Documento de constituição da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR

1. Missão

Planejar, coordenar e executar atividades de tratamento e resposta a incidentes em redes computacionais, receber e notificar qualquer evento adverso à segurança da informação, confirmado ou sob suspeita, relacionado às redes de computadores, preservando os dados, as informações e a infraestrutura do Ministério da Saúde.

2. Benefícios esperados da ETIR

- Ter uma gestão centralizada para as questões de incidentes em redes computacionais;
- Ser um ponto central para comunicação e registros de incidentes;
- Investigar incidentes;
- Definir planos de contenção e estabelecer ações para promover a continuidade dos serviços e sistemas em caso de incidentes graves;
- Acompanhar de forma objetiva a evolução e o domínio dos aspectos da segurança.

3. Público Alvo

Usuários da rede corporativa de computadores e sistemas do Ministério da Saúde, podendo ainda auxiliar os núcleos Estaduais, Hospitais Federais, órgãos e/ou unidades vinculadas ao Ministério da Saúde no tratamento de incidentes sempre que autorizado ou demandado pela alta direção da instituição.

4. Comunicação

A comunicação dos incidentes de segurança em rede de computadores à ETIR será feita por meio de:

- E-mail, pelos endereços: abuse@saude.gov.br; abuse@datasus.gov.br e abuse@sus.gov.br;
- Contato telefônico via central de suporte e atendimento ao usuário (Ramal 2222) para usuários de Brasília e o telefone 08005410203 para as demais localidades;
- Correspondências oficiais (memorandos, ofícios);
- Pessoalmente, em casos emergenciais;
- Ferramental tecnológico, eventos detectados pelo monitoramento da ETIR.

O agente responsável pela ETIR deve comunicar a ocorrência de incidentes de segurança em redes de computadores ao Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal –

CTIR.Gov, conforme procedimentos a serem definidos pelo próprio CTIR Gov, com vistas a permitir soluções integradas para a Administração Pública Federal - APF, bem como a geração de estatísticas, conforme orienta a Norma Complementar 05/IN01/DSIC/GSIPR.
Nos casos aplicáveis, também é dever do agente responsável pela ETIR interagir com forças policiais especializadas e com o judiciário.
A ETIR emitirá informativos sobre novas vulnerabilidades e novas atualizações utilizando os seguintes meios de comunicação: e-mails informativos, publicações, intranet, além de *feedback* dos incidentes tratados.

5. Registro

Todo incidente deve ser registrado em *software* específico, homologado pelo Ministério da Saúde, por membro da equipe central da ETIR que procederá com a consolidação das informações. Caso o incidente ocorra no período de plantão ou que o membro da ETIR não esteja presente, o registro ficará a cargo do operador do Centro de Operação de Redes – NOC do DATASUS.

6. Atividades da ETIR

Os serviços providos pela ETIR estão divididos em 2 (dois) grupos de atuação, Reativas e Proativas, sendo, sua atuação principal os serviços proativos.

Proativas	
Serviço	**Descrição**
Monitorar incidentes	Observar os eventos de segurança com o objetivo de determinar tendências e padrões de atividades de invasores, com vistas a adotar e recomendar estratégias de prevenção adequadas. Coletar indicadores estatísticos.
Disseminar informações relativas a novos ataques e tendências	Pesquisar informações sobre novas ameaças a redes computacionais, novas soluções para conter as ameaças e informar às áreas responsáveis.
Disseminar informações de novas atualizações de *softwares*	Pesquisar informações referentes a novas atualizações dos *softwares* instalados na rede.
Comunicação	Comunicar incidentes de segurança a órgãos competentes para fins estatísticos.

Tabela 1: Descrição dos serviços prestados pela ETIR

Reativos	
Serviço	**Descrição**
Análise de incidentes	Examinar todas as informações disponíveis sobre um incidente, incluindo artefatos, evidências e *logs* relacionadas ao evento.
Investigação de incidentes	Identificar o escopo do incidente, sua extensão, natureza e quais os impactos causados.
Recomendação de tratamento de incidente	Após análise e investigação do incidente, a ETIR emitirá documentos com recomendações para o tratamento correto dos incidentes.

