PROCEDIMENTO OPERACIONAL PADRÃO DE PREVENÇÃO, TRATAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS

– POP 705/01

SUMÁRIO

1. FINALIDADE 02
2. ÁREA GESTORA 02
3. CONCEITUAÇÃO 02
4. COMPETÊNCIAS 04
5. ATIVIDADES DA ETIR/EBC 04
6. LEGISLAÇÃO DE REFERÊNCIA 12
7. DISPOSIÇÕES GERAIS 12

1. FINALIDADE

1.1 Definir os procedimentos a serem adotados pela Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos em Redes Computacionais da Empresa Brasil de Comunicação S.A. – ETIR/EBC, no caso de incidentes cibernéticos que possam comprometer a rede e sistemas de informação dos usuários da 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 na EBC, 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 AUTORIDADE COMPETENTE DA EBC

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

3.4 CERT.BR

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil – CERT.Br é um Grupo de Resposta a Incidentes de Segurança – CSIRT de responsabilidade nacional do Comitê Gestor da Internet no Brasil.

3.5 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.

3.6 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.

3.7 GESTÃO DE INCIDENTES CIBERNÉTICOS

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

3.8 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.

3.9 CENTRO DE OPERAÇÕES DE REDE (NETWORK OPERATIONS CENTER – NOC)

Software que realiza o monitoramento e a gestão dos eventos de TI, atuando de forma preventiva e proativa com o objetivo de manter o ambiente de TI o mais estável possível.

3.10 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.

3.11 SEGURANÇA DA INFORMAÇÃO

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

3.12 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.

3.13 VULNERABILIDADE

Conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou uma organização, os quais podem ser evitados por uma ação interna de segurança da informação.

3.14 REDE VIRTUAL LOCAL (VIRTUAL LOCAL AREA NETWORK – VLAN)

Criação de rede virtual dentro de um único equipamento, compreende a segmentação de rede realizada de maneira virtual.

4. COMPETÊNCIAS

4.1 Compete aos membros da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos na Rede Computacional da EBC – ETIR/EBC:

I - analisar e monitorar incidentes de segurança da informação;

II - analisar, alertar/notificar e responder incidentes de rede;

III - acompanhar alertas/notificações 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;

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

V - classificar os incidentes detectados quanto ao nível de severidade e impacto;

VI - centralizar os pontos de contatos para alerta/notificação de incidentes;

VII - examinar todas as informações disponíveis sobre um incidente, incluindo artefatos e outras evidências relacionadas com o evento;

VIII - identificar o escopo do incidente, sua extensão, sua natureza e quais os prejuízos causados;

IX - propor estratégias de Contenção e Recuperação;

X - disseminar informações relativas a novos ataques e a tendências;

XI - divulgar estatísticas de incidentes alertados/notificados; e

XII - elaborar relatórios de incidentes de segurança e alertas/notificações e submeter ao COSIC.

5. ATIVIDADES DA ETIR/EBC

5.1 ATIVIDADE DE ALERTA/NOTIFICAÇÃO

5.1.1 O objetivo da atividade de Alerta/Notificação é assegurar que incidentes e eventos relacionados à segurança da informação sejam comunicados, permitindo a tomada de ação corretiva em tempo hábil e sejam relatados por meio de canais apropriados, o mais rápido possível.

5.1.2 Um membro da ETIR/EBC procederá a consolidação das informações e dos alertas/notificações ao agente responsável da Equipe ETIR/EBC.

