

Ibmec Business School
Especialização em Segurança da Informação
IBMEC - Petrobras

**Disciplina: Tratamento de Incidentes de
Segurança**

Professor

Frederico Sauer, D.Sc.

fred@sauersecurity.com.br

ESTUDO DE CASO

ESTRUTURAÇÃO DE UM

GRUPO DE RESPOSTA A INCIDENTES

PRIMEIRA VERSÃO

Empresa Gerbet Produtos Radiológicos

1. Apresentação da Organização

Nome da empresa: Guerbet Produtos Radiológicos Ltda.

Negócio:

- Forte presença no mercado farmacêutico brasileiro;
- Empresa de capital estrangeiro;
- Área de atuação: Europa, EUA, Brasil, México, china e Japão;
- Seus produtos e serviços estão disponíveis em mais de 70 países;
- 1200 colaboradores.

Missão:

- Contribuir para o aprimoramento da capacidade diagnóstica de todas as principais doenças: doenças cardiovasculares, câncer, processos inflamatórios e degenerativos;
- Prover aos radiologistas e cardiologistas um completo portfólio de meios de contrastes, produtos e serviços complementares, efetivos inovadores, que ajudem suprir as necessidades da melhor forma possível para seus pacientes;
- Contribuir na solução dos maiores problemas da saúde pública no Brasil.

Visão:

Manter-se líder no negócio de meios de contraste e ocupar posição de destaque nos negócios de produtos e serviços complementares em imagenologia médica.

2. Identificar e obter o apoio e a aprovação dos Stakeholders / Patrocinadores

2.1 - Identificação dos Stakeholders.

Para obter os recursos materiais e financeiros necessários a criação do GRIS, como também a alocação do tempo de trabalho para a estruturação da mesma, identificou-se ser fundamental o patrocínio dos seguintes administradores da Guerbet:

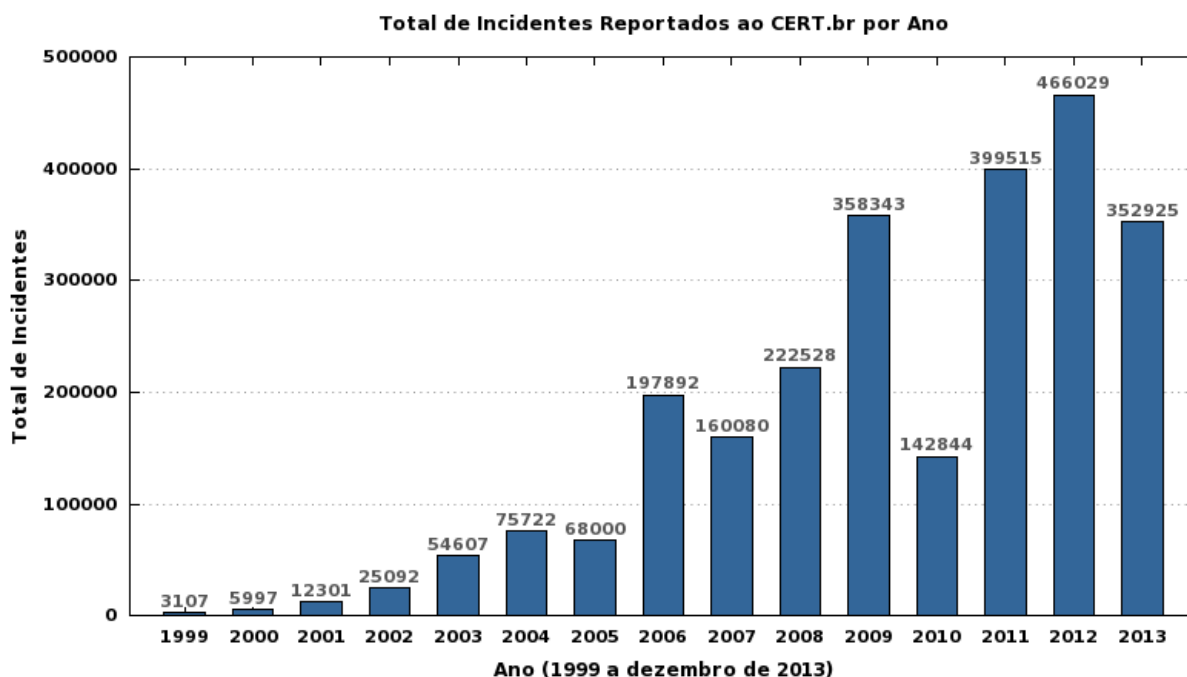
- CIO da matriz (França) – Aprovar o plano e liberar os recursos. Observação: a estrutura de informática da empresa no Brasil, apesar de ter autonomia, precisa seguir as diretrizes da matriz francesa. Desta forma, é necessária a aprovação do CIO da Matriz.

