implantação do Memorial da Anistia Política no Brasil, conforme Portaria nº 203, de 09 de fevereiro de 2010. Passagens do tipo classe econômica, no valor total de R$934,23, e 0,5 diária(s), no valor total de R$215,13.

PAULO ABRÃO PIRES JUNIOR, Presidênte da Comissão de Anistia, em viagem a Rio de Janeiro/RJ, no período de 09/01/2011 a 11/01/2011, para participar de Reunião do Comitê Curador para implantação do Memorial da Anistia Política no Brasil, conforme Portaria nº 203, de 09 de fevereiro de 2010. Passagens do tipo classe econômica, no valor total de R$1.117,24, e 2,5 diária(s), no valor total de R$737,11.

THEREZA CHRISTINA ROSA ABELHA, Assessora Especial do Ministro, em viagem a Rio de janeiro/RJ, no período de 12/01/2011 a 13/01/2011, para acompanhar o Sr. Ministro nos seguintes eventos:dia 12/01 - Reunião com Dr. Jaime Antunes *Arquivo Nacional e no dia 13/01 reunião na Superintendência da Policia Federal do RJ; Visita ao Museu do Indio e reunião/almoço - Governador do Estado do Rio de janeiro Sergio Cabral. Foram pagas 1,5 diária(s), no valor total de R$374,21. Não houve pagamento de passagens.

VALTER VENTURA DA ROCHA POMAR, Colaborador Eventual da Comissão de Anistia, em viagem a Rio de janeiro, RJ, no dia 10/01/2011, para participará no dia 10 de janeiro de 2011 das 09:00hs as 18:00hs, da Reunião do Comitê Curador para implantação do Memorial da Anistia Política no Brasil, conforme Portaria nº 203, de 09 de fevereiro de 2010. Foram pagas 0,5 diária(s), no valor total de R$112,10. Não houve pagamento de passagens.

VIRGINIUS JOSÉ LIANZA FRANCA, Conselheiro da Comissão de Anistia, em viagem a Brasília, DF, no período de 11/01/2011 a 14/11/2011, para comparecer a pedido do Presidente da Comissão de Anistia, nos dias 12 e 13 de janeiro, a confecção de votos e finalização de processos já julgados e ainda não finalizados. Passagens do tipo classe econômica, no valor total de R$2.133,04, e 3,5 diária(s), no valor total de R$1.218,85.

VOLTAR AO INICIO

REVOGADO

SECRETARIA EXECUTIVA – SE

PORTARIA Nº 28 DE 10DE JANEIRO DE 2011

O SECRETÁRIO EXECUTIVO DO MINISTÉRIO DA JUSTIÇA, no uso de suas atribuições legais e na forma dos Decretos nº 3.505, de 13 de junho de 2000, nº 4.073, de 3 de janeiro de 2002, e nº 4.553, de 27 de dezembro de 2002,

Considerando o teor da Portaria nº 2.086, de 22 de novembro de 2005, que cria o Comitê Gestor de Segurança da Informação, o Grupo de Atendimento e Tratamento de Incidentes de Segurança da Informação – GATI;

Considerando o teor da Portaria nº 279, de 10 de março de 2006, que institui a Política de Segurança da Informação do Ministério da Justiça;

Considerando o teor da Instrução Normativa nº 1, de 13 de junho de 2008, do Gabinete de Segurança Institucional, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta; e

Considerando o teor da Norma Complementar nº 5/IN01/DSIC/GSIPR, de 14 de agosto de 2009, que disciplina a criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF, resolve:

Art. 1º Aprovar, na forma dos Anexos, a regulamentação e funcionamento da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR, no âmbito do Ministério da Justiça a qual continuará sendo chamada de GATI.

Parágrafo único. Os anexos de que trata esta Portaria visam prover o Ministério da Justiça de norma na área da segurança da informação, estabelecendo os seguintes pontos: definição da missão, público alvo, modelo de implementação escolhido, estrutura organizacional, autonomia e serviços que serão prestados.

Art. 2º Fica homologado o software livre RT/RTIR para fins de resposta de incidente de segurança da informação no âmbito do Ministério da Justiça, alcançando o público alvo do Anexo A.

Art. 3º Esta Portaria entra em vigor na data de sua publicação.

LUIZ PAULO BARRETO

ANEXO A

MISSÃO

Registrar, analisar e tratar incidentes de Segurança da Informação através da coleta de evidências, da investigação do ataque, do provimento de assistência local ou remota e da intermediação da comunicação entre as partes envolvidas.

