Sumário

Histórico de Revisão			
Versão	**Data**	**Responsável**	**Aprovação**
00	08/12/2014	STI	RD nº 08/324ª de 08/12/2014

Informações Adicionais

Este Instrumento Normativo revoga a CSIC 003 - Norma para Gestão de Incidentes de Segurança da Informação e Comunicações, e o documento CSIC 003ª - Constituição da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais da EPE, aprovados pela RD 01/231ª de 30/11/2011 e vigente até esta data.

1. Objetivo

Estabelecer as regras que norteiam as atividades da Gestão de Incidentes de Segurança da Informação e Comunicações da Empresa de Pesquisa Energética (EPE).

2. Campo de Aplicação

Aplica-se a todas as áreas da EPE.

3. Definições e Siglas

3.1. Definições

Acesso – Ato de ingressar, transitar, conhecer ou consultar a informação, seja local, ou remotamente, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade.

Agente Responsável – Empregado ou servidor público, ocupante de cargo efetivo de órgão ou entidade da Administração Pública Federal, direta ou indireta incumbido de chefiar e gerenciar a ETIR.

Ameaça – Conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.

Artefato Malicioso – Qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores.

Ativos de Informação – Os meios de armazenamento, transmissão e processamento da informação; os equipamentos necessários a isso; os sistemas utilizados para tal; os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso.

Auditoria – Processo de exame cuidadoso e sistemático das atividades desenvolvidas, cujo objetivo é averiguar se estão de acordo com as disposições planejadas e estabelecidas previamente, se foram implementadas com eficácia e se estão adequadas e em conformidade à consecução dos objetivos.

Autenticação – Processo de identificação das partes envolvidas em um processo.

Autenticidade – Propriedade de que a informação foi produzida, modificada ou descartada por uma determinada pessoa física, órgão, entidade ou sistema.

Autorização – Processo que visa garantir que as informações são acessíveis exclusivamente àqueles com permissão de acesso.

Cadeia de Custódia – Refere-se à documentação ou ao registro cronológico, mostrando a coleta, custódia, controle, transferência, análise e o descarte de evidência de um incidente de SIC, desde o momento em que for obtida até quando for apresentada administrativa ou judicialmente.

Caixa Postal – Área de armazenamento de mensagens de correio eletrônico associada a um endereço eletrônico.

Comunidade ou Público Alvo – Conjunto de pessoas, setores, ou entidades atendidas pela ETIR.

Confidencialidade – Propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado.

Coleta de evidências de segurança em redes computacionais – Processo de obtenção de itens físicos que contém uma potencial evidência, mediante a utilização de metodologia e ferramentas adequadas. Este processo inclui a aquisição, ou seja, a geração das cópias das mídias, ou coleção de dados que contenham evidências do incidente.

CTIR-GOV – Integra o DSIC do Gabinete de Segurança Institucional da Presidência da República (GSIPR) e tem como finalidade o atendimento aos incidentes em redes de computadores pertencentes à Administração Pública Federal. Além disso, atua como centro de coordenação entre as partes envolvidas, acompanhando as ações de tratamento e resposta aos incidentes de segurança.

Criticidade – Define a importância da informação para a continuidade do negócio da instituição.

Contêineres dos Ativos de Informação – O contêiner é o local onde “vive” o ativo de informação, onde está armazenado, como é transportado ou processado.

Custodiante do ativo de informação – É o responsável pelos contêineres dos ativos de informação e pela aplicação dos níveis de controles de segurança em conformidade com as exigências de segurança da informação e comunicações comunicadas pelos proprietários dos ativos de informação.

Disponibilidade – Propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade.

Endereço IP (Internet Protocol) – Refere-se ao conjunto de elementos numéricos ou alfanuméricos que identifica um dispositivo eletrônico em uma rede de computadores.

ETIR – Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais, composta por pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores.

Gestor do ativo de informação – Indivíduo legalmente instituído por sua posição e/ou cargo, o qual é responsável primário pela viabilidade e sobrevivência dos ativos de informação.

Incidente de Segurança em redes computacionais – Qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores.

Informação – Conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado.

Informação Sigilosa – Informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquelas abrangidas pelas demais hipóteses legais de sigilo.

Integridade – Propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.

Log ou Registro de Auditoria – Registro de eventos relevantes em um dispositivo ou sistema computacional.

Metadados – Conjunto de dados estruturados que descrevem informação primária.

Navegador – *Software* utilizado para visualização de páginas na web (por exemplo, o Internet Explorer).