- Diretor Geral Brasil – apoio junto ao CIO e viabilizar os recursos humanos e financeiros.
- Diretora de Informática – Brasil – Definir a missão do GRIS e o plano de continuidade do negócio, alinhado com os objetivos da empresa.
- Diretor Industrial – Brasil – Definir os tempos de resposta aceitáveis para a continuidade da produção.

2.2 – Táticas para obtenção de apoio

Através de uma apresentação para a diretoria, serão mostradas as estatísticas de incidentes e os impactos causados, com perda de tempo de trabalho, atrasos na entrega de produtos e consequente prejuízo financeiro.

Também será revelado que os ataques estão se intensificando e ficando cada vez mais especializados, conforme estatísticas do CERT.br:



Fonte: www.CERT.br

Será argumentado que, com a criação de um GRIS, será possível padronizar os procedimentos a serem aplicados na ocorrência de um evento de segurança e melhorar a aplicação de investimentos na área, já que a organização saberá, de antemão, os pontos fracos a serem trabalhados. Desta forma, os impactos e perdas financeiras serão minimizados, aumentando o retorno do investimento (ROI) e melhorando da imagem da empresa junto aos seus clientes.

É importante que, neste momento, a administração da Guerbet coloque suas expectativas e percepções da função e responsabilidades do GRIS. Estas informações

devem ser consideradas no planejamento estratégico da criação do GRIS, de forma que sua missão e objetivos estejam devidamente alinhados.

2.3 - Formalização do Apoio

Primeiramente, será solicitada uma carta de compromisso da matriz francesa, ratificando seu apoio e instruindo a administração brasileira a prover os recursos materiais e humanos necessários a criação do GRIS.

Será também criado um termo de compromisso que deverá ser assinado pelos diretores da filial brasileira diretamente envolvidos no processo, garantindo assim seu apoio.

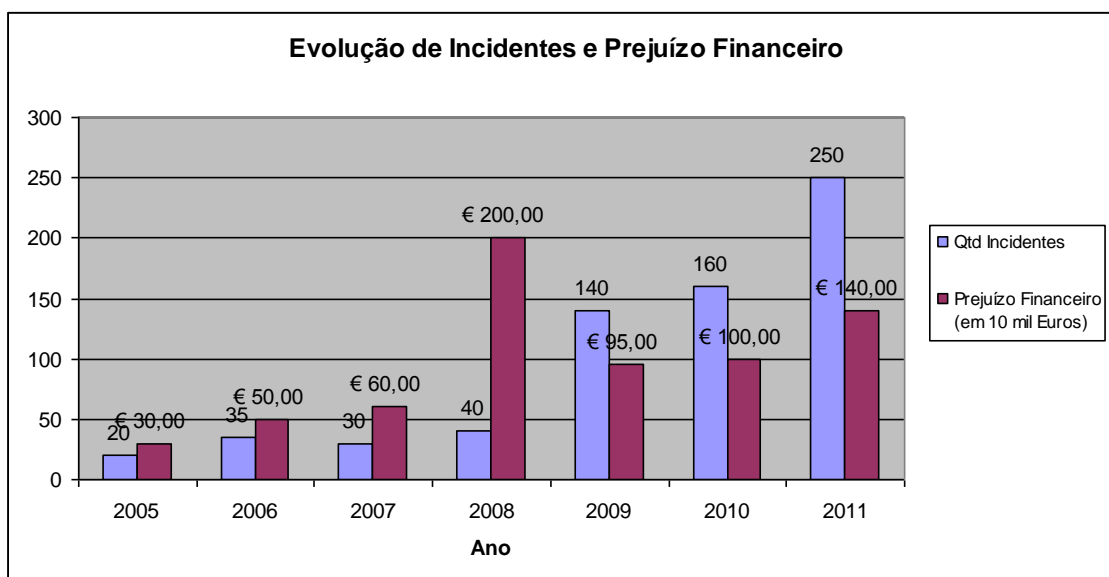
Os *stakeholders* deverão divulgar seu apoio ao projeto de criação do GRIS por meio de um comunicado utilizando a Intranet, o Boletim da Comunicação Interna e o Jornal Mural.