Tabela 2: Descrição dos serviços prestados pela ETIR

7. Acionamento

A ETIR será acionada para atividades reativas, sempre que ocorrer a confirmação de um incidente na rede corporativa de computadores e sistemas do Ministério da Saúde.
O agente responsável acionará a equipe central que juntamente com a equipe distribuída realizará os serviços reativos, que devem ter acesso aos arquivos de registros de atividades (*logs*), além de evidências coletadas por outras equipes, de forma a apoiar a ETIR na análise e investigação dos incidentes.
Em casos de recorrência de incidentes identificados no serviço de monitoramento de incidentes, a ETIR encaminhará as análises das ocorrências às equipes responsáveis juntamente com uma proposta de tratamento adequado dos incidentes. Serão informados os impactos que poderão advir caso as recomendações da ETIR não sejam seguidas. Todas as etapas devem ser documentadas e armazenadas para o acesso de gestores e técnicos envolvidos na investigação e tratamento.

8. Modelo de Implementação

O modelo adotado será o ***Modelo 4 – combinado ou misto***, descrito na Norma Complementar 05/IN01/DSIC/GSIPR, para o qual será utilizada uma equipe central de tratamento e respostas a incidentes e equipes de apoio distribuídas pela organização.
A Equipe central será a responsável por criar as estratégias, gerenciar as atividades e distribuir as tarefas entre as equipes distribuídas, enquanto essas equipes serão responsáveis por implementar as estratégias e exercer suas atividades em suas respectivas áreas de responsabilidade
A ETIR deverá guiar-se por padrões e procedimentos técnicos e normativos no contexto de tratamento de incidentes de rede, desenvolvidos internamente no Ministério da Saúde, ressalvado que as normas estarão de acordo com a legislação do Departamento de Segurança da Informação e Comunicação – DSIC/GSI/PR.

