Norma de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos

SUMÁRIO

Sumário das Revisões

Versão	Data	Responsável	Observações
01	08/12/2014	STI	Versão Inicial, aprovada na RD nº 08/324ª de 08/12/2014
02	31/07/2026	CGR	Aprovada na RD 04/889ª de 31/07/2026

Informações Adicionais:

A versão 01 deste 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 19/01/2015.

A versão 02 ajusta a Norma à nova Estrutura de Gestão de Segurança da Informação, decorrente da separação entre os papéis de Gestor de Segurança da Informação, de Superintendente de TIC e do Agente Responsável da ETIR; atualiza o Glossário de Segurança da Informação, de acordo com a Portaria GSI/PR nº 93 de 18 de outubro de 2021; ajusta-se à IN GSI 01 de 27/05/2020 e suas atualizações e atualiza a lista de serviços oferecidos pela ETIR. Foi aprovada conforme Resolução de Diretoria 04/889ª de 31/07/2026.

CAPÍTULO I - DISPOSIÇÕES PRELIMINARES

Seção I - Objetivo

Art. 1º Esta Norma estabelece as ações de prevenção, tratamento e resposta a incidentes cibernéticos da EPE atribuídas à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos, ETIR, conforme previsto na Política de Segurança da Informação e Comunicações da EPE.

Parágrafo único. Esta Norma cumpre ainda o papel de documento de constituição da ETIR, previsto na Norma Complementar 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009.

Seção II - Âmbito de Aplicação

Art. 2º Esta Norma aplica-se a todas as áreas da EPE.

Seção III - Responsabilidades

Art. 3º Compete à Diretoria Executiva aprovar esta Norma e suas revisões.

Art. 4º Compete à Superintendência de Tecnologia da Informação e Comunicações (STI):

I - indicar o Agente responsável pela ETIR e estabelecer o seu regime de dedicação às atividades da ETIR;

II - disponibilizar e estabelecer a alocação de pessoal técnico da equipe da STI para compor a ETIR;

III - prover a infraestrutura necessária à ETIR;

IV - gerenciar os contratos para prestação de serviços necessários à atividade da ETIR;

V - realizar a identificação e classificação de criticidade dos ativos de informação sob custódia da STI; e

VI - garantir a perfeita adequação dos ativos de informação sob custódia da STI para atendimento a esta Norma.

Art. 5º Compete ao Gestor de Segurança da Informação e Comunicações (GSIC) da EPE:

I - propor à STI perfil e capacitações necessários para os membros da ETIR, bem como ferramental e procedimentos para funcionamento da equipe.

II - acompanhar as atividades da ETIR;

III - apoiar o Agente Responsável na emissão de comunicados ao público-alvo.

Art. 6º Compete ao Agente Responsável pela ETIR:

I - manter o relacionamento com o CTIR-GOV;

II - criar os procedimentos internos da ETIR;

III - gerenciar as atividades e distribuir tarefas para a ETIR;

IV - negociar com a supervisão de cada um dos membros da ETIR o percentual do esforço dedicado à equipe;

V - manter o GSIC atualizado a respeito da atividade da ETIR, em especial durante o tratamento de incidentes;

VI - acompanhar o processo de identificação e classificação de criticidade de ativos de informação sob custódia da STI;

VII - acompanhar o registro dos eventos de segurança;

VIII - propor a utilização de metodologia e ferramentas reconhecidas e recomendadas em referenciais técnicos para o processo de coleta e preservação de evidências;

IX - acionar as instâncias superiores quando algum incidente grave for detectado; e

X - divulgar alertas sobre vulnerabilidades e problemas de incidentes de segurança na rede computacional da EPE, com o apoio do GSIC.

Art. 7º Compete à ETIR:

I - efetuar análises detalhadas da infraestrutura de segurança na rede computacional da EPE, com base nas melhores práticas do mercado;

II - executar tarefas que viabilizem ou facilitem a detecção de intrusão na rede computacional da EPE; e

III - executar os procedimentos estabelecidos, bem como executar as tarefas determinadas pelo Agente Responsável.

Art. 8º Compete aos usuários da rede da EPE comunicar imediatamente à ETIR sobre todo e qualquer evento ou vulnerabilidade que afete a segurança da informação e comunicações.