3. Levantamento de Informações

3.1 - Histórico de Incidentes

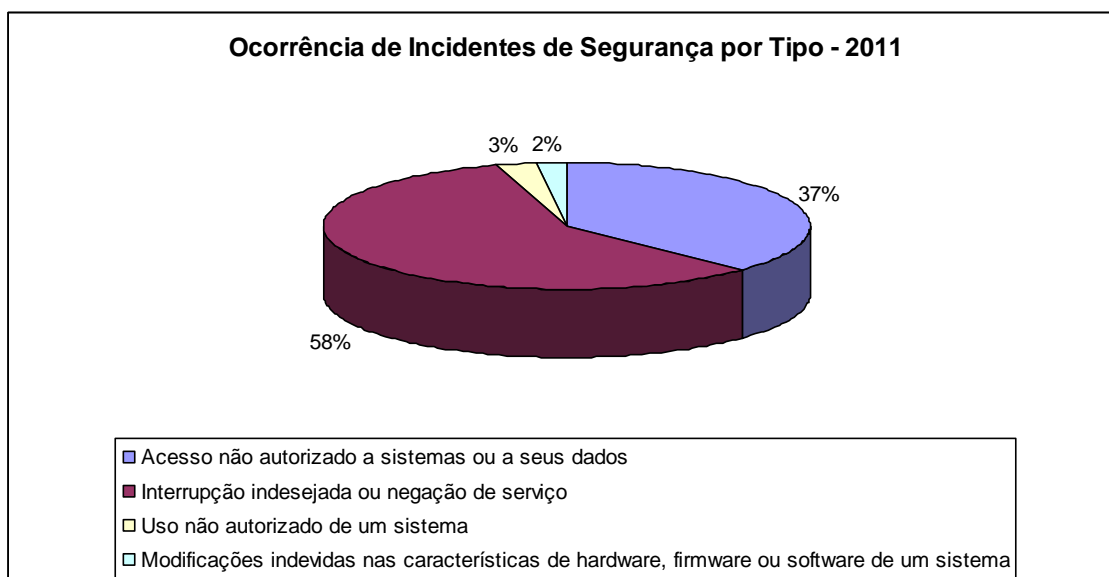
O levantamento de histórico de incidentes será elaborado levando em conta os dados do sistema de suporte que registra os chamados de Help Desk.

A empresa em 2009 passou a fazer um registro formal de incidentes de segurança através de um sistema de Help Desk, o que é demonstrado pelo aumento significativo do número de ocorrências neste ano. A motivação para a adoção de um processo formal foi um incidente grave no ano anterior, que causou prejuízos significativos, com perda de vendas e devolução de produtos. O gráfico a seguir demonstra a relação entre o impacto financeiro e a evolução de incidentes de segurança.



Com o crescimento do número de incidentes de segurança ao longo dos anos e o impacto financeiro também crescente, percebe-se que há a necessidade da organização estar mais preparada para responder aos incidentes de segurança e assim minimizar o impacto financeiro causado. Para tanto, é fundamental a criação de uma equipe especializada, independente do Help Desk.

Além da constatação de que o aumento dos incidentes de segurança está diretamente relacionado às perdas financeiras da empresa, foi feita uma análise dos tipos de incidentes mais frequentes no ano de 2011, com o objetivo de verificar quais ataques à Guerbet são mais comuns. O resultado encontrado (ver gráfico a seguir) mostra que a interrupção indesejada ou negação de serviço, a exemplo dos ataques DDoS, foi o tipo de incidente de maior ocorrência no ano de 2011 e que, portanto, merece uma atenção maior por parte da GRIS.



