

Resposta a Incidentes de SegInfo

Prof. Dr. Frederico Sauer
fred@sauersecurity.com.br

NP-1

Gestor: CI/ICM
Versão 1 - Junho/2013

Objetivo



Discutir as fases para elaboração de um **Grupo** de Resposta a Incidentes de Segurança da Informação (GRIS) e de **Planos** de Resposta a Incidentes de SegInfo (PRI).

NP-1

Gestor: CII/ICM
Versão 1 - junho/2013

O objetivo prático do curso é CAPACITAR os alunos a planejar a formação e a capacitação de um GRIS (Grupo de Resposta a Incidentes de Segurança), e a elaborar os PRI (Planos de Resposta a Incidentes), de acordo com as prioridades do negócio e os resultados das Análises de Risco.

Os documentos em inglês e até mesmo alguns em português chamam o Grupo de Respostas a Incidentes de CSIRT (Computer/Cyber Security Incident Response Team). Neste curso usaremos a sigla GRIS.

Há várias metodologias propostas. No curso, vamos seguir a principal tendência no Brasil, em função do apoio do CERT-BR (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil), que é um “braço” do Comitê Gestor da Internet no Brasil.

A principal fonte de referências adicionais é o site do CERT.BR. Para facilitar, selecionei as mais importantes e disponibilizei em <http://www.fredsauer.com.br>

Perguntas Iniciais a Responder...



- Quais são os requisitos básicos para se estabelecer um GRIS ?
- Que tipo de GRIS será necessário?
- Que tipos de serviços devem ser oferecidos?
- Qual deve ser o tamanho de um GRIS ?
- Onde o GRIS deve estar localizado na organização?
- Qual será o custo para implementar e manter um GRIS?
- Quais são os passos iniciais que devem ser seguidos para criar um GRIS ?

NP-1

Gestor: CI/ICM
Versão 1 - junho/2013

Estes questionamentos e o seu detalhamento acaba por inviabilizar a construção de um GRIS e elaborar PRIs. É fundamental que a atividade não se torne mais uma rotina cotidiana obrigatória, e sim um conjunto de processos de grande importância para o negócio e para as pessoas. Para alcançar este objetivo, o caminho é planejar com sabedoria, ajustando às demandas técnicas com as do negócio e dando visibilidade aos resultados, principalmente com o uso de indicadores.

Sumário



- Motivações
- Definições e Conceitos básicos
- Tipos de Incidentes
- Pré-Requisitos
- O processo de criação do Grupo de Resposta a Incidentes
- A Elaboração de um Plano de Resposta a Incidentes de SegInfo
- Trabalhos em Grupo
 - Trabalho de Estruturação de um GRIS
 - Trabalho de Plano de Resposta a Incidentes



Gestor: CI/ICM
Versão 1 - junho/2013

Esta será a sequência de apresentação de assuntos. A nota da cadeira será composta de uma prova com peso de 70% e dois trabalhos em grupo feitos em sala, um sobre a estruturação de um GRIS e outro sobre a construção de um PRI, com peso total de 30% da nota.

Motivações



- Uma boa Gestão de Riscos depende de dados estatísticos sobre incidentes e seus impactos
- Para isso são necessários dados sobre:
 - Incidentes de segurança ocorridos e seus efeitos
 - Percepção do grau de cultura corporativa de segurança
 - Tipos e comportamentos de novas ameaças
- Esta atitude possibilita às corporações:
 - Identificação da demanda de novas políticas para proteção das informações
 - Identificação de prioridades, treinamentos específicos, auditorias, etc.

NP-1

Gestor: CII/ICM
Versão 1 - junho/2013

A tendência atual é a de alinhar a Segurança da Informação às demandas do negócio, em lugar da pura e simples adoção das boas práticas.

Observe os comentários feitos por um importante diretor executivo:

“Nossa empresa passou por ocorrências cuja importância não foi dada, causando impactos que todos acompanharam...”

“Na nossa empresa, as ROTINAS prevaleceram sobre o CONTROLE...”

“Procedimentos importantes de segurança sempre foram tratados como ROTINAS, e não como algo importante para o negócio...”

“São necessárias práticas transparentes, com uma visão clara da importância da Segurança da Informação para a empresa, não devendo receber tratamento de rotina...”

Theodoros Marcopoulos, Diretor da Petrobras, durante o Encontro Técnico de Segurança Empresarial do Abastecimento, realizado em 12 de novembro de 2014 na Universidade Petrobras.

As declarações acima demonstram a importância de se romper os paradigmas antigos da Segurança da Informação, adotando metodologias que permitam uma ampla discussão para possibilitar a participação de todos.

Motivações para o uso de uma Metodologia de Tratamento de Incidentes



- Padronização dos Procedimentos em caso de crise
 - Soluções *ad-hoc* nem sempre são as ideais
- Visão Geral dos Incidentes
 - Indicadores/Métricas
 - Lições Aprendidas
 - Ganho de desempenho em novas ocorrências
 - Mudança de postura para evitar novos incidentes
 - Melhor aplicação de Investimentos em SegInfo
 - São identificadas tendências de possíveis incidentes que nunca ocorreram
- Alguns ataques não são bloqueados por ferramentas automatizadas, como firewall ou proxies de aplicação
- Avanço das técnicas de invasão, cada vez mais *sthealth*

NP-1

Gestor: CII/ICM
Versão 1 - junho/2013

Grande parte das empresas sequer mapeia estratégias para tratamento de incidentes. De uma forma geral, especialistas em seus respectivos assuntos são convocados de acordo com a ocorrência, com todas as óbvias desvantagens desta abordagem: indisponibilidade do especialista, descontinuidade do suporte com o seu afastamento, não-acompanhamento do estado da arte, falta de ferramentas apropriadas, etc.

O ideal então é o uso de uma metodologia que possibilite a existência de um conhecimento documentado que possa ser usado não apenas por um especialista, mas por qualquer técnico da área.

Incidentes de segurança são probabilísticos, e todas as empresas estão sujeitas a eles. Seus indicadores (ou métricas) normalmente são percentuais, indicando a probabilidade de ocorrência de acordo com as características ambientais. Podem ser facilmente obtidos em relatórios de empresas especializadas, mas estes números não levam em consideração o perfil de cada empresa, e sim apenas o número de ocorrências verificadas em um intervalo de tempo. O ideal é que cada empresa crie e alimente o seu próprio histórico de ocorrências, bem como da evolução dos eventos de segurança que fazem aumentar a probabilidade de ocorrência de um incidente.

Também é fundamental que, após a ocorrência de incidentes, a empresa modifique seus controles para evitar que os mesmos voltem a ocorrer.

Também é importante ressaltar que, por mais que se invista em proteções, muitas ameaças são novas e não há bloqueios eficazes disponíveis, além do fator humano que pode desabilitar qualquer controle existente.

Definições e Conceitos



- O que é um Evento de Segurança ?
 - Ocorrência em um sistema, serviço ou rede que indique um POSSÍVEL descumprimento de Política de Segurança ou falha nos controles, ou ainda uma situação previamente desconhecida que possa ser relevante para a SegInfo
- E um Incidente de Segurança ?
 - Um ou mais EVENTOS que tenham uma significativa probabilidade de comprometer o negócio e ameaçar a SegInfo
- Todo Incidente é composto de um ou mais eventos, então ambos devem ser foco do trabalho do GRIS e do PRI.

NP-1

Gestor: CII/ICM
Versão 1 - junho/2013

É importante ressaltar esta diferença. Suponha que um terrorista altamente capacitado tente alcançar o Datacenter da empresa para instalar dispositivos maliciosos, mas não consiga em virtude de controles existentes. Isso não é um INCIDENTE de segurança, uma vez que não houve impacto, já que o invasor não obteve êxito. Porém, a probabilidade de ocorrência de incidente aumentou bastante, já que houve a tentativa de acesso e possivelmente o atacante voltará a tentar, usando outros recursos. Infelizmente, os dados de tentativas de acesso não autorizado bloqueadas não são mapeadas para uso na atualização das estatísticas.

Uma das funções do GRIS, além obviamente RESPONDER aos incidentes, deve ser justamente a obtenção desta modalidade de ocorrência (eventos de segurança), para um correto direcionamento das ações e prioridades.

Definições e Conceitos



- **GRIS (Grupo de Resposta a Incidentes de Segurança da Informação)**
 - Responsável por serviços e suporte para um determinado público alvo, **para prevenção, tratamento e resposta a incidentes de segurança**.
 - Pode desempenhar **diversos papéis** e serviços dentro de uma organização
 - Tratamento de Incidentes, Auditoria, Monitoramento, Testes, Tratamento de Riscos, assessorar a criação de recomendações de SegInfo, Contato entre organizações afins (outros GRIS e CERT-BR, polícia especializada, provedores).

NP-1

Gestor: CI/ICM
Versão 1 - junho/2013

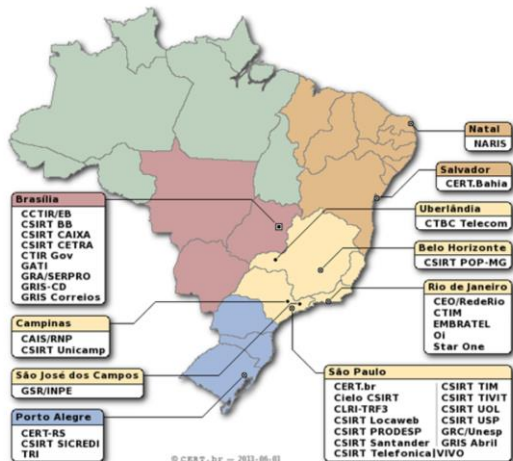
Uma questão importante a definir é a **comunidade** a ser atendida, e a **missão** a cumprir. Um GRIS tipicamente atende a um grupo comunitário específico, como por exemplo um GRIS acadêmico, que atende à comunidade de estudantes e usuários dos serviços prestados através da rede acadêmica, ou um GRIS de PIC/PIIC (Proteção de Informações Críticas e de Infraestruturas de Informação Críticas), que atendem indiretamente aos cidadãos de um país protegendo setores de informática críticos do mesmo.

Há vários serviços que podem ser prestados pelo GRIS, mas tipicamente nem todos são prestados pela grande demanda de estrutura para tal. Por isso, é de vital importância a seleção adequada dos serviços a serem prestados pela GRIS antes de seu planejamento. Estes serviços serão enquadrados em ações proativas, reativas, gestão de artefatos ou gestão da qualidade da segurança. Em resumo, o primeiro passo é definir:

1. **Compreender o que é um GRIS e que benefícios ele pode proporcionar.**
2. **A que setor (comunidade) o GRIS prestará os seus serviços?**
3. **Que tipo de serviços o GRIS poderá prestar à sua comunidade utilizadora?**

Definições e Conceitos

- Tipos de GRIS
 - Departamentos
 - Empresas
 - Países
 - *Backbones*
 - Órgãos Governamentais



NP-1

Gestor: CI/ICM
Versão 1 - junho/2013

Dependendo do nível de risco, pode ser necessária a criação de uma célula local de resposta a incidentes, com escopo de atuação departamental, ou um escopo global, muito mais de coordenação e normatização do que atuação de resposta efetiva.

Definições e Conceitos



■ Abordagens

■ Centralizada

- Recomendado para pequenas organizações, onde não existem unidades remotas

■ Distribuída

- Recomendado para grandes organizações. Possui diversos GRIS espalhados pelas várias unidades da empresa que deverão responder a um Centro Organizacional, que será responsável por todos os GRIS
 - Exemplo: Marinha do Brasil

■ Terceirizada

- Parcial: São terceirizados alguns Serviços especializados
- Total: Todo Serviço de Resposta é terceirizado

NP-1

Gestor: CI/ICM
Versão 1 - junho/2013

A Marinha do Brasil possui um GRIS central, denominado CTIM, fisicamente sediado no Rio de Janeiro, porém ele distribui diretrizes e tarefas proativas para os seus distritos navais (regionais), além de apoiar as eventuais demandas reativas. Periodicamente realiza auditorias remotas e in-loco para verificar a conformidade com as políticas vigentes.

