ESTADO DO CEARÁ
PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA
SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO
SERVIÇO DE SEGURANÇA DA INFORMAÇÃO

Plano de Gestão de Incidentes de Segurança da Informação

Data	Versão	Descrição	Responsável
22/06/2022	1.0	Elaboração de Documento	Endson Pereira da Silva
12/07/2022	1.0	Revisão de Documento	Adarildo de Brito Figueiredo

1. INTRODUÇÃO

1.1. Um incidente de segurança pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação levando a perda de um ou mais princípios básicos de segurança da informação: Confidencialidade, Integridade e Disponibilidade.

1.2. O tratamento de incidentes de segurança da informação consiste na implementação de procedimentos e etapas bem definidas que conduzirão a equipe para a resolução destes incidentes. Estes procedimentos permitem determinar um fluxo lógico, especificando ações a serem realizadas nas diferentes etapas do processo.

2. OBJETIVO

2.1. O Plano de Gestão de Incidentes de Segurança da Informação tem o objetivo de estabelecer princípios, conceitos, diretrizes e responsabilidades nas fases de detecção, resolução, prevenção e redução da ocorrência sobre a gestão de incidentes de segurança da informação no TJCE, orientando o funcionamento do

processo, de forma que este seja tratado adequadamente, mitigando ao máximo os impactos para o negócio, proporcionando um ambiente cada vez mais confiável, disponível e íntegro.

3. ABRANGÊNCIA

3.1. Este plano abrange todos os recursos computacionais pertencentes, operados, mantidos e controlados pelo TJCE.

4. CONCEITOS E DEFINIÇÕES

4.1. **Invasão:** Evento de exploração de vulnerabilidades, ocorre quando um atacante tenta executar ações maliciosas, como invadir um sistema, acessar informações confidenciais ou tornar um serviço inacessível;

4.2.

4.3. **Vírus:** Programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos;

4.4.

4.5. **Base de Conhecimento:** biblioteca on-line de autoatendimento de informações sobre um produto, procedimento, serviço, departamento ou tópico

4.6.

4.7. **Incidente:** qualquer ato, suspeita, ameaça ou circunstância que comprometa a confidencialidade, integridade ou a disponibilidade de informações que estão em posse da SEFIN ou que ela venha a ter acesso;

4.8.

4.9. **Sistemas:** hardware, software, network de dados, armazenador de mídias e demais sistemas usados, adquiridos, desenvolvidos, acessados, controlados, cedidos ou operados pelo TJCE para dar suporte na execução de suas atividades.

4.10.

4.11. **Tratamento:** qualquer operação ou conjunto de operações efetuadas sobre os dados, por meios automatizados ou não, incluindo, mas não se limitando, a coleta, gravação, organização, estruturação, alteração, uso, acesso, divulgação, cópia, transferência, armazenamento, exclusão, combinação, restrição, adaptação, recuperação, consulta, destruição ou anonimização;

4.12.

4.13. **Vazamento de dados:** qualquer quebra de sigilo ou vazamento de dados que possa resultar, criminosamente ou não, na perda, alteração, compartilhamento, acesso, transmissão, armazenamento ou processamento de dados não autorizado.

5. PAPEIS E RESPONSABILIDADES

5.1. **Notificador** - pessoa ou sistema de monitoração que notifica o incidente;

5.2. **Acionadores** (Atendimento e Suporte de TI): equipe de 1°, 2°, 3° nível e ETIR (Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernéticas);

5.3. **Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernéticas (ETIR)** - Denominação tradicionalmente atribuída a grupos de resposta a incidentes de segurança da informação, embora os incidentes não mais se limitem a tecnologia;

5.4. **Comitê de Governança de Segurança da Informação e de Crises Cibernéticas (CGSICC)** - no âmbito do Poder Judiciário do Estado do Ceará, vinculado à Presidência do TJCE, que atuará com vistas à promoção da cultura de segurança da

informação, inclusive no que diz respeito à prevenção e ao tratamento de crises cibernéticas de forma contínua, estabelecendo um modelo de gestão de segurança da informação.

5.5. **Responsável por Sistema ou Controlador de Sistema** – analista responsável identificado no inventário de soluções tecnológicas (quando houver), com capacidade de propor soluções de resposta a serem apreciadas pela ETIR, para autorizar ou vetar procedimentos de emergência (preferencialmente deve ser identificado no inventário de soluções, com formas de contato para emergências);

5.6. **Responsável por Processo ou Negócio** – gestor de unidade identificado na estrutura organizacional, com capacidade de propor soluções de resposta a serem apreciadas pela ETIR, para autorizar ou vetar procedimentos de emergência;

5.7. **Comitê de Gestão de Tecnologia da Informação e Comunicação (CGETIC):** Obter aprovação da alta gestão ou outros órgãos para execução de plano de ação com impacto em diversas áreas ou outros órgãos.