PÚBLICO ALVO

É composta pelos usuários da rede de computadores e sistemas dos:

I. Órgãos de assistência direta e imediata ao Ministro de Estado

- Chefia de Gabinete do Ministro;
- Comissão de Anistia;
- Consultoria Jurídica;
- Secretaria-Executiva.

II. Órgãos específicos singulares

- Defensoria Pública da União;
- Departamento de Polícia Federal;
- Departamento de Polícia Rodoviária Federal;
- Departamento Penitenciário Nacional;
- Secretaria de Assuntos Legislativos;
- Secretaria de Direito Econômico;
- Secretaria de Reforma do Judiciário;
- Secretaria Nacional de Justiça;
- Secretaria Nacional de Segurança Pública.

III. Órgãos Colegiados

- Conselho Federal Gestor do Fundo de Defesa dos Direitos Difusos – CFDD;
- Conselho Nacional de Combate à Pirataria e Delitos contra a Propriedade Intelectual – CNCP;
- Conselho Nacional de Política Criminal e Penitenciária – CNPCP;
- Conselho Nacional de Segurança Pública – CONASP.

IV. Entidades Vinculadas

- Autarquia: Conselho Administrativo de Defesa Econômica – CADE;
- Fundação: Fundação Nacional do Índio – FUNAI.

O relacionamento com organismos de tratamento de incidentes externos, tanto no Brasil, quanto no exterior será realizado somente pela coordenação do GATI.

MODELO DE IMPLEMENTAÇÃO

- Modelo 4 – Combinado ou Misto

ESTRUTURA ORGANIZACIONAL

Considerando a Portaria n° 359/SE-MJ, de 16 de março de 2009, o Grupo de Atendimento e Tratamento de Incidentes de Segurança da Informação – GATI é composto pelos seguintes membros:

I - Secretaria Executiva : Jorilson da Silva Rodrigues

II - Gabinete do Ministério da Justiça: Valdecir Barella

III - Departamento de Polícia Federal: Ivo de Carvalho Peixinho

IV - Departamento de Polícia Rodoviária Federal: Rodney Loeffler Ramos Portilho

V - Defensoria Pública da União: Joelzo Francisco da Silva

VI - Fundação Nacional do Índio: Alex Miquetti de Almeida

VII - Conselho Administrativo de Defesa Econômica: Cezar Romero Carvalho de Souza

Considerando a Portaria nº 2.086, de 22 de novembro de 2005, compete ao Grupo de Atendimento e Tratamento de Incidentes de Segurança da Informação:

I - registrar, analisar e tratar incidentes de Segurança da Informação através da coleta de evidências, da investigação do ataque, do provimento de assistência local ou remota e da intermediação da comunicação entre as partes envolvidas;

II - coordenar, analisar e sugerir ações apropriadas para remoção de qualquer arquivo, objeto ou vulnerabilidade que possa sondar ou atacar sistemas e redes de computadores ou que possa ser utilizado para a quebra dos controles de segurança;

III - coordenar a elaboração de procedimentos para a área de Segurança da Informação;

IV - disseminar no âmbito do Ministério da Justiça alertas de vulnerabilidades, de intrusão ou qualquer assunto relacionado à Segurança da Informação;

V - assessorar tecnicamente os órgãos e unidades do Ministério da Justiça;

VI - monitorar e acompanhar a evolução de técnicas de Segurança da Informação e atividades de intrusão;

VII - realizar, por solicitação do Comitê Gestor, análises de Segurança da Informação, de forma a assegurar o estrito cumprimento da PSI/MJ;

VIII - avaliar ou desenvolver ferramentas de Segurança da Informação;

IX - analisar Registros de Eventos gerados por sistemas de informação;

X - avaliar e analisar riscos atuais ou iminentes, bem como propor ações para mitigação de riscos;

XI - desenvolver atividades de consultoria em Segurança da Informação ao MJ;

XII - promover seminários, discussões, cursos e tutoriais relativos à Segurança da Informação;

XIII - realizar testes para homologação dos Sistemas de Segurança da Informação do Ministério da Justiça;

XIV - o GATI será coordenado pelo Gerente de Segurança.

AUTONOMIA DA ETIR

- Autonomia Compartilhada

SERVIÇOS

- Serviço 1: Registrar, Analisar e Tratar Incidentes de Segurança da Informação – ANEXO A1
- Serviço 2: Disseminar conhecimento relacionado à Segurança da Informação – ANEXO A2

Anexo A1

Serviço 1: Registrar, Analisar e Tratar Incidentes de Segurança da Informação

1. - Objetivo

Efetuar registro e análise dos Incidentes de Segurança da Informação ocorridos no âmbito do Ministério da Justiça, bem como proceder ao devido tratamento conforme procedimento definido.

