

**Análise de Ambiente Cibernético**

**NIST CSF 2.0**

**Proposta de Melhoria e Implementação de**

**Política de Segurança Cibernética**

I. **Introdução**

Este relatório visa apresentar uma análise das estratégias para gerenciamento de crise nunca ocorrida anteriormente, sobre a qual não há qualquer literatura ou experiência a que se possa comparar, e que afetou a empresa de modo a impedir o acesso físico e tecnológico do local, e ainda, o comprometimento de uma antena sequestrada por forças criminosas impedindo o fornecimento de sinal de intenet e telefonia celular e fixa.

Dada a compressão de tempo a que se enfrenta a crises, foram validadas neste relatório itens de segurança em caráter de urgência, tratando-se portanto de um trabalho que será complementado em tempo breve.

Dada a origem sem precedentes, o incidente será tratado como decorrente de falha nos processos de segurança publica originarios do local onde está instalado fisicamente.

As referências utilizadas neste estudo, foram criadas para gerencia de risco em infraestrutura crítica e são aplicadas internacionalmente, vindo a tratar-se do NIST CSF, na sua versão 2.0, cuja governança é item alvo para a analise da tomada de decisão da diretoria.

O incidente em questão envolve a interferência criminosa em uma antena de propriedade da empresa, acarretando a interrupção dos serviços de telecomunicações e exigências financeiras por parte dos perpetradores.

O framework apresenta seis funções: (1) Governar, (2) Identificar; (3) Proteger; (4) Detectar; (5) Responder; (6) Recuperar.

Dada a urgência, itens satélites ao caso serão aplicados em segundo momento, tratando-se portanto no presente estudo das funções e categorias urgentes a resolução do problema, e intenção de reestabelecimento de sinal, além de resgate da reputação da empresa.

**II - Da classificação da notícia e posicionamento no Framework**

Foram avaliadas as questões de segurança física e tecnológica do local, de modo a posicionar a maturidade frente ao cenário estabelecido, considerando que não há análise de risco anterior para a anormalidade enfrentada, classificados na seguinte conformidade:

• **Nível 1 –** Quando há o conhecimento dos riscos, mas não há documentação dos processos e atividades de segurança, não há formalização ou os processos de mitigação são implementados de maneira irregular;

• **Nível 2** – Há o conhecimento dos riscos e o processo de mitigação foi desenvolvido e aprovado, mas pode ser ou não implementado, e quando há implementação, esta é realizada irregular e informalmente;

• **Nível 3** – Há o conhecimento dos riscos, houve o desenvolvimento dos processos de mitigação, os quais foram formalizados, devidamente implantados e sofrem atualizações por funcionários devidamente capacitados;

• **Nível 4** – Há o conhecimento dos riscos, desenvolveram-se os processos de mitigação, os quais foram formalizados, devidamente implantados e sofrem atualizações com base em práticas avançadas de cibersegurança e são monitorados por executivos seniores, sofrendo atualizações regulares e inserções de melhorias, otimização do processo.

É pertinente salientar que para o cálculo de risco específico de que trata o presente documento, consideramos classificar em “0” o nível atual, uma vez que não há registro ou qualquer projeto em nível global que atenda de imediato as necessidades da presente crise.

**III - Do Contexto atual da situação:**

**O** sequestro das antenas ocorreu pela manhã de 01/05/21, afetando, segundo operadoras, 26 antenas que já estão sob o controle dos criminosos, impactando 158 mil pessoas em 72 bairros na capital e em mais 3 cidades da Região Metropolitana: São Gonçalo, Niterói e Itaboraí.

Em resposta a falta do serviço, foi adotada medida de urgência para informar os usuários de serviços de telefonia fixa e móvel além de internet a seguinte mensagem:

***“em função da segurança pública não é possível restabelecer o sistema uma vez que seus profissionais sofrem ameaças de morte com relação à prestação dos serviços feita por bandidos do local"***

A seguir, mapa de antenas comprometidas por região no Estado do Rio de Janeiro, Brasil.

**https://g1.globo.com/rj/rio-de-janeiro/noticia/2021/05/01/faccoes-criminosas-sequestram-antenas-de-telefonia-e-internet-no-rj.ghtml**

**IV – Da Aplicação do NIST CSF – para a operação de retomada das antenas e sinais de serviço após o estabelecimento da crise.**

Dentre as categorias e subcategorias foram eleitas as que são atinentes aos fatos ocorridos de modo a serem aplicadas em caráter de urgência, vindo as demais serem alvo de estudo em momento futuro.

O Framework elenca função, categoria, posicionamento de risco e plano de ação para retomada do serviço e justificativa para a ação, cujo custo ainda não foi avaliado em detalhes, contudo, pode-se prever valores acima de $ 500 mil dolares.