Seção IV - Documentos de Referência

Art. 9º Os seguintes documentos servem de referência a esta Norma:

I - Decreto nº 12.573, de 4 de agosto de 2025, que aprova a Estratégia Nacional de Segurança Cibernética;

II - Instrução Normativa GSI nº 1 de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;

III - Norma Complementar nº 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009, que 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;

IV - Norma Complementar nº 08/IN01/DSIC/GSIPR, de 24 de agosto de 2010, que 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;

V - Portaria GSI/PR nº 93 de 18 de outubro de 2021, que aprova o Glossário de Segurança da Informação;

VI - Norma Técnica ABNT NBR ISO/IEC 27002:2022, que 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;

VII - Política de Segurança da Informação e Comunicações da EPE: 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; e

VIII - Computer Security Incident Response Team (CSIRT) Framework, Version 2.1.0, do Forum of Incident Response and Security Teams (FIRST).

Parágrafo único. As referências normativas mencionadas neste artigo deverão ser interpretadas considerando suas alterações, revogações, substituições ou atos supervenientes aplicáveis, cabendo ao Gestor de Conformidade e Riscos propor a atualização deste Instrumento Normativo quando houver alteração relevante no arcabouço normativo de segurança da informação e cibernética.

Seção V - Definições

Art.10. Adotam-se as seguintes definições no âmbito desta Norma:

I - **acesso:** ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique;

II - **agente responsável pela ETIR:** servidor público, militar de carreira ou empregado público, ocupante de cargo efetivo em órgão ou entidade da administração pública federal, direta ou indireta, incumbido de chefiar e gerenciar a equipe de prevenção, tratamento e resposta a incidentes cibernéticos;

III - **ameaça:** conjunto de fatores externos com o potencial de causar dano para um sistema ou organização;

IV - **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 ou redes de computadores;

V - **ativo**: tudo que tenha valor para a organização, material ou não;

VI - **ativos de informação:** meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, recursos humanos que a eles têm acesso e conhecimento ou dado que tem valor para um indivíduo ou organização;

VII - **ativos de informação sob custódia da STI:** os ativos de informação que sejam formalmente colocados sob a responsabilidade da STI;

VIII - **auditoria:** processo de exame cuidadoso e sistemático das atividades desenvolvidas, cujo objetivo é averiguar se elas 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;

IX - **autenticação:** processo que busca verificar a identidade digital de uma entidade de um sistema, no momento em que ela requisita acesso a esse sistema. O processo é realizado por meio de regras preestabelecidas, geralmente pela comparação das credenciais apresentadas pela entidade com outras já pré-definidas no sistema, reconhecendo como verdadeiras ou legítimas as partes envolvidas em um processo;

X - **autenticidade**: propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade;

XI - **autorização:** processo que ocorre após a autenticação e que tem a função de diferenciar os privilégios atribuídos ao usuário que foi autenticado. Os atributos de autorização normalmente são definidos em grupos mantidos em uma base de dados centralizada, sendo que cada usuário herda as características do grupo a que ele pertence; portanto, autorização é o direito ou a permissão de acesso a um recurso de um sistema;

XII - **cadeia de custódia:** processo que acompanha o movimento de evidência, por meio de sua coleta, salvaguarda e ciclo de análise, documentando cada indivíduo que manuseou a evidência, o momento (data e hora) em que a evidência foi coletada ou transferida e o propósito de cada transferência. Contribui para a validação da prova pericial e do respectivo laudo gerado, porque garante a idoneidade e rastreabilidade dos vestígios, com a finalidade de preservar a confiabilidade e transparência até que o processo seja concluído;

XIII - **coleta de evidências de segurança em redes computacionais:** processo de obtenção de itens físicos que contêm uma potencial evidência, mediante a utilização de metodologia e de ferramentas adequadas. Esse processo inclui a aquisição, ou seja, a geração das cópias das mídias ou a coleta de dados que contenham evidências do incidente;

XIV - **comunidade ou público-alvo:** conjunto de pessoas, setores, órgãos ou entidades atendidas por uma Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos;

XV - **confidencialidade:** propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada à pessoa, ao sistema, ao órgão ou à entidade não autorizados nem credenciados;

XVI - **CTIR-GOV:** Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, subordinado ao Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República;

XVII - **disponibilidade**: propriedade pela qual se assegura que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;

XVIII - **ETIR:** sigla de Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos;

XIX - **GSIC**: Gestor de Segurança da Informação e Comunicações;

XX - **incidente cibernético:** ocorrência que pode comprometer, real ou potencialmente, a disponibilidade, a integridade, a confidencialidade ou a autenticidade de sistema de informação ou das informações processadas, armazenadas ou transmitidas por esse sistema. Poderá também ser caracterizada pela tentativa de exploração de vulnerabilidade de sistema de informação que caracterize violação de norma, política de segurança, procedimento de segurança ou política de uso. De maneira geral, os tipos de atividade comumente reconhecidas como incidentes cibernéticos são: a) tentativas de obter acesso não autorizado a um sistema ou a dados armazenados; b) tentativa de utilização não autorizada de sistemas para a realização de atividades de processamento ou armazenamento de dados; c) mudanças não autorizadas de firmware, hardware ou software em um ambiente computacional; d) ataques de negação de serviço (DoS); e e) demais ações que visem afetar a disponibilidade ou integridade dos dados. Um incidente de segurança cibernética não significa necessariamente que as informações já estão comprometidas; significa apenas que a informação está ameaçada;

