Eletrobras

REGULAMENTO DE TRATAMENTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO DAS EMPRESAS ELETROBRAS

Versão 1.0
11/05/2020

Regulamento de Tratamento de Incidentes de Segurança da Informação das Empresas Eletrobras

Vinculado à Política de Segurança da Informação das Empresas Eletrobras

Área responsável pela emissão

Diretoria de Governança, Riscos e Conformidade / Superintendência de Gestão de Riscos, Controles Internos e Segurança da Informação.

Público-alvo

Empregados, dirigentes, conselheiros e prestadores de serviço das empresas Eletrobras.

Aprovação

Resolução 248/2020, de 11/05/2020, da Diretoria Executiva da Eletrobras.

Repositório

Os regulamentos das empresas Eletrobras podem ser encontrados na *intranet* das empresas.

Direitos de autor e confidencialidade

O conteúdo deste documento não pode ser reproduzido sem a devida autorização. Todos os direitos pertencem às Centrais Elétricas Brasileiras S.A. – Eletrobras e suas subsidiárias.

Prazo máximo de revisão: 3 anos

Histórico de versões: não se aplica

Sumário

Capítulo I – Geral

Seção I – Introdução

Objetivo

Instituir o Processo de Tratamento de Incidentes de Segurança da Informação das Empresas Eletrobras (PTISIEE) como elemento norteador das estratégias de segurança e proteção para as empresas Eletrobras, por meio de: definição de atividades e limites do processo; definição de atores e responsabilidades; orientação quanto aos ambientes aplicáveis e respectivas especificidades; e estabelecimento de indicadores e elaboração de normas e procedimentos, segundo o ambiente de cada empresa.

Abrangência

Este regulamento dispõe sobre os ambientes que utilizam a Tecnologia da Informação e Telecomunicação (TIC) e a Automação da Operação (TO), em qualquer área dos negócios empresariais no âmbito das Centrais Elétricas Brasileiras S.A. – Eletrobras e de suas controladas sediadas no território nacional, bem como de escritórios em outros países.

Referências legais e institucionais

Foram utilizadas as seguintes referências legais e institucionais na elaboração deste regulamento:

a) Política de Segurança da Informação das Empresas Eletrobras – Versão 2.0

b) Política de Proteção a Dados Pessoais e Privacidade das Empresas Eletrobras – 1ª edição

c) *Defining Incident Management Processes for CSIRTs: A Work in Progress* – TECHNICAL REPORT CMU/SEI-2004-TR-015 ESC-TR-2004-015 – 2004

d) ABNT NBR ISO/IEC 27001:2013 – Tecnologia da Informação – Técnicas de segurança – Sistemas de gestão da segurança da informação – Requisitos

e) ABNT NBR ISO/IEC 27002:2013 – Tecnologia da Informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação

f) ABNT NBR ISO/IEC 27701:2019 – Técnicas de segurança – Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação – Requisitos e diretrizes

g) IEC 61850 – Comunicação e automação de subestações de energia elétrica

h) IEC 62351 – *Standards for Securing Power System Communications*

i) ISA/IEC 62443 – *Network and system security for industrial-process measurement and control*

j) NERC CIP-008-1: *Incident Reporting and Response Planning*

k) CERT.br – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

l) Lei 13.709/2018 – Lei Geral de Proteção de Dados Pessoais – LGPD

Seção II – Diretrizes

Artigo 1º – O PTISIEE estabelece uma estrutura segmentada em três fases, conforme segue:

a) 1ª fase – DETECÇÃO;
b) 2ª fase – TRIAGEM; e
c) 3ª fase – RESPOSTA.

Fase de DETECÇÃO

Artigo 2º – A fase de detecção envolve a observação e a notificação de qualquer evento adverso (incidente confirmado ou sob suspeita), a coleta das informações pertinentes – tais como origem e destino, sistemas e serviços afetados, data e horário da ocorrência e outras variáveis – seguida do registro na ferramenta de registro de chamados.

Parágrafo 1º – A detecção pode ser reativa – quando alguma atividade incomum/maliciosa é observada por qualquer colaborador ou algum tipo de alerta é emitido por uma organização especializada em segurança da informação; ou pode ser proativa – quando a atividade é observada por meio de ferramentas de monitoramento de sistemas, redes e vulnerabilidades.

Parágrafo 2º – Funcionam como agentes notificadores de incidentes de SI: os notificadores comuns, as ferramentas automatizadas, entidades externas e as ouvidorias das empresas Eletrobras.

Parágrafo 3º – São atividades comuns da fase de detecção:

a) Notificação de incidentes de SI à Central de Serviços – Ocorre quando agentes notificadores acionam a Central de Serviços e esta procede com o registro na ferramenta de registro de chamados, com sua classificação inicial baseada na Tabela de Classificação de Incidentes de SIi.

b) Notificação ou detecção pelo GRSI – Ocorre quando membros das equipes que compõem o GRSI, além de detectarem, de forma reativa ou proativa, também registram incidentes de SI na ferramenta de registro de chamados para tratamento.

c) Notificação ou detecção pela CTISI – Ocorre quando as ouvidorias das empresas Eletrobras enviam para apuração pela CTISI as comunicações e denúncias relacionadas com SI em geral.

