PORTARIA MCOM Nº 3.857, de 14 de outubro de 2021.

Aprova a Norma Complementar para Tratamento de Incidentes Cibernéticos.

A GESTORA DE SEGURANÇA DA INFORMAÇÃO, no uso das atribuições que lhe confere o inciso XII, do art. 2º, da Portaria nº 67/SEI-MCOM, de 4 de março de 2021, e tendo em vista o disposto no art. 15, inciso III, do Decreto nº 9.637, de 26 de dezembro de 2018, a Portaria MCOM Nº 2.454, de 22 de abril de 2021, os arts. 10, 15 e 19, da Instrução Normativa nº 1, de 27 de maio de 2020, do Gabinete de Segurança institucional da Presidência da República, resolve:

Art. 1º Aprovar a Norma Complementar para Tratamento de Incidentes Cibernéticos.

Art. 2º Esta Portaria entra em vigor na data de sua publicação.

**WANESSA QUEIROZ DE SOUZA OLIVEIRA**
Gestora de Segurança da Informação

## NORMA COMPLEMENTAR PARA TRATAMENTO DE INCIDENTES CIBERNÉTICOS

### OBJETIVO

Estabelecer as diretrizes para o Serviço de Tratamento de Incidentes Cibernéticos no âmbito do Ministério das Comunicações - MCOM.

### APLICAÇÃO

Os termos definidos nesta norma aplicam-se a todos os agentes públicos do Ministério das Comunicações.

### REFERÊNCIA LEGAL E NORMATIVA

Instrução Normativa 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;

Instrução Normativa nº 2, de 24 de julho de 2020, altera a Instrução Normativa 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;

Norma Complementar nº 05/IN01/DSIC/GSIPR, que disciplina a criação de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública

Federal;

Norma Complementar nº 08/IN01/DSIC/GSIPR, que estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal;

Portaria MCOM Nº 2.454, de 22 de abril de 2021, que aprova a Política de Segurança da Informação do Ministério das Comunicações;

Portaria MCOM nº 2.120, de 4 de março de 2021, que institui a Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR);

Portaria MCOM Nº 67, de 4 de março de 2021, que designa a Gestora de Segurança da Informação do Ministério das Comunicações.

**1. CONCEITOS E DEFINIÇÕES**

1.1. Ativo 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.
1.2. Agente Responsável pela ETIR - servidor público ocupante de cargo efetivo ou militar de carreira de órgão da Administração Pública Federal (APF), direta ou indireta incumbido de chefiar e gerenciar a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos.
1.3. Ataque: Evento de exploração de vulnerabilidades, ocorre quando um atacante tenta executar ações maliciosas, como invadir um sistema, acessar informações confidenciais ou tornar um serviço inacessível;
1.4. Bot: Código malicioso o qual permite que o invasor controle remotamente o computador ou dispositivo que hospeda;
1.5. Central de Serviços - equipe responsável pelos serviços de suporte técnico de tecnologia da informação do MCOM. Normalmente está associada aos colaboradores pertencentes ao contrato de sustentação da infraestrutura de rede do órgão.
1.6. Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo do Gabinete de Segurança Institucional da Presidência da República (CTIR Gov) - centro de tratamento subordinado ao Departamento de Segurança de Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República - DSIC/GSI/PR.
1.7. Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR - grupo de pessoas com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas à incidentes de segurança em redes computacionais.
1.8. Evidência - informação ou dado, armazenado ou transmitido eletronicamente que pode ser reconhecida como parte de um evento.
1.9. Gestora de Segurança da Informação - autoridade responsável por coordenar e instituir a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR.
1.10. Incidente de Segurança - qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores.
1.11. Metadados - Conjunto de dados que descrevem outros dados.
1.12. Preservação de evidência - 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.
1.13. Scripts: conjunto de instruções para que uma função seja executada em determinado aplicativo;
1.14. Serviço de Tratamento de Incidentes Cibernéticos - serviço que consiste em receber, filtrar, classificar e responder as solicitações e os 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.
1.15. Spam: Termo usado para se referir aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas;
1.16. Spyware: Programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros;
1.17. Trojan: Programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário;

1.18. Vírus: Programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos;
1.19. Worm: Programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador.