XXI - **incidente de segurança:** qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

XXII - **informação:** dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

XXIII - **informação sigilosa:** informação submetida temporariamente à restrição de acesso público, em razão de sua imprescindibilidade para a segurança da sociedade e do Estado; e aquela abrangida pelas demais hipóteses legais de sigilo;

XXIV - **integridade:** propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XXV - **metadados:** conjunto de dados estruturados que descrevem informação primária;

XXVI - **preservação de evidências de incidentes cibernéticos:** 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;

XXVII - **registro de auditoria:** registro de eventos relevantes em um dispositivo ou sistema computacional;

XXVIII - **risco de segurança da informação e comunicações:** risco potencial associado à exploração de uma ou mais vulnerabilidades de um ou mais ativos de informação, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;

XXIX - **SIC**: Segurança da Informação e Comunicações;

XXX - **STI**: Superintendência de Tecnologia da Informação e Comunicações;

XXXI - **tratamento de incidentes cibernéticos:** consiste nas ações e procedimentos tomados imediatamente após a identificação do incidente, visando garantir a continuidade de operações, preservar evidências e emitir as notificações necessárias;

XXXII - **tratamento de incidentes de segurança em redes computacionais:** vide tratamento de incidentes cibernéticos;

XXXIII - **usuário:** qualquer empregado ocupante de cargo efetivo, função gratificada ou cargo em comissão, servidor ou empregado cedido ou movimentado para a EPE, ocupante de cargo estatutário, prestador de serviço terceirizado, estagiário ou qualquer outro indivíduo que tenha acesso, de forma autorizada, aos recursos computacionais da EPE; e

XXXIV - **vulnerabilidade:** condição que, quando explorada por um criminoso cibernético, pode resultar em uma violação de segurança cibernética dos sistemas computacionais ou redes de computadores, e consiste na interseção de três fatores: suscetibilidade ou falha do sistema, acesso possível à falha e capacidade de explorar essa falha.

CAPÍTULO II - DISPOSIÇÕES GERAIS

Seção I - Gestão de Incidentes Cibernéticos

Art.11. Esta Norma explicita as atividades de prevenção, tratamento e resposta a incidentes cibernéticos que possam comprometer a Segurança da Informação e Comunicações, SIC, da EPE.

§ 1º Estas atividades têm caráter técnico e objetivam proteger redes, servidores, aplicativos e dispositivos contra o uso mal-intencionado por agentes não autorizados, tais como:

I - tentativas de obter acesso não autorizado a um sistema ou a dados armazenados;

II - tentativa de utilização não autorizada de sistemas para a realização de atividades de processamento ou armazenamento de dados;

III - mudanças não autorizadas de firmware, hardware ou software em um ambiente computacional;

IV - ataques de negação de serviço (DoS); e

V - demais ações que visem afetar a disponibilidade ou integridade dos dados.

§ 2º As ações de prevenção, tratamento e resposta a incidentes cibernéticos serão majoritariamente executadas pela ETIR.

§ 3º Outras ações, principalmente de prevenção e resposta a incidentes cibernéticos, poderão ser executadas por outros atores, tais como o Gestor de SIC, o Comitê de SIC, a Superintendência de Tecnologia da Informação e os usuários da rede.

Art.12. Demais ações visando a Segurança da Informação e Comunicações da EPE e que extrapolem o ambiente cibernético estão fora do escopo desta Norma e deverão ser tratadas com o Gestor de Segurança da Informação e Comunicações.

Seção II - Constituição da ETIR

Subseção I - Missão

Art.13. A ETIR tem por finalidade facilitar e coordenar as atividades de prevenção, detecção, tratamento e resposta a incidentes cibernéticos da rede computacional da EPE, contribuindo para a preservação da disponibilidade, integridade, confidencialidade e autenticidade da informação da empresa. A ETIR também tem como objetivo realizar o intercâmbio de informações com o CTIR-GOV, com o intuito de integrar a Rede Federal de Gestão de Incidentes Cibernéticos e contribuir para a resiliência da Administração Pública Federal.