Parágrafo 4º - A CTISI pode, de forma proativa ou reativa, identificar ocorrências, eventos e incidentes de SI e registrar, tratar ou orientar tratamento.

Fase de TRIAGEM

Artigo 3º – Na fase de triagem deve ser realizada a avaliação das informações relevantes associadas ao incidente, com a finalidade de determinar se este está associado com SI corporativa, privacidade, TO ou TIC, bem como prover a sua classificação, criticidade e prioridade de acordo com a Tabela de Classificação de Incidentes.

Parágrafo único – Com o intuito de diminuir o tempo de resposta ao incidente de SI, alguns aspectos importantes devem ser observados para sua correta classificação/categorização:

a) a qualidade das informações disponibilizadas e registradas;
b) a identificação dos serviços afetados; e
c) a mensuração dos impactos nos ativos da informação.

Artigo 4º – A Central de Serviços deve verificar se o incidente de SI notificado possui solução conhecida – caso positivo, será tratado internamente; caso negativo, o incidente de SI deve ser enviado ao GRSI para tratamento.

Parágrafo 1º – Grande parte da triagem é realizada pelo GRSI, que recebe os incidentes de SI não tratados ou escalados pela Central de Serviços para validação da classificação apontada.

Parágrafo 2º – O GRSI deve ter pelo menos um colaborador nomeado para conduzir tratamento e resposta aos incidentes de SI, distribuindo demandas, delegando tarefas e elaborando o Relatório Executivo de Incidente de SI para encaminhamento à CTISI.

Artigo 5º – O GRSI deve verificar se realmente se trata de um incidente de SI e se a categorização está correta. Não se tratando de um incidente de SI, este deve ser reclassificado e enviado à equipe responsável ou devolvido à Central de Serviços.

Artigo 6º – Os incidentes de SI registrados diretamente pelo GRSI, bem como os registrados pela CTSI devem ser classificados de acordo com a Tabela de Classificação de Incidentes.

Artigo 7º – Os incidentes de SI recebidos da Central de Serviços com a classificação incorreta devem ser reclassificados pelo GRSI de acordo com a Tabela de Classificação de Incidentes.

Artigo 8º – Os incidentes relacionados a violação de privacidade ou que gerem danos aos titulares de dados pessoais devem ser encaminhados para tratamento pelo DPO de cada empresa.

Artigo 9º – Em todos os casos, após ter sido corretamente classificado, o incidente de SI segue para a fase de resposta.

Fase de RESPOSTA

Artigo 10 – Na fase de resposta deve ser realizado o tratamento do incidente de SI, sendo o momento em que as ações necessárias acontecem de acordo com a classificação de severidade e de impacto para o negócio das empresas Eletrobras.

Artigo 11 – Os incidentes com soluções conhecidas devem ser tratados pela Central de Serviços, enquanto incidentes complexos e com soluções desconhecidas devem passar por análise técnica especializada, pelo GRSI, podendo seguir as etapas de contenção, erradicação e recuperação total do ambiente afetado, conforme segue:

a) **Contenção** – deve-se adotar ações temporárias, também conhecidas como mitigação, que limitem o dano causado pelo incidente ao ambiente. Exemplo: isolar o sistema ou um artefato afetado da rede de forma a evitar danos maiores ao ambiente.

b) **Erradicação** – deve-se identificar a causa raiz do incidente e promover ações de solução, removendo as ameaças e restaurando o ativo afetado.

c) **Recuperação** – deve-se adotar ações de retorno à situação anterior ao incidente, após realização de testes e validações que garantam que os itens de configuração afetados foram devidamente tratados e estão livres de ameaças.

Artigo 12 – Na fase de resposta devem ser efetuados testes que permitam avaliar se as soluções aplicadas foram adequadas, se o ambiente se encontra livre de ameaças e se a causa raiz do incidente foi identificada e erradicada.

Artigo 13 – De acordo com o escopo do incidente, pode haver a necessidade de envolvimento de outras áreas das empresas Eletrobras, representadas no GApTISI, e a CTISI deve identificá-las e acioná-las. Neste momento, deve ser observado um cuidado especial em relação ao sigilo e à classificação da informação, ao envolvimento dos responsáveis, à forma como se dará o tratamento do incidente e à preservação das evidências para qualquer necessidade posterior, especialmente quando se tratar de necessidades de investigações na esfera legal, de descumprimento de leis, regulamentações e normativos de segurança da informação.

Artigo 14 – No momento da análise do incidente pelo GRSI, deve ser observada a extensão e o impacto quanto a áreas e quantidade de usuários afetados e, caso necessário, deve ser disparado um comunicado à área impactada, de acordo com orientações da CTISI.

Artigo 15 – Após o encerramento do incidente devem ser realizadas:

a) a comunicação formal às áreas envolvidas e, se necessário, a entidades externas;
b) a atualização da base de conhecimento de incidentes, em contribuição ao aprendizado das equipes e a melhorias nos esforços futuros de detecção, prevenção e respostas aos incidentes; e
c) a análise pós-incidente, que deve avaliar o processo de tratamento de incidente de SI, observando se as soluções aplicadas na resolução foram adequadas e se o processo requer melhorias em suas fases.

