NORMA DE PREVENÇÃO, TRATAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS

– NOR 705

SUMÁRIO

1. FINALIDADE

1.1 Regulamentar a criação e a atuação da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos na Rede Computacional – ETIR da Empresa Brasil de Comunicação S.A. – EBC.

2. ÁREA GESTORA

2.1 Diretoria de Operações, Engenharia e Tecnologia – DOTEC.

3. CONCEITUAÇÃO

3.1 AGENTE RESPONSÁVEL PELA ETIR

Empregado, preferencialmente ocupante de cargo efetivo, que se enquadre em qualquer das opções seguintes:

a) possuidor de credencial de segurança;

b) quando nomeado, será incumbido de chefiar e gerenciar a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos em Redes Computacionais – ETIR;

c) incumbido de chefiar ou gerenciar o processo de Inventário e Mapeamento de Ativos de informação;

d) incumbido de chefiar e gerenciar o uso de dispositivos móveis; ou

e) incumbido da gestão do uso seguro de redes sociais.

3.2 ATIVIDADE DA ETIR

Conjunto de procedimentos, estruturados em um processo bem definido, oferecido à comunidade da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos em Redes Computacionais.

3.3 ATIVO DE INFORMAÇÃO

Meios de armazenamento, transmissão e processamento de informação, os sistemas de informação, bem como os locais onde se encontram esses meios, as pessoas que a eles têm acesso, a imagem institucional, os serviços e tudo aquilo que tem valor para a EBC e que esteja relacionado com a informação e a comunicação.

3.4 AUTORIDADE COMPETENTE DA EBC

Qualquer pessoa que tenha autoridade ou poder delegado ou investido legalmente para desempenhar uma função designada.

3.5 COMUNIDADE DA ETIR

Conjunto de pessoas, setores, órgãos ou entidades atendidas por uma Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos em Redes Computacionais. Também chamado de público-alvo da ETIR.

3.6 CTIR.GOV

Centro de Prevenção, Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores – CTIR da Administração Pública Federal, subordinado ao Departamento de Segurança da Informação – DSI do Gabinete de Segurança Institucional da Presidência da República – GSI.

3.7 EQUIPE DE PREVENÇÃO, TRATAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS EM REDES COMPUTACIONAIS – ETIR

Grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores.

3.8 GESTÃO DE INCIDENTES CIBERNÉTICOS

Ações sobre qualquer evento adverso relacionado à segurança cibernética dos sistemas ou da infraestrutura de computação.

3.9 GESTOR DE SEGURANÇA DA INFORMAÇÃO

Responsável pelas ações de Segurança da Informação no âmbito do órgão ou entidade da Administração Pública Federal.

3.10 INCIDENTE DE SEGURANÇA

Qualquer evento adverso, confirmado ou sob suspeita, ou ocorrência que promova uma ou mais ações tendentes a comprometer ou ameaçar a disponibilidade, a integridade, confidencialidade ou a autenticidade de qualquer ativo de informação da EBC.

3.11 REDE DE COMPUTADORES

Conjunto de computadores, interligados por ativos de rede, capazes de trocar informações e de compartilhar recursos, por meio de um sistema de comunicação.

3.12 SEGURANÇA DA INFORMAÇÃO

Ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.

3.13 TRATAMENTO DE INCIDENTES CIBERNÉTICOS DE SEGURANÇA EM REDES COMPUTACIONAIS

Atividade que consiste em receber, filtrar, classificar e responder às solicitações e aos alertas/notificações; e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e a identificação de tendências.

4. COMPETÊNCIAS

4.1 Compete ao Comitê de Segurança da Informação e da Comunicação – COSIC instituir a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos na Rede Computacional da EBC – ETIR/EBC.

4.2 Compete aos membros da ETIR/EBC:

I - monitorar, receber e registrar eventos de incidentes de segurança e alertas/notificações;

II - elaborar relatórios de incidentes de segurança e alertas/notificações;

III - categorizar, priorizar e atribuir eventos e incidentes de segurança;

IV - analisar os impactos, ameaças ou danos ocorridos, definindo a reparação e os passos de mitigação a serem seguidos;

V - prestar assessoria técnica na elaboração de políticas, normas, pareceres e na especificação técnica de produtos e equipamentos direcionados à Segurança da Informação e Comunicação; e

VI - acompanhar alertas/notificações de incidentes de segurança na rede computacional e encaminhá-los para tratamento.