Preservação de evidência de incidentes em redes computacionais – É o processo que compreende a salvaguarda das evidências e dos dispositivos, de modo a garantir que os dados ou metadados não sofram alteração, preservando-se a integridade e a confidencialidade das informações.

Recurso de Trabalho Remoto – Categorias de ativos de informação (notebooks, telefones celulares, pagers, modems, pendrives), disponibilizados aos usuários para fins de execução de trabalho remoto (fora das instalações da empresa), ou para permitir a comunicação dos mesmos, visando a otimização e flexibilização do trabalho.

Risco de Segurança da Informação e Comunicações – Potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da Empresa.

Serviço de Correio Eletrônico – Sistema de mensageria utilizado para criar, enviar, encaminhar, responder, transmitir, arquivar, manter, copiar, mostrar, ler ou imprimir informações, com o propósito de comunicação entre redes de computadores ou entre pessoas ou grupos.

Serviço de Rede – É uma aplicação distribuída que executa em dois ou mais computadores conectados por uma rede.

Site – Conjunto de páginas disponibilizadas no ambiente web (rede mundial de computadores).

Tratamento da Informação Classificada – Conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle de informação classificada em qualquer grau de sigilo.

Tratamento de Incidentes de Segurança em Redes Computacionais – Serviço que 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.

Usuário – Qualquer empregado ocupante de cargo efetivo, cargo em comissão, cedido, prestador de serviço terceirizado, estagiário ou qualquer outro indivíduo que tenha acesso, de forma autorizada, aos recursos computacionais da EPE.

Vulnerabilidade – Conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação.

3.2. Siglas

CTIR-GOV – Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal

ETIR – Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais

GSIC – Gestor de Segurança da Informação e Comunicações

SIC – Segurança da Informação e Comunicações

4. Documentos de Referência

- GSI IN 1/2008: Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.
- INC Nº 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009: 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.
- INC Nº 08/IN01/DSIC/GSIPR, de 19 de agosto de 2010: Disciplina o gerenciamento de Incidentes de Segurança em Redes de Computadores realizado pelas Equipes de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais (ETIR) dos órgãos e entidades da Administração Pública Federal, direta e indireta.
- INC Nº 21/IN01/DSIC/GSIPR, de 08 de outubro de 2014: Fornece diretrizes para registro, coleta e preservação de evidências de incidentes de segurança em redes computacionais dos órgãos e entidades da Administração Pública Federal, direta e indireta, e a comunicação às autoridades competentes.
- ABNT NBR ISO/IEC 27002:2013: Fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação e comunicações da Empresa.
- Política de Segurança da Informação e Comunicações: Estabelece orientações específicas sobre as práticas de Segurança da Informação a serem adotadas para o cumprimento da Missão e o alcance da Visão da Empresa.

5. Descrição

5.1. Gestão de Incidentes de Segurança da Informação e Comunicações

Estabelece regras para a gestão de incidentes de SIC a fim de minimizar o impacto em segurança.

5.1.1. Papéis e Responsabilidades

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

- Executar as atividades de tratamento e resposta a incidentes na rede computacional da Empresa.
- Executar o tratamento de artefatos maliciosos e vulnerabilidades.

- Executar a emissão de alertas e advertências relacionadas a incidentes de SIC.
- Divulgar, de forma proativa, alertas sobre vulnerabilidades e problemas de incidentes de segurança em redes de computadores em geral.
- Efetuar análises detalhadas da infraestrutura de segurança em redes de computadores da organização com base nos requisitos da própria Empresa e nas melhores práticas do mercado.
- Executar tarefas que viabilizem ou facilitem a detecção de intrusão.
- Disseminar informações relacionadas à segurança, que sejam ostensivas, e que facilitem a pesquisa e utilização por todos os membros da ETIR.

Gestor de Segurança da Informação e Comunicações - GSIC

- Coordenar a instituição, implementação e manutenção da infraestrutura necessária à ETIR.
- Tomar medidas que visem minimizar os prejuízos causados por falhas e incidentes de SIC e garantir que tais incidentes sejam monitorados.

Usuários

- Comunicar imediatamente ao GSIC sobre todo e qualquer evento, vulnerabilidade ou incidente que afete a segurança da informação e comunicações.
- Registrar e comunicar pontos fracos de segurança, observados ou suspeitos, e quaisquer ameaças a sistemas ou serviços, a sua gerência, ou diretamente ao GSIC, com a máxima rapidez.