5.8. **Gestor da área de Segurança da Informação:** responsável pelas ações de segurança da informação e comunicações na organização.

5.9. **Coordenador da Equipe de Tratamento e Resposta a Incidentes:** responsável por gerenciar os membros e as atividades da equipe de resposta a incidentes.

5.10. **Coordenador do Comitê de Crises Cibernéticas:** responsável por analisar o cenário de crise, solicitar preparação da Sala de Situação, convocar os membros do Comitê e demais áreas e responder a ETIR em caso de não reconhecimento da inexistência de Crise.

5.11. **Ponto de Contato:** responsável estratégico pela comunicação e ponto focal de contato da equipe de resposta a incidentes com outros setores da organização ou grupos externos.

5.12. **Administrador de Infraestrutura Computacional:** profissional com conhecimento em sistemas operacionais e suas aplicações, responsável por instalar, configurar, suportar e manter servidores e outros sistemas.

5.13. **Administrador de banco de dados:** responsável por gerenciar, instalar, configurar, atualizar e monitorar um banco de dados ou sistemas de banco de dados.

5.14. **Administrador de redes de dados e comunicações:** responsável por projetar e manter uma rede de computadores em funcionamento, gerenciando a rede local e os recursos computacionais e ativos a ela relacionados, direta ou indiretamente.

6. DESCRIÇÃO DOS PROCESOS

6.1. A entrada dos chamados de incidentes de SI segue o fluxo descrito no processo “Gerenciar Incidentes”.

6.2. Após o incidente de SI ser registrado, deve ser realizado a triagem e verificação do “Plano de Gestão de Incidentes – (PGI)” e da “Base de Conhecimento – BC”:

6.2.1. Acessar as ferramentas de registro de chamados de TIC;

6.2.2. Verificar no Plano de Gestão de Incidentes e se encontrar um incidente semelhante ou igual, verificar o histórico de lições aprendidas;

6.2.3. Anexar Plano de Gestão de Incidentes ao chamado.

6.3. Após a verificação acima, deve-se iniciar a análise do incidente, seguindo os passos abaixo:

6.3.1. Investigar o Incidente com base nas informações registradas no AssytWeb, suporte de fornecedores das tecnologias utilizadas no TJCE, sites de parceiros de segurança da informação, orientações de instituições do governo e do judiciário, deverá averiguar as possíveis causas, extensão e

impacto do incidente, a fim de subsidiar as decisões e ações para sua contenção ou para seu encaminhamento. Poderá solicitar informações às áreas técnicas responsáveis, a fim de elucidar a extensão e o impacto do problema, quais ativos e sistemas estão sendo afetados e começar a definir uma ação para conter o incidente. A identificação do tipo* e impacto** do incidente é muito importante pois ela definirá o encaminhamento a ser dado quanto à necessidade de ações de contenção, de comunicação a outras áreas sobre a ocorrência do incidente e de realização de investigação de acessos.

6.3.2. OBS: Nesta fase o incidente ainda poderá ser recategorizado.

6.3.3. * Averiguar se é uma investigação de acesso indevido, descumprimento da Política de Segurança da Informação, indisponibilidade de um serviço ou sistema por falha de segurança, invasão, propagação de vírus, vazamento de dados etc.

6.3.4. ** Se necessário, envolver outras equipes (Manutenção TJCE/FCB, Assistência Militar, etc);

6.3.5. Verificar se ocorreram eventos semelhantes, quais foram as ações tomadas, os impactos gerados, consultando os registros de incidentes anteriores e os registros de lições aprendidas;

6.3.6. Verificar a origem, extensão, danos do incidente e ações necessárias;

6.3.7. Verificar a necessidade de tratamento imediato;

6.3.8. Identificar os setores responsáveis por executar as ações necessárias;

6.3.9. Se o incidente for acerca de investigação sobre acessos de determinado(s) servidor(es) em sistemas e serviços disponibilizados, investigação de acessos não autorizados ou que exijam a verificação de dados dos usuários, a equipe técnica de Resposta e Tratamento de Incidentes realizará a auditoria necessária e compilará os dados em relatório a ser encaminhado às áreas competentes;

6.3.10. Identificar os dados necessários à elucidação do incidente, os dados podem ser coletados de sistemas de monitoramento diversos;

6.3.11. Realizar a coleta e compilação de dados.

6.3.12. NOTA: Quando envolver outras áreas, verificar o envolvimento, se sim, acioná-las, se não, prosseguir com ações autorizadas pelos gestores da Setin ou Gerência de Informática do Fórum Clóvis Beviláqua.