Quem na turma vai explicar para os colegas como é a abordagem da Petrobras e quais são as responsabilidades de cada colaborador em relação às atividades de Resposta a Incidentes ?

Definições e Conceitos



- **Dedicação**
 - A organização deverá refletir sobre a sua situação quanto ao risco para definir a disponibilidade do GRIS, que poderá ser:
 - Dedicação Integral
 - Dedicação Compartilhada
- **Nível de Autoridade**
 - Total
 - Parcial
 - Nenhuma

NP-1

Gestor: CII/ICM
Versão 1 - junho/2013

A escolha do modelo de dedicação dos componentes do GRIS depende diretamente do nível de risco da corporação. Observe que, mesmo havendo dedicação integral de seus componentes, o GRIS pode dispor de especialistas internos ou terceirizados para casos específicos. A dedicação compartilhada inevitavelmente reduz a capacidade do grupo de produzir de forma proativa.

Níveis de autoridade:

Total: Os componentes do GRIS possuem a autoridade para adotar medidas e tomar decisões em benefício da comunidade atendida, sem a necessidade de prévia consulta.

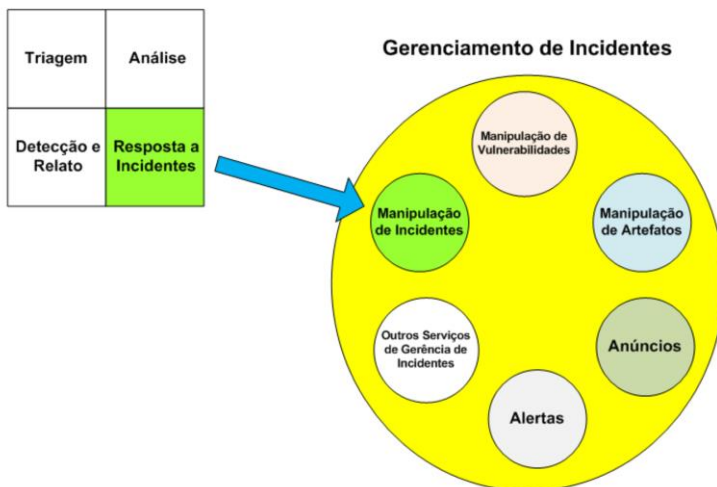
Parcial: Os membros do GRIS prestam assistência direta à comunidade a qual atendem e contribuem no processo de tomada de decisões e definição de ações. Observe que, neste caso, não podem agir autonomamente em nome da comunidade atendida.

Nenhuma: Os componentes do GRIS apenas atuam como conselheiros ou eventualmente como seus representantes formais.

Exemplo: suponha que o GRIS detecta a disponibilidade de um *patch* para corrigir uma vulnerabilidade em um aplicativo largamente utilizado por sua comunidade. O GRIS com autoridade **TOTAL** pode determinar que todos os membros que não tenham executado o *patch* não acessem os serviços de rede até que tenham atualizado, inclusive desconectando manualmente os que descumprirem a medida; Na modalidade **PARCIAL**, o GRIS pode RECOMENDAR e INTERVIR sugerindo que os membros da comunidade não usem os serviços de rede até que atualizem os seus sistemas, APOIANDO e ORIENTANDO os usuários a seguir a recomendação. No modelo **SEM AUTORIDADE**, o GRIS pode RECOMENDAR a utilização do *patch* e ORIENTAR quanto à sua execução, buscando MOTIVAR a comunidade para a importância da operação, entretanto, o GRIS não possui mecanismos para OBRIGAR os membros da comunidade a instalar o *patch*.

Definições e Conceitos

- Relação entre os termos Gerenciamento/Manipulação/Respostas:



NP-1

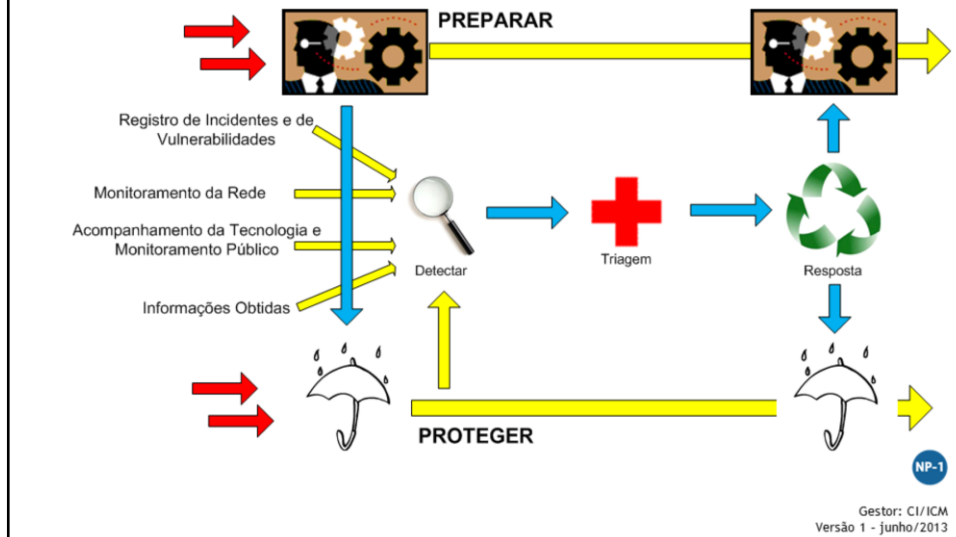
Gestor: CI/ICM
Versão 1 - junho/2013

A figura ilustra a relação entre os termos “Resposta à Incidentes”, “Manipulação de Incidentes” e “Gerenciamento de Incidentes”. A “Resposta a Incidentes” é uma das funções executadas na “Manipulação de Incidentes”, e a “Manipulação de Incidentes” é um dos serviços providos como parte do Gerenciamento de Incidentes.

Um artefato é qualquer arquivo ou objeto encontrado em um sistema que pode estar envolvido na varredura de sistemas e redes ou ataques para transpor medidas de segurança. Artefatos podem incluir, mas não estão limitados a vírus, cavalos de Tróia, worms, scripts maliciosos e toolkits.

Definições e Conceitos

■ Processo de Gerenciamento de Incidentes



O Processo de Gerenciamento de Incidentes é mais visível na tarefa de proteger o negócio referente à sua missão e a comunidade apoiada, mas a competência deste trabalho depende vitalmente da sua preparação. Além disso, é fundamental a existência de uma competente estrutura de controle, que proporcione o recebimento de *reports* de incidentes e da percepção da existência de vulnerabilidades, assim como o monitoramento contínuo da rede, o acompanhamento do estado da arte e das tendências extrínsecas, além da capacidade de se obter no ambiente indicativos de possíveis sintomas de incidentes. Estas entradas possibilitam a **DETECÇÃO** de anomalias, que devem passar por um processo de **TRIAGEM**, que indicarão a **RESPOSTA** mais adequada ao problema identificado. Este processo deve garantir o feedback tanto para a melhoria do processo de resposta a incidentes quanto dos controles existentes, visando evitar que os incidentes deste tipo voltem a ocorrer.

A **TRIAGEM** na verdade é um processo complexo e altamente especializado, onde são realizadas tarefas como ordenar, categorizar e priorizar os relatos recebidos, como forma de agrupá-los por afinidade e possibilitar a identificação precisa do incidente. Pode ser comparada a uma triagem feita em um hospital, onde os pacientes que precisam de tratamento emergencial são priorizados em relação aos casos com menor demanda de urgência e até mesmo falsos positivos através de uma técnica chamada de ANAMNESE, onde o médico procura sintomas decisivos. Você já assistiu "House" ?

Definições e Conceitos

■ Categorias de Serviços:

Serviços Reativos	Serviços Proativos	Gerenciamento da Qualidade da Seginfo
<ul style="list-style-type: none"> ➤ Emissão de alertas e avisos (warnings) ➤ Manipulação de incidentes <ul style="list-style-type: none"> ✓ Análise do incidente ✓ Resposta in-loco ✓ Suporte à resposta ✓ Coordenação da resposta ➤ Manipulação de Vulnerabilidades <ul style="list-style-type: none"> ✓ Análise de Vulnerabilidades ✓ Resposta às Vulnerabilidades ✓ Coordenação da Resposta às Vulnerabilidades ➤ Manipulação de Artefatos <ul style="list-style-type: none"> ✓ Análise do Artefatos ✓ Resposta à ação de Artefatos ✓ Coordenação da Resposta à ação de Artefatos 	<ul style="list-style-type: none"> ➤ Emissão de anúncios (Announcements) ➤ Auditorias e Análises de Segurança ➤ Configuração e Manutenção de ferramentas de Segurança e de Infra necessária ➤ Desenvolvimento ou aquisição de ferramentas de segurança ➤ Detecção de intrusos ➤ Disseminação de informações sobre Segurança da Informação 	<ul style="list-style-type: none"> ➤ Análises de Risco ➤ Continuidade dos Negócios e DRP ➤ Consultoria de Segurança ➤ Criação da Cultura de Segurança corporativa ➤ Treinamento e Educação ➤ Avaliação e Certificação de produtos

Gestor: CI/ICM
Versão 1 - junho/2013

Alertas e Warnings são ações reativas que orientam a comunidade a como reagir de acordo com uma ameaça como um vírus, ou uma vulnerabilidade detectada. Podem ser criados pelo GRIS ou redistribuídos a partir de outras fontes. A **Manipulação de Incidentes** envolve uma triagem inicial, respostas e análise das notificação de eventos e incidentes pela comunidade e externas. Esta reação pode, por exemplo, envolver ações objetivas para interromper o ataque, obter mais informações sobre a ameaça e reconstruir o ambiente original.

Análise de incidentes. Existem vários níveis de análise de incidentes. Essencialmente, é um exame de todas as informações disponíveis e as provas ou artefatos relacionados a um incidente ou evento de apoio. O objetivo da análise é a de identificar o âmbito de alcance do incidente, a extensão dos seus danos, a natureza do incidente e estratégias de resposta ou soluções disponíveis. Envolve dois sub-serviços:

Forense computacional - obtenção, preservação, documentação e análise de evidências a partir de um sistema computacional comprometido para determinar mudanças no sistema e para ajudar na reconstrução de eventos que levaram ao comprometimento; e Rastreamento das origens e caminhos utilizados por um intruso ou *malware*.

Resposta In-Loco: O próprio GRIS analisa fisicamente o sistema afetado e realiza a reparação e recuperação dos sistemas, ao invés de apenas fornecer apoio de resposta a incidentes por telefone ou e-mail.

Suporte à Resposta: O GRIS orienta a vítima do ataque na recuperando de um incidente via telefone , e-mail , fax, ou documentação.