5.1.3 Orientações para essa atividade:

I - todas as comunicações da ETIR devem ser transmitidas por meios seguros;

II - estabelecer procedimento de alerta/notificação formal (Central de Chamados; e-mail abuse@ebc.com.br; ou correspondências oficiais – Despachos e Ofícios) para relatar os incidentes de segurança da informação, juntamente com um procedimento de resposta a incidente, no qual estabeleça a ação a ser tomada ao receber o alerta/notificação; e

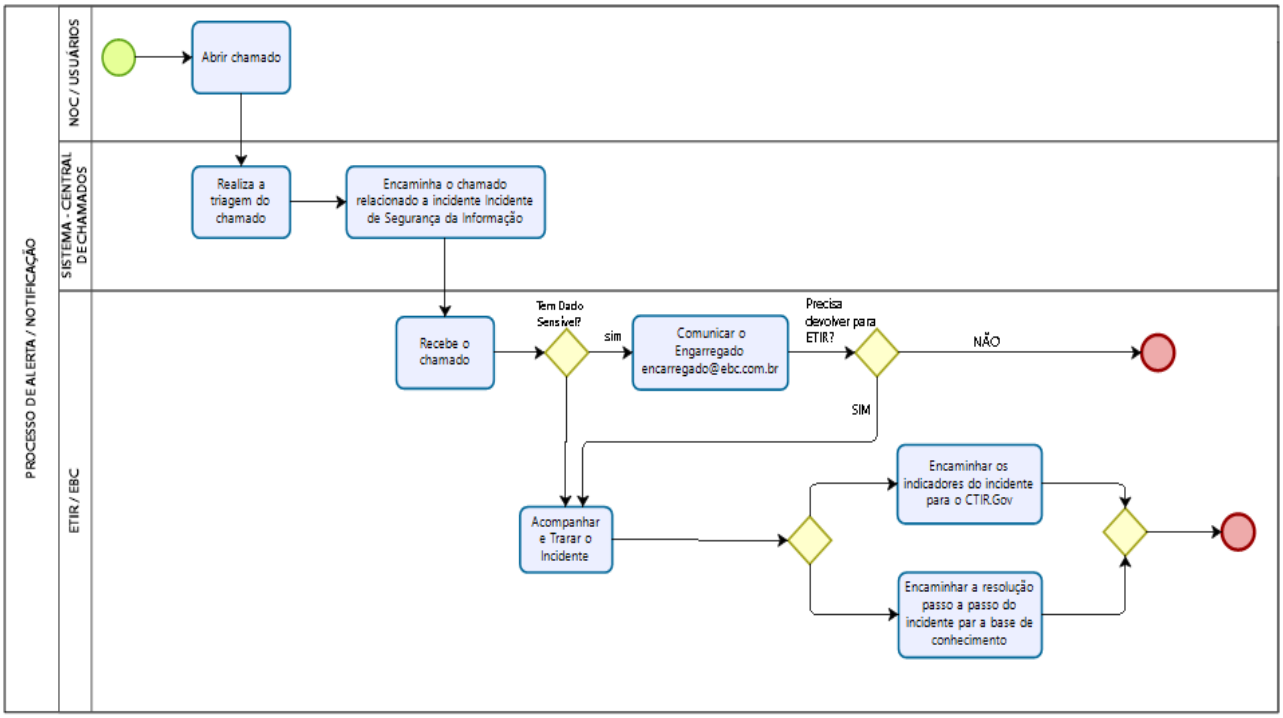
III - estabelecer ponto de contato para receber os alertas/notificações dos incidentes de segurança da informação. Este ponto de contato deverá ser do conhecimento de toda a Empresa e estar sempre disponível e em condições de assegurar uma resposta rápida e adequada.

5.1.4 PASSO A PASSO DO PROCESSO DE ALERTA/NOTIFICAÇÃO

5.1.4.1 O NOC ou os Usuários utilizam a Central de Chamados para abrir uma ocorrência.

5.1.4.2 O Sistema faz a triagem. Se o chamado for relacionado a incidentes de segurança da informação, ele será encaminhado para a ETIR/EBC, que a partir desse momento será responsável pelo acompanhamento do incidente (inclusive encaminhando os indicadores para o CTIR.Gov). Há o recebimento de *e-mails* (abuse@ebc.com.br) pela ETIR/EBC.

5.1.4.3 Caso a ETIR/EBC identifique incidentes de segurança da informação relativos a dados pessoais e sensíveis no âmbito da EBC, deverá comunicar ao Encarregado de Dados imediatamente para que ele proceda com a análise do incidente e o possível encaminhamento à Autoridade Nacional de Proteção de Dados – ANPD.