Artigo 16 – A análise pós-incidente pode ser feita por meio de indicadores que evidenciem a eficiência do processo; são sugestões de indicadores:

a) quantidade de chamados abertos/fechados;
b) percentual de chamados reabertos;
c) percentual de chamados atrasados em relação ao Acordo de Nível de Serviço (SLA – *Service Level Agreement*);
d) quantidade de incidentes de SI por severidade; e
e) quantidade de incidentes de SI por categoria.

Seção III – Responsabilidades

Artigo 17 – **Agente notificador**:

a) Informar aos órgãos nomeados a ocorrência de qualquer incidente de SI, baseado nos instrumentos normativos da empresa.

b) Notificar a Central de Serviços, que por sua vez notifica as equipes especializadas da TIC e SI ou a própria CTISI sobre qualquer evento adverso (incidente confirmado ou sob suspeita) relacionado a SI.

Artigo 18 – **Central de Serviços**:

a) Receber notificações e registrá-las na ferramenta de registro de chamados.

b) Assegurar que todas as informações essenciais estejam contidas nos registros.

c) Classificar/categorizar incidentes de SI, exceto de TO.

d) De acordo com a criticidade, escalonar incidentes de SI para o GRSI que envolve as equipes de TIC e SI.

e) Solucionar o incidente de SI de baixa criticidade.

Artigo 19 – **Comitê de Segurança da Informação da Eletrobras (COSEG)**:

a) Manter este regulamento atualizado.

b) Orientar e acompanhar o estabelecimento e a observância dos processos, controles, metodologias, subsídios, modelos, padrões, estruturas organizacionais de projetos, distribuição de responsabilidades e ferramentas necessários à sua implementação e operação.

c) Analisar as questões específicas apresentadas pelos representantes das empresas no referido Comitê para sua posterior aplicação.

Artigo 20 – **Coordenação de Tratamento de Incidentes de Segurança da Informação (CTISI)**:

a) Coordenar o tratamento de incidentes de SI, quando convocada, podendo ser acionada em todas as fases do PTISIEE.

b) Orientar e prover suporte de nível corporativo às equipes do GRSI.

c) Convocar o GApTISI em eventos que possam demandar resposta ou orientações por parte de áreas estratégicas ao negócio.

d) Convocar o GRSI.

e) Registrar e orientar o tratamento de incidentes de SI notificados, assim como os detectados por seus membros.

f) Receber, apurar e dar tratamento às comunicações e denúncias sobre incidentes de SI em geral, vindas das ouvidorias das empresas Eletrobras.

g) Ser responsável pela comunicação dos incidentes de SI, no âmbito das empresas Eletrobras, e ser a facilitadora da interação com entidades externas, no âmbito de SI.

h) Concentrar e fornecer informações e estatísticas sobre incidentes de SI, para responder a solicitações diversas.

i) Validar o Relatório Executivo de Tratamento de Incidentes de SI encaminhado pelo GRSI.

j) Mediar eventuais dificuldades de alocação de recursos das diversas áreas envolvidas no tratamento do incidente de SI.

Artigo 21 – **Encarregado pelo Tratamento dos Dados Pessoais (*Data Protection Officer – DPO)***:

a) Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências.

b) Receber comunicações da autoridade nacional e adotar providências.

Artigo 22 – **Grupo de Apoio ao Tratamento de Incidentes de Segurança da Informação (GApTISI)**:

Parágrafo único – Sem exaurir a ampla variedade de atuações e responsabilidades, pode-se elencar as seguintes:

a) Prestar assessoria em casos de incidentes graves que possam ocasionar sanções jurídicas à empresa.

b) Prestar esclarecimentos e efetuar comunicados diversos à sociedade civil, aos veículos de comunicação e à mídia em geral.

c) Atuar em apurações gerais que envolvam proteção física de instalações corporativas e industriais.

d) Encaminhar os artefatos encontrados e eventos para diligências, sindicâncias e perícias forenses em ativos da empresa para unidade organizacional competente.

Artigo 23 – **Grupo de Resposta e Tratamento a Incidentes de Segurança da Informação (GRSI)**:

a) Registrar incidente de SI, notificado ou detectado, na ferramenta de registro de chamados.

b) Validar ou reclassificar o incidente de SI.

c) Solucionar os incidentes de SI, executando respostas rápidas para minimizar o impacto ao negócio e recuperar o ambiente afetado.

d) Elaborar o Relatório Executivo de Tratamento de Incidentes de SI para encaminhamento à CTISI.

e) Realizar análises pós-incidente, verificando a eficiência do processo e se há melhorias a implementar.

f) Propor estratégias proativas para eliminação de problemas e proteção dos recursos da organização.

Capítulo II – Procedimentos

Artigo 24 – Este capítulo registra os procedimentos para o Processo de Tratamento de Incidentes de Segurança da Informação das Empresas Eletrobras – PTISIEE, com suas fases e respectivas responsabilidades, contidos nos itens 1 a 3 a seguir.

1 DETECTAR

1.1 Registrar o incidente

Objetivo: Documentar para permitir a rastreabilidade de todo o ciclo de vida do incidente de SI.