Coordenação da Resposta: O GRIS coordena o esforço de resposta entre todos os envolvidos no incidente. Isso geralmente inclui a vítima do ataque, outros sites envolvidos no ataque e sites que necessitem de assistência na análise do ataque. Pode também incluir as partes que fornecem suporte de TI para a vítima, como provedores, outros GRIS e administradores de rede e sistemas no local. O trabalho de coordenação pode envolver a coleta de informações de contato, notificando partes de seu envolvimento potencial (como vítima ou fonte de um ataque), a captura de estatísticas sobre o número de locais envolvidos ou

Definições e Conceitos



■ Categorias de Serviços:

Serviços Reativos	Serviços Proativos	Gerenciamento da Qualidade da Seginfo
<ul style="list-style-type: none"> ➢ Emissão de alertas e avisos (warnings) ➢ Manipulação de incidentes <ul style="list-style-type: none"> ✓ Análise do incidente ✓ Resposta in-loco ✓ Suporte à resposta ✓ Coordenação da resposta ➢ Manipulação de Vulnerabilidades <ul style="list-style-type: none"> ✓ Análise de Vulnerabilidades ✓ Resposta às Vulnerabilidades ✓ Coordenação da Resposta às Vulnerabilidades ➢ Manipulação de Artefatos <ul style="list-style-type: none"> ✓ Análise de Artefatos ✓ Resposta à ação de Artefatos ✓ Coordenação da Resposta à ação de Artefatos 	<ul style="list-style-type: none"> ➢ Emissão de avisos (Anouncements) ➢ Auditorias e Análises de Segurança ➢ Configuração e Manutenção de ferramentas de Segurança e de Infra necessária ➢ Desenvolvimento ou aquisição de ferramentas de segurança ➢ Detecção de intrusos ➢ Disseminação da informações sobre Segurança da Informação 	<ul style="list-style-type: none"> ➢ Análises de Risco ➢ Continuidade dos Negócios e DRP ➢ Consultoria de Segurança ➢ Criação da Cultura de Segurança corporativa ➢ Treinamento e Educação ➢ Avaliação e Certificação de produtos

Gestor: CI/ICM
Versão 1 - junho/2013

Manipulação de vulnerabilidades envolve a recepção de informações e relatórios sobre vulnerabilidades de hardware e software; analisar a natureza, a mecânica operacional e os efeitos das vulnerabilidades. A partir disso, desenvolver estratégias de resposta para detectar e reparar as vulnerabilidades. Envolve:

Análise de Vulnerabilidades: Inclui a verificação de suspeita de vulnerabilidades e o exame técnico da vulnerabilidade em hardware ou software, para determinar onde a mesma se encontra e como ela pode ser explorada. A análise pode incluir a revisão do código fonte, usando um *debugger* para determinar onde ocorre a vulnerabilidade, ou tentando reproduzir o problema em um ambiente de teste.

Resposta às Vulnerabilidades: determinar e implementar a resposta adequada para mitigar ou reparar uma vulnerabilidade. Isso pode envolver o desenvolvimento ou a busca de patches, versões corrigidas e soluções alternativas. Envolve também notificar outros sobre a estratégia de mitigação, bem como a criação e distribuição de avisos ou alertas.

Coordenação da resposta: semelhante à resposta a incidentes.

Manipulação de Artefatos: envolve receber e analisar informações e cópias de artefatos que são usados em ataques de intrusão, reconhecimento e outras atividades não autorizadas. Isso inclui analisar a sua natureza e a mecânica de operação. Desenvolver ou obter estratégias de resposta para a detecção, remoção e na defesa contra esses artefatos. Envolve:

Análise de Artefatos: O GRIS realiza um exame técnico e análise de qualquer artefato encontrado num sistema. A análise feita pode incluir a identificação do tipo de arquivo e estrutura do artefato, a comparação de um novo artefato com artefatos conhecidos para ver semelhanças e diferenças, ou engenharia reversa / desmontagem de código para determinar a finalidade e função do artefato.

Resposta a ação de artefatos: Este serviço consiste em determinar as ações apropriadas para detectar e remover artefatos de um sistema, bem como ações para prevenir artefatos de serem instalados. Isso pode envolver a criação de assinaturas que podem ser adicionadas ao software antivírus e ao IDS.

Definições e Conceitos



■ Categorias de Serviços:

Serviços Reativos	Serviços Proativos	Gerenciamento da Qualidade da Seginfo
<ul style="list-style-type: none"> ➢ Emissão de alertas e avisos (warnings) ➢ Manipulação de incidentes <ul style="list-style-type: none"> ✓ Análise do incidente ✓ Resposta in-loco ✓ Suporte à resposta ✓ Coordenação da resposta ➢ Manipulação de Vulnerabilidades <ul style="list-style-type: none"> ✓ Análise de Vulnerabilidades ✓ Resposta às Vulnerabilidades ✓ Coordenação da Resposta às Vulnerabilidades ➢ Manipulação de Artefatos <ul style="list-style-type: none"> ✓ Análise de Artefatos ✓ Resposta à ação de Artefatos ✓ Coordenação da Resposta à ação de Artefatos 	<ul style="list-style-type: none"> ➢ Emissão de anúncios (Announcements) ➢ Auditorias e Análises de Segurança ➢ Configuração e Manutenção de ferramentas de Segurança e da Infra necessária ➢ Desenvolvimento ou aquisição de ferramentas de segurança ➢ Detecção de Intrusões ➢ Disseminação de informações sobre Segurança da Informação 	<ul style="list-style-type: none"> ➢ Análises de Risco ➢ Continuidade dos Negócios e DRP ➢ Consultoria de Segurança ➢ Criação da Cultura de Segurança corporativa ➢ Treinamento e Educação ➢ Avaliação e Certificação de produtos

Gestor: CI/ICM
Versão 1 - junho/2013

Coordenação da Resposta: Este serviço envolve o compartilhamento de resultados e estratégias de resposta referentes a um artefato com outros pesquisadores, GRIS, fornecedores e outros especialistas em segurança. As atividades incluem notificar outros e sintetizar análise técnica a partir de uma variedade de fontes. As atividades também podem incluir a manutenção de um arquivo público para a comunidade apoiada sobre artefatos conhecidos e seus impactos, bem como as correspondentes estratégias de resposta.

Os anúncios incluem - mas não estão limitados a - alertas, avisos de intrusão, vulnerabilidades ou ferramentas de intrusão descobertas. Os anúncios tem a intenção de possibilitar que a comunidade proteja seus sistemas e redes contra problemas recém-encontrados antes de poderem ser explorados.

A Auditoria oferece uma análise detalhada da segurança de uma organização, com base nos requisitos já definidos pela própria organização e/ou por normas de boas práticas. Há vários tipos diferentes de auditorias:

- revisão da infraestrutura crítica – verificação das configurações de hardware e software de roteadores, firewalls, servidores e dispositivos de desktop, para garantir que elas coincidam com as práticas organizacionais ou da indústria e configurações padrão
- entrevistas com usuários e administradores para determinar se suas práticas usuais correspondem à política de segurança organizacional definida ou normas específicas da indústria
- varredura de vulnerabilidades e vírus com scanners
- testes de penetração simulando o uso de técnicas reais. É importante que todas as auditorias sejam APROVADAS e APOIADAS pela alta direção, de forma que sejam vistas como instrumento de apoio e contribuição positiva, e não como uma forma de apontar erros e incompetências pontuais.

A configuração/manutenção de ferramentas de segurança identifica ou fornece orientações sobre a forma de configurar de forma segura e manter as ferramentas, aplicações e infraestrutura de computação em geral utilizadas pela comunidade apoiada e o próprio GRIS. Além de proporcionar orientação, o GRIS pode exercer atualizações de configuração e manutenção de ferramentas e serviços de segurança, como IDS, sistemas de monitoramento, filtros, firewalls, redes privadas virtuais (VPN), e mecanismos de autenticação. O GRIS também pode configurar e manter servidores, desktops, laptops, assistentes pessoais digitais (PDAs), celulares e outros dispositivos em função de acordo com as diretrizes de segurança.

Definições e Conceitos



■ Categorias de Serviços:

Serviços Reativos	Serviços Proativos	Gerenciamento da Qualidade da SegInfo
<ul style="list-style-type: none"> ➢ Emissão de alertas e avisos (warnings) ➢ Manipulação de incidentes <ul style="list-style-type: none"> ✓ Análise do incidente ✓ Resposta in-loco ✓ Suporte à resposta ✓ Coordenação da resposta ➢ Manipulação de Vulnerabilidades <ul style="list-style-type: none"> ✓ Análise de Vulnerabilidades ✓ Resposta às Vulnerabilidades ✓ Coordenação da Resposta às Vulnerabilidades ➢ Manipulação de Arquivos <ul style="list-style-type: none"> ✓ Análise de Arquivos ✓ Resposta à ação de Arquivos ✓ Coordenação da Resposta à ação de Arquivos 	<ul style="list-style-type: none"> ➢ Emissão de anúncios (Announcements) ➢ Auditorias e Análises de Segurança ➢ Configuração e Manutenção de ferramentas de Segurança e da Infra necessária ➢ Desenvolvimento ou aquisição de ferramentas de segurança ➢ Detecção de Intrusos ➢ Disseminação de Informações sobre Segurança da Informação 	<ul style="list-style-type: none"> ➢ Análises de Risco ➢ Continuidade dos Negócios e DRP ➢ Consultoria de Segurança ➢ Criação da Cultura de Segurança corporativa ➢ Treinamento e Educação ➢ Avaliação e Certificação de produtos

Gestor: CII/ICM
Versão 1 - junho/2013

O Desenvolvimento ou Aquisição de Ferramentas inclui qualquer ferramenta específica necessária ou desejada pela comunidade ou pelo próprio GRIS. Isso pode incluir, por exemplo, o desenvolvimento patches, *scripts* que ampliem a funcionalidade de ferramentas de já existentes, como um *plug-in* para um *scanner* de rede, *scripts* que facilitem o uso de criptografia ou a distribuição de *patches*.

Detecção de Intrusos – O GRIS revisa os logs de IDS existentes, analisam o conteúdo e iniciam uma resposta para quaisquer eventos que alcancem um limiar definido, ou então emitem um alerta de acordo com a estratégia adotada. Detecção e análise de intrusão a partir de logs de segurança pode ser uma tarefa trabalhosa, não só para determinar e localizar os sensores no ambiente, mas também a coleta e, em seguida, analisar as grandes quantidades de dados capturados. Em muitos casos, ferramentas e conhecimentos especializados são necessários para sintetizar e interpretar as informações para identificar alarmes, ataques, ou eventos de falso positivo/falso negativo e implementar estratégias para eliminar ou minimizar tais eventos. Algumas organizações optam por terceirizar essa atividade para outros que têm mais experiência na realização destes serviços.

Disseminação de Informações - Este serviço oferece à comunidade componentes com uma coleção abrangente e fácil de encontrar de grande utilidade, que auxilia na criação e manutenção da cultura de segurança. Tal informação pode incluir:

- Diretrizes para elaboração de relatos e informações de contato com o GRIS
- Arquivos de alertas, avisos e outras comunicações
- Documentação sobre as melhores práticas atuais
- Orientação de segurança geral do computador e seus sistemas
- Políticas, procedimentos e listas de verificação
- Informação sobre o desenvolvimento e distribuição de *patches*
- Sites de fornecedores e outras fontes de informação de segurança
- Estatísticas atuais e tendências de ocorrência de incidentes

Definições e Conceitos



■ Categorias de Serviços:

Serviços Reativos	Serviços Proativos	Gerenciamento da Qualidade da SegInfo
<ul style="list-style-type: none"> ➤ Emissão de alertas e avisos (warnings) ➤ Manipulação de incidentes <ul style="list-style-type: none"> ✓ Análise do incidente ✓ Resposta in-loco ✓ Suporte à resposta ✓ Coordenação da resposta ➤ Manipulação de Vulnerabilidades <ul style="list-style-type: none"> ✓ Análise de Vulnerabilidades ✓ Resposta às Vulnerabilidades ✓ Coordenação da Resposta as Vulnerabilidades ➤ Manipulação de Artefatos <ul style="list-style-type: none"> ✓ Análise de Artefatos ✓ Resposta à ação de Artefatos ✓ Coordenação da Resposta a ação de Artefatos 	<ul style="list-style-type: none"> ➤ Emissão de anúncios (Announcements) ➤ Auditorias e Análises de Segurança ➤ Configuração e Manutenção de ferramentas de Segurança e da infra necessária ➤ Desenvolvimento ou aquisição de ferramentas de segurança ➤ Detecção de Intrusos ➤ Disseminação de informações sobre Segurança da Informação 	<ul style="list-style-type: none"> ➤ Análises de Risco ➤ Continuidade dos Negócios e DRP ➤ Consultoria de Segurança ➤ Criação da Cultura de Segurança corporativa ➤ Treinamento e Educação ➤ Avaliação e Certificação de produtos

Gestor: CI/ICM
Versão 1 - junho/2013

Aproveitando a experiência adquirida na prestação dos serviços reativos e proativos descritos, um GRIS pode vislumbrar serviços de gestão que possam não estar ainda disponíveis. Estes serviços de gerenciamento da qualidade são projetados para incorporar o *feedback* e as lições aprendidas com base no conhecimento adquirido respondendo a incidentes, vulnerabilidades e ataques.