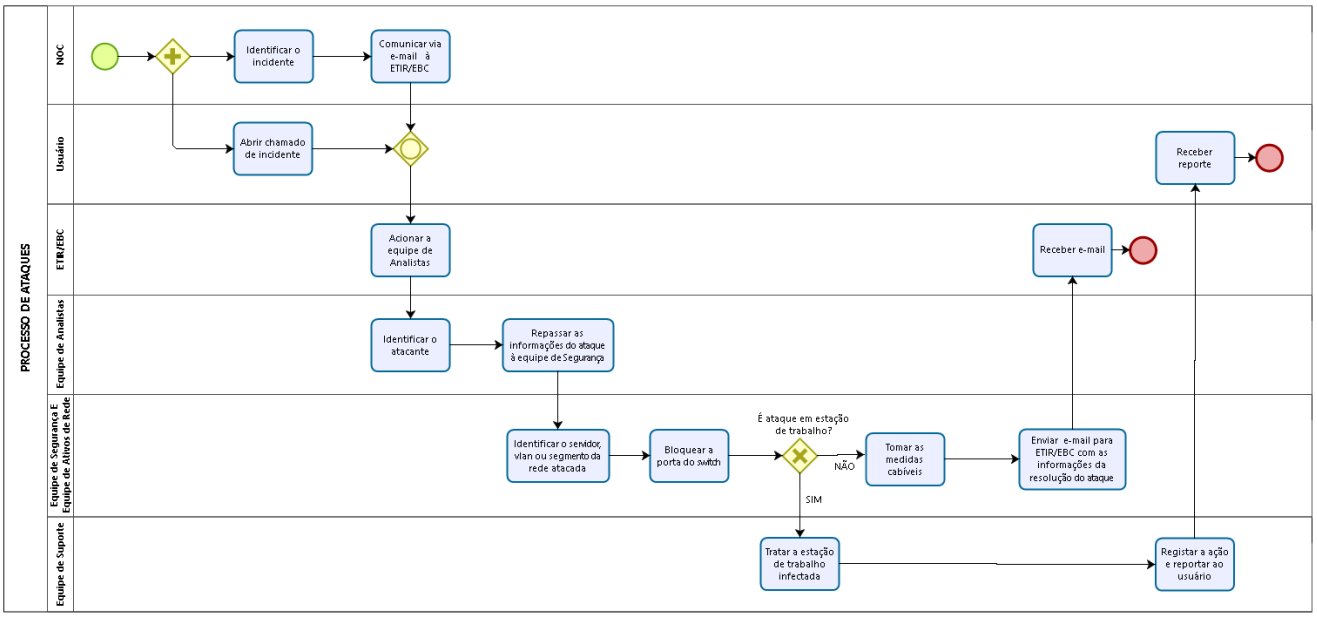


5.1.5 PASSO A PASSO DO PROCESSO DE ATAQUES

5.1.5.1 O NOC identifica um incidente de segurança e comunica diretamente à ETIR/EBC por meio do e-mail abuse@ebc.com.br.

5.1.5.2 Usuário utiliza a Central de Chamados na classificação de incidentes de segurança da informação, quando o usuário faz a abertura do chamado diretamente na classificação de incidentes de segurança da informação, este segue direto para a ETIR/EBC, que acionará a equipe de Analistas; esta equipe identifica o atacante e repassa as informações para a Equipe de Segurança, que juntamente com a Equipe de Ativos de Rede, identificam o servidor, vlan ou segmento da rede sendo atacada.

5.1.5.3 Bloquear a porta do *switch*. Em seguida, verificar se o incidente foi contido, caso contrário, deve-se acionar a Equipe de Suporte para tratar a estação infectada em caso de ataque à estação ou ao servidor**;** ou acionar a Equipe de Ativos ou Segurança para tomar as medidas cabíveis (que pode ser acionar o fabricante do antivírus, *antispam* ou *firewall*).