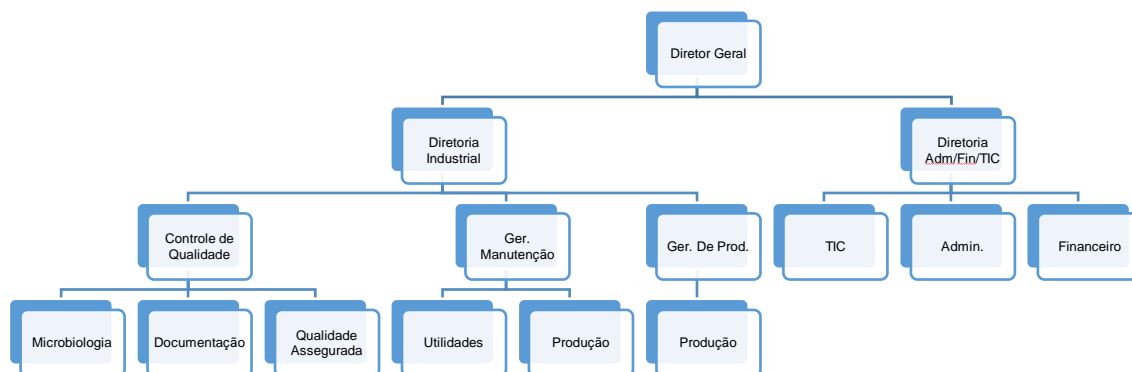
3.2 - Documentação

Um levantamento criterioso de documentos foi realizado, procurando identificar possíveis interessados, recursos e proprietários de sistemas. Procurou-se ter uma visão geral de políticas existentes e que devem ser seguidas pelo GRIS.

Os documentos coletados servirão de base para o desenvolvimento de políticas, procedimentos e documentos do GRIS. A partir deles, também serão identificadas as pessoas na organização que devem ser contatadas durante uma emergência.

Dentre as informações encontradas, destacam-se:

1. Organograma da Empresa



2. Inventário dos Sistemas e Recursos Críticos

A Guerbet tem como maior produto a fabricação de meios de contraste para auxílio de diagnóstico. No processo de fabricação deste contraste, o produto tem um tempo de quarentena de 14 dias. Devido a esse fato, qualquer incidente que implique em parada de produção, irá acarretar em atraso na entrega do produto, perda de matéria prima e consequentemente prejuízos financeiros.

3. Regulamentos Institucionais Existentes

Como empresa da área farmacêutica, a Guerbet tem que seguir normas e leis, tanto nacionais como internacionais. O não cumprimento delas implica em multas e sanções e, portanto, configura-se como incidente de segurança grave. A indústria farmacêutica segue as diretrizes da RDC17 (ANVISA), GAMP5 (ISPE), CFR PART11 (FDA).

Internamente, a Guerbet possui como norma o reporte de incidentes por meio de formulário próprio, que é preenchido pela área específica. As áreas envolvidas são notificadas formalmente e é aberto um procedimento de tratamento do desvio para a sua solução ou justificativa (ex: falta de dados em um determinado intervalo de tempo devido ao desligamento do equipamento para manutenção).

A política de segurança da informação da empresa trata das linhas gerais de segurança, e cada sistema computadorizado tem o seu ciclo de vida com instruções de recuperação de desastre específicas.

4. Planejamento Estratégico do GRIS

Missão

Atuar de forma proativa no diagnóstico e solução de incidentes de segurança, minimizando os impactos e apoiando a melhoria do plano de continuidade dos serviços da organização.

Visão

Ser capaz de identificar as maiores ameaças de segurança da informação, agindo de forma proativa e respondendo tempestivamente aos eventos que possam interferir nas atividades da organização.

Objetivos

- Identificar as principais ameaças de segurança;
- Definir um plano de resposta a incidentes;
- Tratar os incidentes de segurança, minimizando seus impactos e garantindo a continuidade dos serviços afetados;
- Estabelecer e gerar indicadores e métricas sobre os incidentes de segurança;
- Compilar informações e estatísticas, gerando pareceres que possam ser úteis a gerencia no processo de tomada de decisão;

Desenvolvimento do Projeto

Inicialmente, devido a não existência de um GRIS, entende-se que a equipe atuará de forma reativa. A expectativa inicial é de que, uma vez a equipe estabelecida e funcional, dentro de 9 meses se consiga atingir um nível de maturidade em que se possa apresentar uma proposta para que a equipe passe a atuar também de maneira proativa, contemplando recursos humanos, materiais e processuais para execução da missão.