9. Estrutura Organizacional

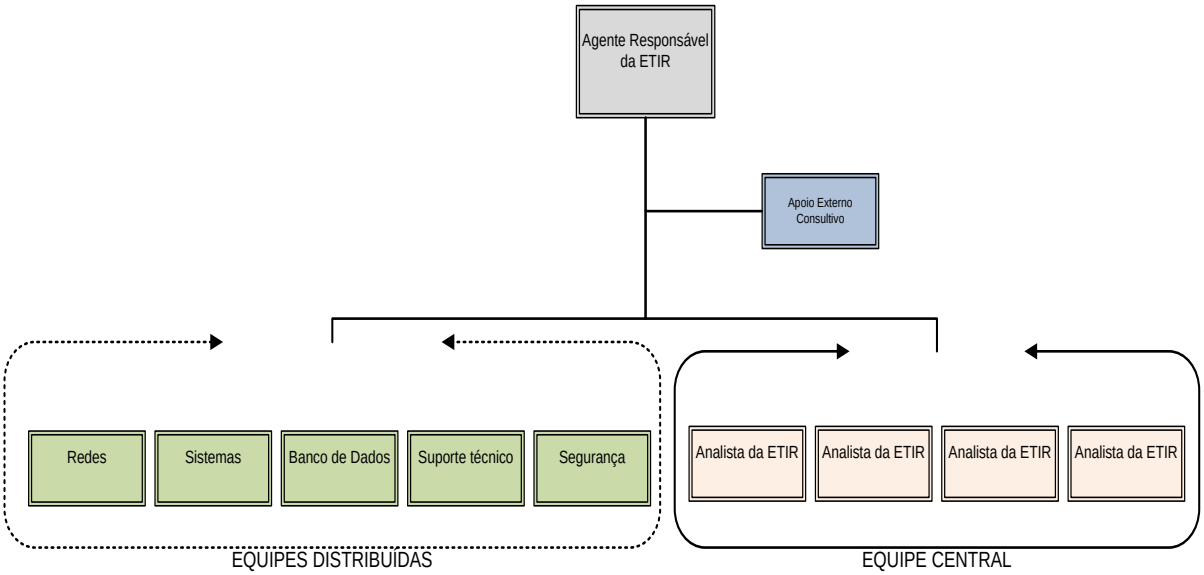

Figura 1: Organograma de composição da ETIR

Perfil	Agente responsável pela ETIR
Habilidade Profissional	• Experiência em Gerência de Projetos; • Conhecimentos avançados em Segurança da Informação; • Conhecimentos gerais sobre tratamento de incidentes em redes computacionais; • Conhecimentos em gestão de pessoas.
Habilidade Pessoal	• Capacidade de liderar equipes; • Aptidão para explicar questões técnicas difíceis com termos de fácil entendimento; • Alta capacidade de organização; • Capacidade de atuar sob pressão; • Habilidade na comunicação verbal e escrita; • Facilidade de comunicação com diferentes níveis da organização.
Competências	• Coordenar as atividades de análise, investigação e resposta a incidentes; • Coordenar e orientar os membros da ETIR na gestão de incidentes; • Coordenar o processo de capacitação e

	treinamento dos membros da ETIR.
Atribuições	• Prover os meios necessários para a capacitação e o aperfeiçoamento técnico dos membros da Equipe; • Prover infraestrutura necessária para o funcionamento da ETIR; • Garantir que os incidentes em Redes Computacionais do DATASUS sejam registrados e investigados; • Assegurar que haja canal de comunicação com os usuários informantes de incidentes de segurança da informação; • Interagir com as demais áreas do Ministério da Saúde durante os incidentes; • Prestar assessoria técnica na elaboração de políticas, normas, pareceres e na especificação técnica de produtos e equipamentos direcionados a segurança da informação e comunicação.
Responsabilidades	• Planejar, coordenar e orientar as atividades relacionadas à gestão de incidentes; • Informar às autoridades competentes os assuntos relacionados a incidentes de redes computacionais; • Informar ao CTIR.GOV as estatísticas de incidentes para manutenção e atualização da base de dados do Governo Federal; • Exercer funções necessárias para implementação e manutenção das atividades da ETIR.

Tabela 3: Perfil agente responsável pela ETIR

Perfil	Sistemas
Habilidade Profissional	• Conhecimentos avançados em sistemas operacionais para servidores *Windows* e *Linux;* • Conhecimentos avançados dos sistemas corporativos do DATASUS; • Conhecimentos avançados em ferramentas de mensageria.
Habilidade Pessoal	• Flexibilidade, criatividade e espírito de equipe; • Capacidade analítica; • Organização; • Capacidade de atuar sob pressão;

	• Habilidade na comunicação verbal e escrita. • Facilidade de aprendizado e implementação de novas tecnologias.
Competências	• Realizar atividades de gestão a incidentes em sistemas operacionais e corporativos.
Atribuições	• Analisar e investigar incidentes em sistemas operacionais e sistemas corporativos; • Conter incidentes em sistemas operacionais e sistemas corporativos; • Tratar incidentes em sistemas operacionais e sistemas corporativos; • Recomendar ações para tomada de decisões sobre os incidentes em sistemas corporativos e sistemas operacionais.
Responsabilidades	• Receber notificações sobre incidentes em sistemas operacionais e sistemas corporativos; • Efetuar análise e investigação dos incidentes em sistemas operacionais e sistemas corporativos, recomendando melhorias e procedimentos de contenção e minimização de impactos.

Tabela 4: Perfil de Sistemas

Perfil	Segurança Lógica
Habilidade Profissional	• Conhecimentos avançados em ferramentas de segurança; • Conhecimentos avançados em Squid / Microsoft ISA Server; • Conhecimento avançado em leitura de *LOG*; • Conhecimento avançado das ameaças à segurança; • Conhecimentos avançados de ferramentas de IDS e IPS; • Conhecimentos avançados em roteamento, elementos de conectividade e firewalls.
Habilidade Pessoal	• Flexibilidade, criatividade e espírito de equipe; • Capacidade analítica; • Organização; • Capacidade de atuar sob pressão; • Boas competências de comunicação oral e escrita;.
Competências	• Realizar atividades de gestão a incidentes em

	segurança de redes.
Atribuições	• Analisar e investigar incidentes em firewalls e proxies; • Conter incidentes relacionados aos ativos de segurança de rede; • Apoiar o tratamento de incidentes em sistemas operacionais e sistemas corporativos; • Recomendar ações para tomada de decisões na recuperação de incidentes.
Responsabilidades	• Receber incidentes em segurança de ativos de rede; • Efetuar análise e investigação dos incidentes relacionados à segurança de rede de computadores.