5.1.2. Detalhamento

Estão abrangidos nesta norma o tratamento de todos os eventos de SIC contrários ao ordenamento jurídico em vigor, bem como com a Política de SIC da EPE e com as normas que a apoiam, como por exemplo:

- Divulgação não autorizada de dado ou informação sigilosa contida em sistema, arquivo ou base de dados da EPE;
- Invasão de dispositivo informático;
- Interrupção de serviço telemático ou de informação de utilidade pública;
- Inserção ou facilitação de inserção de dados falsos, alteração ou exclusão de dados corretos nos sistemas informatizados ou bancos de dados da EPE;

- Modificação ou alteração por usuário de sistema de informação ou programa de informática sem autorização;
- Distribuição, armazenamento ou conduta vinculada à pornografia infantil; e
- Interceptação telemática clandestina.

5.1.2.1. Identificação das Falhas e Incidentes

Para minimizar os prejuízos causados por falhas e incidentes de SIC e garantir que tais incidentes sejam monitorados, deverão ser seguidas as seguintes regras:

- Estabelecer canais de comunicação para incidentes de segurança da informação que sejam de fácil acesso aos empregados e divulgá-los apropriadamente.
- Atuar proativamente na identificação de potenciais falhas de segurança de informação.
- Assegurar que as pessoas que comunicarem incidentes de SIC sejam informadas dos resultados depois que o incidente tenha sido tratado e encerrado (solucionado ou não).
- Utilizar casos de incidentes de segurança da informação e comunicações como exemplo no treinamento de conscientização dos usuários sobre o que poderia acontecer e como reagir a tais incidentes e, principalmente, como evitá-los no futuro, desde que respeitando as questões referentes ao nível de sigilo e confidencialidade da informação.
- Tomar medidas para prevenir a recorrência dos incidentes de SIC.
- Coletar trilhas de auditoria e evidências similares para embasamento de eventuais processos administrativos, criminais ou judiciais.
- Documentar detalhadamente todas as ações de emergência adotadas no tratamento de incidentes de SIC.

5.1.2.2. Constituição da ETIR

A ETIR da EPE tem por finalidade a facilitação e a coordenação das atividades de tratamento e resposta a incidentes em redes computacionais, através da gestão dos comunicados de fragilidades e eventos de SIC, buscando viabilizar o cumprimento da missão organizacional e assegurar as propriedades básicas de SIC.

5.1.2.2.1. Estrutura Funcional da ETIR

O agente responsável pela ETIR será o GSIC da EPE, que, dentre outras atribuições e competências, será o interlocutor junto ao CTIR-GOV. Esse Agente também será o responsável por criar os procedimentos internos, gerenciar as atividades e atribuir tarefas para os componentes da ETIR.

Cabe, também, ao Agente Responsável pela ETIR o acompanhamento do processo de identificação e classificação de ativos de informação, o acompanhamento e registro de eventos de segurança e a utilização de metodologia e ferramentas reconhecidas e recomendadas em referenciais técnicos quanto ao processo de coleta e preservação de evidências.

Não existirá um grupo dedicado exclusivamente às funções da ETIR.

A equipe será formada por:

- Membros da área de TIC (administradores de sistema ou de segurança, administradores de banco de dados, administradores de rede, analistas de suporte) que, além de suas funções regulares, passarão a desempenhar as atividades relacionadas ao tratamento e à resposta a incidentes em redes computacionais;
- 1 (um) representante da Consultoria Jurídica;
- 1 (um) representante da área de Recursos Humanos; e
- 1 (um) representante da Assessoria de Comunicação Social.

A equipe desempenhará suas atividades de forma reativa e/ou proativa, realizando a classificação, filtragem, resolução e acompanhamento dos incidentes de SIC.

O GSIC da EPE será o responsável por providenciar os meios necessários para a capacitação e o aperfeiçoamento técnico dos membros da equipe, bem como a infraestrutura necessária para a condução dos serviços.

5.1.2.2.2. Autonomia da ETIR

A ETIR da EPE participará do processo de decisão acerca dos incidentes de segurança de forma compartilhada, trabalhando em acordo com os demais setores pertinentes da EPE, a fim de estabelecer quais medidas devam ser adotadas para resposta e tratamento de incidentes em redes computacionais.

O agente responsável pela ETIR atuará no processo decisório, podendo recomendar os procedimentos a serem executados ou as medidas de recuperação durante um ataque e discutirá as ações a serem tomadas (ou as repercussões se as recomendações não forem seguidas) com os setores pertinentes da EPE.