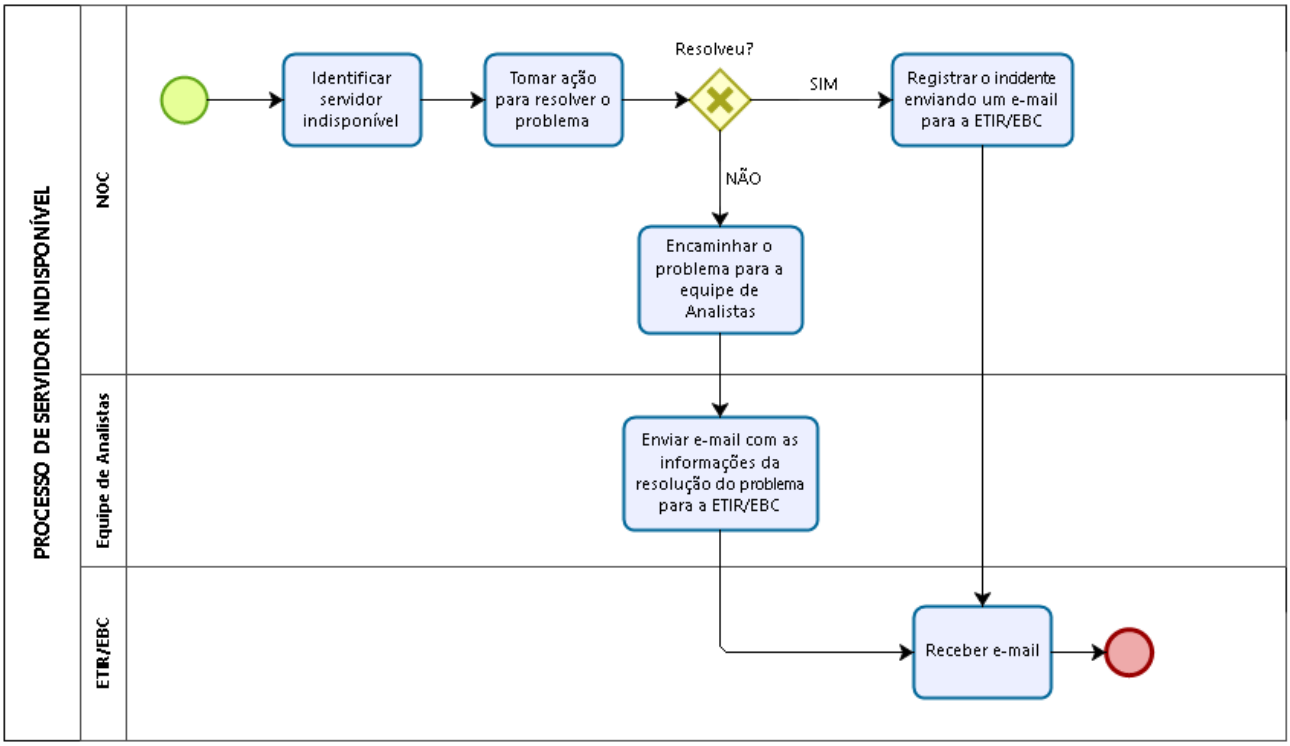


5.1.6 PASSO A PASSO DO PROCESSO DE SERVIDOR INDISPONÍVEL

5.1.6.1 Servidor é identificado indisponível pelo NOC, que comunica a ETIR/EBC. O NOC toma a ação.

5.1.6.2 Se o NOC resolver o problema, registra o incidente enviando um *e-mail* para a ETIR/EBC.

5.1.6.3 Caso não resolva o problema, o NOC deve encaminhar o problema para a equipe de Analistas que, após solucionado, comunica por *e-mail* à ETIR/EBC com o passo a passo da resolução.



