda precisa ser corrigido. Tudo isso dentro de uma **ordem de prioridade** que é calculada automaticamente por meio de diversos parâmetros.

AVALIAÇÃO DA SEGURANÇA DAS APLICAÇÕES WEB

Os ataques de aplicações Web são uma das principais causas de violação de dados. Permitimos às empresas gerir e desenvolver aplicações de forma segura, fornecendo avaliações de vulnerabilidades específicas da aplicação, tais como a elaboração de scripts cruzados (xss), erros de configuração, autenticação quebrada e muito mais.

DOCUMENTAÇÃO E DEFINIÇÃO DOS MECANISMOS DE MITIGAÇÃO DE RISCOS

Assim que levantamos os riscos cibernéticos, partimos para a documentação e apresentação ao comitê dos resultados coletados na pré-auditoria, contendo o levantamento e a classificação dos riscos. Em seguida, elaboramos um plano de ação de curto, médio e longo prazo.

GESTÃO DE RISCOS DE TERCEIROS

(FORNECEDORES, SUBSIDIÁRIAS OU ESCRITÓRIOS REGIONAIS)

Fornecemos à sua organização uma visão completa e transparente do ecossistema de risco de terceiros (fornecedores, subsidiárias, ou escritórios regionais), permitindo-lhe dar prioridade aos recursos e visar os terceiros com o maior risco cibernético. Fornecemos, também, avaliações abrangentes de terceiros potenciais e existentes de uma forma contínua.

DESENVOLVIMENTO E GESTÃO DE POLÍTICAS

A equipe da **Alerta Security** irá fornecer, adaptar e discutir as **políticas de segurança**, que serão a base da defesa cibernética em sua organização. As políticas que desenvolvemos são:

- Política geral de segurança da informação;
- Política de controle de acesso lógico e físico;
- Política de uso aceitável de recursos e ativos de informação dos colaboradores;
- Política de admissão e demissão de colaboradores;
- Política de trabalho remoto;
- Acordos de Confidencialidade NDA.

Todas as políticas de segurança são constantemente revisadas com o Comitê de Segurança.

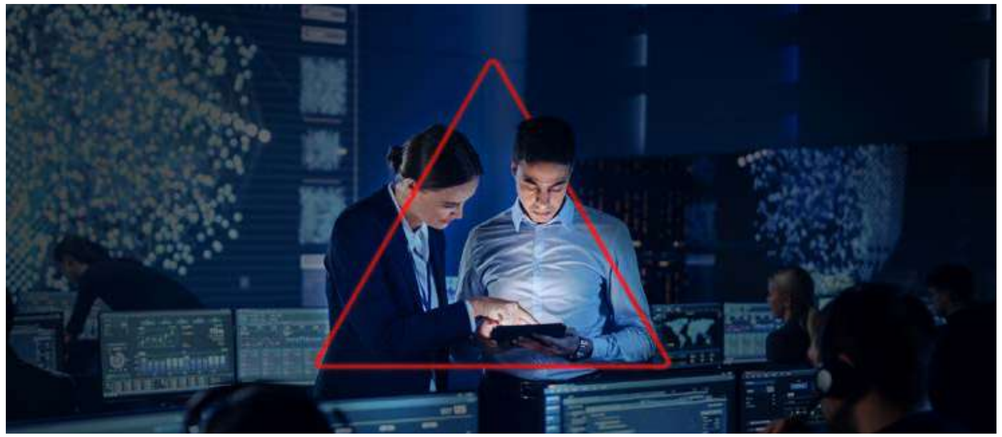
SISTEMA DE OPERAÇÕES DE T.I. - ITIL

A Alerta Security irá disponibilizar um sistema para gerenciamento das operações de TI que é totalmente alinhado ao ITIL. O sistema foi projetado com as melhores práticas em mente e será usado para que ambas as organizações estejam alinhadas com processos de gestão adequados. O sistema é flexível o suficiente para se adaptar aos processos específicos das organizações sem perder o alinhamento ao ITIL.

O objetivo do Sistema de Operações é coordenar as atividades de TI, documentar sua infraestrutura e todos os relacionamentos entre as várias partes interessadas da infraestrutura (servidores, aplicativos, dispositivos de rede, máquinas virtuais, contatos, locais, entre outros).