6.3.13. Verificar também se há necessidade de autorização do CGSI ou da Presidência.

6.4. Caso seja identificado a necessidade do gerenciamento de crise, o processo “Gerenciar Crise de Segurança da Informação” deve ser consultado (link abaixo).

6.4.1. LINK: https://www.tjce.jus.br/seplag/Processos/Administrativos/Desenv_e_Prover_TI/Gerir_Seg_Info/ProcSetin060/HTML/index.html#diagram/d2f934ca-4eed-4e75-8c67-34a6d6a8c063

6.5. Quando for identificado a necessidade de coletar evidencias, o processo “Coletar Preservar Evidências” deve ser consultado (link abaixo).

6.5.1. Link:https://www.tjce.jus.br/seplag/Processos/Administrativos/Desenv_e_Prover_TI/Gerir_Seg_Info/ProcSetin060/HTML/index.html#diagram/b1ec2ff8-b5ed-4bc3-984f-7c474c4eff81

6.6. O próximo passo é a execução das ações de contenção:

6.6.1. Confirmar a não identificação da causa-raiz do incidente;
6.6.2. Verificar que solução/procedimento é possível ser executada para contornar o incidente reportado.
6.6.3. Executar a solução definida pela equipe;
6.6.4. Verificar se o incidente foi contornado/resolvido;
6.6.5. Registrar a sugestão de problema no sistema de gerenciamento de serviços;
6.6.6. Informar o registro no chamado de Incidente em andamento.

6.7. Posteriormente devemos comunicar o incidente as áreas de negócio quando afetar um ou mais grupos de serviço/sistemas ou uma grande quantidade de usuários:
6.7.1. Se o incidente de segurança afetar um ou mais grupos de serviço/sistemas ou usuários, o gestor da ETIR/GRISI ou segurança da informação, de posse da extensão e do impacto do incidente, deverá comunicar as áreas da Setin e afins sobre a ocorrência e, em conjunto com a área de Segurança da informação, deliberar se é necessário informar outras áreas do TJCE sobre o incidente;
6.7.2. A área de segurança da informação comunicará as áreas afetadas internas do TJCE com as informações necessárias, com relatório de Incidentes preenchido e com as informações sobre o plano de comunicações;
6.7.3. Informar a extensão do impacto e quais sistemas/ serviços foram afetados.
6.8. Caso os procedimentos necessários para resolução não constem no PGI e/ou na BC os procedimentos abaixo são necessários:
6.8.1. Investigar, analisar e avaliar a natureza do incidente.
6.8.2. Definir grupo de trabalho, com o envolvimento de especialistas no assunto, referente ao incidente de segurança.
6.8.3. Determinar as premissas e restrições das ações/projeto a ser executado.
6.8.4. Avaliar a necessidade de contratação de fornecedores ou aquisição de equipamentos para mitigar ou prevenir o risco de novos incidentes.
6.8.5. Definir as ações preventivas/corretivas necessárias para contenção ou prevenção de novos incidentes.
6.8.6. Elaborar cronograma de execução.
6.8.7. Identificar os recursos necessários (humanos, tecnológicos, financeiros).
6.8.8. Avaliar a necessidade de realizar investigação legal do incidente e analisar as evidências que poderão ser coletadas.
6.8.9. Definir os resultados desejados com a implementação das ações.
6.8.10. Enviar, quando necessário, plano de ação para aprovação do CGSI ou Presidência ou para outras áreas;
6.9. Caso necessário a obtenção de aprovação da alta gestão ou outros órgãos para execução do plano de ação com impacto em diversas áreas ou outros órgãos, você deverá:
6.9.1. Solicitar aprovação;
6.9.2. Obter aprovação.

