

- na Portaria-SEI nº 73, de 18 de maio de 2021, publicada no Boletim de Serviço nº 1069, de 20 de maio de 2021, que reinstituíu o Comitê de Segurança da Informação no âmbito da Administração Central; resolve:

Art. 1º Instituir a Equipe de Tratamento e Resposta a Incidentes Cibernéticos da Ebserh (Etir-Ebserh), em observância à determinação estabelecida no item 6.2 da Política de Segurança da Informação e Comunicação da Ebserh, conforme Regimento Interno da Etir-Ebserh, que regulamenta o funcionamento da equipe, disposto no Anexo I desta Portaria-SEI.

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

Oswaldo de Jesus Ferreira

ANEXO I - REGIMENTO INTERNO

Equipe de Tratamento e Resposta a Incidentes Cibernéticos da Ebserh (Etir-Ebserh)

Portaria Ebserh Nº 113/2021

SEÇÃO I – MISSÃO

1.1. A Equipe de Tratamento de Incidentes Cibernéticos da Rede Ebserh, denominada Etir-Ebserh, tem por missão receber, registrar e notificar qualquer evento adverso à segurança da informação, confirmado ou sob suspeita, planejar, facilitar e coordenar atividades de prevenção e tratamento da ocorrência de incidentes cibernéticos relacionado aos ativos de informação da Ebserh, preservando os dados, as informações e a infraestrutura da Rede Ebserh.

1.2. A Etir-Ebserh tem por visão ser reconhecida como ponto focal de assuntos relacionados à segurança cibernética da Rede Ebserh, incluindo a Administração Central e suas filiais.

SEÇÃO II – PÚBLICO-ALVO

2.1. As atividades da Etir-Ebserh abrangem todos os recursos tecnológicos de rede, sistemas e serviços utilizados por todos os usuários dos serviços públicos prestados pela Ebserh, e que são suportados, direta ou indiretamente, pela infraestrutura cibernética da Rede Ebserh.

I - Inclui-se dentre os usuários: profissionais de saúde, técnicos e analistas administrativos, pacientes e quaisquer outros usuários de serviços prestados pela Ebserh;

II - A infraestrutura cibernética da Ebserh envolve:

1. Sistemas de informação hospedados e administrados pela Diretoria de Tecnologia da Informação;
2. Sistemas de informação hospedados e administrados pelos Setores de Tecnologia da Informação e Saúde Digital (SETISDs) dos HUFs;
3. Domínios registrados na Internet sob administração da Ebserh; e

4. Rede Ebserh, composta pelos blocos de endereçamento IPv4 e IPv6 designados aos HUFs.

2.2. O contato com a Etir-Ebserh, para fins de envio e recebimento de notificações de incidentes de rede computacional, e outras comunicações institucionais relacionadas à segurança cibernética, deve ser realizado através do e-mail abuse@ebserh.gov.br.

2.3. As atividades devem ser realizadas com o intercâmbio de informações e em cooperação com as seguintes organizações:

- CTIR GOV - Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo;
- CAIS/RNP - Centro de Atendimento a Incidentes de Segurança;
- CERT.br - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil;
- Órgãos, entidades, empresas públicas ou privadas que tenham contratos, acordos ou convênios com a Ebserh.

SEÇÃO III – SERVIÇOS

3.1. A Etir-Ebserh deve prover os seguintes serviços ao seu público:

3.1.1. Tratamento de incidentes de segurança cibernética.

Tratar as ocorrências de incidentes de segurança cibernética, examinando artefatos, evidências e registros relacionados;

3.1.2. Monitoramento de segurança cibernética.

Analisar o tráfego de rede e eventos de segurança relacionados aos serviços, com o objetivo de identificar e notificar padrões maliciosos de tráfego e de ataques cibernéticos, bem como coletar indicadores para estudo de tendências e recomendações de estratégias de prevenção adequadas e tomadas de decisão.