Tabela 5: Perfil Segurança Lógica

Perfil	Redes
Habilidade Profissional	• Conhecimentos avançados em protocolos de rede; • Conhecimentos avançados de DNS; • Conhecimentos avançados em servidores de aplicação web.
Habilidade Pessoal	• Flexibilidade, criatividade e espírito de equipe; • Capacidade analítica; • Organização; • Capacidade de atuar sob pressão; • Boas competências de comunicação e escrita.
Competências	• Realizar atividades de gestão de incidentes em redes de computadores.
Atribuições	• Analisar e investigar incidentes em roteadores, *switches e* elementos de conectividade; • Conter incidentes relacionados aos ativos de conectividade de rede; • Apoiar o tratamento de incidentes em sistemas; • Recomendar ações para tomada de decisão na recuperação do ambiente após incidentes.
Responsabilidades	• Receber incidentes relacionados aos ativos de redes; • Efetuar análise e investigação dos incidentes

	relacionados aos ativos de redes.

Tabela 6: Perfil de Redes

Perfil	Banco de Dados
Habilidade Profissional	• Conhecimentos em *Oracle*; • Conhecimentos em *MSSQL*; • Conhecimentos em *PLSQL*; • Conhecimentos em *PostgreSQL*; • Conhecimento em *MySQL*; • Conhecimento nos sistemas aplicativos utilizados no Ministério da Saúde.
Habilidade Pessoal	• Flexibilidade, criatividade e espírito de equipe; • Capacidade analítica; • Organização; • Capacidade de atuar sob pressão; • Boas competências de comunicação e escrita.
Competências	• Realizar atividades de gestão de incidentes em sistemas de gerenciamento de bancos de dados.
Atribuições	• Analisar e investigar incidentes em bancos de dados; • Conter incidentes relacionados aos bancos de dados; • Apoiar o tratamento de incidentes em sistemas; • Recomendar ações para tomada de decisão na recuperação dos incidentes.
Responsabilidades	• Receber notificações sobre incidentes relacionados aos bancos de dados; • Efetuar análise e investigação dos incidentes ocorridos nos ambientes de banco de dados.

Tabela 7: Perfil de Bancos de Dados

Perfil	Suporte de técnico
Habilidade Profissional	• Conhecimentos avançados em sistemas operacionais *Windows* e *Linux (estações de trabalhos)*; • Conhecimentos avançados em *hardware*; • Conhecimentos avançados em antivírus.
Habilidade Pessoal	• Flexibilidade, criatividade e espírito de equipe; • Capacidade analítica; • Organização;

	• Capacidade de atuar sob pressão; • Boas competências de comunicação oral e escrita.
Competências	• Realizar atividades de gestão de incidentes ocorridas em estações de trabalho.
Atribuições	• Analisar e investigar incidentes ocorridos ou que envolvam estações de trabalho; • Conter incidentes em estações de trabalho; • Apoiar o tratamento de incidentes em sistemas aplicativos; • Recomendar ações para tomada de decisão na recuperação dos incidentes.
Responsabilidades	• Receber notificações de incidentes relacionados a estações de trabalho; • Efetuar análise e investigação dos incidentes ocorridos em estações de trabalho.