Responsáveis:

- Central de Serviços
- GRSI
- CTISI

Ferramentas: Ferramenta de registro de chamados.

Entrada	Principais Atividades	Saída
• Notificação de incidente de SI • Detecção de incidente de SI (ferramenta de SI com automatização integrada, caso exista, e/ou GRSI)	• Receber a notificação ou detectar o incidente de SI • Assegurar que todas as informações essenciais foram disponibilizadas • Registrar na ferramenta de registro de chamados todas as informações do incidente de SI, seja este notificado ou detectado	• Incidente de SI registrado na ferramenta de registro de chamados

2 REALIZAR TRIAGEM

2.1 Validar a classificação

Objetivo: Assegurar que o incidente de SI recebido da Central de Serviços possua classificação/categorização correta.

Responsável: GRSI

Ferramentas: Ferramenta de registro de chamados e Tabela de Classificação de Incidentes.

Entrada	Principais Atividades	Saída
• Incidente de SI registrado e classificado pela Central de Serviços	• Receber os incidentes de SI vindos da Central de Serviços, de solução desconhecida ou tratados, mas não solucionados • Checar se o incidente de SI foi classificado com a categoria/subcategoria apropriada, conforme Tabela de Classificação de Incidentes	• Incidente de SI com a classificação correta

3 APRESENTAR RESPOSTA

3.1 Analisar o incidente

Objetivo: analisar o incidente de SI como um todo, observando quais ações serão necessárias ao seu tratamento e erradicação.

Responsáveis:

- Central de Serviços
- GRSI

Ferramentas: Ferramentas necessárias à resolução dos incidentes de SI.

Entrada	Principais Atividades	Saída
• Incidente de SI com solução conhecida pela Central de Serviços • Incidente devidamente classificado pelo GRSI	• Analisar a causa raiz do incidente e as ações para tratamento do incidente de SI (contenção, erradicação e recuperação) • Identificar o grau de criticidade do incidente de SI	• Soluções para tratamento da causa raiz identificada • Grau de criticidade definido

3.2 Tratar o incidente

Objetivo: aplicar as ações mais adequadas à solução do incidente de acordo com a análise da causa raiz.

Responsável:

- Central de Serviços
- GRSI

Ferramentas: Ferramentas necessárias à resolução dos incidentes de SI.

Entrada	Principais Atividades	Saída
• Análise das ações de solução conhecida pela Central de Serviços • Análise técnica especializada da causa raiz do incidente de SI pelo GRSI • Diretrizes vindas da CTISI e do GApTISI	• Aplicar as ações de tratamento do incidente (contenção, erradicação e recuperação), de acordo com o resultado da análise técnica e das diretrizes da CTISI e do GApTISI	• Incidente tratado para aplicação de testes

3.3 Avaliar o tratamento do incidente

Objetivo: identificar se as soluções aplicadas foram satisfatórias.

Responsáveis:

- Central de Serviços
- GRSI

Ferramentas: Ferramenta de análise de incidentes de SI (a definir).

Entrada	Principais Atividades	Saída
• Incidentes devidamente tratados.	• Realizar testes específicos para identificar se o incidente foi remediado.	• Incidente avaliado quanto à solução aplicada para encerramento ou novas ações de tratamento.

3.4 Encerrar o incidente

Objetivo: finalizar o incidente e restabelecer o ambiente.

Responsáveis:

- Central de Serviços
- GRSI

Ferramentas: Ferramenta de registro de chamados.

Entrada	Principais Atividades	Saída
• Incidentes devidamente tratados • Avaliação do tratamento realizada	• Finalizar o incidente inserindo todas as ações realizadas na fase de tratamento, detalhando cada etapa com as respectivas evidências • Inserir todos os testes e resultados que evidenciem que a disponibilidade, integridade, confidencialidade, autenticidade, legalidade e privacidade do ambiente estejam preservadas	• Incidente encerrado

3.5 Comunicar às áreas envolvidas

Objetivo: comunicar o encerramento dos incidentes de SI aos agentes notificadores envolvidos.

Responsáveis:

- Central de Serviços
- GRSI

Ferramentas: Ferramentas necessárias à comunicação.

Entrada	Principais Atividades	Saída
• Incidente totalmente encerrado	• Comunicação da resolução e do encerramento do incidente de SI a todos os agentes notificadores envolvidos e, caso necessário, entidades externas	• Todas as áreas envolvidas cientes do encerramento do incidente de SI

3.6 Atualizar a base de conhecimento de incidentes

Objetivo: manter um histórico de todos os incidentes de SI com as devidas evidências para facilitar atuações futuras e registros para auditorias.

Responsáveis:

- Central de Serviços
- GRSI

Ferramentas: Ferramenta de Base de Conhecimento.

Entrada	Principais Atividades	Saída
• Incidente totalmente encerrado	• Registrar todas as ações realizadas em cada fase do Processo de Tratamento de Incidentes de SI • Registrar o detalhamento do incidente de SI, sua causa raiz e todo caminho percorrido até o encerramento do incidente	• Base de conhecimento de incidentes de SI atualizada

3.7 Realizar análise pós-incidente

Objetivo: avaliar a eficiência e a eficácia de execução do PTISIEE e identificar os pontos de melhoria.