6.10. O próximo passo é adicionar à base de conhecimento informações sobre o incidente, suas características e solução implementada:

6.10.1. Abrir chamado referente a registro de conhecimento;

6.10.2. Informar no chamado de conhecimento os procedimentos e informações relevantes que devem ser executados para a resolução do incidente registrado;

6.10.3. Vincular o chamado aberto de Conhecimento ao chamado de Incidente em andamento;

6.10.4. Adicionar o tipo de incidente no documento Plano de Gestão de Incidentes de SI.

6.11. Após adicionarmos os documentos a base de conhecimento ou caso o mesmo já exista, vamos agora executar os procedimentos que foram definidos no plano de ação para tratamento do incidente:

6.11.1. Executar as ações definidas no plano de ação.

6.11.2. Coletar e registrar evidências do incidente.

6.11.3. Elaborar Relatório de Implementação de Tratamento Incidente

6.11.4. NOTA: Poderá haver o armazenamento das evidências com o formulário no Assyst “Tratamento de Incidentes de Segurança”.

6.12. Agora devemos analisar todas as etapas do incidente, objetivando propor outras providências necessárias ao encerramento do incidente:

6.12.1. Analisar Causa Raiz;

6.12.2. Propor melhorias no ambiente investigado;

6.12.3. Elaborar Relatórios (Investigações que envolvam acessos, o GRISI /ETIR deverá analisar logs e utilizar as ferramentas de auditoria disponíveis para elucidar a suspeita informada e encaminhar o relatório à apreciação do CGSI.);

6.12.4. Avaliar mudanças nos processos de negócios, na política de segurança, na tecnologia utilizada, no comportamento;

6.12.5. Avaliar impacto na Organização;

6.12.6. Atualizar os Indicadores de Segurança da Informação;

6.12.7. Enviar Relatório Final de Incidentes para a Alta Gestão;

6.12.8. Atualizar o repositório (base de conhecimento) de Incidentes de Segurança;

6.12.9. NOTA: Outras áreas poderão ser envolvidas

6.13. Para finalizar, devemos realizar a avaliação de histórico de incidentes:

6.13.1. Realizar reunião de análise crítica após a elaboração do relatório final de Incidentes com o objetivo de determinar quais as melhorias e ações necessárias para o refinamento e ajustes no processo de controle de incidentes;

6.13.2. Esta reunião deverá ocorrer em até uma semana após a emissão do relatório e deverá emitir um relatório de Lições Aprendidas.

6.13.3. Assessorar o Comitê Gestor de Segurança da Informação, a ETIR/GRISI e a Setin na análise e tomada de decisões a respeito de situações resultantes de incidentes de segurança da informação.

6.13.4. NOTA: Esta reunião deverá ocorrer em até uma semana após a emissão do relatório e deverá emitir um relatório de Lições Aprendidas.

7. TIPOS DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

7.1. Este item por ser dinâmico pode alterado a qualquer tempo,

Item	Indicação de Incidente Cibernético	Descrição	Procedimento
01	Campanha de phishing	O órgão é alvo de uma campanha de phishing.	https://www.tjce.jus.br/seplag/Processos/Administrativos/Desenv_e_Prover_TI/Gerir_Seg_Info/ProcSetin060/HTML/index.html#diagram/51f83baa-6d70-4e74-92b3-2b11a3469a6e
02	Degradação de Serviços	Degradação ou interrupção de serviços ou sistemas por ataque de negação de serviço (DoS).	https://www.tjce.jus.br/seplag/Processos/Administrativos/Desenv_e_Prover_TI/Gerir_Seg_Info/ProcSetin060/HTML/index.html#diagram/51f83baa-6d70-4e74-92b3-2b11a3469a6e
03	Comprometimento de Credenciais	Comprometimento de credenciais com acesso a informações sensíveis.	https://www.tjce.jus.br/seplag/Processos/Administrativos/Desenv_e_Prover_TI/Gerir_Seg_Info/ProcSetin060/HTML/index.html#diagram/51f83baa-6d70-4e74-92b3-2b11a3469a6e
04	Impossibilidade de Acesso à Informação	Importantes informações organizacionais inacessíveis por encriptação (ransomware).	https://www.tjce.jus.br/seplag/Processos/Administrativos/Desenv_e_Prover_TI/Gerir_Seg_Info/ProcSetin060/HTML/index.html#diagram/51f83baa-6d70-4e74-92b3-2b11a3469a6e
05	Vazamento de Informação e Dados Pessoais	Informações críticas encontradas fora da organização.	https://www.tjce.jus.br/seplag/Processos/Administrativos/Desenv_e_Prover_TI/Gerir_Seg_Info/ProcSetin060/HTML/index.html#diagram/51f83baa-6d70-4e74-92b3-2b11a3469a6e
06	Conteúdo Abusivo	Spam, Assédio, etc	https://www.tjce.jus.br/seplag/Processos/Administrativos/Desenv_e_Prover_TI/Gerir_Seg_Info/ProcSetin060/HTML/index.html#diagram/51f83baa-6d70-4e74-92b3-2b11a3469a6e
07	Código Malicioso	Worm, Vírus, Trojan, Spyware, Scripts	https://www.tjce.jus.br/seplag/Processos/Administrativos/Desenv_e_Prover_TI/Gerir_Seg_Info/ProcSetin060/HTML/index.html#diagram/51f83baa-6d70-4e74-92b3-