Análises de Risco – O GRIS pode ser capaz de agregar valor à análise e avaliação de riscos. Isto pode melhorar a capacidade da organização para avaliar ameaças reais e fornecer avaliações mais realistas dos riscos para ativos de informação qualitativas e quantitativas e avaliar as estratégias de proteção e resposta propostas.

Continuidade dos Negócios e DRP - Com base em ocorrências passadas e futuras previsões de tendências de ocorrência de incidentes de segurança, mais e mais incidentes têm o potencial para resultar em grave degradação das operações do negócio. Portanto, o planejamento deve considerar a experiência do GRIS para determinar a melhor forma de responder a esses incidentes e garantir a continuidade das operações de negócios.

Consultoria de Segurança – O GRIS pode ser usado para fornecer aconselhamento e orientação à Direção sobre as melhores práticas de segurança para implementar para as operações comerciais da corporação. A prestação deste serviço pelo GRIS está envolvida na preparação de recomendações ou identificação de requisitos para aquisição, instalação, ou captação de novos sistemas, dispositivos de rede, aplicações de software, ou de desenho de novos processos de negócios em toda a empresa. Este serviço inclui o fornecimento de orientação e assistência no desenvolvimento de políticas de segurança organizacionais.

Definições e Conceitos



■ Categorias de Serviços:

Serviços Reativos	Serviços Próativos	Gerenciamento da Qualidade da Seginfo
<ul style="list-style-type: none"> ➢ Emissão de alertas e avisos (warnings) ➢ Manipulação de incidentes <ul style="list-style-type: none"> ✓ Análise do incidente ✓ Resposta in-loco ✓ Suporte à resposta ✓ Coordenação da resposta ➢ Manipulação de Vulnerabilidades <ul style="list-style-type: none"> ✓ Análise de Vulnerabilidades ✓ Resposta às Vulnerabilidades ✓ Coordenação da Resposta às Vulnerabilidades ➢ Manipulação de Artefatos <ul style="list-style-type: none"> ✓ Análise de Artefatos ✓ Resposta à ação de Artefatos ✓ Coordenação da Resposta à ação de Artefatos 	<ul style="list-style-type: none"> ➢ Emissão de anúncios (Announcements) ➢ Auditorias e Análises de Segurança ➢ Configuração e Manutenção de ferramentas de Segurança e de Infra necessária ➢ Desenvolvimento ou aquisição de ferramentas de segurança ➢ Detecção de Intrusos ➢ Disseminação de informações sobre Segurança da Informação 	<ul style="list-style-type: none"> ➢ Análises de Risco ➢ Continuidade dos Negócios e DRP ➢ Consultoria de Segurança ➢ Criação da Cultura de Segurança corporativa ➢ Treinamento e Educação ➢ Avaliação e Certificação de produtos

Gestor: CI/ICM
Versão 1 - junho/2013

Criação de Cultura Corporativa – O GRIS pode ser capaz de identificar onde a comunidade precisa de mais informações e orientação para estar em conformidade com as práticas de segurança aceitas e as políticas de segurança da organização. Visa aumentar a conscientização da comunidade da segurança em geral, não só melhorando a sua compreensão das questões de segurança, mas também ajudando a realizar suas operações do dia-a-dia de uma maneira mais segura. Isto pode reduzir a ocorrência de ataques bem sucedidos e aumentar o probabilidade de que os membros da comunidade vão detectar e relatar ataques proativamente, diminuindo assim o tempo de recuperação e eliminar ou minimizar as perdas. Com o GRIS realizando este serviço, a empresa busca oportunidades para aumentar a sensibilização para a segurança através da produção de artigos, cartazes, boletins informativos, sites ou outros recursos que apresentem as melhores práticas de segurança e prestem aconselhamento sobre as precauções a tomar. As atividades podem incluir o agendamento de reuniões e seminários para manter componentes atualizados com cursos sobre procedimentos de segurança e potenciais ameaças aos sistemas organizacionais.

Treinamento e Educação - Este serviço envolve a prestação de informações aos membros da comunidade sobre questões de segurança através de seminários, *workshops*, cursos e palestras. Os tópicos podem incluir relatórios de incidentes, orientações de outros GRIS, métodos de resposta adequados, ferramentas de resposta a incidentes, métodos de prevenção de incidentes e outras informações importantes para proteger, detectar, relatar e responder a incidentes de segurança.

Avaliação e Certificação de Produtos - Para este serviço, o GRIS poderá realizar avaliações de produtos, ferramentas, aplicações, ou outros serviços para garantir a segurança na operação destes produtos e sua conformidade com as práticas de segurança da organização. Ferramentas e aplicativos de avaliação podem ser de código aberto ou produtos comerciais. Este serviço pode ser fornecido como uma avaliação avulsa ou através de um programa de certificação, de acordo com as normas que são aplicadas pela organização ou pelo GRIS.

Definições e Conceitos

- Outros Termos Importantes:
 - IRT = Incident Response Team
 - IRC = Incident Response Capability
 - IHT = Incident Handling Team
 - IMT = Incident Managing / Management Team
 - CSIRT = Computer/Cyber Security Incident Response Team
 - CIRT = Computer Incident Response Team
 - CIRC = Computer Incident Response Capability or Center
 - SIRT = Security Incident Response Team
 - SERT = Security Emergency Response Team

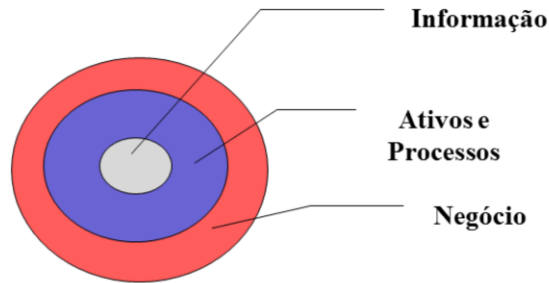
NP-1

Gestor: CI/ICM
Versão 1 - junho/2013

Estas formas alternativas serão encontradas na bibliografia sobre o tema.

Definições e Conceitos

- O GRIS deve definir suas ações em função dos ativos de TI ?



Na verdade, o foco deve ser no NEGÓCIO. No entanto, é fato que muitas corporações atuais são altamente sensíveis à incidentes com comprometimento da CID da informação. Equivocadamente, as referências usadas como base para a criação de estruturas de proteção, como Firewalls, IDS e outros são elaboradas por técnicos, sem conhecimento do negócio, tornando o produto final essencialmente focado nos ativos e em sua recuperação. Devemos evitar isso.

Classificação dos Incidentes



- Quanto ao Tipo:
 - **Negação de Serviço (Indisponibilidade)**
 - Utilização indevida dos recursos da rede e de sistemas, levando à impossibilidade de atender solicitações legítimas
 - **Código Malicioso (Integridade)**
 - Vírus, Worms, Trojan horse, exploits, etc.
 - **Acesso não autorizado (Confidencialidade)**
 - Pessoas sem permissão ganham acesso físico ou lógico à rede, sistemas, aplicativos, ambientes, outros recursos/locais
 - **Uso indevido de recursos (CID)**
 - Violação da Política de Segurança por pessoas direta ou indiretamente envolvidas
 - **Diversos**
 - Combinação de 2 ou mais tipos de incidentes

NP-1

Gestor: CII/ICM
Versão 1 - junho/2013

A Negação de Serviço (*Deny of Service – DoS*) é um ataque à DISPONIBILIDADE, que pode tanto ser feito através da sobrecarga de aplicações, como um servidor WEB que recebe mais requisições do que pode suportar, ou também da sobrecarga da rede de destino, com o envio massivo de mensagens que necessariamente terão que ser processadas, como por exemplo de *broadcasts*. É de difícil contorno, tanto que recentemente todos os bancos nacionais foram vítimas de ataques do grupo *Anonymous* em represália às leis internacionais SOPA e PIPA, tendo suas operações online interrompidas por horas.

Vírus são códigos maliciosos que são propagados anexos a arquivos contaminados. Ao serem executados, se propagam através da contaminação de outros arquivos no ambiente do hospedeiro. Apenas se propagam SE forem executados, logo, dependem da ação humana.

Worms são códigos maliciosos que se propagam pela rede sem a demanda de serem executados, fazendo uso de vulnerabilidades existentes nos sistemas e aplicações, especialmente as chamadas *zero-day*. *Zero-day* são vulnerabilidades ainda desconhecidas pelo público em geral e muitas vezes pelo próprio comerciante do software, portanto, não possuem correções disponíveis.

Trojan Horse (cavalo de tróia) é um tipo de *malware* que é intencionalmente aderido a um arquivo legítimo e enviado a um usuário-alvo. Ao usuário executar o arquivo, o *trojan* é executado em seguida cumprindo sua função, que pode ser a instalação de um *rootkit*, *backdoor*, *keylogger* ou qualquer outra atividade maliciosa.

Exploits são códigos desenvolvidos especificamente para explorar vulnerabilidades conhecidas em uma determinada aplicação.

O Controle do Acesso não autorizado é dependente da prévia CLASSIFICAÇÃO dos recursos críticos da organização. Após isso, e uma DIVULGAÇÃO eficaz dos papéis e responsabilidades de todos com relação à segurança é que se pode controlar o acesso.

O mesmo comentário vale para a CID, já que a definição de criticidade de cada informação é que permite avaliar as demandas de CID.

Classificação dos Incidentes



■ Quanto a Severidade:

- Alerta 1
 - Falso Positivo
- Alerta 2
 - Ocorrência de evento (sem consequências)
- Alerta 3
 - Ocorrência do evento com consequências suportáveis, dentro dos critérios de aceitação (ex. propagação de vírus controlada)
- Alerta 4
 - Ocorrência do evento com consequências próximas dos critérios de aceitação (ex. servidor com *malware* instalado, porém aparentemente sem danos à CID)
- Alerta 5
 - Ocorrência do evento com consequências Altas (ex. Servidor de Banco de Dados fora do ar)

Obs.: A classificação dos Incidentes poderá mudar de acordo com o cenário de cada empresa e deverá levar em consideração o histórico dos incidentes da organização!

NP-1

Gestor: CII/ICM
Versão 1 - junho/2013

Esta classificação sugerida é um reflexo da demanda por uma rápida e útil identificação do problema, de forma a agilizar as ações de resposta.