**2. DISPOSIÇÕES GERAIS**

2.1 A ETIR, em atenção à Norma Complementar nº 08/IN01/DSIC/GSIPR, deve observar e adotar, para a execução do Serviço de Tratamento de Incidentes Cibernéticos, no mínimo, os seguintes aspectos e procedimentos:
2.1.1 Registro de incidentes de segurança: todos os incidentes de segurança notificados ou detectados devem ser registrados, adotando o procedimento previsto nesta Norma, com a finalidade de assegurar o registro histórico das atividades da ETIR;
2.1.2 Tratamento da informação: o tratamento da informação pela ETIR deve ser realizado de forma a viabilizar e assegurar disponibilidade, integridade, confidencialidade e autenticidade da informação, observada a legislação em vigor, naquilo que diz respeito ao estabelecimento de graus de sigilo;
2.1.3 Recursos disponíveis: a ETIR deve possuir os recursos materiais, tecnológicos e humanos, suficientes para prestar os seus serviços;
2.1.4 Capacitação dos membros da ETIR: os membros da ETIR devem estar capacitados para operar os recursos disponíveis para a condução dos seus serviços;
2.2 Durante o gerenciamento de incidentes de segurança, havendo indícios de ilícitos criminais, a ETIR tem como dever:
2.2.1 Acionar as autoridades policiais competentes para a adoção dos procedimentos legais julgados necessários;
2.2.2 Observar os procedimentos para preservação das evidências, conforme previsto na Norma Complementar nº 21/IN01/DSIC/GSIPR, que estabelece as Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes nos órgãos e entidades da Administração Pública Federal, direta e indireta;
2.2.3 Priorizar a continuidade dos serviços da ETIR e da missão institucional da organização, observando os procedimentos previstos no item 2.8 desta Norma Complementar.
2.3 Os papéis, responsabilidades, fluxos de trabalho e procedimentos necessários para o processo de Serviço de Tratamentos de Incidentes Cibernéticos, no âmbito do Ministério, serão detalhados no Plano de Gestão de Incidentes Cibernéticos.

**3. PROCEDIMENTOS**

**3.1 Identificação de Incidente de Segurança**

3.1.1 Todos os agentes públicos que tenham conhecimento de incidentes de segurança devem notificar a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR), por meio da Central de Serviços, pelo telefone “+55 (61) 2027-5505” ou por meio de abertura de chamado em ferramenta específica, disponível em https://atendimento.mcom.gov.br;
3.1.2 Os incidentes de segurança identificados pela ETIR, por softwares especializados ou pela Central de Serviços devem ser registrados diretamente em ferramenta específica, disponível em https://atendimento.mcom.gov.br;

**3.2 Registro de Incidente de Segurança**

3.2.1 O registro deverá conter, no mínimo, as seguintes informações:
a) identificação do usuário que registrou o incidente de segurança;
b) descrição dos fatos do incidente de segurança;
c) data, hora e fuso horário do incidente de segurança;
d) outras informações relevantes sobre o incidente de segurança.

**3.3 Análise do Incidente de Segurança**

3.3.1 Após o registro, a ETIR deverá analisar a ocorrência registrada.
3.3.2 Caso a ETIR confirme que a ocorrência registrada é um incidente de segurança, deverá identificar os ativos de informação e serviços afetados e mensurar os impactos do incidente nos ativos de informação.
3.3.3 Após a mensuração dos impactos, deve-se classificar, priorizar e atribuir as responsabilidades para o tratamento do incidente.

**3.4 Tratamento do incidente de segurança**

3.4.1 A ETIR deve acompanhar a resolução do incidente de segurança, verificando se o tratamento do incidente segue os processos, os métodos e as normas estabelecidas.

3.4.2 A ETIR deve garantir a recuperação dos ativos de informação e serviços impactados em conformidade com os planos de recuperação, quando disponíveis.

3.4.3 O conhecimento adquirido na resolução dos incidentes deve ser registrado em base de conhecimento específica, no intuito de aprimorar a segurança do órgão e compartilhar as informações com o CTIR Gov.

3.4.4 As evidências do incidente devem ser armazenadas seguindo o disposto na Norma Complementar nº 21/IN01/DSIC/GSIPR, que estabelece as Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes nos órgãos e entidades da Administração Pública Federal, direta e indireta.

3.4.5 A ETIR deve adotar, após a resolução do incidente de segurança, as providências necessárias para eliminar ou minimizar a possibilidade de uma nova ocorrência do incidente.

**3.5 Comunicação do Incidente de Segurança**

3.5.1 O agente responsável pela ETIR deverá comunicar a ocorrência de incidente de segurança à Gestora de Segurança da Informação e ao proprietário do ativo.

3.5.2 O Centro de Prevenção, Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal - CTIR Gov, quando couber, deverá ser comunicado, conforme procedimentos a serem definidos pelo próprio CTIR Gov, com vistas a permitir que sejam dadas soluções integradas para a APF, bem como a geração de estatísticas.

---

Documento assinado eletronicamente por **Wanessa Queiroz de Souza Oliveira**, **Subsecretária de Planejamento e Tecnologia da Informação**, em 14/10/2021, às 17:19 (horário oficial de Brasília), com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

---

A autenticidade deste documento pode ser conferida no site http://sei.mctic.gov.br/verifica.html, informando o código verificador **8249370** e o código CRC **3F8DB28A**.

---

**Referência:** Processo nº 53115.007158/2021-12 SEI nº 8249370