Responsáveis:

- Central de Serviços
- GRSI

Ferramentas: Ferramenta de Base de Conhecimento.

Entrada	Principais Atividades	Saída
• Incidente totalmente encerrado	• Analisar se as soluções aplicadas ao tratamento do incidente de SI foram as mais adequadas • Analisar se existe a existência de gaps na execução do processo e sinalizar à CTISI	• Processo analisado e finalizado • Relatório Executivo de Tratamento de Incidente de SI

3.8 Comunicar à coordenação

Objetivo: comunicar à coordenação o incidente para as devidas ações.

Responsável: GRSI

Ferramentas: não se aplica.

Entrada	Principais Atividades	Saída
• Informações gerais sobre o incidente	• Dar ciência do incidente grave/crítico à CTISI	• Incidente comunicado à CTISI

3.9 Avaliar o incidente

Objetivo: identificar qual responsável deverá atuar no tratamento do incidente de SI.

Responsável: CTISI

Ferramentas: não se aplica.

Entrada	Principais Atividades	Saída
• Incidente de SI registrado pela CTISI • Incidente com necessidade de apoio para o tratamento	• Identificar quais os responsáveis pelo tratamento do incidente de SI de acordo com o seu escopo • Verificar se existe a necessidade de orientação aos responsáveis • Identificar a necessidade de acionar o GApTISI	• Responsáveis pelo tratamento do incidente de SI identificado • Necessidade de orientação para o tratamento do incidente de SI verificada

3.10 Orientar o tratamento do incidente

Objetivo: fornecer informações que orientem no tratamento do incidente de SI.

Responsável: CTISI

Ferramentas: não se aplica.

Entrada	Principais Atividades	Saída
• Avaliação do incidente com necessidade de orientação	• Direcionar as orientações para o tratamento do incidente de SI aos responsáveis (GRSI) de acordo com o escopo do incidente	• Incidente encaminhado para o tratamento com as devidas orientações

3.11 Convocar GRSI

Objetivo: encaminhar o incidente aos responsáveis pelo seu tratamento.

Responsável: CTISI

Ferramentas: não se aplica.

Entrada	Principais Atividades	Saída
• Resultado da avaliação do incidente	• Convocar GRSI • Direcionar o incidente de SI aos responsáveis pelo tratamento (GRSI)	• Incidente encaminhado aos responsáveis para o tratamento

3.12 Acionar o Grupo de Apoio

Objetivo: obter apoio das Unidades Organizacionais do negócio em nível tático/estratégico.

Responsável: CTISI

Ferramentas: não se aplica.

Entrada	Principais Atividades	Saída
• Necessidade de colaboração do GApTISI para o tratamento do incidente	• Encaminhar as necessidades de apoio para o tratamento do incidente de SI ao GApTISI	• GApTISI acionado para atender as necessidades para o tratamento do incidente

3.13 Atender às necessidades de apoio

Objetivo: atuar junto à CTISI para o tratamento do incidente, de acordo com as necessidades apresentadas.

Responsável: GApTISI.

Ferramentas: não se aplica.

Entrada	Principais Atividades	Saída
• Necessidade de colaboração do GApTISI	• Responder as necessidades encaminhadas pela CTISI • Encaminhar diretrizes para o tratamento dos incidentes ao GRSI para o tratamento do incidente, por meio da CTISI • Fornecer apoio consultivo ao GRSI para o tratamento do	• Diretrizes encaminhadas ao GRSI para o tratamento do incidente

3.14 Enviar para GRSI

Objetivo: Garantir que o incidente de SI com solução não conhecida seja encaminhado para o GRSI.

Responsável: Central de Serviços

Ferramentas: Ferramenta de registro de chamados.

Entrada	Principais Atividades	Saída
• Incidente de SI com solução não conhecida	• Enviar o incidente de SI de solução não conhecida para o GRSI	• Incidente escalado para o GRSI

Capítulo III – Disposições Gerais e Transitórias

Artigo 25 – A Diretoria Executiva da Eletrobras deve aprovar este regulamento e garantir sua implementação.

Artigo 26 – As diretorias executivas das empresas Eletrobras devem ratificar a aprovação deste regulamento e garantir sua implementação.

Artigo 27 – As ações decorrentes deste regulamento devem estar rigorosamente alinhadas com o Plano Estratégico, o Plano Diretor de Negócio e Gestão, a Política de Segurança da Informação e a Política de Tecnologia da Informação, Automação e Telecomunicação das Empresas Eletrobras.

Artigo 28 – As diretrizes estabelecidas neste regulamento devem ser cumpridas por todos os seus destinatários, estando os mesmos sujeitos, no caso de descumprimento, ao estabelecido na Política de Consequências das Empresas Eletrobras.

Artigo 29 – As Centrais Elétricas Brasileiras S.A. – Eletrobras e suas controladas sediadas no território nacional, bem como os escritórios em outros países, devem garantir a aplicação deste regulamento no tratamento dos incidentes, por meio do estabelecimento de documentos normativos internos formais.

Artigo 30 – As empresas Eletrobras devem adequar a este regulamento os documentos normativos e os controles internos que se fizerem necessários, no prazo máximo de 180 dias a partir da aprovação pela Diretoria Executiva da Eletrobras.