2. - Definição

O registro é o armazenamento de eventos no sistema de tratamento de incidentes para prover informações necessárias às análises e tratamento dos incidentes de segurança da informação. É fundamental para a gerência dos processos de tratamento e respostas de incidentes.

Análise de incidentes é um exame de toda informação disponível, levantamento de evidências, artefatos relacionados a um incidente ou evento, dentre outras atividades. O propósito da análise é a identificação dos envolvidos e do escopo do incidente, a extensão dos danos causados, a natureza e a estratégia de resposta disponível ou soluções de contorno.

O tratamento envolve as ações realizadas para resolver ou mitigar um incidente, seja diretamente ou por coordenação ou disseminação de informações. No decorrer deste documento o termo “tratamento de incidentes” refere-se especificamente aos relacionados à segurança da informação.

3. - Descrição das funções e procedimentos que compõem o serviço

O tratamento de incidentes segue o fluxo abaixo:

- Detecção e registro: receber e registrar eventos, relatórios de incidentes e alertas;

- Triagem: ações de categorização, priorização e atribuição de eventos e incidentes;

- Investigação: esforço para determinar o que aconteceu, qual impacto, ameaças ou danos que ocorreram e qual a reparação e os passos de mitigação que devem ser seguidos. Isto inclui caracterização de novas ameaças que podem impactar na infraestrutura. Também inclui-se encaminhamento ao devido órgão de persecução criminal, quando necessário.

- Tratamento: ações realizadas para resolver ou mitigar um incidente, seja diretamente ou por articulação ou disseminação de informações.

3.1. - Detecção e Registro

O registro, a análise e o tratamento de incidentes possuem os seguintes objetivos:

- Manter estatísticas sobre os incidentes;

- Acompanhar e coordenar os procedimentos necessários para mitigação e resolução de um incidente;

- Articular com outras entidades de modo a coordenar a mitigação de incidentes externos;

- Acompanhamento de tendências, de modo a subsidiar ações de disseminação de informações.

Todo e qualquer usuário poderá solicitar via email ou por meio das Centrais de Atendimento dos seus respectivos órgãos, atendimento quanto a incidentes de segurança da informação.

As informações recebidas por intermédio das Centrais de Atendimento ao Usuário deverão ser repassadas à equipes do GATI através dos e-mails oficiais, seguindo o padrão gati@mj.gov.br.

Os registros também poderão ser coletados através das ferramentas automáticas de monitoramento da rede.

O registro das notificações deve ser feito em ferramenta própria, homologada como ferramenta oficial de registro de incidentes.

Esta ferramenta funcionará como sistema central para visualização e gerenciamento de todas as notificações, mantendo suas bases independentes nos demais Órgãos participantes. Assim, os e-mails recebidos são automaticamente convertidos em tickets, com numeração única.

Sempre que possível, o registro de incidentes deverá conter as seguintes informações:

- Endereços IP de origem e destino envolvidos;

- Resumo descrevendo do que se trata;

- Responsável pelo registro do incidente;

- Identificação dos responsáveis pelos endereços IP envolvidos (whois);

- Informações de fuso horário e formato das datas;

- Registros de eventos (logs), expedientes, emails ou qualquer informação que comprove a existência e forneça informações acerca do incidente de segurança.

3.2. - Triagem

A triagem inclui:

- Interpretação das notificações;

- Categorização;

- Priorização;

- Identificar se é incidente:

o Se incidente:

▪ Determinar escopo;

▪ Relacionar com incidentes em andamento;

o Se não:

▪ Comunicar usuário;

▪ Fechar ticket.

3.2.1. - Interpretação das notificações

Sempre que possível, identificar:

- Quem são os envolvidos?
- Qual o tipo de organização representada? Como está envolvida? Qual sua atividade?
- Qual a natureza do incidente?
- Qual é o escopo do incidente?
- Quanto tempo se passou entre a ocorrência e a notificação?
- Existem outras evidências e referências?

3.2.2. - Categorização

Nível de sensibilidade

A sensibilidade pode variar de acordo com as circunstâncias. Segue abaixo os níveis de sensibilidade definidos.