Sua organização poderá gerenciar incidentes, solicitações de usuários, interrupções planejadas, documentações de serviços de TI e contratos com provedores externos, incluindo acordos de nível de serviço.

- Gerenciamento de Ativos de TI;
- Gerenciamento de Tickets;
- Gerenciamento de Incidentes;
- Gerenciamento de Problemas;
- Gerenciamento de Mudanças.



Poderá ser usado por diversas equipes tais como:

- Agentes de help desk;
- Engenheiros de suporte (1º nível, 2º nível, etc.);
- Gerentes de serviço;
- Gerentes de TI;
- Usuários finais,

VOLTAR AO ÍNDICE

MONITORAMENTO CONTÍNUO DE CAPACIDADE E DISPONIBILIDADE (ARGOS)

As operações de TI são compostas por diversos componentes que sustentam todos os processos de negócio. Quando um problema ocorre em algum recurso tecnológico, temos como resultado a degradação ou a interrupção de algum serviço de TI e, consequentemente, prejuízos financeiros e operacionais.

O Serviço de Monitoramento de Capacidade e Disponibilidade (Argos) irá apoiar sua organização na difícil tarefa de **monitorar cada detalhe das complexas infraestruturas de TI**. Em caso de incidente, o sistema abrirá um incidente no Sistema de Operações de TI e será tratado com o devido processo.

FUNCIONALIDADES DO MONITORAMENTO

Coleta de dados

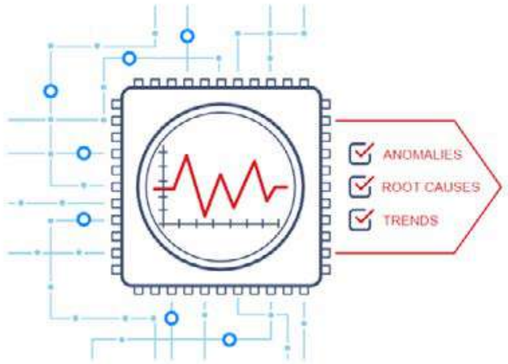
- Coleta de dados de dispositivos, sistemas, aplicações e muito mais.

- Diversos métodos de coleta:
  - Agentes de monitoramento para qualquer sistema operacional;
  - Coleta SNMP e IPMI;
  - Monitoramento sem agentes;
  - Customização de coletas;
  - Cálculos em coletas;
  - Monitoramento Web.

VOLTAR AO ÍNDICE

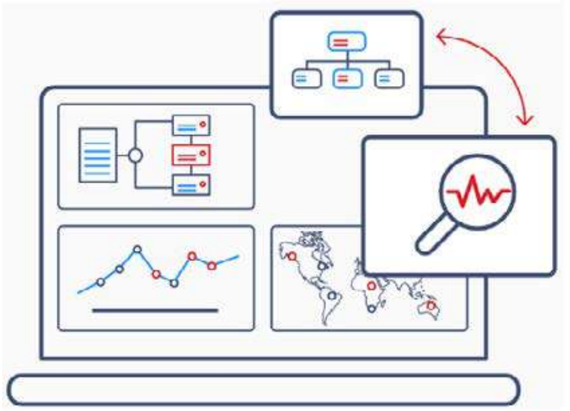
Detecção de Problemas

- Definição de limiares inteligentes;
- Detecção automática de falhas;
- Condições de problemas e condições de resolução separadas;
- Vários níveis de severidade;
- Análise de causa raiz;
- Detecção de anomalias;
- Previsão de tendências.



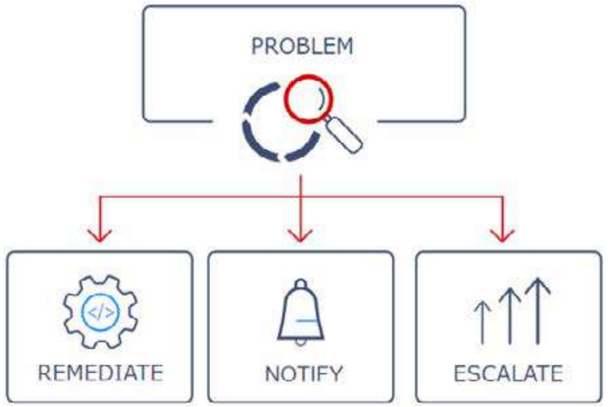
Interface Web

- Painéis Baseados em Widget;
- Gráficos;
- Mapas de rede;
- Slideshows;
- Relatórios de detalhamento.