Artigo 31 – Devem ser revogados, em todo ou em parte, os documentos normativos das empresas Eletrobras que estabeleçam diretrizes e procedimentos contrários aos descritos neste regulamento, salvo se esses documentos normativos contemplarem direitos já inseridos no contrato de trabalho dos colaboradores, quando deverão seguir disciplina própria de revogação.

Capítulo IV – Glossário

Seção I – Conceitos e Definições

Agente notificador – Qualquer agente, dentre notificadores comuns, entidades externas, ferramentas automatizadas e ouvidorias das empresas, que comunique incidentes de segurança da informação em qualquer atividade ou processo, utilizando os recursos da Central de Serviços, da ouvidoria da empresa ou do Grupo de Resposta e Tratamento de Incidentes de Segurança da Informação (GRSI).

Agente Notificador Comum – Qualquer pessoa que utilize os recursos disponíveis para comunicar incidentes de segurança da informação, em qualquer atividade ou processo.

Autenticidade da informação – Propriedade que exige veracidade sobre a autoria e a origem da informação e que haja identificação e registro sobre o usuário que está enviando ou modificando a mesma.

Central de Serviços – Entidade que atua no atendimento aos usuários dos serviços de tecnologia da informação que suporta os processos administrativos, sendo um dos pontos de entrada das notificações de incidentes de segurança da informação.

Colaborador – Diretores, conselheiros, empregados, contratados, prestadores de serviço, estagiários e jovens aprendizes que atuem nas empresas Eletrobras.

Confidencialidade da informação – Propriedade que exige que a informação não seja disponibilizada, sem autorização, a pessoa física, sistema, órgão ou entidade, evitando a possibilidade de prejuízo à empresa e à privacidade dos indivíduos. Trata-se de caráter atribuído aos dados ou informações sigilosas em decorrência de sua natureza ou conteúdo, restringindo o acesso somente ao colaborador autorizado.

Coordenação de Tratamento de Incidentes de Segurança da Informação (CTISI) – Atua em atividades relacionadas ao processo de tratamento de incidentes de SI, em nível tático e estratégico, sob responsabilidade das áreas que tratam segurança da informação de forma corporativa nas empresas Eletrobras.

Dado Pessoal – Informação relacionada a pessoa natural identificada ou identificável.

Encarregado pelo Tratamento dos Dados Pessoais (*Data Protection Officer – DPO)* – Profissional indicado, em cada empresa, para tratar os incidentes relacionados a violação de privacidade ou que gerem danos aos titulares de dados pessoais e para atuar como canal de comunicação entre o controlador, os titulares dos dados e a autoridade nacional de proteção de dados.

Entidades externas – Parceiros comerciais, fornecedores e entidades externas e de cooperação para SI, tais como: o Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR.Gov), o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.Br) e outros Grupos de Resposta a Incidentes de SI (conhecidos como CSIRT, do inglês *Computer Security Incident Response Team*); também são considerados agentes notificadores.

Ferramentas automatizadas – Ferramentas que, por tratarem de segurança e monitoramento de rede, são consideradas agentes notificadores.

Ferramenta de registro de chamados – Sistema utilizado para registro, classificação e acompanhamento de incidentes de SI.

Gestão da segurança da informação – Sistema de gestão que enfatiza (conforme conceitua a ABNT NBR ISO/IEC 27001:2013):

a) o entendimento dos requisitos de segurança da informação de uma organização e da necessidade de estabelecer uma política e objetivos para a segurança de informação;
b) a implementação e a operação de controles para gerenciar os riscos de segurança da informação de uma organização, no contexto dos riscos de negócio globais;
c) o monitoramento e a análise crítica de desempenho e eficácia do SGSI; e
d) a melhoria contínua baseada em medições objetivas.

Grupo de Apoio ao Tratamento de Incidentes de Segurança da Informação (GApTISI) – Grupo multidisciplinar composto por representantes da alta direção das empresas e representantes das áreas estratégicas e de suporte ao negócio (que podem ser as áreas jurídica, de recursos humanos, de segurança física e patrimonial, de governança, riscos e conformidade e de comunicação institucional ou assessoria de comunicação), sendo acionado para prestação de suporte consultivo ou executivo ao tratamento de incidentes de segurança da informação, de acordo com suas áreas de atuação – cada empresa pode agregar áreas, comissões ou grupos de trabalho cuja participação julgue pertinente.

Grupo de Resposta e Tratamento de Incidentes de Segurança da Informação (GRSI) – Equipe técnica multidisciplinar (grupo não formal) que facilita o entendimento de situações no contexto do PTISIEE, atendendo às solicitações encaminhadas pela Central de Serviços que demandem soluções mais complexas e/ou especializadas e que não tenham solução de contingência e interface junto aos usuários demandantes; composto por representantes dos serviços de suporte ao correio eletrônico, à infraestrutura, ao gerenciamento da rede corporativa, à administração de banco de dados, à segurança de TIC, à automação, à proteção, à telecomunicação, à segurança da informação corporativa e outros.