Severidade de um incidente é uma avaliação isolada do mesmo, independente da sua abrangência. A Criticidade é um conceito mais amplo, onde a abrangência do incidente é avaliada, além de sua severidade, mas é uma análise mais demorada de ser realizada. Assim, podemos dizer que: $C \text{ (criticidade)} = E \text{ (efeito / severidade)} + A \text{ (Abrangência)}$, e usar parâmetros como:

Efeito no Sistema (Severidade):

- 1 - Suportável
- 2 - Moderado
- 3 - Catastrófico / Alto

Abrangência:

- 1 - Local
- 2 - Em uma área da empresa
- 3 - Em toda a empresa

Pré-Requisitos



- Todos os GRIS devem possuir as mesmas Características, Estrutura e Formação?



Comunicação relacionada à
Incidentes com parceiros
externos

NP-1

Gestor: CI/ICM
Versão 1 - junho/2013

Conforme já ilustrado até aqui, um GRIS é fruto de uma demanda específica de uma comunidade, de sua cultura de segurança e da sensibilidade das informações e dos processos da organização. Por isso, o cenário existente em uma corporação dificilmente se repetirá em outras organizações, então a construção do GRIS deve ser particularizada.

Pré-Requisitos



- Então o que levar em consideração na criação do GRIS ?
 - Missão, Visão e Objetivos do GRIS
 - Tipo/Natureza e Escopo dos serviços prestados pelo GRIS
 - Experiência/conhecimentos necessários para formação da Equipe
 - Tamanho e abrangência da organização → tamanho do GRIS
 - Classificação dos Incidentes por Níveis de Criticidade
 - Patrocinadores/*Stakeholders*
 - Natureza do Negócio
 - Leis, Normas e Regulamentos

NP-1

Gestor: CII/ICM
Versão 1 - junho/2013

Após um intenso levantamento inicial voltado para definir a estrutura e os processos do GRIS, iniciamos a sua construção.

Stakeholder (parte interessada) é qualquer indivíduo ou grupo com interesse – ainda que subjetivo e inconsciente – no sucesso do GRIS e sua missão. As partes interessadas podem ser aqueles que se reportarão ao GRIS, receber a sua ajuda, fornecer financiamento e patrocínio para o GRIS, ou representar uma interface com o GRIS através da partilha de informação ou a coordenação da atividades de manipulação de incidentes e vulnerabilidades.

O Processo de criação do GRIS



■ Tópicos para Reflexão!

- Qual o verdadeiro papel do GRIS ?
 - Tratamento do Incidente?
 - Apenas como identificador do incidente?
 - Apenas como Controlador/Mantenedor da SegInfo ?
- Qual deve ser o tamanho e *expertise* da Equipe?
- Qual a previsão de custo para implementação e manutenção
 - Manter equipe capacitada em TI e Negócio
- Em que posição deve estar localizado na hierarquia da organização?
- Quem apoiará o processo? Quem são as partes interessadas ?
- De que forma o GRIS irá contribuir para o negócio da organização ?

NP-1

Gestor: CI/ICM
Versão 1 - junho/2013

Estas questões devem ser tratadas com cuidado e profundidade, porque é a questão chave da busca de um GRIS atuante e competente. É importante que a estrutura atenda às expectativas do negócio e que seja reconhecido como útil para o NEGÓCIO da corporação.

O Processo de Criação do GRIS



■ As Macro Etapas:

- Fase 1: Identificar e obter o apoio e a aprovação dos *Stakeholders* / Patrocinadores
- Fase 2: Levantamento de Informações
- Fase 3: Planejamento Estratégico do GRIS
- Fase 4: Implantação
- Fase 5: Campanha de divulgação do GRIS
- Fase 6: Avaliações e Métricas

NP-1

Gestor: CI/ICM
Versão 1 - junho/2013

São fases aparentemente sequenciais, mas que podem ter alto nível de superposição. O levantamento de informações, por exemplo, deve ser contínuo e forte indicador da demanda de mudança de rumos para o GRIS. A Divulgação do GRIS também deve ser contínua.

O Processo de Criação do GRIS



■ Fase 1: Identificar e obter o apoio e a aprovação dos Stakeholders/patrocinadores

- Carta de compromisso da Alta Direção
- Termo de Compromisso dos Envolvidos no Processo
- Identificar claramente as forças envolvidas (Positivas e Negativas)
- Possíveis Stakeholders (Partes Interessadas)
 - Diretores/Gerentes de negócios
 - Gerentes/Coordenador de TI
 - Gerente/Coordenador de RH
 - Representante(s) do departamento jurídico
 - Representantes da Organização
 - Equipe de Auditoria
 - Equipe de Segurança
 - Representantes das áreas que serão atendidas pelo GRIS

NP-1

Gestor: CI/ICM
Versão 1 - junho/2013

1) Identificar Stakeholders. **A)** Determinar quem precisa estar envolvido em cada nível do planejamento, implementação e operação do GRIS. **B)** Determinar quem é servido ou apoiado pelo GRIS. **C)** Identificar as pessoas com quem você vai coordenar ou compartilhar informações, tanto dentro como fora da organização. **D)** Identificar as pessoas que desempenham funções de segurança ou de resposta a incidentes e envolvê-los. **E)** Identificar as organizações internas e externas que podem interagir com ou participar do GRIS. Os problemas mais comuns a evitar: uma ampla gama de interessados e participantes não são identificados e incluídos na fase de planejamento e desenvolvimento; incapacidade de identificar e compreender onde as atividades de resposta a incidentes de segurança acontecem e como isso irá mudar com os planos para a implementação de um GRIS.

2) Obter apoio à gestão e patrocínio. **A)** Encontre um gerente executivo para patrocinar e defender o estabelecimento do GRIS com boa ligação a outros gerentes do negócio da organização. **B)** Apresentar um caso de negócios descrevendo os benefícios que o GRIS vai trazer para a organização. **C)** Obter recursos para o tempo em que a equipe irá passar fazendo pesquisa e coleta de informações durante o processo de planejamento. **D)** Na fixação de um GRIS dentro de uma organização, explicar as ideias, conceitos e benefícios para outros gestores de processos de negócio. **E)** Requisitar à alta direção o anúncio da formação do GRIS com a recomendação que todos forneçam informações quando necessário durante o planejamento e implementação. Os problemas mais comuns a evitar: as partes interessadas, os participantes, gerentes de negócios e parceiros estratégicos não estão cientes de que um GRIS está sendo planejado.

3) Desenvolver um plano de projeto para o GRIS. **A)** Formar uma equipe de projeto para ajudar a planejar e estabelecer o GRIS. **B)** Nomear um líder do projeto, que vai informar a administração sobre o andamento do planejamento. **C)** Aplicar os conceitos de gerenciamento de projetos para a tarefa de criar um GRIS. Os problemas mais comuns: a equipe do projeto não envolve um conjunto diverso de partes interessadas; não é estabelecido um prazo razoável para a conclusão do projeto - muitas vezes os calendários são muito curtos ou irreais para um GRIS se tornar plenamente funcional; um líder de projeto competente não é escolhido e o projeto definitivamente não chega à conclusão.

O Processo de Criação do GRIS



■ Fase 2: Levantamento de Informações

- Obter histórico de incidentes
- Mapear os Serviços e Estrutura da Organização
- Quantificar, e possivelmente identificar os profissionais que tenham o perfil para participar do Projeto
- Realizar reuniões com os envolvidos para discutir ideias, alinhar as expectativas e responsabilidades. Sempre que possível envolver as partes interessadas
- Recursos relevantes:
 - Organogramas da empresa e das áreas de negócio
 - Infraestrutura de TI (topologia da rede, sistemas, provedores, etc.)
 - Inventários dos sistemas e recursos, classificados de acordo com a criticidade
 - Planos de DRP/continuidade dos negócios existentes
 - Normas para comunicar violações de segurança física e Lógica já existentes
 - Informação sobre eventuais GRIS já existentes
 - Leis, Normas e Regulamentos aos quais a organização esteja sujeita
 - Políticas, Normas e Procedimentos de SegInfo existentes

NP-1

Gestor: CII/ICM
Versão 1 - junho/2013

4) Reunir informações . A) Manter conversas com uma variedade de partes interessadas para: i. determinar as necessidades e exigências da comunidade e qualquer entidade hierarquicamente superior. ii. coletar informações sobre os tipos de incidentes e eventos que já ocorreram para estudar os serviços que o GRIS precisará fornecer. iii. conhecer qualquer gerenciamento de incidentes que já esteja ocorrendo. iv. compreender o mercado, empresas ou questões jurídicas, culturais que definem o ambiente em que o GRIS vai operar. v. compreender questões de propriedade de dados e intelectual, relacionadas a qualquer tipo de publicações, produtos ou informações obtidas ou produzidas pelo GRIS. **B)** Definir as questões políticas e de *compliance*, incluindo toda legislação pública, privada, acadêmica, de governo, militar, regulamentos e políticas que devem ser seguidas. **C)** Entenda a história anterior. i. descobrir se alguém já tentou criar um GRIS na organização. Se sim, descobrir o que aconteceu e verificar se há qualquer informação que possa ser usada. ii. Identificar quaisquer expectativas da organização para o GRIS, com base nesta atividade anterior. iii. Determinar há um domínio disponível (ou seja, se o GRIS terá o seu próprio nome de domínio). Se o nome ideal estiver disponível, obtê-lo o mais rapidamente possível. Os problemas mais comuns: o GRIS não envolver ou recolher contribuições de todos os interessados; há divergências sobre quem são os proprietários dos dados, causando atrasos no fornecimento de informações para o GRIS.

O Processo de Criação do GRIS



■ Fase 3: Planejamento Estratégico do GRIS

- Conceber a Missão, a Visão e os Objetivos
- Desenvolvimento do Projeto com *milestones* para a Equipe
- Questões administrativas e processuais de Gerência do Projeto ou de TI
- Planejar a equipe e os envolvidos (direta e/ou indiretamente)
 - Ter sempre substitutos definidos para cada responsável por uma função relevante
- Canais de Comunicação / Divulgação
 - Determinar a melhor forma de obter apoio da organização
 - Facilitar a interação entre departamentos
- Definir o armazenamento das informações
 - Dependerá da estrutura adotada

NP-1

Gestor: CII/ICM
Versão 1 - junho/2013

5) Identificar a Comunidade apoiada. **A)** Determine grupo de indivíduos, setores ou organizações ao qual o GRIS fornecerá serviços e suporte. **B)** Identificar quais os tipos de serviços que o GRIS irá fornecer. Por exemplo, os serviços prestados ao público em geral podem ser diferentes dos serviços prestados a organizações governamentais ou em infraestruturas críticas. **C)** Identificar e estabelecer parcerias estratégicas, se necessário. Parceiros estratégicos podem **i.** ajudar a orientar as prioridades do GRIS, e ajudar a definir e amadurecer suas capacidades e serviços. **ii.** participar na partilha de informação e pesquisa. **iii.** participar de interações personalizadas com o GRIS. **iv.** ajudar a aumentar a visibilidade e influenciar positivamente a equipe. **v.** ajudar a promover a adoção e uso das melhores práticas de segurança em toda a empresa. **D)** Identificar como os membros da comunidade apoiada obterão serviços do GRIS. **E)** Identificar serviços que o GRIS pode não suportar inicialmente, mas que poderá fornecer após estar operacional e pronto para expandir seus serviços. Os problemas mais comuns: nem todos os membros da comunidade são identificados ou definidos, não possuindo uma Interface formal com o GRIS; o GRIS não cria adequadamente uma visão dos benefícios que seus serviços podem fornecer para a comunidade definida; não está claro como a comunidade deve contatar o GRIS e obter assistência; o GRIS tenta apoiar muitos e diversos públicos durante a sua inicialização, sofrendo sobrecarga.