Nível	**Exigência de Comunicação**	**Comunicação opcional**	**Acesso à ferramenta de tratamento de incidentes**
Extremamente Sensível – S1	Coordenador de TI, Gerente de Segurança da Informação, GATI e o usuário reclamante.	Autoridade máxima da unidade, Diretor, Comitê Gestor, Comunicação Social, Assessoria Jurídica, outras partes envolvidas.	Coordenador da TI, Gerente de Segurança da Informação, GATI, dentre outros.
Sensível – S2	Gerente de Segurança da Informação, GATI e usuários reclamantes.	Analistas, Técnicos de Segurança da Informação e Gestor.	Analistas e Técnicos de Segurança da Informação
Não sensível – S3	GATI, usuários reclamantes.	N/A	N/A

A matriz de criticidade abaixo define o tempo mínimo para resposta ao usuário e a exigência de comunicação contínua para o ocorrido.

Nível	**Aplicação**	**Exigência de retorno de comunicação**	**Tempo de resposta esperado**

C1	Afeta sistemas críticos Informações ou dados de caráter sigiloso. Interrupção de serviços que afetem a missão, a reputação ou interesse da instituição. Danos graves. Injúrias a indivíduos.	A atualização do caso deverá ser enviada as partes envolvidas diariamente durante a fase crítica. Se o envolvimento do GATI for necessário para restaurar sistemas críticos em serviços, então a atualização do caso deverá ser enviada no mínimo a cada 2 horas. A atualização do caso deverá ser enviada para as partes envolvidas semanalmente durante a fase de resolução.	Resposta Inicial	60 min
			Fase crítica	24X7
			Fase de Resolução	Comercial
C2	Afeta sistemas não críticos ou Informações não financeiras ou sem impacto. Pequenos períodos de interrupção dos serviços oferecidos podem ser admitidos. Danos significantes a indivíduos sem envolver perda de vidas ou sérias injúrias. Investigações sensíveis ao tempo.	A atualização do caso deverá ser enviada as partes envolvidas diariamente durante a fase crítica. A atualização do caso deverá ser enviada para as partes envolvidas semanalmente durante a fase de resolução.	Resposta Inicial	4 horas
			Fase crítica	Comercial
			Fase de Resolução	Comercial
C3	Possibilidade de incidente. Sistemas não críticos. Investigações a longo prazo envolvendo pesquisa extensiva e/ou trabalho de detalhamento forense. Não afeta a Missão, a reputação ou o interesse da Instituição.	A atualização do caso deverá ser enviada para as partes envolvidas semanalmente.	Resposta Inicial	48 horas
			Fase crítica	De acordo com o tempo e os recursos disponíveis
			Fase de Resolução	De acordo com o tempo e os recursos disponíveis

	Investigações não sensíveis ao tempo.			

O tempo inicial de resposta especifica a quantidade máxima de tempo decorrido antes que o responsável técnico pelo GATI responda ao usuário. No mínimo, as etapas abaixo devem ocorrer durante este prazo:

- Triagem;
- Classificação da ocorrência conforme o nível de criticidade;
- A inserção da ocorrência no sistema de tratamento de incidentes
- O responsável técnico deverá ser estabelecido;

Fases de resolução de um incidente:

Fase do Incidente	**Descrição**	**Atividades Típicas**
Crítica	Período de tempo no ciclo de vida da ocorrência quando a resposta ao incidente imediato é necessária para garantir uma resolução bem sucedida.	Detecção, avaliação, triagem, confinamento, preservação de evidência, recuperação inicial.
Resolução	Período de tempo no ciclo de vida da ocorrência quando a resposta ao incidente imediato não é necessário para uma resolução bem sucedida.	Coleta de evidência, análise e investigação, informática forense, remediação, recuperação completa e pós-morte.

Todos os incidentes deverão ser classificados conforme abaixo:

Categorias	**Sensibilidade Inicial**	**Criticidade Inicial**	**Descrição**
Informação comprometida	S1	C1	Tentativa ou destruição bem sucedida, corrupção ou divulgação de informações sensíveis da organização ou propriedade intelectual.
Atividades ilegais	S1	C2	Roubo, fraude, segurança de pessoas, pornografia envolvendo crianças e/ou adolescentes, computador envolvido em incidentes de natureza criminal, solicitação judicial, investigações globais e prevenção de perdas.
Informática Forense	S1	C3	Qualquer trabalho de informática forense realizado pelo GATI