Reunião de alinhamento com os Stakeholders:

A pauta apresentará a concepção da ERSI, Visão, Missão e Objetivos da equipe, buscando alinhar as expectativas das áreas envolvidas no projeto.

Crescimento e Desenvolvimento da Equipe

Devido a questões de orçamento, inicialmente a equipe constará de dois (02) Analistas Senior da Divisão de Segurança da Informação, destacados exclusivamente às atividades de RISI e um (01) Líder de CSIRT, que atua hoje como Gerente de Redes. A equipe será capacitada em RISI através dos cursos que seguem abaixo:

Fundamentals of Incident Handling – **CERT.br**

Overview of Creating and Managing Computer Security Incident Response Teams – **CERT.br**

Advanced Incident Handling for Technical Staff – **CERT.br**

Revisão de Recursos humanos e capacitação

A partir da implementação desta Equipe, ficará determinada a revisão de recursos humanos e capacitação a cada 6 meses, seguindo os critérios baseados no volume de trabalho do período vigente ou tempestivamente, devido a revisões nos objetivos, missão e visão da organização ou do GRIS.

Descrição dos membros associados, funções e responsabilidades

Segue abaixo os quadros relativos aos membros associados do GRIS, suas funções e responsabilidades:

Membros associados

Membro associado	Descrição da função
Contato de TI	Responsável pela coordenação da comunicação entre o líder de incidentes do GRIS e o restante do grupo de TI, sendo basicamente responsável pela localização das pessoas no grupo de TI que devem tratar eventos de segurança em especial.
Representante legal	<p>Advogado muito familiarizado com as diretivas estabelecidas para resposta a incidentes. O representante legal determina como proceder durante um incidente com responsabilidade legal mínima e autorização máxima para processar transgressores.</p> <p>Antes que haja um incidente, o representante legal deve ter informações sobre as diretivas de monitoramento e resposta para assegurar que a organização não esteja correndo riscos legais durante uma operação de limpeza ou de retenção. É muito importante levar em consideração as implicações legais do desligamento de um sistema e da possibilidade de violação dos contratos de nível de serviço ou de associação firmados com seus clientes ou do não desligamento de um sistema com e responsável por danos causados por ataques iniciados a partir deste sistema.</p> <p>Toda a comunicação externa com autoridades competentes ou órgãos investigativos externos deve ser coordenada com o representante legal.</p>
Diretor de relações públicas	Este membro faz parte do departamento de relações públicas, sendo responsável por resguardar e promover a imagem da organização, sendo responsável pela elaboração da mensagem (o conteúdo e o objetivo desta mensagem costumam ser de responsabilidade da gerência). Todas as solicitações de imprensa devem ser direcionadas ao departamento de Relações Públicas.
Gerência	<p>Dependendo do incidente em especial, serão envolvidos apenas os gerentes do departamento ou todos os gerentes de toda a organização. A pessoa responsável pela gerência apropriada varia de acordo com o impacto, o local, a gravidade e o tipo de incidente.</p> <p>A Gerência é responsável pela aprovação e orientação da diretiva de segurança, sendo responsável pela determinação do impacto total (em termos financeiros ou não) do incidente na organização. A Gerência orientará o diretor de comunicação a respeito das informações a serem divulgadas à imprensa e determina o nível de interação entre o Representante legal e as autoridades competentes.</p>

Definição de Responsabilidades durante o processo de resposta ao incidente

Atividade	Função				
	Líder de incidentes do GRIS	Contato de TI	Representante legal	Diretor de comunicação	Gerência
Avaliação inicial	Proprietário	Avisa	Nenhuma	Nenhuma	Nenhuma
Resposta inicial	Proprietário	Implementa	Atualiza	Atualiza	Atualiza
Obtém evidências forenses	Implementa	Avisa	Proprietário	Nenhuma	Nenhuma
Implementa correção temporária	Proprietário	Implementa	Atualiza	Atualiza	Avisa
Envia a comunicação	Avisa	Avisa	Avisa	Implementa	Proprietário
Consultar as autoridades competentes locais	Atualiza	Atualiza	Implementa	Atualiza	Proprietário
Implementa correção permanente	Proprietário	Implementa	Atualiza	Atualiza	Atualiza
Determina o impacto financeiro nos negócios	Atualiza	Atualiza	Avisa	Atualiza	Proprietário

Gerenciamento do Projeto

As atividades de gerenciamento de projetos serão realizadas pelo escritório de projetos da empresa, conforme estabelecido no regimento interno da empresa.