6) Definir a missão do GRIS. **A)** Determinar a missão do GRIS, que deve ser de longo prazo e de natureza geral. A missão não deve mudar muito ao longo do tempo, por isso deve ser escrita ampla o suficiente para acomodar qualquer alteração nos serviços ou funções enquanto a finalidade e função do GRIS ainda estão definidos de forma sucinta. A declaração de missão deve fornecer um valor tanto para comunidade apoiada quanto às instâncias hierarquicamente superiores. **B)** Determinar os objetivos primários e os objetivos do GRIS. Estes serão mais práticos e podem ser mudados conforme o GRIS amplia seu escopo ou serviços. **C)** Obter um acordo em relação à missão de todas as partes interessadas (por exemplo, área de gestão, comunidade apoiada, colaboradores e funcionários); garantir que todos entendem a missão. Os problemas mais comuns: o Staff do GRIS NÃO entende a Missão e a "Mission Creep" (fuga da missão) ocorre. O GRIS perde o foco em seu objetivo e torna-se menos Eficaz; interesses particulares ou políticos

O Processo de criação do GRIS



■ Fase 3: Planejamento Estratégico do GRIS (cont.)

- Alinhar as expectativas com as partes envolvidas e com os clientes (usuários internos, externos, terceiros, etc.)
- Comunicar com antecedência a Visão, Missão e os Objetivos
 - Pode ajudar a identificar problemas no processo
 - Permite um *feedback* antes da operacionalização do processo
 - Inicia o marketing do Grupo
- O que levar em consideração na criação da Visão:
 - Identificar a comunidade a ser atendida. A quem o GRIS presta serviços e suporte ?
 - Definir a missão e os objetivos do GRIS. O que o GRIS faz para a comunidade a qual ele atende ?
 - Como o GRIS dará suporte à sua missão ?
 - Determinar o modelo organizacional. Como o GRIS é estruturado e organizado ?
 - Identificar os recursos necessários. Que pessoal, equipamentos e infraestrutura são necessários para operar o GRIS ?
 - Determinar o modelo de financiamento do GRIS na fase de implantação e durante as fases de crescimento e manutenção a longo prazo?

NP-1

Gestor: CII/ICM
Versão 1 - junho/2013

7) Assegurar financiamento para as operações do GRIS. A) Obter recursos para o *startup*, ações de curto e longo prazo. Inclui: **i.** pessoal para o *staff* inicial, treinamento e aprimoramento profissional. **ii.** equipamentos, programas e infraestrutura para detectar, analisar, acompanhar e responder aos incidentes. **iii.** instalações protegidas para o pessoal do GRIS. **B)** Definir o modelo de financiamento para o GRIS. Os problemas mais comuns: O GRIS pode perder a eficácia por não poder financiar esforços para a equipe manter-se atualizada com as tecnologias emergentes, ou não permitindo que a equipe participe de cursos para melhorar suas habilidades e conhecimentos; isso pode fazer a equipe perder capacidade de lidar com as novas ameaças, ataques e riscos que afetem sua missão.

8) Decidir sobre o alcance e nível de serviços que o GRIS oferecerá. A) Começar pequeno e crescer. Ser realista sobre o tipo e número de serviços que o GRIS pode prestar em função das competências e recursos existentes. **B)** Determinar os serviços que o GRIS irá fornecer, e identificar em que parte da comunidade será oferecido. **C)** Definir o processo de entrega de serviços, como o horário de funcionamento, formas de entrar em contato e métodos para a difusão de informações. Os problemas mais comuns: o GRIS é acionado para serviços não oferecidos; O GRIS tenta oferecer muitos serviços, e alguns não são prioritariamente necessários, ou outra organização já está oferecendo; não prestação de serviços efetivamente necessários.

9) Determinar a estrutura, autoridade e modelo organizacional de relacionamento do GRIS. A) Determine onde o GRIS vai se encaixar na estrutura organizacional. Por exemplo, um em nível nacional, o GRIS pode funcionar no governo, como uma entidade nacional autônoma, ou como parte de outra organização. Se for colocado dentro de outra organização, como ele será percebido pela comunidade apoiada ? **B)** Criar um organograma e mantê-lo atualizado. **C)** Determinar se o GRIS deve relatar acima de sua hierarquia para outra organização. **C)** Preparar-se para educar as pessoas sobre o trabalho que o GRIS será capaz de fazer. Membros do GRIS podem precisar “diplomaticamente” recusar algumas solicitações de trabalho e deve preparar respostas adequadas para tal. Os problemas mais comuns: atribuições não-GRIS são impostas por agentes externos comprometendo o desempenho eficaz de serviços normais.

Fase 4: Implantação



■ Fase 4: Implantação

- Com base no Planejamento, executar:
 - Contratar e/ou capacitar a equipe responsável
 - Comprar equipamentos e software
 - Montar a infraestrutura necessária para dar suporte ao grupo, como Notebook, salas, telefones, câmeras para monitoramento, etc.
 - Desenvolver as políticas e procedimentos para o GRIS, de maneira a dar suporte aos serviços
 - Definir as especificações para os Plano de Gerenciamento de Incidentes e implementá-los
 - Desenvolver recomendações e formulários para o acompanhamento/tratamento dos incidentes
 - Executar as demais tarefas pré-estabelecidas no Planejamento Estratégico.

NP-1

Gestor: CII/ICM
Versão 1 - junho/2013

10) Identificar os recursos necessários, tais como pessoal, equipamentos e infraestrutura. A) Determine como a infraestrutura do GRIS será protegida, segura e monitorada, especialmente as instalações físicas e repositórios de dados. **B)** Definir processos para a obtenção, registro, acompanhamento e arquivamento de informações. **C)** Criar descrições de trabalho que listem as competências necessárias para cada função no GRIS. **D)** Criar um plano de orientação e formação para o pessoal, garantindo que todas as competências necessárias estão disponíveis. **E)** Determinar os requisitos para verificação de pessoal, como de antecedentes e certificações. Os problemas mais comuns: não ter substitutos para as funções; não são dadas oportunidades aos funcionários para o desenvolvimento profissional ou de carreira, resultando em desmotivação e rotatividade de pessoal; pessoal não-qualificado responsável por atividades-chave.

11) Definir interações e interfaces. A) Identificar as interações e interfaces com peças-chave da comunidade, as partes interessadas, e com eventuais parceiros internos ou externos, colaboradores, ou terceiros. **B)** Determine com quais outros elementos o GRIS compartilhará a coordenação. **C)** Identificar quais são os fluxos de informação entre esses elementos. **D)** Definir e estabelecer interfaces e métodos de colaboração e comunicação com as outras entidades, incluindo a aplicação da lei, como fornecedores, provedores de componentes da infraestrutura crítica, provedores de serviços de internet (ISPs). **E)** Verifique se há bons métodos para comunicação interna entre os membros do GRIS. **F)** Por todas essas interfaces, entender: **i.** quem é o proprietário dos dados que são compartilhados. **ii.** quem tem autoridade e responsabilidade dos dados. **iii.** como os dados são compartilhados e com quem eles são compartilhados. **iv.** como os dados são protegidos, controlados e armazenados de forma segura. **G)** Definir métodos para divulgar informações para a comunidade e *stakeholders* relevantes. **H)** Desenvolver e divulgar documentos padrão para a divulgação de informações para a comunidade apoiada. Os problemas mais comuns: dados não são compartilhados de forma controlada e segura, resultando em quebra de confidencialidade; interfaces não estão formalmente estabelecidas, causando atraso no processo de resposta quando é necessário escalar ou a partilha de dados e a coordenação da resposta.

O Processo de Criação do GRIS



■ Fase 5: Campanha de divulgação do GRIS

- Envolver RH e Marketing
 - Folhetos, Brindes, GRIS Day, Palestras, etc.
- Comunicar a Missão, Visão e Princípios à Organização e às Partes interessadas
- Divulgar Carta de Compromisso da Alta Direção
- Uso da Intranet para divulgar elementos de contato no GRIS, telefones para reportar incidentes, Disque-denúncia anônimo, etc.

NP-1

Gestor: CII/ICM
Versão 1 - junho/2013

12) Definir os papéis, responsabilidades e autoridade correspondente. **A)** Desenvolver papéis e responsabilidades para todas as funções do GRIS. **B)** Definir e desenvolver as interfaces entre elementos do GRIS e externos. **C)** Identificar áreas onde a autoridade pode ser ambígua ou sobreposta, e definir funções e papéis entre os grupos. Os problemas mais comuns: as pessoas não sabem onde termina o seu papel e de outra pessoa começa; mais de um grupo recebe a mesma responsabilidade, ou a ninguém é dada uma responsabilidade específica e a tarefa não é concluída.

13) Documentar o fluxo de trabalho. **A)** Criar um diagrama (modelo gráfico, fluxograma, etc.) para documentar os processos e interações do GRIS, incluindo quem executa o trabalho e onde no processo as interfaces e *handoffs* devem ocorrer. **B)** Construir medidas e componentes de garantia da qualidade nos processos e fluxos de trabalho do GRIS. Problemas comuns: membros desconhecem como seguir determinados processos ou executar várias atividades de coordenação e colaboração.

14) Desenvolver políticas e procedimentos correspondentes. **A)** Estabelecer definições para a terminologia (por exemplo, é um "evento de segurança" ou "incidente de segurança" ?), juntamente com outros termos exclusivos para a organização. **B)** Determine categorias de incidentes, prioridades e critérios de escalação. **C)** Identificar as políticas e os procedimentos iniciais que precisam ser formalizados antes do início da operação do GRIS, e aqueles que podem ser criados após o GRIS estar operacional. **D)** Desenvolver orientações para a comunidade apoiada relatar incidentes e formas de divulgá-los. **E)** Definir e documentar os critérios para a prestação de serviços do GRIS para garantir processos confiáveis e repetíveis seguidos fielmente pela equipe. Os problemas mais comuns: definições comuns não são compartilhadas entre o GRIS e a comunidade, resultando em confusão e mal-entendidos; incapacidade para resumir dados sobre as tendências de incidentes, porque não há uma definição clara dos termos; falta de formalização de políticas podem atrasar o tempo de resposta, porque os processos devem ser definidos ao mesmo tempo que o incidente ocorre. 33

O Processo de Criação do GRIS



■ Fase 6: Avaliação e Métricas

- Benchmarking entre o seu e outros GRIS
- Criar padrões de Qualidade e Controle
- Questionário de Qualidade de Atendimento periódico
- Criar um critério para avaliar a evolução da equipe
- Métricas básicas
 - % de incidentes reportados
 - % de incidentes resolvidos com sucesso
 - % de incidentes não resolvidos
 - tempo médio de resposta
 - % de capacitação da equipe

NP-1

Gestor: CII/ICM
Versão 1 - junho/2013

15) Criar um plano de implementação e solicitar feedback. **A)** Obter demandas para o plano de implementação das partes interessadas e a comunidade apoiada (eventualmente, outros peritos em GRIS), para pedir as suas observações, e garantir que o plano atenda a missão. **B)** Atualizar e melhorar o plano com base em feedback. **C)** Obter apoio e suporte da comunidade apoiada para a implementação. Os problemas mais comuns: a comunidade não está informada sobre a execução do GRIS e não fornece suporte, o que pode resultar em incidentes não sendo reportados ao GRIS ou conselhos e recomendações do GRIS não sendo seguidas; o plano não é enviado para análise, resultando em um plano que não é suportado por não estar apoiado pela alta direção.

16) Anunciar o GRIS quando estiver operacional. **A)** Solicite à alta direção para fazer um anúncio formal. **B)** Divulgue materiais de marketing e as diretrizes para relato de incidentes, explicando como a comunidade deve interagir com o GRIS. **C)** Incorporar nos programas de treinamento da empresa a orientação sobre os serviços de GRIS e as formas de interação. **D)** Encontrar maneiras de divulgar informações sobre os serviços do GRIS, como intranets organizacionais, web sites, artigos, seminários e aulas de treinamento. Os problemas mais comuns: o GRIS não é formalmente anunciado, e ninguém sabe como ele funciona ou como fazer a interface com a equipe.