5.1.2.2.3. Serviços Básicos da ETIR

São serviços básicos providos pela ETIR:

Serviço	Descrição
Tratamento de artefatos maliciosos	Este serviço prevê o recebimento de informações ou cópia do artefato malicioso que foi utilizado no ataque, ou em qualquer outra atividade desautorizada ou maliciosa. Uma vez recebido o artefato, o mesmo deve ser analisado, ou seja, deve-se buscar a natureza do artefato, seu mecanismo, versão e objetivo, para que seja desenvolvida, ou pelo menos sugerida, uma estratégia de detecção, remoção e defesa contra estes artefatos.
Serviço	**Descrição**
Tratamento de vulnerabilidades	Este serviço prevê o recebimento de informações sobre vulnerabilidades, quer sejam em *hardware* ou *software*, objetivando analisar sua natureza, mecanismo e suas consequências, além de desenvolver estratégias para detecção e correção dessas vulnerabilidades.
Emissão de alertas e advertências	Este serviço consiste em divulgar alertas ou advertências imediatas em reação a um incidente de segurança ocorrido em redes de computadores, com o objetivo de advertir a comunidade ou dar orientações sobre como a comunidade deve agir diante do problema.
Anúncios	Este serviço consiste em divulgar, de forma proativa, alertas sobre vulnerabilidades e problemas de incidentes de segurança em redes de computadores em geral, cujos impactos sejam de médio e longo prazo, possibilitando que a comunidade se prepare contra novas ameaças.
Prospecção ou monitoração de novas tecnologias	Este serviço prospecta e/ou monitora o uso de novas técnicas das atividades de intrusão e tendências relacionadas, as quais ajudarão a identificar futuras ameaças. Inclui a participação em listas de discussão sobre incidentes de segurança em redes de computadores e o acompanhamento de notícias na mídia em geral sobre o tema.
Avaliação de segurança	Este serviço consiste em efetuar uma análise detalhada da infraestrutura de segurança em redes de computadores da EPE com base em requisitos da própria EPE ou em melhores práticas de mercado. O serviço pode incluir: revisão da infraestrutura, revisão de processos, varredura da rede e testes de penetração.

Detecção de intrusão	Este serviço prevê a análise do histórico de dispositivos que detectam as tentativas de intrusões em redes de computadores, com vistas a identificar e iniciar os procedimentos de resposta a incidente de segurança em redes de computadores, com base em eventos com características pré-definidas, que possam levar a uma possível intrusão e, ainda, possibilitar o envio de alerta em consonância com padrão de comunicação previamente definido entre a ETIR e o CTIR Gov.
Disseminação de informações relacionadas à segurança	Este serviço fornece de maneira fácil e abrangente a possibilidade de encontrar informações úteis no auxílio do tratamento de incidentes de segurança em redes computacionais.

Para a execução de seus serviços, a ETIR utilizará produtos e serviços disponibilizados pela STI, dentre eles: processos de gestão de serviços de TIC (gestão de incidentes, gestão de problemas, gestão de configuração e de mudanças), *hardware* e *software* que permitam a gestão automatizada dos serviços e registro e trato dos incidentes relacionados à SIC.

5.1.2.3. Tratamento e Resposta a Incidente

Com a finalidade de executar as atividades de tratamento e de resposta a incidentes em redes computacionais, a ETIR deve:

- Registrar todos os incidentes notificados ou detectados, a fim de manter um registro histórico de todas as atividades da ETIR.
- Investigar as causas dos incidentes de segurança da informação e comunicações e tomar as ações corretivas necessárias.
- Acionar as autoridades policiais competentes para a adoção dos procedimentos legais julgados necessários, ouvido o diretor da DGC.
- Observar os procedimentos para preservação das evidências, exigindo consulta às orientações sobre a cadeia de custódia, conforme procedimento específico.
- Executar uma análise crítica sobre os registros de falhas para assegurar que as mesmas tenham sido satisfatoriamente resolvidas.
- Executar uma análise crítica sobre as medidas corretivas adotadas para assegurar que não tenham ocorrido comprometimentos (criação de vulnerabilidades) na execução de medidas para solucionar um incidente de SIC e que as ações tenham sido devidamente autorizadas pelo Agente Responsável ou pelo GSIC.
- Implementar mecanismos para permitir a quantificação e monitoração dos tipos, volumes e custos de incidentes e de falhas de funcionamento.

