GOVERNO DO DISTRITO FEDERAL

POLÍCIA CIVIL DO DISTRITO FEDERAL

PORTARIA Nº 220, DE 18 DE MAIO DE 2023.

Aprova o Documento de Constituição da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais -ETIR, da Polícia Civil do Distrito Federal.

O DELEGADO-GERAL DA POLÍCIA CIVIL DO DISTRITO FEDERAL, no uso de suas atribuições legais, conferidas pelo artigo 4°, incisos I do Decreto Federal nº 10.573, de 14 de dezembro de 2020, e artigo 5º, inciso I do Decreto Distrital nº 42.940, de 24 de janeiro de 2022,

CONSIDERANDO a Resolução nº 01, de 10 de agosto de 2022, que aprova a Política de Segurança da Informação no âmbito da Polícia Civil do Distrito Federal,

R E S O L V E:

Art. 1º Aprovar em forma de anexo, o **Documento de Constituição da Equipe de Prevenção, Tratamento e Resposta a Incidentes de Segurança da Informação (ETIR)**, nos termos da Política de Segurança da Informação da PCDF, aprovada pela Resolução CGSIC nº 01/2022.

Art. 2º Esta Portaria entre em vigor na data de sua publicação em Boletim de Serviço.

ANEXO

DOCUMENTO DE CONSTITUIÇÃO DA EQUIPE DE TRATAMENTO E RESPOSTA A INCIDENTES EM REDES COMPUTACIONAIS DA POLÍCIA CIVIL DO DISTRITO FEDERAL

1. MISSÃO

Facilitar e coordenar as atividades de tratamento e resposta a incidentes em redes computacionais da Polícia Civil do Distrito Federal, apoiar e coordenar as atividades de recuperação de sistemas, analisar ataques e intrusões, cooperar com equipes de outros órgãos e participar em fóruns e redes nacionais e internacionais.

2. PÚBLICO-ALVO

Todos os servidores e colaboradores em atividade na Polícia Civil do Distrito Federal, além da comunidade como um todo, visto que, em razão de incidentes, podem ser prejudicados ou paralisados os serviços prestados pela PCDF.

3. MODELO DE IMPLEMENTAÇÃO

A PCDF adotará o modelo de implementação combinado ou misto, proposto pelo item 7.4 da Norma Complementar nº 05/IN01/DSIC/GSIPR. Nesse modelo, a ETIR/PCDF atuará como equipe central e será responsável por criar as estratégias, gerenciar as atividades e distribuir as tarefas entre as equipes

descentralizadas, além de ser a responsável, perante toda a organização, pela comunicação com o CTIR GOV, bem como com equipes de resposta a incidentes externas.

Além da ETIR/PCDF, haverá equipes distribuídas, autônomas, responsáveis por implementar as estratégias e exercer suas atividades em suas respectivas áreas de responsabilidade.

Sempre que necessário, a ETIR/PCDF poderá solicitar o apoio de equipes especializadas, tais como Perícia, Investigação de Crimes Cibernéticos, Inteligência etc., para a realização de suas atividades.

4. ESTRUTURA ORGANIZACIONAL

A ETIR/PCDF será composta por um Agente Responsável da Divisão de Tecnologia (DITEC), que coordenará os demais membros da equipe e se reportará à Direção da Divisão e ao Gestor de Segurança da Informação. Além disso, o Agente Responsável coordenará as atividades de resposta a incidentes, a elaboração de informes sobre segurança e assuntos correlatos, bem como a comunicação com os demais grupos de resposta a incidentes existentes.

As equipes descentralizadas serão as Seções da DITEC/PCDF, bem como equipes de unidades externas que gerenciem ativos de TI próprios. Tais equipes não possuem vínculo de subordinação com a ETIR.

5. AUTONOMIA

A ETIR/PCDF terá autonomia compartilhada no processo decisório, ou seja, será mais um membro do processo. Poderá recomendar procedimentos a serem executados ou medidas de recuperação durante um ataque, bem como discutir ações a serem tomadas, porém suas recomendações não terão caráter vinculante aos demais membros da DITEC, os quais manterão sua autonomia, bem como aos membros integrantes de outras unidades policiais, subordinados às respectivas chefias.