**V-Da Aplicação Imediata das medidas de Urgência:**

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Descrição da subcategoria** | **Justificativa** | **Ações** |
| GV.OC-01 : | A missão organizacional é compreendida e informa o gerenciamento de riscos de segurança cibernética (anteriormente ID.BE-02, ID.BE-03) | A missão é compreendida mas os riscos cibernéticos referentes ao caso em estudo não eram dimensionados pela gestão.  **Onde estamos: NÍVEL 1**  **Onde devemos chegar: NÍVEL 3** | Desenvolver política de segurança cibernética específica para as antenas. |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Descrição da subcategoria** | **Justificativa** | **Ações** |
| **ID.AM1** | Dispositivos físicos e sistemas devem ser inventariados. | O inventário ocorre a cada ano, contudo os documentos não foram localizados pela área patrimonial  **Onde estamos: NÍVEL 1**  **Onde devemos chegar: NÍVEL 3** | Fixar o controle do inventário com o facilities  Determinar o responsável e para quem será atribuida visibilidade e controle  Organizar os bens de todas as antenas em uso no estado do RJ. |
| **ID.AM5** | Recursos (por exemplo, hardware, dispositivos, dados, tempo, pessoal e software) são priorizados com base em sua classificação, criticidade e valor comercial | O capital foi atribuido com base no valor de compra, contudo não foram localizados registros, nem responsáveis.  **Onde estamos: NÍVEL 1**  **Onde devemos chegar: NÍVEL 3** | Atribuição de valores parq o calculo de perdas diárias, com base no valor de compra, depreciação e capacidade de cobertura na área de instalação. |

**VI-Da Aplicação Imediata das medidas de Urgência:**

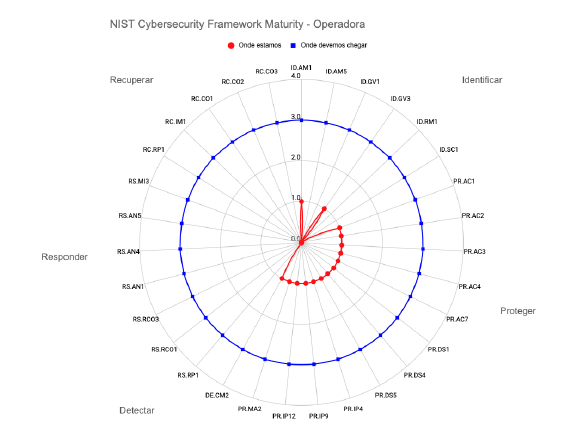
|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Descrição da subcategoria** | **Justificativa** | **Ações** |
| **PR.AA-01**  **(PR AC-01)** | **Identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados.** | **Ausência de credenciais de acesso ao ambiente bem como cadastro de usuários autorizados.**  **Onde estamos: NÍVEL 1**  **Onde devemos chegar: NÍVEL 3** | Instalação de controle de acesso no local com identificação biométrica |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Descrição da subcategoria** | **Justificativa** | **Ações** |
| **DE.CM-1** | rede é monitorada para detectar potenciais eventos de cibersegurança | Não há monitoramento dos sistemas ativos nas antenas.  **Onde estamos: NÍVEL 1**  **Onde devemos chegar: NÍVEL 3** | Implantação imediata de solucão IDS E IPS para detecção de suspeitas. |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Descrição da subcategoria** | **Justificativa** | **Ações** |
| RS.CO-2: | Os incidentes são relatados de acordo com os critérios estabelecidos | Existe politica de relatos para incidentes, contudo, o cenário apresentado neste evento não tem referêncial.  **Onde estamos: NÍVEL 1**  **Onde devemos chegar: NÍVEL 3** | Estrutura de novo plano de ação em caso de incidente envolvendo antenas e template específico. |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Descrição da subcategoria** | **Justificativa** | **Ações** |
| RC.RP-1 | O plano de recuperação é executado durante ou após um incidente de segurança cibernética | O plano de recuperação foi desenhado especificamente para este evento, não tendo sido registrado evento anterior para medição.  **Onde estamos: NÍVEL 1**  **Onde devemos chegar: NÍVEL 3** | Reestabelecimento do fornecimento do sinal com antenas próximas que possam suprir a demanda, e instalação de novas antenas em locais estratégicos. |

**VI - Da Análise de Maturidade da situação atual do incidente:**



**VII – Do Plano de Ação e Prazos estabelecidos**

|  |  |
| --- | --- |
| **Ação** | **Prazo** |
| Realização de Inventário | 5 Dias |
| Análise de Risco específica para antenas | 2 Dias |
| Missão com disseminação para terceiros | 1 Dia |
|  |  |

**VIII – Do Cronograma**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **AÇÃO** | **MESES** | | | | | |
|  | **maio** | **maio** | **maio** | **maio** | **maio** |  |
| **Reformulação do inventário** | **06** | **07** | **08** | **09** | **10** |  |
| **Análise de Risco** |  |  |  |  |  |  |

**IX – Dos Investimentos**

|  |  |
| --- | --- |
| Ação | **Investimento** |
| Reforma Instalação física |  |
| Controles de Acesso |  |
| Tecnologia Protetora |  |
| Tecnologia de controle de acesso Monitoramento |  |
|  |  |

**X - Considerações Finais**

O objetivo do presente estudo é trazer solução para o crime que se consolidou frente a 26 antenas do Rio de Janeiro, e que, causam impedimento de acesso além de impactar 150 mil moradores e comerciantes, além de postos polciais, unidades médicas, entre outros serviços essenciais que dependem do serviço.

Além das analises em curso, existe a possibilidade de abandono das antenas visto a dificuldade de acessar a área fisica e virtualmente.

Desse modo, esclarecemos que é viável intervenção juridica para ações junto a forças de lei, bem como ciência ao Ministério Publico, uma vez que as autoridades já foram informadas sobre o ocorrido, que por suas vez, aconteceu em massa (organizadamente).