4.3 Cabe ao Agente Responsável pela ETIR/EBC:

I - coordenar as ações da ETIR/EBC; e

II - solicitar, junto as áreas técnicas da EBC envolvidas nos Incidentes Cibernéticos, a indicação dos membros para atuar na ETIR/EBC.

III - manter a comunicação com o Gestor de Segurança da Informação.

4.3.1 A indicação de que trata o inciso II do item 4.3 deverá considerar o perfil profissional desejável adequado às funções, conforme estabelecido no item 5.7 desta Norma.

5. ORIENTAÇÕES GERAIS

5.1 MISSÃO

5.1.1 A ETIR/EBC tem como missão planejar, coordenar e executar atividades de prevenção, tratamento e resposta a incidentes cibernéticos em redes computacionais, receber e alertar/notificar qualquer evento adverso à segurança da informação, confirmado ou sob suspeita, relacionado às redes de computadores, preservando os dados, as informações e a infraestrutura da EBC.

5.2 PÚBLICO-ALVO

5.2.1 Como público-alvo a ETIR/EBC fará a gestão dos incidentes cibernéticos que comprometa a rede computacional e sistemas de informação dos usuários da EBC.

5.3 AUTONOMIA DA ETIR/EBC

5.3.1 A autonomia da ETIR/EBC descreve o escopo de atuação e o nível de responsabilidade que essa Equipe tem sobre as suas próprias ações, as atividades de resposta e tratamento dos incidentes na rede de computadores da EBC.

5.3.2 A ETIR/EBC possui a autonomia compartilhada, no entanto poderá trabalhar em comum acordo com os outros setores da Empresa a fim de participar do processo de tomada de decisão sobre quais medidas devem ser adotadas.

5.3.3 A depender da recomendação dada como resposta e tratamento do incidente de segurança, a Equipe da ETIR deverá consultar outras instâncias de governança, tal como o Comitê de Segurança da Informação e a Diretoria Executiva, conforme o impacto e a alçada da recomendação.

5.3.3.1 Neste caso a ETIR/EBC participará do processo decisório manifestando a opinião técnica e, recomendando os procedimentos a serem executados ou as medidas de recuperação durante o incidente e discutindo as possíveis ações a serem tomadas. Também informarão os impactos que poderão ocorrer caso as recomendações não sejam seguidas.

5.4 MODELO DE ATUAÇÃO

5.4.1 A ETIR/EBC será formada por Analista de Segurança, Analista de Desenvolvimento, Analista de Rede e Analista de Sistemas Operacionais, empregados lotados na da área de Tecnologia da Informação da EBC, que, além de suas funções regulares, passarão a desempenhar as

atividades relacionadas ao tratamento e resposta a incidentes cibernéticos na rede computacional da EBC.

5.5 IMPLANTAÇÃO DA ETIR/EBC

5.5.1 As etapas abaixo são recomendadas para a implantação da ETIR na EBC:

I - nomear o Agente Responsável e seu substituto;

II - definir membros;

III - capacitar/qualificar membros da ETIR/EBC:

a) procedimentos/técnicas;

b) ferramentas/equipamentos;

IV - definir e documentar processos;

V - divulgar e conscientizar o público sobre a ETIR/EBC; e

VI - avaliar a ETIR/EBC regularmente.

