NORMATIVA DE RESPOSTA A INCIDENTES

SUMÁRIO:

RESPONSÁVEL E APROVADORES:

Área Responsável	Governança CTIO
Aprovadores	Infraestrutura e Segurança de TI, NOC, Site Management

1. OBJETIVO

Este documento tem por objetivo estabelecer o processo de tratamento de incidentes de segurança cibernética no âmbito da FiBrasil, com intuito de:

i. Mitigar danos causados por incidentes que não puderem ser evitados e a sua reincidência;
ii. Reduzir o número de ocorrência de incidentes de segurança, por meio de ações preditivas de eventos e corretiva de causas que permitam a ocorrência;
iii. Estabelecer diretrizes para a identificação de incidentes que possam comprometer a operação, confidencialidade, integridade e disponibilidade da rede e dos dados.

2. APLICABILIDADE

Aplica-se aos empregados, clientes e fornecedores da FIBRASIL.

3. ACRÔNICOS E ABREVIATURAS

As siglas e acrônimos aqui utilizados seguem a Portaria Número 93, de 26 de setembro de 2019 (Glossário de Segurança da Informação).

4. INCIDENTES DE SEGURANÇA CIBERNÉTICA

São considerados incidentes de segurança cibernética todos os incidentes, confirmados ou sob suspeita, que envolvam os ativos informatizados, como servidores, roteadores, aplicações, estações de trabalho etc. da FiBrasil, tais como:

i. Violação das normativas de segurança da informação;
ii. Dispositivos que estejam conectados à rede da FiBrasil que estejam contaminados com malware;
iii. Conexão de dispositivos não autorizados;
iv. Utilização de credenciais de autenticação por indivíduo não proprietário;
v. Atividades maliciosas por detecção automática ou manual, envolvendo dispositivos identificados por grupos como fonte de atividades maliciosas;
vi. Ausência de comunicação de fragilidade de segurança conhecida em processo ou sistema de TI;
vii. Tentativas de fraude, independentes se causam ou não danos;
viii. Todas as situações que possam colocar em risco os dados pessoais de indivíduos que se relacionam com a FiBrasil, sejam realizados por fatores internos ou externos à companhia.

5. PROCEDIMENTOS

Em caso de incidentes de segurança cibernética, os procedimentos descritos abaixo devem ser seguidos pelo colaborador que o identificar:

5.1. NOTIFICAÇÃO DO INCIDENTE

O empregado, cliente ou fornecedor da FIBRASILque identificar qualquer incidente, suspeito ou confirmado, seja interno ou externo, deverá realizar a notificação imediatamente ao incidentes@fibrasil.com.br ou no portal de *helpdesk* https://helpdesk.fibrasil.com.br, a partir da identificação do evento, relatando o ocorrido detalhadamente com as informações a seguir:

i. Contato: Dados do indivíduo que identificou o incidente, tais como nome, telefone e e-mail.
ii. Origem do Incidente: Unidade, setor, organização a qual pertence o dispositivo (estações de trabalho, roteadores, aparelhos celulares etc.) ou processo que originou o incidente, informando também, quando disponível, endereço IP, protocolos, portas, aplicações e sistemas.
iii. Quando ocorreu: Data e horário (hh mm ss Fuso Horário) da identificação do incidente.
iv. Impactados: Serviços afetados e/ou alvos do incidente.
v. Descrição: Tipo de incidente, provável motivação.
vi. Evidências: Quando disponível e sempre que possível, anexar imagens, códigos de erros e/ou outros registros que possam evidenciar o incidente.

5.2. IDENTIFICAÇÃO DO INCIDENTE

A notificação feita pelos canais indicados acima será analisada previamente pelo SOC para identificar o correto direcionamento do incidente. O SOC comunicará imediatamente o Jurídico, para devidas comunicações às autoridades administrativas, quando se tratar de incidentes envolvendo dados pessoais ou alguma das situações previstas na Resolução nº 740/2020 da ANATEL e seus Despachos Decisórios[1]. O SOC poderá solicitar ao notificante informações complementares referentes ao incidente relatado.

5.3. INVESTIGAÇÕES E CLASSIFICAÇÃO

Caberá ao SOC realizar uma investigação e classificará o incidente conforme a seguir:

i. Tipo de Incidente:
   a) Vazamento de dados

[1] Segundo a ANATEL, são considerados como incidentes relevantes os seguintes casos:

a. Vazamentos de dados (dados corporativos ou de clientes);
b. Ransomwares bem-sucedidos;
c. Comprometimentos decorrentes de Ameaças Persistentes Avançadas (*Advanced Persistent Threat - APT*);
d. Ataques de Negação de Serviço, considerando os seguintes parâmetros de tráfego e de quantidade de pacotes por segundo: igual ou superior a 50Gbps ou a 20Mpps;
e. Problemas de roteamento (sequestro de prefixos, vazamento de rotas e/ou erros de configuração) que venham a ocasionar impacto na entrega de serviços aos clientes das prestadoras, órgãos ou entidades que operam na Internet; e
f. Indisponibilidade de serviço causada por incidente de segurança cibernética.

b) Exfiltração
c) Conteúdo abusivo
d) Código malicioso
e) Tentativa de intrusão
f) Intrusão
g) Indisponibilidade de serviço ou informação
h) Segurança da informação
i) Fraude
j) Outros

ii. Criticidade do incidente:

a) Alta: Incidente impacta sistemas críticos ou dados sensíveis que possam impactar negativamente a FiBrasil.
b) Média: Incidente impacta sistemas ou dados não sensíveis, sem potencial de impacto negativo a FiBrasil.
c) Baixa: Incidentes não impacta sistemas críticos.