Tabela 8: Perfil de Suporte técnico

Perfil	Analista da ETIR
Habilidade Profissional	• Conhecimentos básicos do negócio; • Conhecimentos de ferramentas de monitoração de incidentes; • Conhecimentos avançados de ferramentas de monitoramento de intrusão; • Conhecimentos avançados de *scanners* de vulnerabilidades; • Conhecimentos avançados do *software* de registro de incidentes; • Conhecimentos sobre a tipificação de incidentes; • Conhecimentos sobre gerenciamento de incidentes; • Conhecimentos sobre tratamentos de incidentes em redes e sistemas computacionais; • Conhecimento de análise e interpretação de *logs* de sistemas; • Conhecimentos de auditoria de sistemas; • Conhecimentos de ferramentas de segurança de sistemas; • Conhecimentos para treinamento de equipes;
Habilidade Pessoal	• Flexibilidade e espírito de equipe; • Criatividade; • Capacidade analítica;

	• Análise crítica; • Raciocínio lógico; • Organização; • Capacidade de atuar sob pressão; • Boas competências de comunicação oral e escrita;
Competências	• Realizar atividades de monitoramento de eventos para registro de incidentes; • Realizar atividades de gerenciamento de incidentes; • Acompanhar a resposta aos incidentes; • Coletar os *logs* e evidencias dos incidentes; • Analisar e investigar os *logs* e evidencias junto com as equipes distribuídas; • Apoiar as equipes distribuídas no processo de tratamento e erradicação de incidentes; • Auditar o processo de tratamento e erradicação de incidentes; • Criar métodos de prevenção a ocorrência de incidentes; • Elaborar treinamentos de gerenciamento de incidentes;
Atribuições	• Registrar incidentes de segurança no ambiente computacional do Ministério da Saúde; • Encaminhar as demandas de incidentes para que as equipes distribuídas respondam aos incidentes; • Acompanhar o processo de resposta aos incidentes juntos as equipes distribuídas; • Coletar e examinar *logs* de sistemas, firewalls e aplicativos; • Elaborar juntamente com as equipes distribuídas mecanismos de tratamento e erradicação de incidentes; • Emitir relatórios diagnósticos sobre o ambiente monitorado; • Emitir relatórios com recomendações de tratamento de incidentes; • Gerar relatórios estatísticos sobre ocorrências externas de incidentes para apoiar o processo proativo; • Gerar relatórios de indicadores sobre incidentes ocorridos para colaborar na tomada de decisão da alta direção; • Reportar-se ao gestor com soluções e avaliações

	relacionadas aos incidentes;
Responsabilidades	• Monitorar os ativos tecnológicos em busca de eventos que sejam caracterizados como incidentes, efetuando o registro para tratamento; • Colaborar com a análise e investigação de incidentes; • Recomendar tratamentos de incidentes; • Propor melhorias no processo de gerenciamento e auditoria dos incidentes;

Tabela 9: Perfil Analista da ETIR

O agente responsável pela ETIR deve ser obrigatoriamente um servidor efetivo de carreira, conforme a orientação da Norma Complementar 05/IN01/DSIC/GSIPR. Os membros serão selecionados dentre o pessoal existente, com perfil técnico adequado às funções de tratamento de incidentes de rede.
Cada membro deve ter ao menos um substituto com conhecimentos técnicos comprovados e equivalentes aos efetivos, sendo que a equipe poderá ser estendida com a inclusão de representantes legais de áreas especificas da organização, advogados, estatísticos, recursos humanos, gestão de risco, controle interno, consultores técnicos, grupo de investigação ou qualquer outro que a ETIR entenda ser adequado para o desenvolvimento de suas atividades.

Os membros da ETIR estarão subordinados ao agente responsável pela ETIR sempre que estes forem acionados. A subordinação da ETIR será definida posteriormente pela direção do Departamento de Informática do SUS – DATASUS por meio de dispositivo próprio da instituição.

10. Autonomia da ETIR

A ETIR terá autonomia compartilhada trabalhando em conjunto com outros setores do Ministério da Saúde a fim de auxiliar no processo de tomada de decisão.
A ETIR poderá participar ativamente do processo decisório. Neste caso, a equipe poderá recomendar os procedimentos a serem executados ou as medidas de recuperação durante um ataque e discutirá as ações a serem tomadas (ou os impactos possíveis caso não sejam seguidas as recomendações), com os outros membros da organização.

11. Revisão e Publicação

Este documento deve ser revisado ao menos uma vez a cada 24 (vinte e quatro) meses a partir da data publicação, para que seja adequado às normas e legislações vigentes à época ou sempre que houver necessidade de adequação.