Subseção II - Público-Alvo

Art.14. O público-alvo servido pela ETIR são todos os colaboradores da EPE que recebem credenciais para utilizar os recursos computacionais da empresa, incluindo os empregados efetivos, estagiários, terceirizados e membros dos conselhos, bem como usuários externos que utilizem os sistemas disponibilizados pela EPE.

Subseção III - Modelo de Implementação e Estrutura

Art.15. A ETIR será composta preferencialmente por empregados efetivos designados pela STI.

§ 1º Em caso de insuficiência quantitativa ou qualitativa de pessoal nos quadros da STI, a ETIR pode ser complementada por meio de serviço especializado terceirizado.

§ 2º Alguns serviços oferecidos pela ETIR exigem atuação em regime de prioridade pela equipe alocada, de forma que a equipe seja capaz de reagir imediatamente à demanda do serviço e que esteja disponível até a conclusão das atividades decorrentes.

Art.16. O Agente Responsável pela ETIR deverá ser empregado efetivo da EPE e será designado pela Superintendência de TI, que também determinará seu percentual de dedicação à ETIR.

Art.17. O Agente Responsável pela ETIR será o responsável:

I - pela interlocução com o CTIR-GOV;

II - pela criação de procedimentos internos;

III - pelo gerenciamento das atividades; e

IV - pela atribuição de tarefas aos componentes da ETIR.

Subseção IV - Autonomia

Art.18. A ETIR 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.

Seção III - Serviços Oferecidos pela ETIR

Art.19. Para efeito desta Norma, os serviços oferecidos pela ETIR são descritos nas subseções seguintes de acordo com o modelo de serviços de CSIRT (Computer Security Incident Response Team) do FIRST (Forum of Incident Response and Security Teams), versão 2.1 November 2019.

§ 1º Para facilidade de correlação com o modelo FIRST, o nome do serviço nas subseções a seguir será seguido do número do item correspondente no modelo, entre parênteses.

§ 2º O modelo utilizado é uma referência, não sendo obrigatória a implementação de todos os serviços nele descritos.

Subseção I - Monitoração e Detecção de Eventos (5.1)

Art.20. O serviço Monitoração e Detecção de Eventos consiste no processamento do log de eventos dos equipamentos da rede, por meio de ferramentas automatizadas do tipo SIEM (Security Information and Event Management), visando a identificar eventos com potencial de se tornarem incidentes.

§ 1º A programação dos equipamentos de rede para geração dos logs de eventos deverá ser realizada ou, no mínimo, acompanhada por empregados efetivos da EPE.

§ 2º A definição das regras para identificar atividades suspeitas (gestão de casos de uso) deve ser feita com a participação efetiva de empregados da EPE, podendo haver assessoramento por equipes terceirizadas.

Subseção II - Análise de Eventos (5.2)

Art.21. O serviço Análise de Eventos consiste na análise dos potenciais incidentes classificados pelo serviço de Monitoração e Detecção de Eventos, buscando correlação entre os eventos e fazendo a qualificação como incidentes (verdadeiros positivos) ou falsos alarmes.

Parágrafo único. As funções de correlação e qualificação serão de responsabilidade da ETIR e poderão ser terceirizadas.

Subseção III - Recepção de Relatos de Incidentes (6.1)

Art.22. O serviço Recepção de Relatos de Incidentes consiste em receber relatos de potenciais incidentes de segurança provenientes do público-alvo, do serviço de Análise de Eventos ou ainda de entidades externas à EPE. Trata-se de importante atividade da ETIR.

Art.23. A STI deverá providenciar canais de comunicação eficientes e de fácil acesso para relato de incidentes de SIC pelo público-alvo.

§ 1º Devido às diferentes características, os canais para usuários internos e os para usuários externos poderão ser diferenciados.

§ 2º Os canais de comunicação deverão ser amplamente divulgados ao público-alvo.

Art.24. Todos os relatos de incidentes deverão ser prontamente respondidos, com a finalidade de acusar o recebimento. Após o tratamento do incidente, os responsáveis pelo relato deverão ser informados sobre o desenrolar das ações, com a finalidade de demonstrar a credibilidade da equipe.

Art.25. Este serviço exige atuação em regime de prioridade pela equipe alocada, conforme definido no Art.15.

Subseção IV - Análise de Incidentes (6.2)

Art.26. O serviço Análise de Incidentes consiste em ganhar conhecimento sobre o incidente e sobre os impactos reais e potenciais, a fim de identificar vulnerabilidades e as causas-raiz que possibilitaram o incidente.

Parágrafo único. Este serviço pode contar com a ajuda de outras equipes da EPE ou terceirizadas.