5.6 ESTRUTURA OPERACIONAL

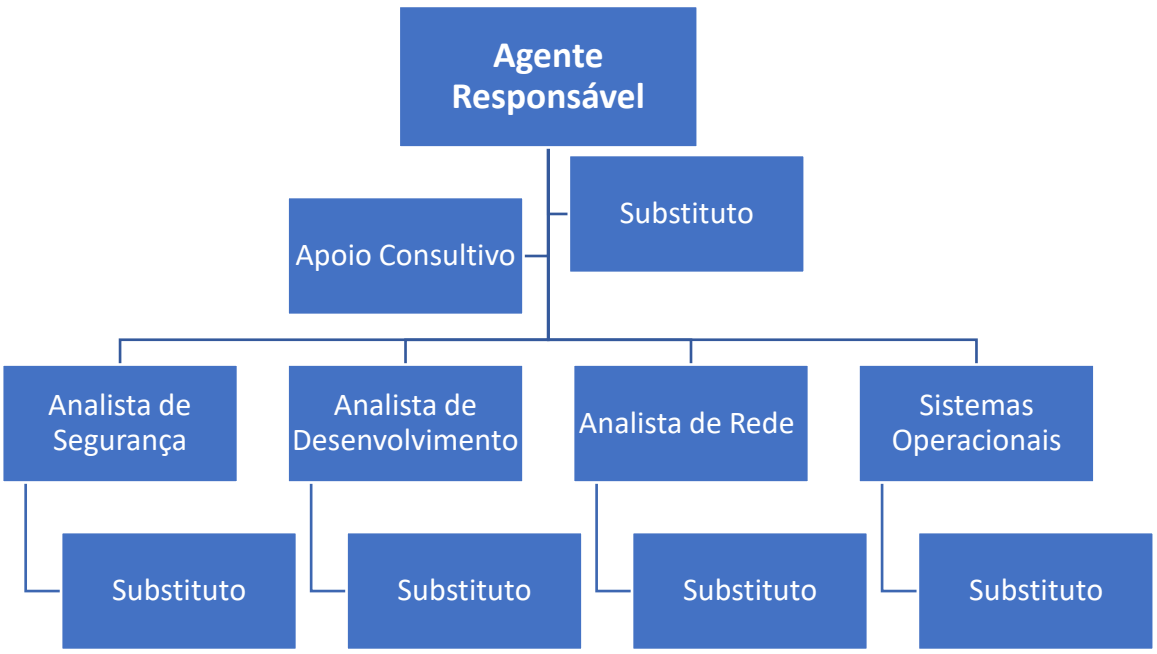

Figura ilustrativa

5.6.1 Para gestão das atividades da ETIR/EBC, o Agente Responsável e seu substituto, preferencialmente empregados efetivos de carreira, deverão ser formalmente nomeados para essa função, por autoridade competente da EBC, bem como suas atribuições.

5.6.2 A gestão da ETIR/EBC será instituída na Coordenação de Segurança da Informação e Governança de TI, vinculada à Diretoria de Operações, Engenharia e Tecnologia – DOTEC.

5.7 PERFIS PROFISSIONAIS

5.7.1 A ETIR/EBC deve ser treinada para lidar com análise de incidentes, priorização, encaminhamento, correção e geração de relatórios em todo o ciclo de vida do incidente.

5.7.2 Os membros da ETIR/EBC devem possuir experiência nas áreas de gestão de sistema ou de segurança, de banco de dados, de rede, analista de suporte ou quaisquer outras pessoas da Empresa com conhecimento técnico comprovado.

5.7.2.1 A ETIR/EBC poderá ser estendida com a inclusão dos seguintes membros de áreas específicas da EBC com conhecimento em: direito, estatística, gestão de pessoas, relações públicas, gestão de riscos, controle interno e grupo de investigação, ou outro que a Empresa entenda ser adequado.

5.7.3 A adequação dos perfis profissionais traz benefícios como o aumento da probabilidade de sucesso no estabelecimento da Equipe e perenidade do processo de trabalho.

5.7.4 A ETIR/EBC deverá ser composta por, no mínimo, 5 (cinco) integrantes, sendo 4 (quatro) deles da área técnica e 1 (um) da área de gestão.

5.7.5 A ETIR/EBC deverá ser formada, preferencialmente, por profissionais com os seguintes perfis:

I - para coordenar as atividades da ETIR/EBC: profissional com experiência em gerenciamento de projetos, conhecimentos em segurança da informação, coordenar equipes, liderança e gestão de pessoas.

II - para lidar com ataques baseados em Rede (*Network-Based*): profissional com experiência em *Firewalls*, Roteadores, *Switches*, protocolos de rede e modelo OSI.

III - para lidar com ataques baseados em Estações (*Host-Based*): profissional com experiência em Sistemas Operacionais Windows, Linux e UNIX.

IV - para lidar com ataques ao Banco de Dados: profissional com experiência em *Oracle*, MSSQL, PLSQL, PostgreSQL.

V - para lidar com ataques em que o alvo seja os Sistemas: profissional com experiência em ferramentas de desenvolvimento, linguagens de programação Java, *Java Script*, *Delphi*.

VI - para lidar com ataques em que o alvo seja o E-mail Coorporativo: profissional com conhecimento em Servidores de e-mail como Microsoft Exchange Server, PostFix, Qmail, Zimbra.

VII - para lidar com ataques em que os alvos sejam os Sítios relacionados à EBC: profissional com experiência em desenvolvimento *Web*, *Web Designers*, Sistemas Operacionais, Microsoft IIS ou Apache.

VIII - para lidar com Vírus, *Spam*, *Phishing/Scam* e semelhantes: profissional com experiência em ferramentas antivírus, Sistemas Operacionais e Microsoft Exchange.