6. SERVIÇOS

6.1. Tratamento de Incidentes de Segurança

- **Objetivo**: serviço principal da equipe de resposta a incidentes. Dá suporte ao público-alvo no caso de incidentes no parque computacional da PCDF.
- **Definição**: este serviço consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências. Além disso, comunicar imediatamente ao Encarregado Setorial da PCDF os incidentes de segurança que envolverem dados pessoais.
- **Descrição das funções e dos procedimentos:** Gerenciar o ciclo de vida do incidente de segurança da informação em redes de computadores, analisar de sistemas comprometidos, receber informações ou cópia de artefatos maliciosos utilizados em ataques, ou em outras atividades maliciosas.
- **Disponibilidade**: o serviço será oferecido em regime 24/7. Durante o horário comercial, os servidores da ETIR realizarão suas atividades regularmente. No período noturno, finais de semana e feriados, a equipe descentralizada de plantão irá realizar o tratamento inicial dos incidentes reportados, sendo esse trabalho complementado pela ETIR posteriormente. O Agente Responsável ou seu substituto estarão disponíveis constantemente para dirimir dúvidas ou realizar ações que demandem urgência.

6.2. Avaliação de Segurança

- **Objetivo**: buscar e mitigar vulnerabilidades ou intrusões.
- **Definição:** o serviço consiste em efetuar uma análise detalhada da infraestrutura de segurança em redes de computadores da PCDF, com base em requisitos da própria organização, nos pilares de disponibilidade, integridade e confidencialidade e nas melhores práticas de mercado.
- **Descrição das funções e dos procedimentos**
    - Varredura e tratamento de vulnerabilidades, objetivando analisar natureza, mecanismos, consequências e desenvolver estratégias para detecção e correção dessas vulnerabilidades;

    - Detecção de intrusão, por meio da análise do histórico de dispositivos ou do uso de ferramentas especializadas na detecção de tentativas de intrusão, com vistas a identificar ações maliciosas em curso, reduzindo a possibilidade de perda, vazamento ou destruição das informações de uso policial.
    - Elaboração de relatórios de vulnerabilidade, com base em análises dos ativos de rede e comportamento do usuário, consolidando sugestões de melhoria para o ambiente como um todo.
- **Disponibilidade**: o serviço será oferecido em horário comercial, como atividade corriqueira da ETIR.

6.3. Disseminação de cultura de segurança da informação

- **Objetivo**: reduzir vulnerabilidades advindas de ações humanas.
- **Definição**: o serviço consiste em divulgar, de forma proativa, alertas sobre vulnerabilidades de segurança em redes de computadores em geral, que possam impactar o serviço da PCDF, possibilitando que a comunidade se prepare contra ameaças.
- **Descrição das funções e dos procedimentos:**
    - Elaboração, em conjunto com a equipe de desenvolvimento web da PCDF, bem como outras que se entenda relevantes, de informes de segurança, com o objetivo de conscientizar os usuários da rede da PCDF sobre as melhores práticas de segurança da informação.
    - Levantamento de informações sobre a o comportamento dos policiais ou colaboradores, no que diz respeito às suas ações na PCDF. Compreender como o usuário se comporta em face a tentativas de levantamento de informações com engenharia social, ataques do tipo *phishing scam*, trojans, etc., e utilizar essa informação para retroalimentar os serviços de conscientização dos usuários e de elaboração de relatórios de vulnerabilidade.
- **Disponibilidade**: o serviço será ofertado durante o horário de expediente, em ações direcionadas aos usuários localizados em toda a extensão do DF onde se encontrem unidades da Polícia Civil do Distrito Federal.

6.4 Gerenciamento de eventos e auditoria

- **Objetivo**: prevenir e localizar atividades maliciosas e responder a auditorias
- **Definição**: o serviço prevê a análise do histórico de eventos advindos dos diversos ativos conectados à rede corporativa, tais como firewalls, switches, estações de trabalho, servidores, etc., para auditoria de eventos relevantes em redes de computadores, com vistas a monitorar, identificar e prevenir atividade maliciosa e responder a solicitações advindas de outros órgãos.
- **Descrição das funções e dos procedimentos**: para a execução do serviço serão utilizadas diversas ferramentas disponíveis às equipes de rede e de desenvolvimento da DITEC, bem como de ferramenta de Gerenciamento e Correlacionamento de Eventos de Segurança, por meio da qual é possível analisar em uma única console, logs de diversos ativos.
- **Disponibilidade**: o serviço será executado durante o horário de expediente da PCDF, gerando informações demandadas por diferentes órgãos, tais como a Corregedoria de Polícia, Delegacias de Polícia, Tribunais de Contas, etc.

