MINISTÉRIO DAS COMUNICAÇÕES
Secretaria-Executiva do Ministério das Comunicações
Subsecretaria de Planejamento e Tecnologia da Informação
Coordenação-Geral de Tecnologia da Informação

ATA DE REUNIÃO

Assunto: **7ª Reunião Comitê de Segurança da Informação**

Local: Reunião virtual realizada via TEAMS.

Data: 28.09.2022

Membros Presentes:

Sergio Tito de Araujo - SECOM;

Mirian de Fátima Fiuza Oliveira - SEXEC;

Daniela Naufel Schettino - SETEL;

Luiz Fernando Bastos Coura - CGTI;

Otávio Viegas Caixeta - SERAD; e

Wanessa Queiroz de Sousa Oliveira - SPTI

1. PAUTA

1. Deliberação da Norma Complementar para Uso Seguro de Mídias Sociais;

2. Deliberação da Norma Complementar de Gerenciamento de Vulnerabilidades; e

3. Discussão sobre o bloqueio da rede institucional para equipamentos que não sejam de propriedade do MCOM.

2. ABERTURA

Satisfazendo o quórum mínimo de representatividade previsto na Portaria nº 2.120/SEI-MCOM, de 4 de março de 2021, que institui o Comitê de Segurança da Informação no âmbito do Ministério da Comunicações, em seu art. 8º, a reunião teve início às 15h30min. A Subsecretária de Planejamento e Tecnologia da Informação, sra. Wanessa Oliveira, saudou os representantes apresentando a pauta do comitê e passando ao Luiz Fernando para o início da apresentação.

3. ATA

3.1 Item 1 da pauta: Deliberação da Norma Complementar para Uso Seguro de Mídias Sociais.

Sr. Luiz apresentou a Norma Complementar destacando sua base na Instrução Normativa nº 06 de 23/12/2021 do GSI/PR. A Sra. Wanessa ressaltou que essa norma já havia sido discutida em outra reunião do COSIC mas que acharam muito importante a análise da ASCOM, por ser a unidade mais

impactada pela norma, então a ASCOM fez algumas sugestões, que após analisadas, foram incluídas na minuta da norma.

Atendidas as considerações, o item foi aprovado.

3.2. Item 2 da pauta: Deliberação da Norma Complementar de Gerenciamento de Vulnerabilidades.

Sr. Luiz Fernando apresentou a norma complementar para Gerenciamento de Vulnerabilidades.

Luiz constatou erro de redação no item 2.5.5. A referência ao item 2.5.2 estava erroneamente indicando o item 44.

Sr. Otávio citando o item 1.8 aponta para uma definição futura da métrica e ele gostaria de saber como isso vai funcionar e sugeriu que essa competência já ficasse estabelecida em nível mais operacional, como a própria CGTI ou o ETIR. Sra. Wanessa sugeriu que a definição dessa métrica fosse feita pelo Gestor de Segurança de Informação traria para o COSIC só a título de conhecimento e não mais definição. Assim, ficou decidido alteração do item 1.8 para: “As métricas de gerenciamento de vulnerabilidades devem ser definidas pelo Gestor de Segurança da Informação e suas medições devem ocorrer, no mínimo, a cada 3 meses.”

Sobre os itens 2.2.4 e 2.2.5, Sr. Otávio questionou se a frequência dos testes de segurança vai variar de acordo com cada tipo de teste e ressaltou que a ideia dele é que a norma seja mais autoaplicável, que os requisitos legais, períodos determinados e frequência já estejam determinados. Assim, ficou decidido pela manutenção do 2.2.4 e alteração do item 2.2.5 para: “As varreduras de vulnerabilidades na rede corporativa devem ser realizadas por períodos determinados de até 3 meses ou após alteração significativa na rede, por equipe interna ou por terceiro ou uma combinação de ambos.”

Em relação ao Item 2.3.7 o Sr. Otávio sugere que além de uma atuação reguladora do COSIC, que fosse apresentado ao Comitê um relatório informativo também, que apresente testes, eventuais phishings, tentativas de invasão, para que assim o comitê tenha ciência da natureza dos riscos aos quais estamos expostos. Sra. Wanessa acatou a sugestão e ressaltou que a revisão da portaria do Comitê Ministerial de Governança está em andamento. Solicitou, também, que nas próximas reuniões do COSIC, além das pautas já existentes, sejam apresentados temas relacionados à segurança de TI com os acompanhamentos que já têm sido feitos no ETIR. Após as considerações, a sugestão de novo texto do Sr. Luiz para o item 2.3.7: “Todas as versões do relatório devem ser remetidas ao Comitê de Segurança de Informação e Comunicação.”

Sr. Otávio, no item 2.9.1, questiona a necessidade de testes e aprovações prévios a aplicação de patchs, considerando que os fornecedores já realizaram testes prévios à disponibilização, e sugere aplicarmos imediatamente os patches, assim, minimizaríamos o intervalo de vulnerabilidade do ativo. Sr. Luiz disse que esse ponto é importante que seja discutido, mas entende que a redação permite essa atuação e que já houve patches testados em nível mundial que trouxeram problemas no Brasil e, por este motivo, cabe análise pontual quando da liberação de um patch. Ficou definido que esse item será mantido inalterado.

Atendidas as considerações acima, esse item referente à norma complementar para Gerenciamento de Vulnerabilidades foi aprovado e uma nova redação será elaborada.

3.3. Item 3 da pauta: Discussão sobre o bloqueio da rede institucional para equipamentos que não sejam de propriedade do MCOM.

Sr. Luiz apresentou a proposta para implementação de controle já previsto na Norma Complementar para Controle de Acesso Lógico do Ministério das Comunicações, onde o acesso por meio de computador pessoal será concedido mediante Termo de Responsabilidade, estando a rede fechada para equipamentos não identificados. A solução será aplicada na rede cabeada somente, sendo o Wi-Fi não escopo dessa implementação.

Sr. Luiz informou que após a realização de testes, será definida a data para virada da chave e a divulgação com antecedência mínima de 30 dias para adesão. Sra. Wanessa informou que a comunicação será realizada, também, por Ofício Circular.

4. ENCERRAMENTO

Sem mais considerações, a reunião foi encerrada às 17h.

Documento assinado eletronicamente por **Sergio Tito de Araujo**, **Assessor Técnico**, em 19/10/2022, às 15:25 (horário oficial de Brasília), com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Mirian de Fatima Fiuza de Oliveira**, **Assessora**, em 20/10/2022, às 12:21 (horário oficial de Brasília), com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Otavio Viegas Caixeta**, **Diretor do Departamento de Inovação, Regulamentação e Fiscalização**, em 21/10/2022, às 09:55 (horário oficial de Brasília), com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Wanessa Queiroz de Souza Oliveira**, **Subsecretária de Planejamento e Tecnologia da Informação**, em 26/10/2022, às 09:22 (horário oficial de Brasília), com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Daniela Naufel Schettino**, **Coordenadora-Geral de Projetos de Infraestrutura**, em 03/11/2022, às 14:34 (horário oficial de Brasília), com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Luiz Fernando Bastos Coura**, **Coordenador-Geral de Tecnologia da Informação e Comunicação**, em 10/11/2022, às 13:31 (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 https://super.mcom.gov.br/sei/verifica, informando o código verificador **10460969** e o código CRC **A40297BF**.

Referência: Processo nº 53115.007158/2021-12 SEI nº 10460969