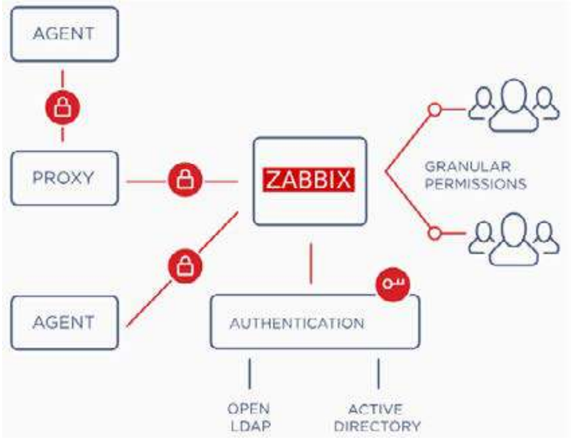
Notificações e remediações

- Notificações em caso de problemas;
- Informe as pessoas responsáveis através de diversos canais;
- Mensagens customizáveis;
- Diversos meios para envio de notificações (email, sms e outros).



Segurança

- Dados de coleta protegidos em todos os níveis;
- Criptografia forte na comunicação entre os componentes;
- Múltiplos métodos de autenticação;
- Esquema de permissionamento flexível.

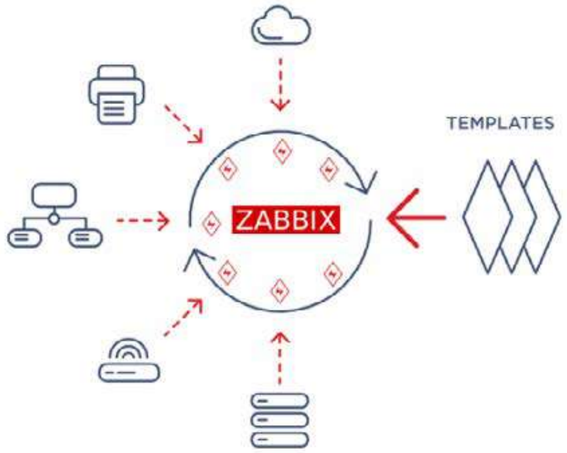


VOLTAR AO ÍNDICE

Implementação sem muito esforço

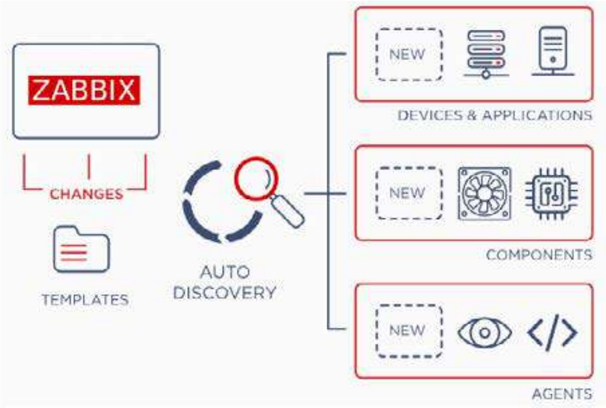
- Defina um perfil de monitoramento e atribua-o a milhares de dispositivos;

- Monitore milhares de dispositivos através de templates customizáveis e flexíveis.



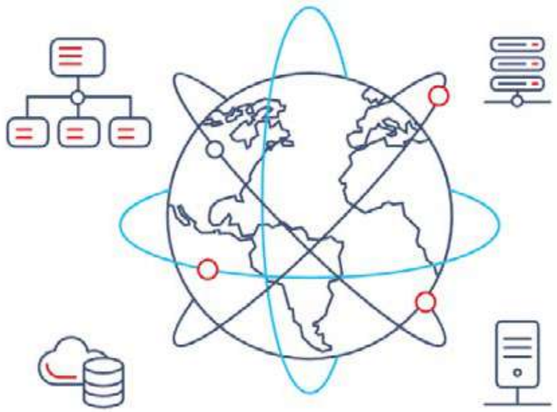
Automação do monitoramento

- Automatize o monitoramento de grandes ambientes;
- Ações automáticas ao adicionar, alterar e remover dispositivos;
- Descoberta e autorregistro de dispositivos;
- Execute comandos remotos em dispositivos.