			2b11a3469a6e
08	Prospecção por Informações	varredura, sniffing, engenharia social	https://www.tjce.jus.br/seplag/Processos/Administrativos/Desenv_e_Prover_TI/Gerir_Seg_Info/ProcSetin060/HTML/index.html#diagram/51f83baa-6d70-4e74-92b3-2b11a3469a6e
09	Tentativa de Intrusão	Tentativas de exploração de vulnerabilidades, tentativas de acesso lógico	https://www.tjce.jus.br/seplag/Processos/Administrativos/Desenv_e_Prover_TI/Gerir_Seg_Info/ProcSetin060/HTML/index.html#diagram/51f83baa-6d70-4e74-92b3-2b11a3469a6e
10	Intrusão	Acesso lógico indesejável, comprometimento de conta de usuário, comprometimento de aplicação	https://www.tjce.jus.br/seplag/Processos/Administrativos/Desenv_e_Prover_TI/Gerir_Seg_Info/ProcSetin060/HTML/index.html#diagram/51f83baa-6d70-4e74-92b3-2b11a3469a6e
11	Indisponibilidade de Serviço ou Informação	Negação de serviço, Sabotagem	https://www.tjce.jus.br/seplag/Processos/Administrativos/Desenv_e_Prover_TI/Gerir_Seg_Info/ProcSetin060/HTML/index.html#diagram/51f83baa-6d70-4e74-92b3-2b11a3469a6e
12	Segurança da Informação	Acesso não-autorizado à informação, modificação não autorizada da informação	https://www.tjce.jus.br/seplag/Processos/Administrativos/Desenv_e_Prover_TI/Gerir_Seg_Info/ProcSetin060/HTML/index.html#diagram/51f83baa-6d70-4e74-92b3-2b11a3469a6e
13	Fraude	Violação de direitos autorais, fingir ou falsificar identidade pessoal ou institucional, uso de recursos de forma não-autorizada	https://www.tjce.jus.br/seplag/Processos/Administrativos/Desenv_e_Prover_TI/Gerir_Seg_Info/ProcSetin060/HTML/index.html#diagram/51f83baa-6d70-4e74-92b3-2b11a3469a6e
14	Ataque de Ransomware	O TJCE pode ser alvo de um ataque do tipo Ransomware. **Ransomware** é um tipo de código malicioso, software, utilizado por cibercriminosos. Se um computador/servidor ou rede for infectado com **ransomware**, este malware bloqueia acesso ao sistema ou criptografa os dados. Os cibe criminosos exigem	https://www.tjce.jus.br/seplag/Processos/Administrativos/Desenv_e_Prover_TI/Gerir_Seg_Info/ProcSetin060/HTML/index.html#diagram/51f83baa-6d70-4e74-92b3-2b11a3469a6e

		dinheiro de resgate em troca da liberação dos dados.	
15	Aplicação com Erro Impeditivo (PJE)	Dar celeridade as soluções de problemas com o sistema Pje 1º e 2º Graus	Plano de Continuidade - Aplicação com erro impeditivo.docx
16	Aplicação com Erro Impeditivo (SAJPG)	Dar celeridade as soluções de problemas com o sistema SAJ PG	Em elaboração
17	Aplicação com Erro Impeditivo (DJE)	Dar celeridade as soluções de problemas com o sistema DJE 1º e 2º Graus.	PC GI Erro Impeditivo DJE Administrativo.docx
18	Indisponibilidade de Banco de Dados (PJE)	Dar celeridade as soluções de problemas com o sistema DJE 1º e 2º Graus	Plano de continuidade - Indisponibilidade de Banco de Dados PJE.docx
19	Indisponibilidade de Banco de Dados (SAJPG)	Dar celeridade as soluções de problemas com o sistema SAJ PG	Em elaboração
20	Indisponibilidade de Banco de Dados (DJE)	Dar celeridade as soluções de problemas com o sistema DJE Administrativo.	PC GI Indisponibilidade do BD DJE Adm.docx

Área de Segurança da Informação
Adarildo de Brito Figueiredo – Matr. 8025