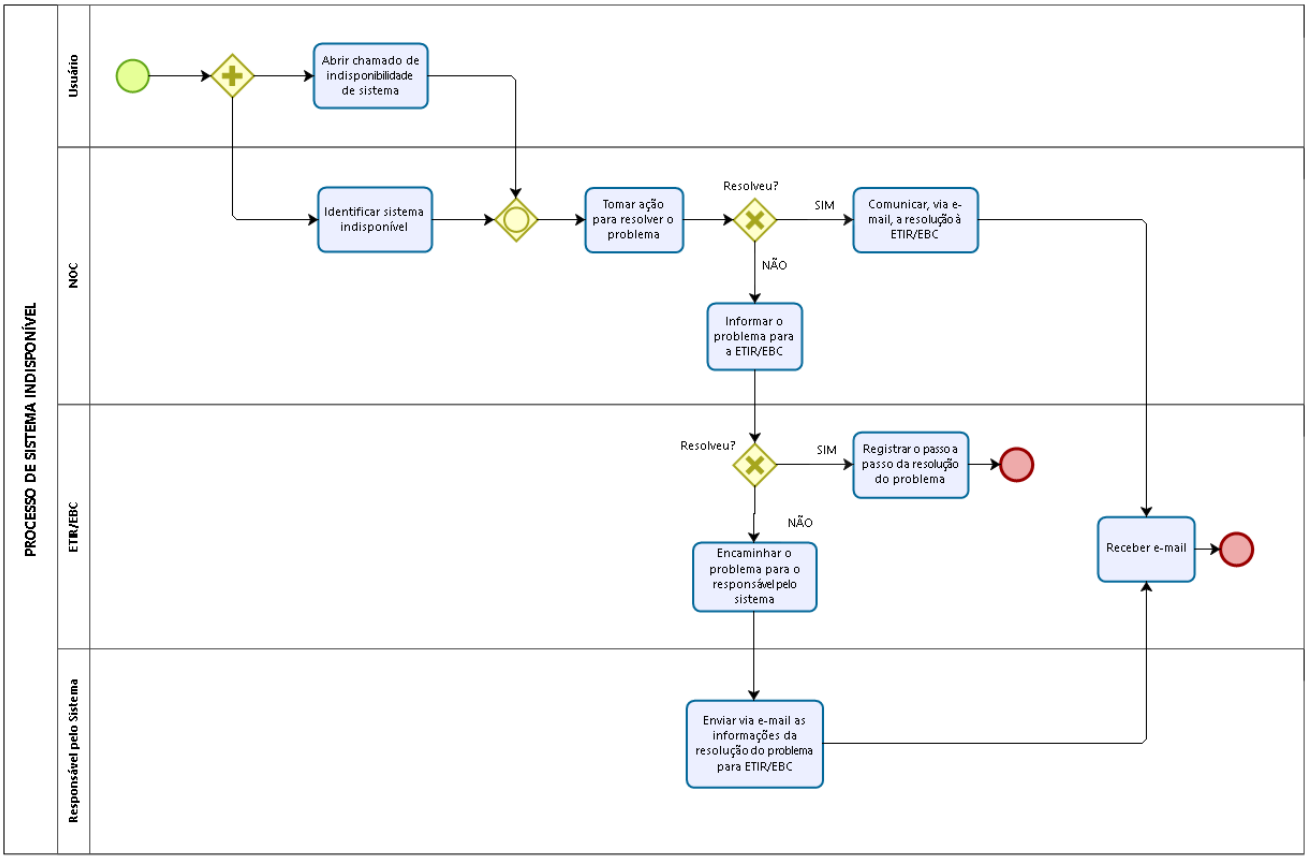
5.1.7 PASSO A PASSO DO PROCESSO DE SISTEMA INDISPONIVEL