Ativo comprometido	S1, S2	C1	Host comprometido (conta root, trojan), serviços de rede, aplicações, conta de usuário. Inclui host contaminados com software malicioso no qual o intruso está ativamente controlando o host.
Ataque interno	S1, S2, S3	C2	Reconhecimento ou atividade suspeita originalmente de dentro da rede da organização, excluindo disseminação de código malicioso.
Ataque externo	S1, S2, S3	C2	Reconhecimento ou atividade suspeita originalmente de fora da rede da organização (redes parceiras, Internet), excluindo malware.
Violação de Políticas	S1, S2, S3	C2	A exemplo de: Compartilhamento de material ofensivo; Violação de direitos autorais; Violação deliberada da Política de Segurança da Informação e Comunicações; Uso inapropriado dos ativos de informação.
Auditoria	S1, S2, S3	C3	Auditoria de Segurança não relacionada com nenhum incidente confirmado.
Software malicioso	S3	C1	Artefato de software tipicamente afetando múltiplos serviços da organização. Isso não inclui hosts comprometidos e que estão sendo controlados ativamente por um intruso via backdoor ou trojan.
SCAM	S3	C1	Scam (ou "golpe") é qualquer esquema ou ação enganosa e/ou fraudulenta que, normalmente, tem como finalidade obter vantagens financeiras.
PHISHING	S3	C1	Tipo de fraude que se dá através do envio de mensagem não solicitada, que se passa por comunicação de uma instituição conhecida, a exemplo de bancos, empresas ou sítios populares, e que procurem induzir o acesso a serviços fraudulentos (não autênticos), projetadas para obter ilegalmente dados pessoais e financeiros de usuários
Negação de Serviço	S3	C1	Negação de Serviço ou ataque de distribuição de negação de serviço

3.2.3. - Priorização

O responsável técnico poderá aplicar a ferramenta administrativa – Matriz GUT (Gravidade, Urgência e Tendência), a fim de priorizar os problemas a serem tratados. Onde:

- Gravidade: Métrica que serve para balizar o impacto sobre o Processo de Negócio em função de sua importância para a organização.

- Urgência: Métrica que serve para balizar o tempo de necessidade de intervenção para solução do problema ocorrido sobre o Processo de Negócio em função de sua importância para a organização.

- Tendência: Métrica que serve para balizar a evolução ou retração do impacto sobre o Processo de Negócio em função tempo usado para intervenção no problema dada a importância do Processo de Negócio para a organização.

Pontuação	**Descrição**	**Significado - Gravidade**
1	Sem Gravidade	A gravidade do impacto é pouco considerável.
2	Pouco Grave	A gravidade é considerável.
3	Grave	O gerenciamento do impacto é até possível, mas os prejuízos são significativos.
4	Muito Grave	O impacto no processo de negócio poderá causar prejuízos muito significativos.
5	Extremamente Grave	A gravidade é tão alta que o impacto poderá causar grandes prejuízos e é difícil avaliar os custos de recuperação.

Pontuação	**Descrição**	**Significado - Urgência**
1	Não há pressa	Não há pressa na correção, pois o impacto é pouco considerável.
2	Pode esperar um pouco	A correção pode esperar um pouco, pois o impacto é considerável.
3	O mais cedo possível	A correção deverá ser feita o mais cedo possível, pois o impacto poderá causar prejuízos significativos.
4	Com alguma urgência	A correção tem que ser feita com alguma urgência, pois o impacto no processo de negócio poderá causar prejuízos muito significativos.
5	Imediata	A correção deverá ser feita imediatamente, pois o impacto poderá causar grandes prejuízos e é difícil avaliar os custos de recuperação.

Pontuação	Descrição	Significado - Tendência
1	Não vai piorar	Se nada for feito, o problema não vai piorar.
2	Vai piorar a longo prazo	Se nada for feito, o problema vai piorar a longo prazo.
3	Vai piorar a médio prazo	Se nada for feito, o problema irá piorar a médio prazo.
4	Vai piorar em pouco tempo	Se nada for feito, o problema irá piorar em pouco tempo.
5	Vai piorar rapidamente	Se nada for feito, o problema irá piorar rapidamente.

3.3. – Investigação

A investigação do incidente é uma seqüência de ações realizadas na tentativa de se verificar o que aconteceu em um incidente determinando a dinâmica dos fatos envolvidos, se possível. É uma visão da situação, pela qual o GATI pode planejar o curso inicial de sua tomada de decisão.

3.3.1. - Objetivos

No curto prazo:

- Entender o incidente ocorrido;
- Determinar a necessidade de coletar outras informações;
- Ajudar a desenvolver um plano de resposta.