3.1.3. Gestão de vulnerabilidades.

Pesquisar informações sobre novas ameaças e vulnerabilidades na infraestrutura cibernética da Ebserh; realizar o escaneamento nos recursos computacionais da Ebserh em busca de versões desatualizadas e vulneráveis; notificar preventivamente as partes interessadas e equipes responsáveis dos SETISDs dos HUFs e da Administração Central sobre a aplicação de *patches*, correções de configuração ou novas versões de software, bem como tendências de incidentes ou eventos prejudiciais à infraestrutura cibernética da Ebserh.

3.1.4. Qualidade / Capacitação.

Realizar ações de capacitação técnica em segurança cibernética para os técnicos de TIC das unidades da Ebserh. Realizar ações de conscientização do uso seguro de recursos computacionais para profissionais e usuários de serviços da Ebserh.

SEÇÃO IV – MODELO ORGANIZACIONAL

4.1. O modelo organizacional adotado é o modelo misto, sendo a Etir-Ebserh composta por uma Equipe Central e Equipes Distribuídas.

4.1.1. A Equipe Central adota o modelo Centralizado. É responsável pela organização das atividades da ETIR junto às Equipes Distribuídas, e é também responsável pela comunicação formal para os níveis internos da Ebserh e para organizações externas.

4.1.2. As Equipes Distribuídas adotam o modelo Equipe de TI. Atuam localmente no respectivo HUF, executando as estratégias definidas pela Equipe Central, bem como na execução dos procedimentos de tratamento dos incidentes de segurança cibernéticos, de acordo com as atribuições definidas.

CAPITULO V – ESTRUTURA ORGANIZACIONAL

5.1 A Etir-Ebserh é gerenciada pelo Serviço de Infraestrutura e Segurança de Tecnologia da Informação, vinculada à Coordenadoria de Infraestrutura, Suporte e Segurança de Tecnologia da Informação, na Diretoria de Tecnologia da Informação da Ebserh.

5.2. A Etir-Ebserh deve ser composta por profissionais com conhecimento e experiência técnica compatíveis com a importância e missão da equipe e de seus respectivos cargos.

5.3 Definições do Agente Responsável da Etir-Ebserh:

5.3.1. O Agente Responsável será o Coordenador de Infraestrutura, Suporte e Segurança de Tecnologia da Informação ou Chefe de Serviço subordinado a ele.

5.3.2. O Agente Responsável responde pela coordenação da Etir-Ebserh.

5.3.3. São responsabilidades do Agente Responsável da Etir-Ebserh:

- Responder pela coordenação da Etir-Ebserh, gerenciar as atividades de seus membros, bem como definir metodologias e procedimentos internos;
- Representar a Etir-Ebserh em reuniões e foros internos com Diretoria, Comitê Gestor de Tecnologia da Informação, Comitê de Segurança da Informação ou outras instâncias internas da Ebserh;
- Ser interface com CTIR Gov.
- Ser interface junto às autoridades policiais e judiciais competentes sobre incidentes de rede computacionais que tipifiquem crime;
- Responder por todas as decisões, ações técnicas e administrativas da Etir-Ebserh;
- Apresentar relatórios executivos sobre os incidentes de rede computacionais e atividades da Etir-Ebserh.

5.4. Definições da Equipe Central da Etir-Ebserh:

5.4.1. Os membros da Equipe Central da Etir-Ebserh devem ser indicados pelo Agente Responsável, devendo ser do quadro funcional da Ebserh, com conhecimento em segurança cibernética, gestão de processos e perfil técnico adequado às funções de tratamento de incidentes de rede.

5.4.1.1. A equipe poderá ser estendida com a inclusão de representantes de áreas específicas da organização, como jurídico, estatística, recursos humanos, gestão de risco, auditoria e controle, consultores técnicos, ou solicitar, conforme necessidade, apoio da equipe de suporte de TI terceirizada da Ebserh, conforme a Etir-Ebserh entenda ser adequada para o desenvolvimento de suas atividades.