5.1.7.1 O Usuário, via Central de Chamados, ou o NOC identifica a indisponibilidade do Sistema.

5.1.7.2 Se o NOC resolver, comunica à ETIR/EBC. Caso não consiga, informa para a ETIR/EBC.

5.1.7.3 Persistindo o problema, a ETIR/EBC encaminha para o responsável pelo Sistema.

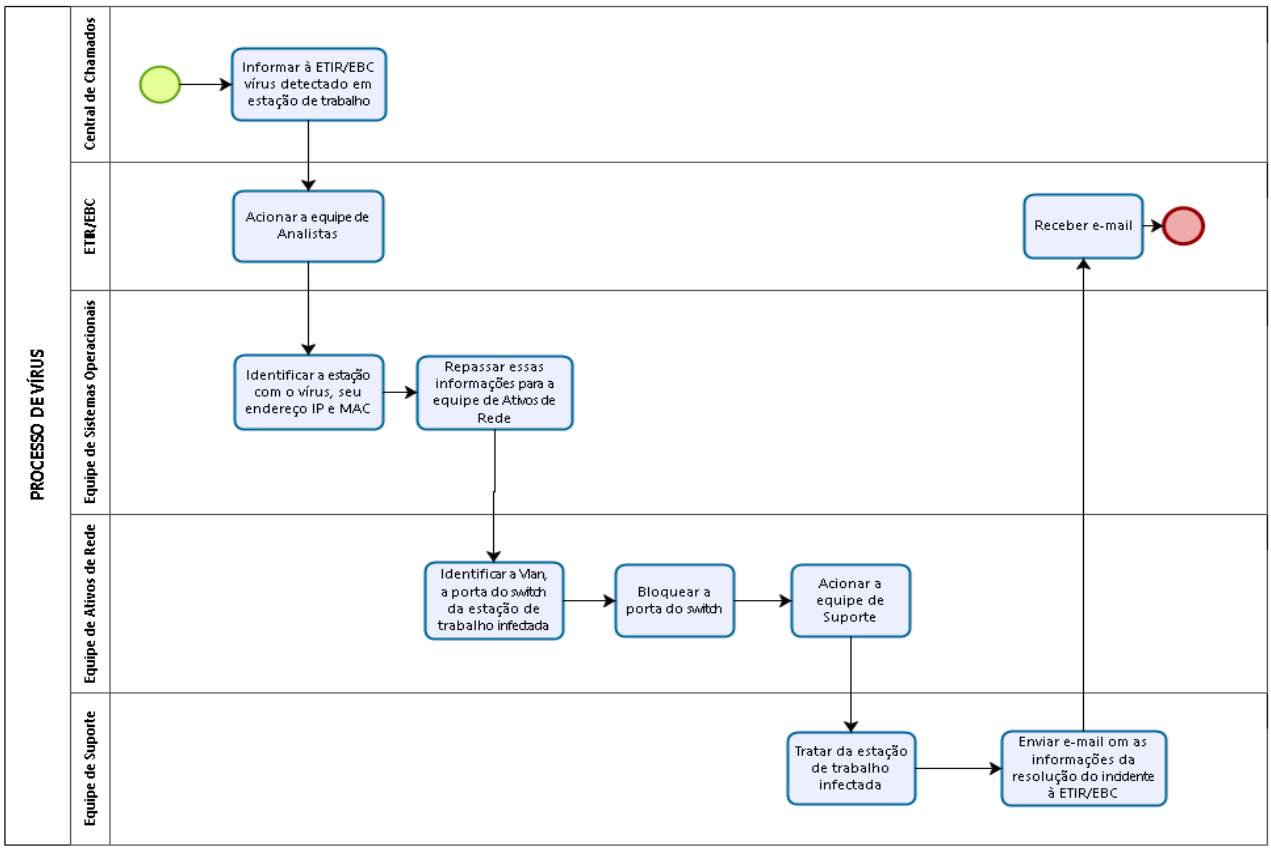
5.1.7.4 Resolvido o incidente, informar por *e-mail* à ETIR/EBC.



5.1.8 PASSO A PASSO DO PROCESSO DE VÍRUS

5.1.8.1 Vírus detectado em uma estação da EBC, a ETIR/EBC aciona o membro da equipe especialista no assunto

5.1.8.2 A Equipe de Sistemas Operacionais identifica a estação com o Vírus, seu endereço IP e MAC, e repassa as informações para a Equipe de Ativos de Rede, que identifica a vlan, a porta do *switch* da estação e toma a 1ª ação, que é bloquear a porta do *switch*. Em seguida, aciona a Equipe de Suporte para tratar da estação infectada e informa por *e-mail* à ETIR/EBC.