No longo prazo:

- Entender como o incidente se encaixa na tendência do intruso e nos padrões de ataque;
- Usar o incidente para expandir os conhecimentos sobre ataques;
- Usar o incidente com propósitos educacionais.

3.3.2. – Categorias Análise de relatos Intra-incidentes

Análise de questões relativas a um incidente específico. Os tipos mais comuns são os seguintes:

- Análise de qualquer artefato deixado pelas atividades de intrusão (arquivos de log, explorações, vírus, programas Cavalo de Tróia, etc);
- Análise do ambiente de software no qual o incidente ocorreu;
- Análise de confiança do ambiente de internet no contexto do incidente.

Análise de relatos Inter-incidentes

Análise de questões a respeito de relacionamentos entre incidentes, que são as análises das ligações entre os incidentes. Essas análises têm como objetivo encontrar simetrias entre incidentes em separado que podem indicar equivalência ou relacionar as fontes das atividades de intrusão.

3.3.3. - Atividades

As atividades possíveis são descritas abaixo:

- Exame e verificação do relatório inicial;
- Exame dos arquivos associados e artefatos;
- Exame dos Sistemas de logs da rede, recursos e processos, conexões, relacionamentos confiáveis, portas e serviços envolvidos;
- Diagrama de fluxo de um incidente e das atividades relacionadas;
- Correlação com atividades de incidentes similares;
- Determinar o impacto e o escopo baseado na informação;
- Identificação dos hosts envolvidos, sites e informação sobre os contatos correspondentes;
- Identificação das soluções, correções e passos de respostas.

3.4. - Tratamento

O tratamento dos incidentes envolve todas as etapas realizadas até a conclusão da resposta a um incidente e pode ser realizado de diversas formas:

- Notificação dos responsáveis;
- Solicitação de providências;
- Articulação com outros grupos e contatos de segurança;
- Acompanhamento da resolução do incidente.

A resposta aos incidentes pode ser:

- Local: O GATI proporciona diretamente, assistência local para ajudar os usuários a se recuperarem de um incidente. O GATI analisa fisicamente os sistemas afetados e conduz o reparo e a recuperação dos sistemas, em vez de somente providenciar a resposta de um incidente por meio telefônico ou email. Este serviço envolve todas as ações tomadas em nível local e que são necessárias se um incidente é suspeito ou que tenha ocorrido. Se o GATI não estiver presente no local afetado, membros da equipe poderão viajar para o local e realizar a resposta. Por outro lado, uma equipe local poderá atuar providenciando resposta ao incidente como parte da rotina de trabalho.

- Remota: O GATI acompanha e orienta as vítimas para recuperação de um ataque via telefone, email, fax ou documentação. Isso pode envolver assistência técnica na interpretação dos dados coletados, providenciando informação de contato ou transmitindo orientação na mitigação e estratégias de recuperação. O GATI pode orientar remotamente o pessoal local a realizar as ações e reparos necessários.

- Articulação: O GATI coordena as atividades de resposta entre as partes envolvidas no incidente. Incluindo as vítimas do ataque e de outros locais envolvidos, podendo ser quaisquer sítios que necessitem de assistência na análise. Isto também inclui as partes que fornecem serviços de TI para as vítimas, tais como, provedores de serviços de internet, outros ETIR e administradores de sistema e redes locais. A coordenação do trabalho pode envolver coleta de informação para contato, notificação de sítios envolvidos nos ataques (neste caso como vítimas ou fontes de ataques), coleta de estatística sobre o número de sites envolvidos e facilitando troca de informações e análises. Parte da coordenação do trabalho pode

envolver notificação e colaboração com a área jurídica, recursos humanos e comunicação social. Isto também pode incluir trabalho policial.

Iniciada a resposta ao incidente de segurança, o responsável pelo tratamento realiza o procedimento de análise das informações relativas ao incidente reportado. Todas as informações levantadas, incluindo emails enviados e recebidos, logs, providências, notificações, etc. devem ser registradas na ferramenta homologada.

No caso de um incidente proveniente da rede interna, deve ser identificado o responsável, para notificá-lo e acompanhar as providências de mitigação.

No caso de um endereço IP externo à rede é verificado o email de contato do responsável.

As providências tomadas em incidentes de segurança são diversas e dependem da natureza do incidente, porém de acordo com a necessidade, as seguintes providências podem ser solicitadas, dentre outras:

- Solicitação de bloqueio do endereço IP nos roteadores e filtros de pacotes da rede, para evitar novos incidentes e resguardar o restante da rede.