5.4.2. Para cada membro titular da Etir-Ebserh que compõe a equipe, deve ser indicado um suplente correspondente.

5.4.2.1. Cada membro deve ter ao menos um substituto com conhecimentos técnicos comprovados e equivalente aos efetivos.

5.4.3. São responsabilidades dos membros da Equipe Central:

- Realizar o monitoramento de segurança cibernética.
- Responder às notificações de incidentes de rede computacional encaminhadas à Ebserh;
- Notificar outras equipes os incidentes de segurança quando identificado um ataque cibernético direcionado à Ebserh;
- Validar a resolução dos incidentes de rede e a recuperação do ambiente computacional após o incidente e recomendar ações para evitar reincidências;
- Manter a base de dados de informações de incidentes e vulnerabilidades sempre consistentes e atualizadas;
- Organização da execução das estratégias definidas para as Equipes Distribuídas;

5.5. Definições das Equipes Distribuídas da Etir-Ebserh:

5.5.1. É composta por:

- Chefe do SETISD local, como ponto focal de contato;
- Analistas de TI das unidades – que podem ser do quadro funcional da Ebserh e/ou de empresas prestadoras de serviço de suporte em TI – como equipe operacional dos serviços da Etir.

5.5.2. Os membros das Equipes Distribuídas devem ter perfil técnico adequado às funções de operação de segurança cibernética e tratamento de incidentes de rede.

5.5.3. São responsabilidades dos membros das Equipes Distribuídas:

- Realizar o monitoramento de segurança cibernética;
- Realizar o tratamento das notificações de incidentes de rede computacional encaminhadas pela Equipe Central;
- Executar as estratégias de operação de segurança cibernética definidas pela Equipe Central;
- Tratar as vulnerabilidades relacionadas a ativos e sistemas da infraestrutura do respectivo HU.

SEÇÃO VI – AUTONOMIA

6.1 A Etir-Ebserh tem autonomia compartilhada, trabalhando em conjunto com outros setores da Ebserh, a fim de auxiliar no processo de tomada de decisão.

6.1.1. A Etir-Ebserh participa ativamente com os outros níveis hierárquicos da Ebserh do processo decisório de ações de tratamento de incidentes de segurança cibernético, define procedimentos necessários a serem executadas, discutindo os impactos.

6.1.2. A Etir-Ebserh deve manter uma base de dados de políticas e procedimentos técnicos e normativos para uso dos SETISDs locais no processo de tratamento dos incidentes de rede computacional, podendo se valer de boas práticas de mercado, desde que não conflitem com dispositivos legais em vigor.

SEÇÃO VII – DISPOSIÇÕES FINAIS

7.1 A Etir-Ebserh deve levar assuntos de interesse relevante ao Comitê de Segurança da Informação da Administração Central da Ebserh, visando, principalmente, a prevenção de novos incidentes de redes computacionais.

7.2. Casos omissos devem ser resolvidos pela Etir-Ebserh, em observância à Política de Segurança da Informação da Ebserh e da legislação em vigor.

COLEGIADO DE JULGAMENTO DISCIPLINAR

SUSPENSÃO

Portaria-SEI nº 49, de 12 de julho de 2021

O Colegiado de Julgamento Disciplinar da Sede da Empresa Brasileira de Serviços Hospitalares - Ebserh, no uso das atribuições que lhe são conferidas pelo art. 109 da Norma Operacional de Controle Disciplinar, e em consonância com o disposto no art. 114 da citada norma,

Considerando a documentação constante nos autos do Processo-SEI 23539.015279/2020-13;

Considerando a deliberação ocorrida em reunião realizada em 09 de julho de 2021;

Considerando o entendimento da Consultoria Jurídica sobre o caso; resolve:

Art. 1º Suspender por 30 (trinta) dias, a empregada pública indiciada no Processo 23539.015279/2020-13, pela prática de infração ao Regulamento de Pessoal da Ebserh, art. 37, inciso VIII e art. 39, inciso XVII.

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

Eduardo Chaves Vieira

Vice-Presidente

Giuseppe Cesare Gatto

Diretor de Ensino, Pesquisa e Atenção à Saúde

Rodrigo Augusto Barbosa

Diretor de Gestão de Pessoas