Incidente de segurança da informação – incidente de SI – Qualquer evento adverso, confirmado ou sob suspeita, que afete a proteção dos sistemas de informação e que comprometa ou tenha potencial para comprometer a disponibilidade, a integridade, a confidencialidade, a autenticidade, a legalidade e/ou a privacidade da informação.
São incidentes de SI de ocorrência mais comum nas organizações (apresentados sem pretensão de limitar, tipificar ou exaurir a ampla diversidade de incidentes de segurança da informação possíveis):

a) tentativa ou acesso não autorizados a sistemas, informações e documentos;
b) modificação não autorizada ou sem conhecimento dos responsáveis em sistemas;
c) infecções por *malware*;
d) ataques de negação de serviço;
e) violações dos termos da Política de Segurança da Informação das Empresas Eletrobras;
f) uso inapropriado dos recursos da rede corporativa ou operativa por parte de colaboradores;
g) exposição de informações sensíveis em ambiente de acesso público;
h) furto de equipamentos;
i) violação da privacidade de dados pessoais;
j) qualquer evento indesejado ou inesperado que comprometa ou tenha possibilidade de comprometer as operações do negócio e ameaçar a segurança da informação.

Informação – Qualquer dado, processado ou não, contido em qualquer meio, suporte ou formato, que pode ser utilizado para produção e transmissão de conhecimento.

Integridade da informação – Propriedade que exige garantias para que a informação não seja modificada ou destruída de maneira não autorizada ou acidental, preservando sua completa exatidão na origem, no trânsito ou no destino.

Legalidade ou conformidade da informação – Propriedade que exige que a informação seja aderente às leis, normas e aos regulamentos vigentes, seja no mercado privado ou na esfera governamental.

Ouvidorias das empresas Eletrobras – Para efeitos deste regulamento,são os agentes notificadores responsáveis por receber as comunicações e denúncias relacionadas com segurança da informação em geral e requerer tratamento exclusivamente à Coordenação de Tratamento de Incidentes de Segurança da Informação (CTISI).

Política de Segurança da Informação das Empresas Eletrobras (PSIEE) – Documento que tem como objetivo "orientar estrategicamente as questões relacionadas à segurança da informação, definindo diretrizes para armazenamento, custódia, processamento, transmissão e descarte de informação no ambiente convencional ou de tecnologia das empresas Eletrobras".

Privacidade da informação – Propriedade que exige o direito à reserva de informações pessoais, além da prerrogativa de controlar a exposição e a disponibilidade de informações acerca de si mesmo (regulação dos limites).

Segurança da Informação (SI) – Proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco, maximizar o retorno sobre os investimentos e as oportunidades, a partir da implementação de um conjunto de controles adequados, incluindo políticas.

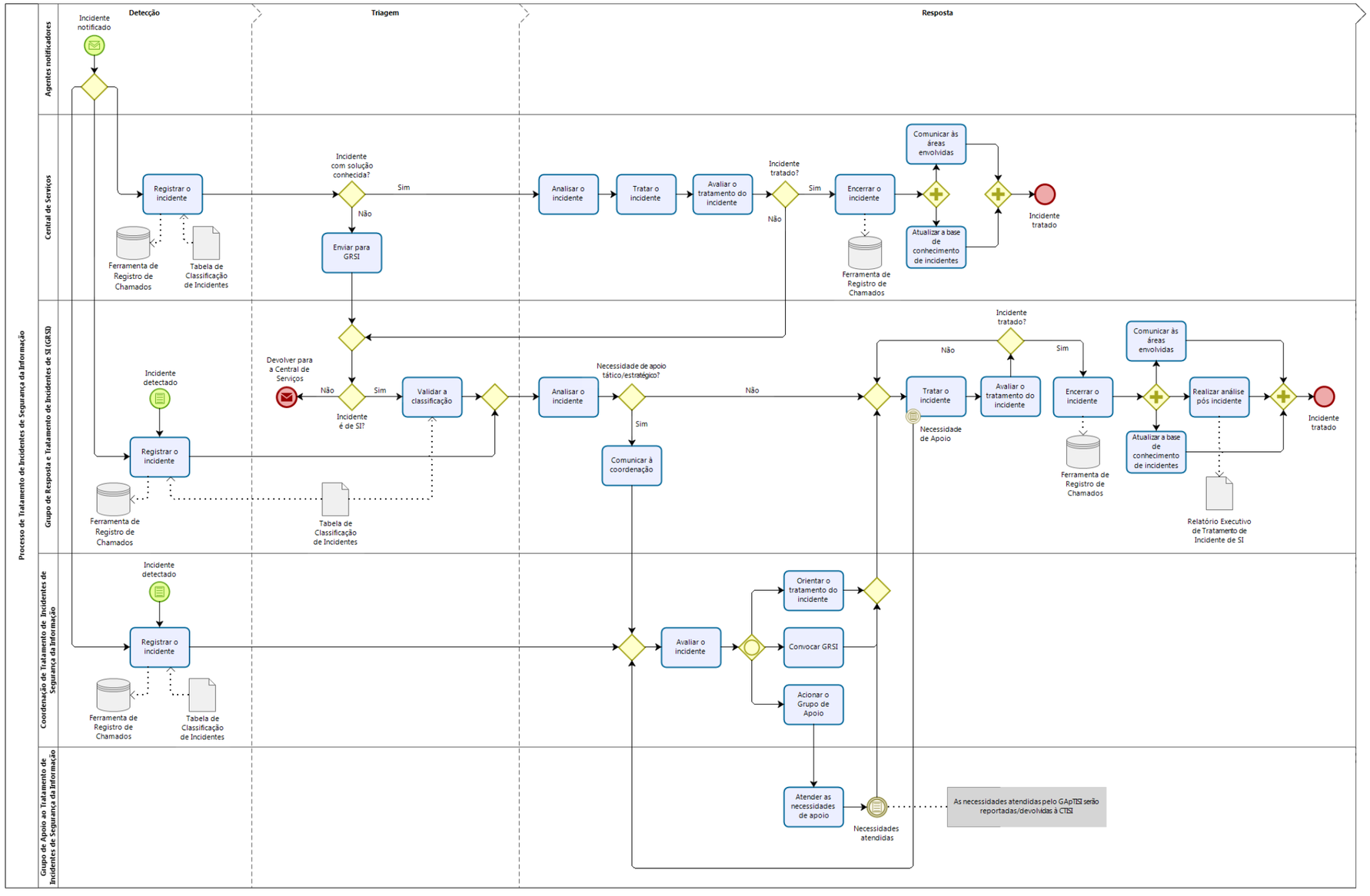
Tabela de Classificação de Incidentes de SI – Base de dados que contém incidentes conhecidos, devidamente categorizados e que podem incluir criticidade/prioridade pré-definidas.