- Determinação ao responsável pela máquina de origem do incidente para retirá-la da rede e efetuar a desinfecção e/ou análise forense do equipamento em questão.

- Solicitação do bloqueio do endereço IP do responsável externo à rede, como medida para proteção da rede frente a esta ameaça.

- Notificação do incidente de segurança aos responsáveis para que o mesmo tome as providências necessárias.

Os incidentes que envolvem participantes externos são obrigatoriamente informados através de correio eletrônico, utilizando o recurso de cópia carbono (CC), para o ETIR de nível superior.

Após o esclarecimento completo do incidente de segurança, e as devidas providências efetuadas pelos envolvidos, o ticket é fechado e o incidente de segurança é concluído.

No longo prazo o GATI pode realizar uma análise de desempenho procurando variações de tendências. Este tipo de análise pode incluir o que se chama de retrospectiva ou análise histórica. Não se procura tendências gerais, mas como os ataques acontecem e quais as estratégias.

4. - Disponibilidade do serviço

O serviço de tratamento de incidentes segue a Tabela de Classificação de Criticidade.

5. - Metodologia para execução do serviço

A metodologia consiste na execução dos procedimentos conforme fluxo do processo de Respostas a Incidentes e tratamento de abuse anexo.

ANEXO A2

Serviço 2: Disseminar conhecimento relacionado à Segurança da Informação

Objetivo

Disseminar informações apropriadas para conscientização em segurança da informação e atualizações regulares em relação às políticas, às normas e aos procedimentos, bem como gerar alertas de segurança.

Definição

Este serviço envolve disseminação da informação que descreve um ataque à rede de dados, vulnerabilidade da segurança, alerta de intrusão, vírus de computador, boato, entre outros, providenciando um procedimento de ação para lidar com a solução do problema. O Alerta tem como objetivo informar aos usuários não técnicos, acerca de incidentes que podem afetar os serviços utilizados. O Aviso notifica os analistas e técnicos em segurança da informação e especialistas em tratamento e resposta a incidente, acerca de ocorrências que demandam sua intervenção, devendo ser enviado como uma reação ao problema apresentado, com intuito de notificar as equipes e providenciar uma orientação para proteção dos seus

sistemas ou recuperação dos sistemas que foram afetados. A Advertência deve ser utilizada para esclarecer ou chamar a atenção dos analistas e técnicos em segurança da informação e especialistas em tratamento e resposta a incidente sobre temas que podem afetar a segurança da rede de dados. A informação pode ser elaborada pela ETIR ou pode ser redistribuída pelos fornecedores, outras ETIR´s , especialistas em segurança.

A disseminação das informações, dentre outras atividades, devem ser para:

- manter as pessoas informadas sobre assuntos de segurança que podem afetá-las;
- oferecer orientações para implantação de correções;
- providenciar materiais de referência que podem ser usados durante atividades de respostas de incidentes.
-

Descrição das funções e procedimentos que compõem o serviço

Tópicos que devem ser rotineiramente cobertos:

- Novas vulnerabilidades
- Atividade de intrusão em andamento
- Documentação técnica e de procedimentos
- Melhores práticas

Para determinar o que publicar levar em consideração:

- A origem da informação
- Quem conhece do problema
- Se o tópico está no âmbito de conhecimento e atribuição formal
- Se existem obrigações legais e/ou contratuais requeridos ou proibitivos

Quando da publicação de problemas de infraestrutura levar em consideração:

- Se um intruso pode adquirir o controle do sistema
- Quantos sistemas são afetados?
- Quais os papéis dos sistemas em risco?
- Qual o impacto de uma exploração bem sucedida?
- ✓ O intruso sempre pode ganhar acesso privilegiado?
- Grau de dificuldade de exploração
- ✓ Simples comandos?
- ✓ Conhecimentos mais amplos?
- Qual o nível de acesso requerido por um intruso?
- O que pode ser feito?
- ✓ Dependendo de como o problema é conhecido, pode-se atrasar a publicação até que correções e soluções estejam prontas.
- ✓ Se não existem correções ou soluções de contorno, deve-se realmente publicar?

Quando publicar:

- Depende do tipo de informação e do público alvo:
- ✓ Local, nacional ou internacional
- ✓ 24 horas de escala de trabalho ou horário comercial
- Grau de relevância da informação
- Pode requerer chamadas telefônicas?
- Considerações sobre tempo para resolução dos problemas podem levar a uma prioridade mais baixa

Disponibilidade do serviço

Serviço	Disponibilidade
Atendimento inicial, triagem e monitoração geral realizado por equipe de monitoramento	24x7

Tratamento de incidentes de grandes proporções	24x7
Demais casos	Horário comercial

Metodologia para execução do serviço

- Verificar se as vulnerabilidades que estão sendo exploradas são mais sérias que problemas teóricos
- Checar estatísticas

As intervenções devem ser realizadas de forma cautelosa.