6. PROCESSOS PARA O TRATAMENTO DE INCIDENTES

O diagrama abaixo representa as etapas de resposta a incidentes que serão coordenadas pela área de Governança:

6.1. PREPARAÇÃO

Consiste em identificar, prever e descrever possíveis situações de violação de dados, bem como, as respectivas ações que deverão ser realizadas, tais como: prazos e formas de registro.

i. Implementar mecanismos de defesa e controle de ameaças.
ii. Desenvolver procedimentos para lidar com incidentes de forma eficiente;
iii. Definição da área que deverá ser informada em situação de ocorrência do sinistro e como reportar;
iv. Detalhamento e ações necessárias que devem escalonar a criticidade do evento.

6.2. IDENTIFICAÇÃO

i. Identificar todos os sistemas e serviços afetados;
ii. Avaliar o impacto do incidente e os potenciais riscos (dados vazados, impacto na organização e na reputação);
iii. Identificar a existência de outros eventos;
iv. Identificar que modalidade de informação e processos foram afetados;
v. Identificação dos responsáveis;
vi. Comunicar o Jurídico, caso seja um incidente envolvendo dados pessoais ou alguma das situações previstas na Resolução nº 740/2020 da ANATEL e seus Despachos Decisórios[2], para que seja feita a comunicação às autoridades competentes.

6.3. MITIGAÇÃO

Realizar a contenção do incidente de forma a atenuar os danos e evitar que demais dados sejam comprometidos:

i. Desconectar o sistema comprometido ou isolá-lo;
ii. Desativação do sistema para evitar quaisquer perdas;
iii. Bloquear padrões de tráfego, interrompendo os fluxos maliciosos;
iv. Desabilitar quaisquer serviços vulneráveis, inibindo comprometimento de outros sistemas;

6.4. ERRADICAÇÃO

Erradicação das causas do incidente, removendo os eventos relacionados, de forma a operarem em sua normalidade:

i. Garantir que as causas do incidente foram removidas, assim como todas as atividades e arquivos associados ao incidente;
ii. Assegurar a remoção de todos os métodos de acesso utilizados.

6.5. RECUPERAÇÃO

Recuperação do sistema ao estado normal:

[2] Vazamentos de dados (dados corporativos ou de clientes); *Ransomwares* bem-sucedidos; Comprometimentos decorrentes de Ameaças Persistentes Avançadas (*Advanced Persistent Threat - APT*); Ataques de Negação de Serviço, considerando os seguintes parâmetros de tráfego e de quantidade de pacotes por segundo: igual ou superior a 50Gbps ou a 20Mpps; Problemas de roteamento (sequestro de prefixos, vazamento de rotas e/ou erros de configuração) que venham a ocasionar impacto na entrega de serviços aos clientes das prestadoras, órgãos ou entidades que operam na Internet; Indisponibilidade de serviço causada por incidente de segurança cibernética.

i. Recuperação da integridade do sistema;
ii. Garantir que o sistema foi recuperado de forma correta e que as funcionalidades estejam integradas;
iii. Implementar medidas de segurança para evitar novos comprometimentos;
iv. Restaurar o *backup* completo e armazenado.

6.6. ATIVIDADES PÓS-INCIDENTE

Documentação de todo o processo e ações realizadas para atendimento de demandas regulatórias, auditorias e/ou treinamentos.

Quando se tratar de um dos casos de comunicação a autoridades administrativas, o Jurídico deverá receber essa documentação, em até 55 dias após identificado o incidente, para que sejam cumpridas as obrigações legais.

6.7. LIÇÕES APRENDIDAS

Avaliação do processo e verificação da eficácia das soluções realizadas. Análise das falhas de detecção e recursos inexistentes ou insuficientes, para que sejam sanados.

Discussão com as áreas envolvidas sobre os erros e dificuldades enfrentados na mitigação do ocorrido, propondo melhorias técnicas e nos processos.

7. OBSERVAÇÕES

Quaisquer comentários, sugestões, críticas, contribuições ou informações relacionadas com a presente publicação, deverão ser dirigidas ao Comitê de Segurança da FiBrasil.

8. COMPOSIÇÃO DO COMITÊ DE SEGURANÇA DA FIBRASIL

O Comitê de Segurança da Fibrasil será composto por um representante de cada uma das seguintes áreas: Gerência de Operações, Gerência *Site Management* e Gerência de Infraestrutura e Segurança de TI. A indicação deverá ser aprovada em Reunião de Diretoria.

9. APROVAÇÃO

Esse documento foi aprovado pelas áreas de Infraestrutura e Segurança de TI, NOC – Operações e Site Management – Engenharia em 06/02/23 e entra em vigor nessa data.

10. DOCUMENTOS RELACIONADOS

- Normativa de Segurança Cibernética
- Normativa de Segurança da Informação FiBrasil
- Normativa de Análise de Vulnerabilidades
- Normativa de Proteção de Dados Pessoais
- Diretrizes e Bases Rede IP – FiBrasil
- Diretrizes e Bases Segurança – FiBrasil
- Normativa de Segurança de Elementos de Rede – FiBrasil
- Framework CIS Controls V8
- Lei Nº 13.709/2018 – Lei Geral de Proteção de Dados
- Lei nº 12.965/2014 (Marco Civil da Internet) e o Decreto nº 8.771/2016;
- Resolução nº 740/2020 da Anatel (Regulamento de Segurança Cibernética) e demais normas que dispõem sobre o tema.

11. VIGÊNCIA

A presente normativa terá validade a partir da data de sua aprovação e permanecerá em vigor até sua expressa revogação.