Subseção V - Análise de Artefatos e de Evidências Forenses (6.3)

Art.27. O serviço Análise de Artefatos e de Evidências Forenses consiste em conhecer o alcance e as intenções de artefato eventualmente encontrado, seus mecanismos de infecção, sua forma de propagação, de detecção e de mitigação e ainda os mecanismos para sua neutralização.

§ 1º Os artefatos devem ser preservados, de forma a possibilitar seu uso em eventuais processos administrativos, criminais ou judiciais.

§ 2º Devido à alta especialização necessária, o serviço deve ser provido por equipe externa especializada.

Subseção VI - Mitigação e Recuperação (6.4)

Art.28. O serviço Mitigação e Recuperação objetiva minimizar os impactos do incidente, limitando o número de vítimas e de perdas e recuperar o ambiente, evitando novos ataques e perdas por meio da remoção das vulnerabilidades exploradas e aumentando a segurança cibernética geral.

§ 1º Todas as ações adotadas deverão ser documentadas, passando a compor o acervo de lições aprendidas.

§ 2º As causas do incidente devem ser identificadas e ações corretivas devem ser tomadas, de forma a evitar novas ocorrências.

§ 3º As ações de mitigação e recuperação podem contar com a ajuda de outras equipes da EPE ou terceirizadas.

Subseção VII - Coordenação de Incidente (6.5)

Art.29. O serviço Coordenação de Incidente visa a:

I - garantir a distribuição de notificações e informações precisas entre a ETIR, a gestão da STI e a gestão de SIC, a manutenção do fluxo de informações necessário e o acompanhamento do estado das atividades; e

II - certificar que os planos de resposta estejam sendo executados e que os desvios devidos a atrasos e a novas informações sejam devidamente gerenciados.

§ 1º O serviço Coordenação de Incidente deverá ser executado pelo Agente Responsável pela ETIR.

§ 2º Todos os incidentes deverão ser registrados em base própria, com a finalidade de permitir uma revisão final dos fatos e conclusões e ainda de fornecer subsídios para o tratamento de futuros incidentes.

Subseção VIII - Gestão de Vulnerabilidade

Art.30. O serviço Gestão de Vulnerabilidade consiste na detecção, análise e tratamento de vulnerabilidades na rede da EPE, de forma a evitar que a vulnerabilidade seja explorada indevidamente.

Art.31. A detecção de vulnerabilidades deverá ser feita, no mínimo, com base no repositório Common Vulnerabilities and Exposures (CVE) mantido pela The Mitre Corporation.

§ 1º Deverão ser consideradas ainda as vulnerabilidades reportadas pelo CTIR-GOV.

§ 2º Devido ao alto grau de especialização, este serviço pode ser terceirizado.

Art.32. O tratamento das vulnerabilidades deve ser realizado pela STI, podendo haver terceirização do serviço.

§ 1º Caso o fabricante do ativo vulnerável não disponibilize correção para a vulnerabilidade detectada, deverá ser considerada a desativação temporária ou definitiva do ativo, levando em consideração os riscos envolvidos.

§ 2º Vulnerabilidades que envolvam alto risco não poderão ficar sem o devido tratamento por tempo indeterminado.

Subseção IX - Comunicação com o Público-Alvo

Art.33. O Agente Responsável fará, em conjunto com o GSIC, as comunicações ao público-alvo relativas a incidentes e vulnerabilidades encontradas.

Parágrafo único. Em caso de decretação de crise pelas instâncias superiores, a comunicação com o público-alvo passa a ser feita de forma centralizada, sob a responsabilidade das instâncias superiores.

CAPÍTULO III - DISPOSIÇÕES FINAIS

Art.34. A não observância dessa Norma pode acarretar ações administrativas, civis e penais, nos termos da legislação aplicável.

Art.35. Casos omissos ou excepcionais serão submetidos à aprovação da Diretoria Executiva.

Art.36. Normativo complementar disciplinará o tratamento de incidentes cibernéticos, os procedimentos operacionais e as demais medidas de controle necessárias à gestão da segurança da informação e comunicações na Companhia.

Parágrafo único. O normativo complementar de que trata o caput deverá contemplar, no mínimo, critérios de classificação de severidade de incidentes e vulnerabilidades, registros obrigatórios, comunicação e reporte às instâncias competentes, preservação de evidências, cadeia de custódia, salvaguardas aplicáveis a serviços terceirizados, relatório pós-incidente, lições aprendidas e interface com continuidade de negócios, recuperação de desastres e tratamento de indisponibilidade de sistemas críticos.

Art.37. Esta versão substitui sua versão anterior.

Art.38. Este Instrumento Normativo entra em vigor na data de sua publicação interna.