



**MINISTÉRIO DO MEIO AMBIENTE**  
**INSTITUTO CHICO MENDES DE CONSERVAÇÃO DA BIODIVERSIDADE**  
GABINETE DA PRESIDÊNCIA  
EQSW 103/104, Bloco "C", Complexo Administrativo - Bloco C - Bairro Setor Sudoeste -Brasília  
Telefone: 61 2028-9011/9013

**PORTARIA Nº 193, DE 09 DE MARÇO DE 2018**

*Instituir a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) no ICMBio.*

**O PRESIDENTE DO INSTITUTO CHICO MENDES DE CONSERVAÇÃO DA BIODIVERSIDADE - ICMBio**, no uso das competências atribuídas pelo artigo 24 do Decreto nº. 8.974, de 24 de janeiro de 2017, e pela Portaria nº. 2.154/Casa Civil, de 07 de novembro de 2016, publicada no Diário Oficial da União de 08 de novembro de 2016,

Considerando a Norma Complementar nº 05, à Instrução Normativa Nº 01 do Gabinete de Segurança Institucional da Presidência da República, de 14/08/2009, doravante denominada NC05 – Trata da Criação de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais no âmbito da Administração Pública Federal;

Considerando a Norma Complementar Nº 08 à Instrução Normativa Nº 01 do Gabinete de Segurança Institucional da Presidência da República, de 19.08.2010, 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 – APF;

Considerando a Portaria nº441 de 20 de novembro de 2012 que institui o Comitê de Segurança da Informação e Comunicação – CSIC;

Considerando a Portaria nº 222, de 23 de agosto de 2013 que institui a Política de Segurança da Informação e Comunicação no âmbito do ICMBio,

**RESOLVE:**

Art. 1º Instituir a Equipe de Tratamento de Incidente em Rede Computadores (ETIR), no âmbito do Instituto Chico Mendes de Conservação da Biodiversidade.

§ 1º Não haverá Equipe exclusiva de tratamento e resposta a incidentes de Rede.

§ 2º Os membros participantes dessa Equipe desempenharão suas atribuições sem prejuízos decorrentes de seus respectivos cargos ou funções, sendo que a participação nessa atividade será considerada prestação de serviço relevante e não remunerada.

I – A Equipe será composta por dois membros Titulares, seus Suplentes e um Agente Responsável.

Art. 2º Os trabalhos serão guiados por padrões e procedimentos técnicos e normativos no contexto de tratamento de incidentes de rede orientados pelo Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal – CTIR GOV.

Art. 3º A estrutura organizacional da ETIR, com base na NC05, adotará o seguinte modelo:

I - A Equipe será formada por membros da Coordenação de Tecnologia da Informação e Comunicação (COTEC), que, além de suas funções regulares, desempenharão as atividades relacionadas ao tratamento e resposta a incidentes em redes computacionais.

II - São serviços a serem implementados e desempenhados pela ETIR:

- a. tratamento de incidentes de segurança em redes computacionais;
- b. tratamento de artefatos maliciosos;
- c. tratamento de vulnerabilidades;
- d. monitoramento da segurança da rede de computadores;
- e. observar os eventos de segurança com o objetivo de determinar tendências e padrões de atividades de invasores;
- f. disseminar informações relativas a novos ataques e tendências;
- g. disseminar informações de novas atualizações de softwares; e
- h. comunicar incidentes de segurança a órgãos competentes para fins estatísticos.

III - A Equipe só poderá agir com autorização do Coordenador de TI e/ou do Coordenador Geral de Tecnologia da Informação.

IV - No desempenho das atividades, a Equipe poderá recomendar os procedimentos a serem executados ou as medidas de recuperação durante um ataque, conduzindo os tomadores de decisão a agir durante um incidente de segurança, ressalvado o caráter sugestivo das recomendações.

V - A ETIR será acionada para atividades reativas, sempre que ocorrer a confirmação de um incidente na rede corporativa de computadores e sistemas do ICMBio.

Art. 4º Deverá ser designado um Agente Responsável, preferencialmente um Analista de Tecnologia da Informação (ATI), que terá a atribuição de criar os procedimentos internos, gerenciar as atividades e distribuir tarefas para a Equipe que compõe a ETIR.

I - Extraordinariamente, o Agente Responsável poderá convocar representantes de outras unidades para atuar em tratamento e resposta de determinado incidente de segurança.

II - O Agente Responsável deverá, gradativamente, implementar as atividades, delegando responsabilidades para que os seus membros as exerçam.

Art. 5º Os procedimentos a serem observados pela ETIR, para cada serviço, deverão ser formalizados em documento a ser elaborado pelo Agente Responsável, com o apoio de toda a equipe.

Art. 6º Esta portaria entra em vigor na data de sua publicação.

**RICARDO JOSÉ SOAVINSKI**



Documento assinado eletronicamente por **Ricardo Jose Soavinski, Presidente**, em 09/03/2018, às 19:14, conforme art. 1º, III, "b", da Lei 11.419/2006.



2608988 e o código CRC **7B13D8C9**.

---