17) Definir métodos para avaliar o desempenho do GRIS. **A)** Identificar o modelo para comunicação e resposta à incidentes existente antes do GRIS ser implementado. Use este modelo para comparar o desempenho após o GRIS estar operacional. **B)** Definir critérios de medição e os parâmetros de garantia de qualidade para que o GRIS possa ser medido de uma forma consistente. **C)** Definir métodos para obtenção de feedback da comunidade apoiada. **D)** Implementar procedimentos de relatórios e auditoria para garantir que o GRIS execute seus processos de forma eficiente e atende acordos de nível de serviço ou métricas de desempenho estabelecidas. Os problemas mais comuns: não há métodos instituídos para avaliar se o GRIS cumpre sua missão; métodos para a melhoria de processos não são implementadas; métricas de desempenho não medem adequadamente o desempenho do GRIS.

18) Tenha um plano de backup para cada elemento do GRIS. **A)** Identificar as principais funções, serviços e equipamentos críticos do GRIS. **B)** Projete um plano de recuperação de desastres e continuidade de negócios para serviços e processos críticos do GRIS; **C)** Planejar o que vai acontecer se alguém não puder cumprir o seu papel. **D)** Instituir exercícios simulados para testar se as funções e instalações do GRIS podem se manter operacionais em situações de emergência. Os problemas mais comuns: o GRIS não tem capacidade de *reach-back* (obtenção de staff adicional em situações de emergência); sistemas e redes que devem fornecer funções e serviços críticos não estão em um plano de backup, resultando no GRIS não ser capaz de funcionar durante uma situação de emergência.

19) Seja flexível. **A)** Não tente fazer tudo de uma vez. No entanto, estar pronto para se adaptar e tomar vantagem de boas oportunidades quando elas surgem, desde que não comprometam severamente os recursos do GRIS e não causem problemas de entrega de outros serviços já fornecidos. **B)** Entenda que os serviços podem evoluir ao longo do tempo, e esteja pronto para aprender novas habilidades obter novos conhecimentos. **C)** Mantenha-se informado sobre a mudança de tecnologias que garantam estratégias de resposta eficazes para lidar com novas ameaças e riscos. **D)** Procure maneiras de colaborar com os outros

profissionais nas áreas de GRIS e de segurança. Veja o detalhamento de cada passo no documento "Checklist do GRIS" disponível em <http://www.fredsauer.com.br>

Estudo de Caso 1 - GRIS



- Empresa multinacional de Produtos Radiológicos
- Altíssima criticidade de processos cuja falha pode comprometer milhares de vidas humanas
- Máquinas e equipamentos controlados por CLP e computadores convencionais, ligados em rede
- Há regulamentações internacionais, como a GAMP, com foco em ações decorrentes do nível de risco
- O case anexo é a primeira versão do documento, elaborado em 2012.

NP-1

Gestor: CII/ICM
Versão 1 - junho/2013

Vamos observar o Estudo de Caso anexo, relativo a uma empresa do segmento farmacêutico com demandas de conformidade com padrões internacionais de gestão de segurança.

Um dos trabalhos a ser realizado em grupo é a elaboração de um plano de criação de um GRIS, para um caso proposto.

Trabalho 1



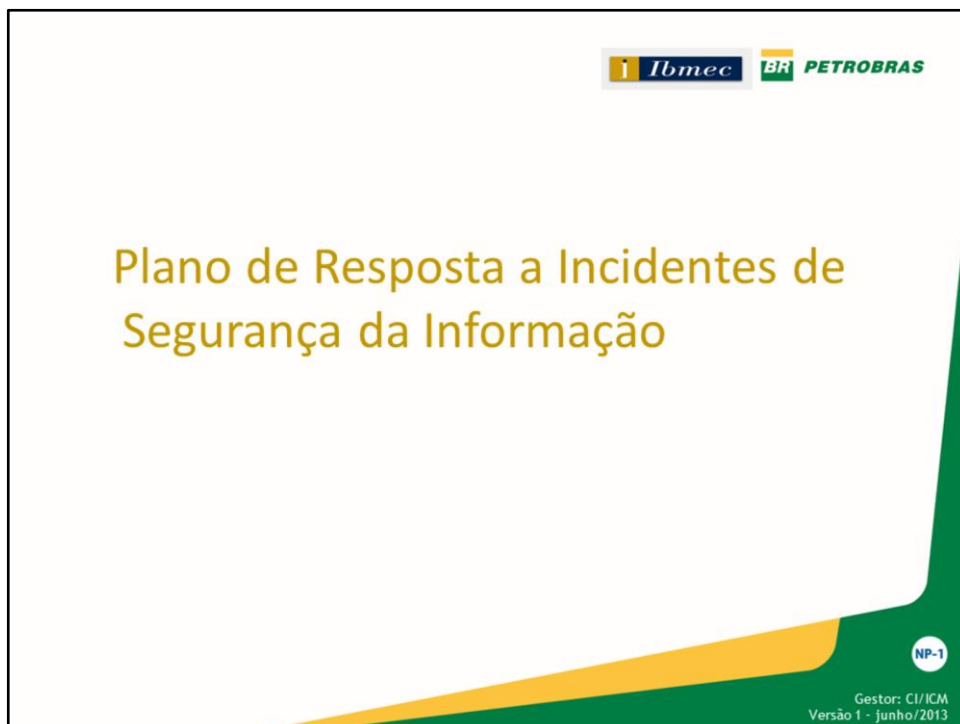
- Elaboração, em grupo, do documento de planejamento do GRIS para a empresa de comércio virtual detalhada em anexo.
- Todas as demandas necessárias para a tomada de decisões devem ser compatíveis com as características típicas de uma empresa deste tipo, e tudo que não estiver explicitamente definido pode ser livremente arbitrado.

NP-1

Gestor: CI/ICM
Versão 1 - junho/2013

Use o *template* de questionamentos anexo – também disponível em formato editável em www.fredsauer.com.br – para o esboço de planejamento inicial para o GRIS da empresa ilustrada nesta apostila.

Arbitrem o que for necessário, documentando estas decisões.



Após o primeiro passo, que é a estruturação de um staff para Respostas a Incidentes (GRIS), o próximo passo é planejar as metodologias a serem utilizadas para cada tipo de incidente. O ideal é que a empresa já possua um esforço de Análise de Riscos, de forma a compreender quais são as suas prioridades e o potencial impactante dos vários tipos de incidente.

Definição - PRI



Processo de resposta a incidentes de Segurança da Informação que pode envolver uma parte ou toda a organização, empresas parceiras e clientes

O objetivo final de um PRI é restabelecer o ambiente anterior ao incidente com as devidas medidas de segurança implantadas e monitoradas

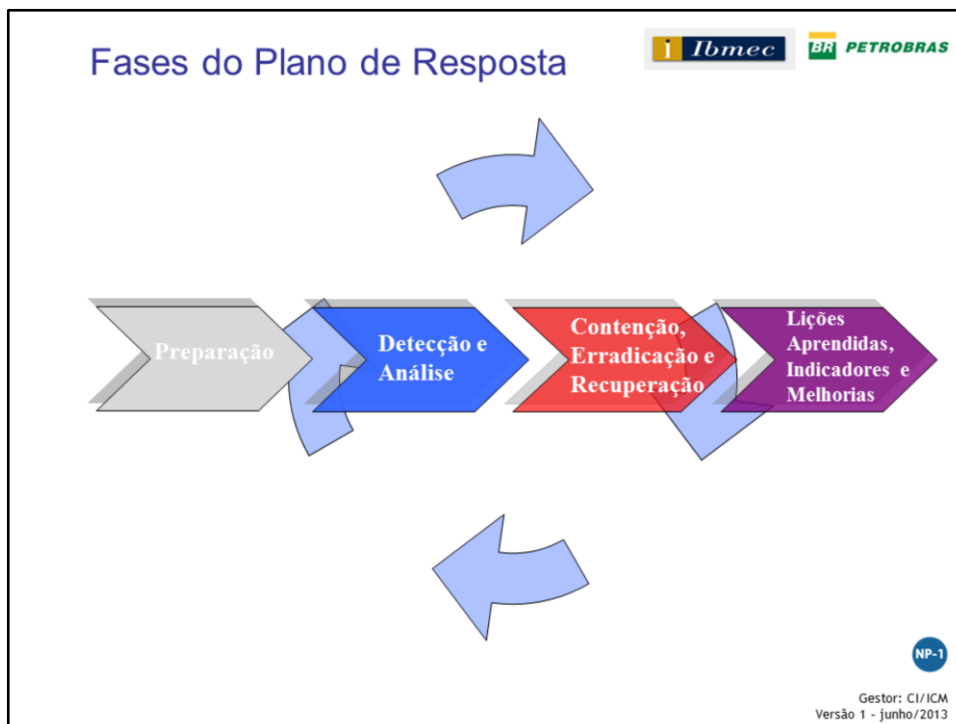
Adicionalmente, deve prover condições para as lições aprendidas, buscando evitar que o incidente volte a ocorrer

NP-1

Gestor: CII/ICM
Versão 1 - junho/2013

O PRI é um instrumento específico, definido para um tipo de incidente ou um grupo de incidentes semelhantes, com o mesmo grau de criticidade para a corporação. Deve ser elaborado com base em características já conhecidas do tipo de incidente, e deve necessariamente ser submetido à avaliações tanto após testes quanto em caso de situações reais de uso. As lições aprendidas são essenciais para o seu aprimoramento, no que diz respeito à eficiência e a eficácia.

Há várias metodologias, como a PDCERF do livro *Incident Response*, de E. Eugene Schultz e Russel Shumway, onde P – Preparation, D – Detection, C – Containment, E – Eradication, R – Recovery e F – Follow-up. Neste material vamos usar uma simplificação com agrupamento de atividades, mas no fundo é a mesma coisa.



Conforme o ciclo de vida apresentado no slide, as fases são sequenciais e complementares, mas a resposta propriamente dita é realizada nas duas etapas intermediárias. Cada uma possui requisitos, objetivos, políticas e *timeouts*. É fundamental uma boa documentação ANTES da sua utilização e mais ainda DURANTE e DEPOIS de um incidente. Isso é vital para sua manutenção e melhoria, e é o principal ponto de falha na maioria das corporações.