IX - para lidar com questões que envolvam o Ministério Público Federal, Tribunal de Contas da União, a Corregedoria Geral da União, Advocacia Geral da União ou Polícia Federal: preferencialmente profissional com formação acadêmica em Direito, conhecimentos em segurança da informação e conhecimentos em análise forense.

5.7.5.1 No caso de um incidente que envolva os órgãos mencionados no inciso IX do item 5.7.5, o Gestor deve acompanhar todo o processo junto com as autoridades. Na ausência do profissional com esse perfil, a Equipe poderá ser estendida com a inclusão de representantes de áreas específicas da EBC, conforme listado no 5.7.2.1, além de formar grupo de investigação ou qualquer outro que a ETIR/EBC entenda ser adequado para o desenvolvimento de suas atividades.

5.7.6 A capacitação/qualificação dos membros da ETIR/EBC para desempenhar atividades relacionadas à prevenção, tratamento e resposta a incidentes cibernéticos na rede computacional da Empresa será definida pelos Gerentes diretamente envolvidos no processo.

5.7.7 Os conhecimentos e habilidades dos profissionais envolvidos com a ETIR devem ser atualizados periodicamente por meio de capacitação.

6. ATIVIDADES DA ETIR/EBC

6.1 Cabe à ETIR/EBC monitorar, receber alertas, analisar, classificar e notificar qualquer incidente de segurança, mediante a realização das seguintes atividades:

I - monitoramento de alertas: identificar atividades maliciosas dentre os eventos de segurança e encaminhá-los para tratamento;

II - acompanhamento de alertas: acompanhar os alertas de incidentes de segurança na rede computacional, encaminhá-los para tratamento, registrar as condutas adotadas, identificar

tendências e padrões de atividades maliciosas e coletar indicadores estatísticos, com o objetivo de criar base de conhecimento sobre os incidentes de segurança com banco de informações na rede da EBC e respectivos tratamentos;

III - registro de incidentes: registrar informações sobre os incidentes de segurança, suas características, danos causados e medidas corretivas e preventivas;

IV - descrição das funções e procedimento a atividade: realizar coleta e registrar informações que permite identificação do escopo do incidente de segurança, incluindo artefatos, evidências, *logs* relacionados, sua extensão, natureza e quais os impactos causados, apresentando aos Gestores das áreas envolvidas as informações levantadas referentes ao incidente e as soluções propostas para o tratamento adotado;

V - análise e tratamento de incidentes de segurança: analisar as informações disponíveis sobre os incidentes e indicação dos tratamentos a serem adotados, com o objetivo de produzir informações e conhecimentos sobre os incidentes de segurança registrados e adotar as medidas corretivas adequadas;

VI - comunicação sobre incidentes de segurança: comunicar incidentes de segurança aos órgãos competentes para fins estatísticos, geração de soluções integradas e investigação com objetivo de manter canal de comunicação sobre incidentes de segurança com órgãos competentes;

VII - comunicação aos órgãos externos competentes: levantar informações sobre incidentes de segurança e comunicar aos órgãos competentes, tais como CTIR.Gov e autoridades policiais;

VIII - disseminação de informações: divulgar, no âmbito da EBC, informações sobre ameaças à rede e respectivas soluções de contenção e prevenção; e

IX - pesquisa de informações: pesquisar sobre ameaças às redes computacionais, soluções de contenção e prevenção, novas atualizações dos *softwares* instalados na rede e a disseminação de informações relativas a ataques, tendências e medidas preventivas.

7. LEGISLAÇÃO DE REFERÊNCIA

I - Decreto nº 9.637, de 26 de dezembro de 2018 – Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional.

II - Decreto nº 10.222, de 5 de fevereiro de 2020 – Aprova a Estratégia Nacional de Segurança Cibernética.

III - Portaria nº 38, de 14 de agosto de 2009 – Homologa a 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.

IV - Portaria nº 57, de 23 de agosto de 2010 – Homologa a Norma Complementar nº 08/IN01/DSIC/GSIPR que estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais - Gestão de ETIR, nos órgãos e entidades da Administração Pública Federal.

V - Portaria nº 93, de 26 de setembro de 2019 – Aprova o Glossário de Segurança da Informação.

8. DISPOSIÇÕES GERAIS

8.1 Todas as ações realizadas pela ETIR/EBC devem ser documentadas e arquivadas para o acesso de gestores e técnicos envolvidos na investigação e tratamento de incidentes cibernéticos que comprometam a Segurança da Informação da EBC.

8.2 A ETIR/EBC manterá contato permanente com o Centro de Prevenção, Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal – CTIR.Gov, para alerta/notificação dos incidentes cibernéticos.