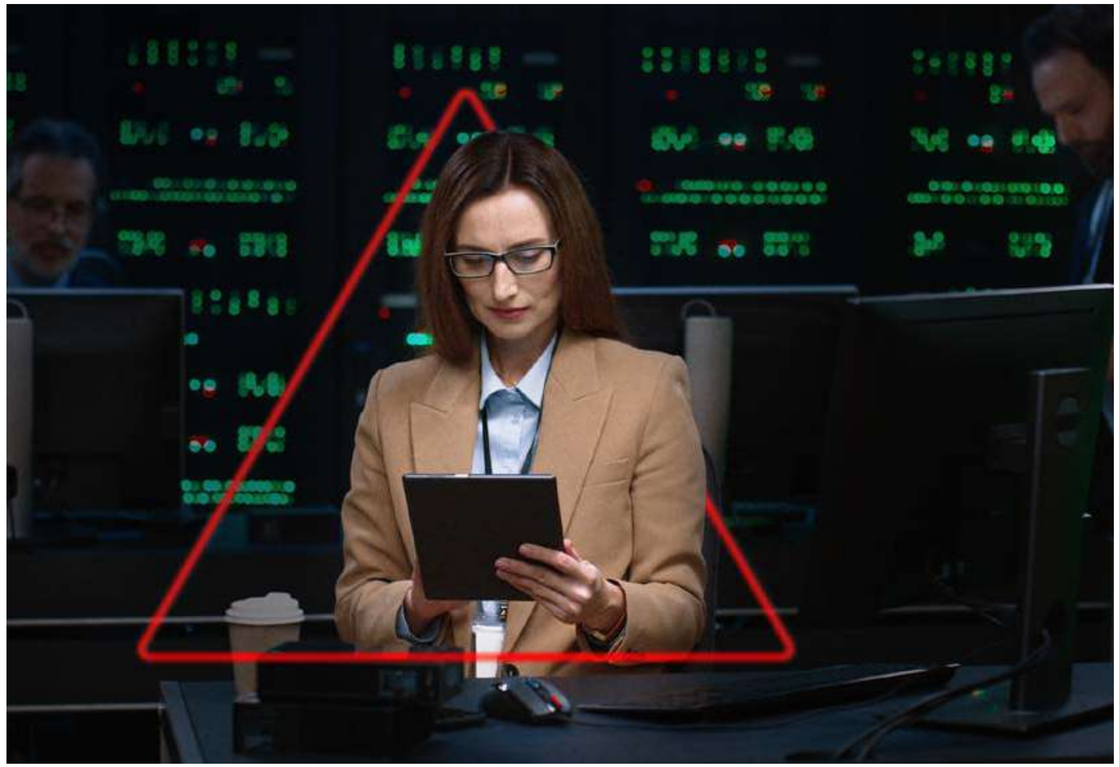
Monitoramento Distribuído

- Sem limites para escalar a plataforma;
- Monitoramento distribuído com controle centralizado;
- Monitore através de firewalls, DMZ, etc.



SERVIÇO DE NOC (NETWORK OPERATIONS CENTER)

O **serviço de NOC da Alerta Security** irá entrar em contato assim que algum ativo apresentar algum problema grave, uma indisponibilidade ou um incidente grave.



CONCLUSÃO

Criar e manter uma equipe desse nível, adquirir e implementar todo este processo de Gerenciamento de Risco e Operações de TI pode custar dezenas de milhares de reais para sua organização. Com a nossa solução, é possível aumentar a segurança com redução de custos, sem perder a qualidade do serviço.

A Alerta Security é uma empresa com mais de 18 anos de experiência e possui um quadro de colaboradores especializados. Toda essa expertise está à disposição do crescimento do seu negócio!

Assista ao vídeo e conheça a Alerta Security

ALERTA SECURITY

FORTIFYDATA

PARCERIA OFICIAL EXCLUSIVA NO BRASIL

+55 11 3105-8655

CONTATO@ALERTASECURITY.COM.BR

RUA PAIS LEME, 215 - 14º ANDAR - PINHEIROS, SÃO PAULO - SP