Fases do Plano de Resposta



- Garantir que os Processos, Recursos e Tecnologia identificados durante a fase de estruturação do GRIS estão disponíveis e funcionais
 - Equipamentos adequados (TAP, notebooks, duplicadores de imagem, mídias para gravação de dados, máquina fotográfica, gravadores de som, etc.)
 - Responsáveis mapeados/disponíveis
 - Informações da organização mapeadas e atualizadas
 - Possuir um local de reunião seguro quanto à CID das informações coletadas
 - Testes periódicos

NP-1

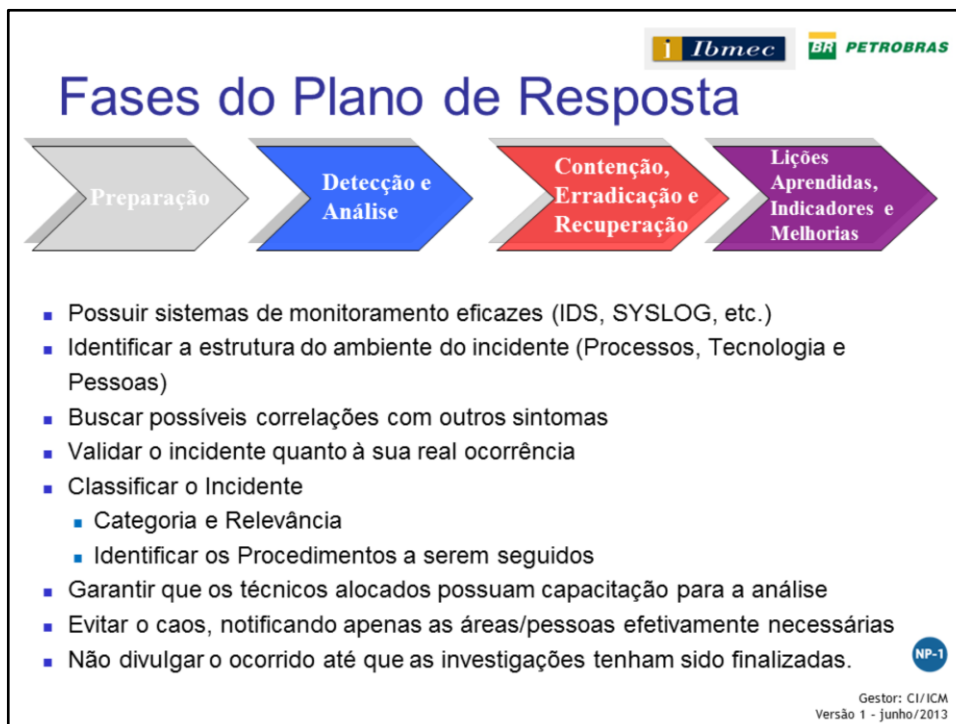
Gestor: CII/ICM
Versão 1 - junho/2013

A **preparação** é necessária para atenuar o risco de um ataque ou incidente antes de surgirem problemas dentro da organização, e para buscar minimizar os impactos em caso de incidente ocorrido. Isso inclui o uso de recursos de segurança na rede, sistemas e aplicações da organização. A Equipe de Resposta a Incidentes deve ter treinamento, bem como possuir todas as ferramentas e recursos necessários para desempenharem as suas funções de trabalho quando ocorrem incidentes. Boas práticas de segurança devem ser implementadas e constantemente aperfeiçoadas nas áreas de avaliação de riscos, segurança do perímetro da rede, prevenção de *malware* e sensibilização para a criação e manutenção da cultura de segurança entre os funcionários.

A meta principal deve ser “**Estar pronto ANTES do incidente efetivamente ocorrer**”. Pode-se alcançar isso através das seguintes medidas:

- ✓ Estabelecer um conjunto de DEFESAS e CONTROLES compatíveis com a natureza das possíveis ameaças;
- ✓ Criar um conjunto de PROCEDIMENTOS para lidar com os incidentes tão eficientemente quanto possível;
- ✓ Obter os RECURSOS e PESSOAL necessário para lidar com os problemas; e
- ✓ Estabelecer uma ESTRUTURA para suportar a atividade de resposta a incidentes.

TAP – Test Access Point – dispositivo passivo de captura de tráfego (veja exemplos em <http://http://www.networkinstruments.com/products/observer-ntaps/index.php>)



Detectar incidentes com rapidez e precisão tornou-se o maior desafio para as organizações. Isso pode ser atribuído a vários fatores, incluindo a detecção através de diferentes meios e o alto volume de tráfego de rede em toda a organização, e ao fato de que a maioria dos ataques não tem precursores facilmente detectáveis. A detecção pode ocorrer por meio de alertas emitidos por várias ferramentas de segurança de rede (IDS / IPS, AV, FW, etc.), análise de logs (sistema operacional, aplicativos, dispositivos de rede), pessoas dentro da organização ou informações publicamente disponíveis sobre novas vulnerabilidades e *exploits*. Em geral, deve-se assumir que um incidente tenha ocorrido até determinação em contrário. A Equipe de Resposta a Incidentes deve trabalhar rapidamente para **Analisar** e validar cada possível incidente, enquanto documenta todas as medidas tomadas. A análise inicial deve incluir a determinação do alcance do ataque, que sistemas/aplicações são afetadas, como o incidente ocorreu e os vetores de ataque. Para ser mais eficaz, um gerente de incidente deve conhecer o comportamento normal da rede dentro de sua organização e manter uma base de informações de conhecimento e pesquisa das últimas vulnerabilidades e *exploits*. A cada incidente ocorrido deve ser atualizada uma base de casos para buscar que novos incidentes sejam rastreados e resolvidos em tempo hábil. Cada registro de incidente deve incluir o status atual, um resumo do incidente, indicadores, ações tomadas, informações de contato para as partes envolvidas, todas as provas coligidas e os próximos passos. Após a análise inicial, a classificação da gravidade deve ser dada a cada incidente, a fim de priorizar incidentes e avaliar o possível impacto para a organização. A equipe deve, então, notificar todos os indivíduos que necessitam ser envolvidos no caso e também fornecer atualizações de status para a direção e outras partes interessadas que tenham necessidade de conhecer.

Fases do Plano de Resposta



- Tomar decisões APENAS com base em evidência
- Preservar as evidências para casos futuros e eventual ação policial
 - Data, local, nomes, telefones, logs, fotos, etc.
- Criar uma estratégia adequada para cada tipo/nível de Incidente
- Determinar o nível de abrangência do incidente (outras partes afetadas)
- Estimar o tempo de contenção e recuperação para cada tipo/nível de Incidente
- Backup Funcional
 - Garantir que a cópia a ser usada está protegida e íntegra
- Garantir que as medidas de segurança necessárias foram implantadas de forma correta
- Manter-se alerta durante um período de tempo após o tratamento do incidente

NP-1

Gestor: CII/ICM
Versão 1 - junho/2013

A **Contenção** é necessária para evitar que um incidente se propague por toda a organização, aumentando os impactos. Uma parte importante da contenção é o processo de tomada de decisão do gerente de incidente. Estratégias e procedimentos de confinamento predeterminados com base no tipo de incidente deve ser estabelecidos para se tomar decisões mais rapidamente. Recolher e preservar provas também é importante por conta de processos judiciais que podem ocorrer a partir do incidente. A **Erradicação** é necessária para eliminar componentes do incidente, incluindo a remoção de *malware* de sistemas e desabilitar contas de usuário. Na **Recuperação**, os administradores do sistema restauram os sistemas de volta às operações normais e corrigem vulnerabilidades para evitar que ataques semelhantes ocorram novamente. Isso pode incluir reconstrução de sistemas e bases de dados à partir de backups, a instalação de *patches*, implementação de controles de segurança mais rígidos na rede de perímetro, etc.

Fases do Plano de Resposta



- Criar um **Mecanismo** para disseminar a experiência adquirida
 - Palestras, Reuniões, Cartilhas, Intranet, etc.
- Documentar todas as ações Positivas e Negativas
- Melhoria Contínua (Obter estatísticas para *Benchmarks*)
- Evidenciar os Fatores Críticos de Sucesso
- Atualizar Políticas, Normas, PCN, etc.
- Criar Indicadores para Avaliar o Processo
- Criar uma forma de registro duradouro das atividades para disseminação do conhecimento e controle da evolução

NP-1

Gestor: CII/ICM
Versão 1 - junho/2013

Após o incidente ter sido contornado, é a hora da equipe realizar uma "lição aprendida" para melhorar a estratégia de segurança da organização e disseminar os conhecimentos adquiridos. A reunião de "lições aprendidas" deve incluir todo o pessoal envolvido, inclusive os responsáveis pela gestão e encerramento do incidente, revendo o que aconteceu, o que foi feito e deu certo, o que foi feito mas não funcionou como planejado, e um plano de ação para evitar que um novo ataque semelhante ocorra. Além disso, um relatório de acompanhamento deve ser criado para fornecer uma referência que possa ser usada para o tratamento de incidentes semelhantes no futuro (Base de Casos). Dados coletados ao longo de todos os incidentes devem ser reunidos a fim de avaliar os prejuízos para a organização, identificar tendências, justificar as necessidades de outros recursos e fornecer métricas de desempenho para a gerência avaliar o sucesso do Plano de Resposta a Incidentes e a equipe do GRIS. Um Plano de Resposta a Incidentes é importante para todas as organizações. Um Plano de Resposta a Incidentes de sucesso atenua a probabilidade de ocorrer incidentes de forma proativa, e também permite a organização reagir rapidamente e de forma eficaz quando ocorrem incidentes, reduzindo seus impactos. Não estabelecer um plano de resposta a incidentes adequada pode deixar uma organização suscetível a ataques de segurança cibernéticos sem métodos para atenuar, conter, erradicar e corrigir incidentes.

- O que não pode faltar em um PRI



- Classificação do Documento
- Pontos de Contato/Comunicação (Departamentos/Áreas e Responsáveis)
 - Plano de Comunicação do Incidente
- Detalhes do Incidente (Classificação, Data, local, Tecnologia, Pessoas e Processos envolvidos, etc.)
- Contextualização do Incidente (possíveis interações com outros incidentes ou localidades)
- Evidências coletadas
- Medidas e Contra Medidas adotadas
- Fechamento e Conclusão do caso
- Padronização na execução
 - Criar uma ficha para cada etapa do Processo de forma a atender a estrutura da organização
- Plano de contingência para o negócio

NP-1

Gestor: CI/ICM
Versão 1 - junho/2013

Eventualmente, o PRI pode conter informações que facilitem a atuação de pessoas mal-intencionadas, então ele deve ser um documento classificado, buscando garantir que apenas os que precisam ter conhecimento do mesmo possam acessá-lo. Algumas questões críticas em incidentes precisam estar bem definidas. Por exemplo, quem é responsável por definir a situação de incidente em andamento, quem deve tomar conhecimento disso e quem deve fazer a comunicação, quais são as informações que DEVEM e quais NÃO DEVEM ser divulgadas.

Estudo de Caso 2 - PRI



- Empresa multinacional de Produtos Radiológicos
- Altíssima criticidade de processos cuja falha pode comprometer milhares de vidas humanas
- Máquinas e equipamentos controlados por CLP e computadores convencionais, ligados em rede
- Há regulamentações internacionais, como a GAMP, com foco em ações decorrentes do nível de risco
- O case anexo é a primeira versão do documento, elaborado em 2012.

NP-1

Gestor: CII/ICM
Versão 1 - junho/2013

Vamos observar o Estudo de Caso anexo, relativo a uma empresa do segmento farmacêutico com demandas de conformidade com padrões internacionais de gestão de segurança.

Um dos trabalhos a ser realizado em grupo é a elaboração de um PRI para a empresa de comércio virtual.

Trabalho 2



- Elaboração, em grupo, do documento de planejamento de um PRI para a empresa de comércio virtual detalhada em anexo.
- Todas as demandas necessárias para a tomada de decisões devem ser compatíveis com as características típicas de uma empresa deste tipo, e tudo que não estiver explicitamente definido pode ser livremente arbitrado.

NP-1

Gestor: CI/ICM
Versão 1 - junho/2013

Use o *template* de questionamentos anexo – também disponível em formato editável em www.fredsauer.com.br – para o esboço de planejamento inicial para um PRI para a empresa ilustrada nesta apostila. A escolha do tipo de incidente é livre.

Arbitrem o que for necessário, documentando estas decisões.

Revisão



- Qual é a utilidade de um GRIS para o negócio de uma corporação ?
- Como devem ser escolhidos os serviços a serem oferecidos ?
- Quais são os fatores críticos de sucesso para um GRIS ?
- Quais são as abordagens de implementação ?
- O que é Forense Computacional ?
- Qual é a utilidade de PRIs para o negócio de uma corporação ?
- Quais são as etapas de um PRI ?
- Qual é a utilidade das “lições aprendidas” de um incidente ?

NP-1

Gestor: CI/ICM
Versão 1 - junho/2013