O escritório de projetos segue todas as fases da Gestão de Projetos preconizadas pelo Project Management Institute (PMI).

Canais de Comunicação

Os canais de comunicação a serem utilizados serão a Intranet, o Boletim da Comunicação Interna e o Jornal Mural. Ambos plenamente difundidos dentro da empresa.

Será adotado também um Plano de Comunicação por incidente de segurança, contendo os itens básicos para comunicação de resposta a incidentes, conforme o modelo descrito no Anexo A.

Armazenamento das informações

Todas as informações referentes ao GRIS serão armazenadas em um servidor localizado no DataCenter da empresa, sendo contempladas as proteções relacionadas à Recursos Computacionais Críticos de Nível Alto, tanto lógicas (ACL, Criptografia e etc.) e físicas (Biometria, Sala Cofre, Backup offsite e etc.) conforme preconizado na Política de SegInfo.

Toda a documentação gerada deve ser organizada em ordem cronológica, verificada, assinada e revisada pelos representantes administrativos e legais.

Fase 4: Implantação

Equipe Responsável

A equipe é formada de 3 analistas que foram capacitados nas áreas:

Administração de sistemas:

- Provêm o conhecimento e habilidades dos recursos do sistema, assim como backups de dados, backup de hardware disponível para uso e outros.

Administração de rede:

- Redirecionamento de tráfego, monitoramento da rede, implementação de alertas e medidas corretivas.

Segurança da informação:

- rastrear e investigar detalhadamente as questões de segurança, analisar os sistemas comprometidos, reprogramação de firewall e análise forense.

A equipe opera em regime de turno, sendo que um analista sempre atua em redundância.

Equipamentos e Infraestrutura

- 3 celulares para equipe.
- 3 notebooks com 3g, com software forense instalado, e software de monitoramento da rede.
- Mapa topológico da rede,
- Descrição dos sistemas
- Telefones de suporte dos fabricantes
- Telefone de suporte dos provedores de telecom.
- Telefone fixo fora da central telefônica, com fio.
- Lanterna.
- Luz de emergência.
- Switch L3 reserva.
- Arquivos de configuração dos switches e roteadores.
- Imagem dos servidores.
- Servidor backup com as máquinas virtuais instaladas.
- Ar condicionado backup.
- Nobreak.
- Gerador.

Fase 5: Campanha de divulgação – GRIS

Os departamentos de RH, Marketing e Comunicação Empresarial atuarão em conjunto para produzir todo o material de divulgação, utilizando os canais de comunicação difundidos dentro da empresa:

- *Folhetos;*
- *Cartazes;*
- *Jornal mural ;*
- *e-mail ;*
- *Brindes;*
- *Palestras;*
- *Dia da GRIS;*

A divulgação deve conter a Visão, Missão e Objetivos da GRIS.

Treinamento formal para todos os funcionários da empresa e colaboradores.

A alta administração da empresa deve demonstrar seu patrocínio, enviando na data da implantação da GRIS, uma carta do presidente a todos os empregados.

Fase 6: Avaliações e Métricas

As métricas utilizadas são duas:

- Tempo de restabelecimento do serviço x tempo de *downtime* suportado.
- Incidentes detectados com potencial impactante contidos.

Anexo do Documento: Estruturação de um Grupo de Resposta a Incidentes

-MODELO-

Plano de Comunicação

Este plano tem como objetivo cientificar os diretores do conselho as informações descritas abaixo:

Fase 1 - Uma vez ocorrido um incidente de DDOS

Informação	Obs.
O que aconteceu?	(Foco nos fatos ou nas acusações.)
Quanto?	(Danos, dinheiro envolvido.)
Quem foi afetado?	(Vítimas, acusados etc.)

Fase 2 - Após um incidente de DDOS

Informação	Obs.
Qual foi a causa?	-
Obedece a um padrão?	Ex: Atacantes do mesmo país
Quem pagará os danos?	Necessidade de acionar meios legais ?
Qual é o prejuízo potencial para a reputação da empresa?	Perda de contratos? credibilidade e etc.
Que impacto terá no preço da ação?	Como se refletirá em seus planos? Realinhamento de estratégias?