CONCESSÃO DE DIÁRIAS

DEZEMBRO/2010

CLAUDIO MARINHO DA SILVA NETO, Agente de Policia, em viagem a Recife/São Paulo/Santa Catarina, no período de 15/12/2010 a 18/12/2010, para participar de atividade do PRONASCI junto à Academia da Polícia Civil de Santa Catarina, oportunidade em que conhecerão o projeto que lá está sendo implantado na área de formação que inclui a disciplina de Relações Interétnicas nas formação policial. Estruturação da Corregedoria de Polícia (nova legislação); Projeto de integração policial implementado pela Secretaria de Segurança de SC e regimento da Polícia Civil SC. . Passagens do tipo classe econômica, no valor total de R$2.443,24, e 3,5 diária(s), no valor total de R$797,10.

FRANCISCO JOSÉ DE SOUSA ALVES, Agente de Polícia Civil, em viagem a Natal/Florianópolis/Natal, no período de 15/12/2010 a 18/12/2010, para participar de atividade do PRONASCI junto à Academia da Polícia Civil de Santa Catarina, oportunidade em que conhecerão o projeto que lá está sendo implantado na área de formação que inclui a disciplina de Relações Interétnicas nas formação policial. Estruturação da Corregedoria de Polícia (nova legislação); Projeto de integração policial implementado pela Secretaria de Segurança de SC e regimento da Polícia Civil SC. Passagens do tipo classe econômica, no valor total de R$1.936,24, e 3,5 diária(s), no valor total de R$797,10.

JULIA MARQUES DALLA COSTA, Técnica de Nível Superior-Ciências Sociais-Nível III , em viagem a Brasília/Rio de Janeiro/Brasília, no período de 14/12/2010 a 19/12/2010, para acompanhar o evento ?III Teia da Memória?, que acontecerá entre os dias 14 a 19 de dezembro, no Museu da Maré, na cidade do Rio de Janeiro. O evento situa-se dentro do ?Programa Pontos de Memórias?, executado pelo Instituto Brasileiro de Museus ? IBRAM/MinC e financiado pelo PRONASCI/MJ. Passagens do tipo classe econômica, no valor total de R$527,24, e 4,5 diária(s), no valor total de R$1.048,63.

MARCOS SOARES MASCARENHAS, Servidor Público e Diretor para Assuntos Parlamentares, em viagem a Brasília/Florianópolis/Brasília, no período de 15/12/2010 a 18/12/2010, para participar de atividade do PRONASCI junto à Academia da Polícia Civil de Santa Catarina, oportunidade em que conhecerão o projeto que lá está sendo implantado na área de formação que inclui a disciplina de Relações Interétnicas nas formação policial. Estruturação da Corregedoria de Polícia (nova legislação); Projeto de integração policial implementado pela Secretaria de Segurança de SC e regimento da Polícia Civil SC. Passagens do tipo classe econômica, no valor total de R$1.195,24, e 3,5 diária(s), no valor total de R$797,10.

NOVEMBRO/2010

SUZETE SANTOS BOMFIM FEITOSA, Arquiteta , em viagem a Brasília/Chile/Brasília, no período de 28/11/2010 a 02/12/2010, para missão Internacional para conhecer uma dessas experiências afim de subsidiá-la na elaboração das propostas. Especialmente, parece-nos importante uma visita Museu da Memória e dos Direitos Humanos do Chile. Passagens do tipo classe econômica, no valor total de R$1.930,62, e 4 diária(s), no valor total de R$1.224,18.

AGOSTO/2010

TATIANA ALENCAR SILVA IVANOSKI, Assessora Técnica , em viagem a Brasília/Leon/Cidade do México/Brasília, no período de 25/08/2010 a 31/08/2010, para participar da Conferência Mundial da Juventude que acontecerá na cidade de leon/Guanajuato, de 25 a 27 de agosto de 2010 e a realizar visita ao Observatório Internacional de Segurança Pública, na Cidade do México, no dia 30 de agosto de 2010. Passagens do tipo classe econômica, no valor total de R$3.323,93, e 6 diária(s), no valor total de R$3.388,45.

JUNHO/2010