- Identificar incidentes ou falhas repetidas ou de alto impacto, isto é, incidentes que possam acarretar graves riscos ao negócio ou que atinjam um grande contingente de usuários.
- Indicar a necessidade de controles aperfeiçoados ou adicionais para limitar a frequência, os danos e o custo de futuras ocorrências de incidentes.
- Observar a legislação em vigor e os normativos internos no tratamento de informações classificadas com algum nível de sigilo, de forma a viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação sob posse ou custódia da ETIR.

5.1.2.4. Comunicação dos Incidentes de Segurança à ETIR da EPE

A comunicação dos incidentes de segurança, vulnerabilidades percebidas e demais eventos de segurança por parte dos usuários com a ETIR se dará por meio de ferramenta de *software* que permita automatização dos registros desses comunicados e incidentes.

5.1.2.5. Comunicação dos Incidentes de Segurança à CTIR GOV

A ETIR da EPE deverá comunicar de imediato a ocorrência de todos os incidentes de segurança ocorridos na sua área de atuação ao CTIR-GOV, conforme padrão definido por esse órgão, a fim de permitir a geração de estatísticas e soluções integradas para a Administração Pública Federal.

A troca de outras informações e a forma de comunicação da ETIR da EPE com CTIR-GOV e as ETIRs de outros órgãos, instituições e empresas deverão ser formalizadas, se necessário, por “Termo de Cooperação Técnica”.

5.1.2.6. Teste de Segurança

Os testes para verificar o grau de segurança alcançado pelas medidas adotadas para tal fim são responsabilidade da ETIR/EPE, sendo vedado aos usuários dos recursos computacionais da EPE tentar provar um ponto fraco de que suspeite, a não ser que seja autorizado pelo GSIC.

O teste de um ponto fraco pode ser interpretado como um uso abusivo do sistema.

5.1.2.7. Requisitos para Adequação dos Ativos de Informação

O horário dos ativos de informação deve ser ajustado por meio de mecanismos de sincronização de tempo, de forma a garantir que as configurações de data, hora e fuso horário do relógio interno estejam

sincronizados com a “Hora Legal Brasileira (HLB)”, de acordo com o serviço oferecido e assegurado pelo Observatório Nacional (ON).

Os ativos de informação devem ser configurados de forma a registrar todos os eventos relevantes de SIC, e no mínimo, os seguintes:

- Autenticação, tanto os bem-sucedidos quanto os malsucedidos;
- Acesso a recursos e dados privilegiados; e
- Acesso e alteração nos registros de auditoria.

Os registros dos eventos previstos anteriormente devem incluir as seguintes informações:

- Identificação inequívoca do usuário que acessou o recurso;
- Natureza do evento, como sucesso ou falha de autenticação, tentativa de troca de senha etc.;
- Data, hora e fuso horário; e
- Endereço IP (*Internet Protocol*), identificador do ativo de informação, coordenadas geográficas, se disponíveis, e outras informações que possam identificar a possível origem do evento.

Os ativos de informação que não permitam os registros de eventos acima listados devem ser mapeados e documentados quanto ao tipo e formato de registros de auditoria que o sistema permita armazenar.

Devem-se acompanhar os sistemas e redes de comunicação de dados, registrando-se os eventos de segurança elencados abaixo, sem prejuízo de outros considerados relevantes:

- Utilização de usuários, perfis e grupos privilegiados;
- Inicialização, suspensão e reinicialização de serviços;
- Acoplamento e desacoplamento de dispositivos de hardware, com atenção às mídias removíveis;
- Modificações de política de senhas, como por exemplo, tamanho, expiração, bloqueio automático após exceder determinado número de tentativas de autenticação, histórico etc;
- Acesso ou modificação de arquivos ou sistemas considerados críticos; e
- Eventos obtidos de quaisquer mecanismos de segurança existentes.

Os servidores de hospedagem de página eletrônica, bem como todo e qualquer outro ativo de informação que assim o permita, devem ser configurados para armazenar registros históricos de eventos (*Logs*) em formato que permita a completa identificação dos fluxos de dados.

Os registros devem ser preservados pelo período mínimo de 6 (seis) meses, sem prejuízo de outros prazos previstos em normativos específicos.

Os ativos de informação devem ser configurados de forma a armazenar seus registros de auditoria não apenas localmente, como também remotamente, por meio do uso de tecnologia aplicável.

6. Disposições Gerais

A não observância dessa Norma pode implicar em ações administrativas, civis e penais, nos termos da legislação aplicável.

Casos omissos ou excepcionais serão submetidos à aprovação da Diretoria Executiva.

Este Instrumento Normativo entra em vigor em 19/01/2015, conforme decisão da Diretoria Executiva da EPE.

7. Anexos

Não se aplica.