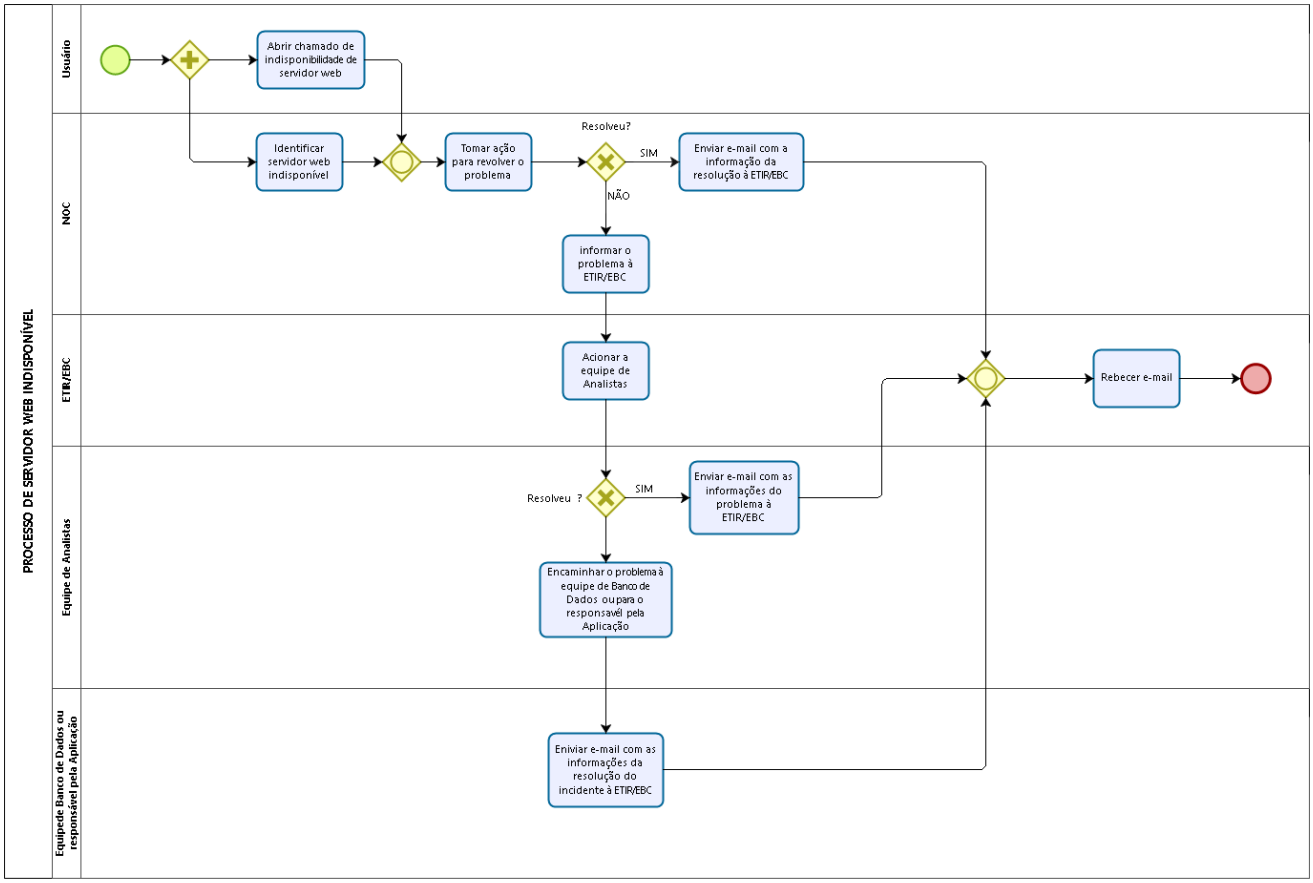


5.1.9 PASSO A PASSO DO PROCESSO DE SERVIDOR *WEB* INDISPONÍVEL

5.1.9.1 O Usuário, via Central de Chamados, ou o NOC identifica o servidor *web* indisponível.

5.1.9.2 Após revolver a indisponibilidade do servidor WEB o NOC comunicará à ETIR/EBC. Caso não consiga, encaminha para a ETIR/EBC que aciona aos analistas da ETIR.