6.5. Coordenação de Gabinete de Crise

- **Objetivo**: prover gerenciamento centralizado para eventos de alto impacto institucional.
- **Definição**: Coordenação de gabinete de crise instaurado pela Direção da DITEC via ordem de serviço, para ventos de alto impacto institucional. O Gabinete de Crise será formado por equipe técnica especializada *ad-hoc* com a finalidade de delimitar, mensurar, analisar e implantar mudanças necessárias para a resolução do incidente.
- **Descrição das funções e dos procedimentos**: com base em informações recebidas das diversas equipes descentralizadas, sugerir ações à Direção da DITEC e aos demais envolvidos, com vistas à rápida resolução de problemas que possam gerar alto impacto à instituição. Após a finalização do evento, elaborar relatório de resposta a incidente, contendo todas as ações sugeridas e executadas, bem como sugestões para melhorias no processo de resposta a incidente.
- **Disponibilidade**: serviço oferecido em regime 24/7, sempre que se detectar evento que se repute passível de gerar alto impacto da instituição. O Agente Responsável, bem como toda a equipe da SRI, estará disponível constantemente, independentemente de horário, para realizar as ações necessárias.

6.6. Receber notificações de incidentes a partir de órgãos de regulação, controle e equipes especializadas

- **Objetivo**: manter canal de comunicação com outras equipes de tratamento e resposta a incidentes, bem como com órgãos de regulação e controle. Pretende-se com isso colaborar efetivamente com a comunidade de segurança da informação, enviando e recebendo informações relevantes sobre o assunto.
- **Definição**: receber alertas provenientes de órgão de regulação e controle da internet no Brasil, de outras equipes de tratamento e resposta a incidentes de segurança em redes computacionais (CSIRT), do CTIR.GOV, bem como de equipes especializadas externas.
- **Descrição das funções e dos procedimentos**: após a formalização da Seção de Resposta a Incidentes da DITEC/PCDF como uma ETIR, nos moldes da normativa existente, será aberto canal de comunicação com a rede de ETIRs de outros órgãos. Serão utilizados os canais formais da Seção (telefone e e-mail) e da PCDF (ofícios).
- **Disponibilidade (quando como e onde será oferecido o serviço)**: o serviço será executado durante o horário de expediente da PCDF, ou em qualquer outro horário, caso se entenda que o assunto a ser informado é urgente.

6.7. Apoiar na construção de políticas e normas de segurança da informação

- **Objetivo:** preservar os ativos de informação, assim como a imagem institucional da PCDF.
- **Definição:** apoio na construção das políticas e normas de segurança da informação e comunicações, que têm por objetivo a instituição de diretrizes estratégicas que visam garantir a disponibilidade, integridade, confidencialidade e autenticidade das informações, bem como atitudes adequadas para manuseio, tratamento, controle e proteção dos dados, informações, documentos e conhecimentos produzidos, armazenados, sob guarda ou transmitidos por qualquer meio ou recurso contra ameaças e vulnerabilidades.
- **Descrição das funções e dos procedimentos:** realização do levantamento das informações necessárias para prestar apoio na elaboração de políticas e normas voltadas à adequação da PCDF às melhores práticas de segurança da informação.
- **Disponibilidade (quando como e onde será oferecido o serviço):** o serviço será executado durante o horário de expediente da PCDF.

7. CANAIS DE COMUNICAÇÃO

No que diz respeito ao público interno, o recebimento de notícias de incidentes poderá ser realizado por abertura de chamado via central de atendimento da empresa de sustentação de Tecnologia da Informação (*e-mail* ou portal de atendimento), telefone da ETIR/PCDF ou *e-mail*. No caso de abertura de chamados abertos junto à empresa de sustentação, o incidente será direcionado à fila do ponto focal da ETIR/PCDF na DITEC, visto ser esta a Divisão responsável pela gerência dos ativos de TI na PCDF.

Em caso de ligações telefônicas ou mensagens de correio eletrônico, iniciados tanto pelo público interno quanto externo, um dos integrantes da equipe irá registrar o chamado e iniciar o atendimento, nos termos do fluxo de operação determinado em documento próprio.

ROBSON CÂNDIDO DA SILVA