Seção II – Siglas e acrônimos

ABNT	Associação Brasileira de Normas Técnicas
CERT.Br	Centro de Estudos, Resposta e Tratamento de Incidente de Segurança do Brasil
CIP	*Critical Infrastructure Protection*
CMU/SEI	Carnegie Mellon University/Software Engineering Institute
COSEG	Comitê de Segurança da Informação da Eletrobras
CSC	Centro de Serviços Compartilhados das Empresas Eletrobras
CSIRT	*Computer Security Incident Response Team*
CTIR Gov	Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo
CTISI	Coordenação de Tratamento de Incidentes de Segurança da Informação
GApTISI	Grupo de Apoio ao Tratamento de Incidentes de Segurança da Informação
GRSI	Grupo de Resposta e Tratamento de Incidentes de Segurança da Informação
IEC	*International Electrotechnical Commission*
ISA	*International Society of Automation*
NBR	Norma Brasileira
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
PSIEE	Política de Segurança da Informação das Empresas Eletrobras
PTISIEE	Processo de Tratamento de Incidentes de Segurança da Informação das Empresas Eletrobras
SGSI	Sistemas de Gestão de Segurança da Informação
SI	Segurança da informação
SLA	*Service Level Agreement*
TIC	Tecnologia da Informação e Comunicação
TO	Tecnologia de Operação

Capítulo V – Anexos

1 Fluxograma do Processo de Tratamento de Incidentes de Segurança da Informação das Empresas Eletrobras – PTISIEE



2 Legenda dos elementos do fluxograma do processo

	**Evento inicial de mensagem**: Sinaliza que o processo é iniciado com o recebimento de uma mensagem de qualquer tipo (documento, e-mail, telefonema etc.).
	**Subprocesso reutilizável**: Elemento que faz referência ao diagrama de outro processo.
	**Evento intermediário condicional**: Sinaliza que o processo prossegue somente quando a condição estipulada acontecer.
	**Repositório de dados:** Representa um repositório de informações de qualquer espécie (banco de dados, sistemas de arquivos etc.) que pode ser consultado ou atualizado durante a realização de uma tarefa.
	**Objeto de dados:** Representa documentos, dados, formulários etc. (eletrônicos ou físicos) usados e/ou atualizados durante o processo e importantes para a compreensão do fluxo.
	**Evento inicial condicional:** Sinaliza que o processo é iniciado quando a condição estipulada acontecer.
	**Gateway exclusivo**: Na divisão: representa, após uma decisão, que apenas um dos caminhos dará prosseguimento ao processo. Semanticamente, funciona como "OU". Na unificação: conecta caminhos distintos, dando sequência a um único fluxo de atividades quando apenas um dos caminhos é completado.
	**Gateway inclusivo:** Na divisão: representa, após uma decisão, que uma ou mais saídas dará prosseguimento ao processo. Semanticamente, funciona como "E/OU". Na unificação: conecta caminhos distintos, dando sequência a um único fluxo de atividades quando os fluxos que estiverem ativos forem concluídos.
	**Gateway paralelo**: Na divisão: representa a divisão do fluxo em dois ou mais, que serão executados paralelamente. Semanticamente, funciona como "E". Na unificação: conecta caminhos paralelos em um, dando sequência apenas quando todos os caminhos forem executados.
	**Evento final de mensagem:** Sinaliza que uma mensagem de qualquer tipo (documento, e-mail, telefonema etc.) é enviada a outro processo quando o fluxo chega ao fim.
	**Evento intermediário de borda condicional:** Um evento condicional anexado à borda de uma atividade sinaliza que, se a condição estipulada se tornar verdadeira durante a execução da tarefa, um fluxo decorrente do evento será iniciado.
	**Evento final simples**: Sinaliza que o fluxo do processo chegou ao fim.