5.1.9.3 Persistindo o problema, a equipe de Analistas encaminha para a Equipe de Banco de Dados ou para o responsável pela Aplicação. Resolvido o incidente, informar por *e-mail* à ETIR/EBC.



5.2 ATIVIDADE DE REGISTRO

5.2.1 Todos os detalhes relacionados a um incidente de segurança devem ser registrados em *software* específico, por membro da ETIR/EBC. O registro adequado dos incidentes fornecerá informações necessárias para o responsável pelo atendimento e para todos os envolvidos à medida que desvendar o curso dos eventos.

5.2.2 A atividade de Registro ajudará a realizar análise final do dano causado pelo incidente e também fornecerá a base para as fases subsequentes de condução do processo: Erradicação, Recuperação e Monitoramento.

5.2.3 Orientações para essa atividade:

I - registrar todas as ações que envolvam a ETIR/EBC;

II - criar uma Base de Conhecimento para o registro de todos os incidentes e de todas as ações tomadas para solucionar tais incidentes; e

III - registrar todas as tratativas externas (inclusive a pessoa com a qual houve o contato telefônico, a data, a hora e o conteúdo da conversa).

5.2.4 A ETIR/EBC terá acesso aos arquivos de registros de atividades (*logs*), além de evidências coletadas por outras equipes, de forma a realizar análise e encaminhamento de investigação do incidente de segurança.

5.3 ATIVIDADE DE CONTENÇÃO

5.3.1 O propósito da atividade de Contenção é limitar a extensão de um ataque. Uma parte essencial da contenção é a tomada de decisão.

5.3.2 A EBC deve definir riscos aceitáveis (definidos pela Análise de Riscos) em lidar com um incidente, e também deve prescrever ações específicas e estratégicas consequentes. Na ausência de procedimentos predefinidos, a pessoa encarregada do incidente não possuirá o poder para tomar difíceis decisões gerenciais.

5.3.3 Ao final da Contenção deverá ocorrer o alerta/notificação do incidente às autoridades competentes.

5.4 ATIVIDADE DE ERRADICAÇÃO

5.4.1 Após o incidente contido a causa dever ser erradicada e as evidências coletadas no sistema comprometido.

5.5 ATIVIDADE DE RECUPERAÇÃO

5.5.1 Uma vez que a causa do incidente foi erradicada, a próxima etapa se refere à atividade de Recuperação.

5.5.2 O objetivo da atividade de Recuperação é retornar o sistema à sua normalidade. Restaurar os serviços na ordem de suas demandas para trazer o mínimo de inconveniência aos usuários.

5.6 ATIVIDADE DE MONITORAMENTO

5.6.1 Após a restauração do sistema, a atividade de monitoramento deve ser realizada para verificação de vulnerabilidades.

5.6.2 Após um incidente, deverá ser elaborado relatório de acompanhamento contendo a sequência dos eventos: o método de descoberta; o procedimento de correção; o procedimento de monitoramento; e o resumo de lições aprendidas.

5.6.2.1 Além disso, deve conter estimativa monetária dos danos causados pelo incidente. Essa estimativa deve incluir custos associados a perda de *software* e arquivos.

5.6.3 Em casos de incidentes e suas recorrências, identificados pela atividade de Monitoramento, a ETIR/EBC encaminhará as análises das ocorrências aos responsáveis pelas áreas afetadas juntamente com uma proposta de tratamento adequado.

6. 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.

7. DISPOSIÇÕES GERAIS

7.1 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.

7.2 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.