MINISTÉRIO DA INTEGRAÇÃO E DO DESENVOLVIMENTO REGIONAL
DEPARTAMENTO NACIONAL DE OBRAS CONTRA AS SECAS

PORTARIA Nº 197 DG, DE 04 DE JULHO DE 2025

Ministério da Integração e do Desenvolvimento Regional - MDR
Departamento Nacional de Obras Contra as Secas – DNOCS
Comitê de Governança Digital - CGD

Institui a Política de Defesas contra Malware do Departamento Nacional de Obras Contra as Secas – DNOCS.

O DIRETOR-GERAL DO DEPARTAMENTO NACIONAL DE OBRAS CONTRA AS SECAS – DNOCS, no uso das atribuições legais que lhe confere o disposto no Art. 68 e respectivo inciso XII da Portaria DNOCS/DG/GAB nº 43, de 31 de janeiro de 2017, em atendimento à Estratégia Federal de Governo Digital e à Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020;

R E S O L V E:

Art. 1º Aprovar a Política de Defesas contra Malware do Departamento Nacional de Obras Contra as Secas – DNOCS, na forma do Anexo I desta Portaria, de observância obrigatória no âmbito dessa Autarquia Federal.

Art. 2º Esta Portaria entra em vigor em 29 de Agosto de 2025

Fernando Marcondes de Araújo Leão
Diretor-Geral do DNOCS

Documento assinado eletronicamente por **Fernando Marcondes de Araújo Leão**, **Diretor Geral**, em 04/07/2025, às 14:13, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

ANEXO I

POLÍTICA DE DEFESAS CONTRA MALWARE

CAPÍTULO I
DOS PRINCÍPIOS GERAIS

Art. 1º. A Política de Defesas contra Malware (PDM) deve estar alinhada com à Política de Segurança da Informação do DNOCS.

Art. 2º. A PDM deve estar alinhada com uma gestão de continuidade de negócios em nível organizacional.

Art. 3º. Esta política apresenta um conjunto de diretrizes para lidar com os incidentes e eventos de malware que porventura possam ocorrer no âmbito institucional. Contudo, isso não anula a necessidade de tratar especificidades de cada tipo. A depender do tipo de malware, pode-se considerar procedimentos diferentes para lidar com incidentes de cada categoria.

Art. 4º. O DNOCS deve implementar políticas que abordam prevenção contra malware.

Art. 5º. O DNOCS deve empenhar-se em detectar e validar ameaças de malware rapidamente para minimizar o número de ativos de informação expostos e a quantidade de danos que possa vir a sofrer.

Art. 6º. A PDM deve ser revisada e atualizada regularmente tanto para refletir as mudanças das ameaças e novas tecnologias quanto para garantir que esteja em conformidade com normas e regulamentações vigentes.

Art. 7º. A eficácia e efetividade da PDM devem ser avaliadas continuamente por meio de auditorias e análise de eventuais incidentes.

CAPÍTULO II
PAPÉIS E RESPONSABILIDADES

Art. 8º. Cabe ao Chefe do Serviço de Tecnologia da Informação do DNOCS estabelecer o responsável por garantir que os ativos da informação conectados à rede estejam devidamente instalados, atualizados e protegidos contra malwares.

Art. 9º. O Chefe do Serviço de Tecnologia da Informação do DNOCS deve indicar o responsável por realizar a monitoração dos ativos de informação que por algum motivo não estejam de acordo com a esta política de proteção contra malware

Art. 10. O Serviço de Tecnologia da Informação do DNOCS deve orientar todos os colaboradores e eventuais usuários dos ativos de informação em relação ao cumprimento das diretrizes estabelecidas nesta política.

Art. 11. O Serviço de Tecnologia da Informação do DNOCS deve manter uma relação de todos os aplicativos que podem ser instalados nos ativos de informação.

Art. 12. Os provedores de serviço de TIC do DNOCS devem garantir que todos os ativos de informação estejam de acordo com as diretrizes estabelecidas nesta política.

Art. 13. O DNOCS deve documentar os procedimentos utilizados na atribuição de responsabilidades para lidar com a proteção nos ativos de informação e recuperação de ataques de malware.

CAPÍTULO III
CONSCIENTIZAÇÃO E TREINAMENTO

Art. 14. O Gestor de Segurança da Informação do DNOCS deve promover ações de conscientização de recursos humanos em temas relacionados à segurança da informação, conforme previsto no art. 19 da Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020.

§ 1º. As ações de conscientização podem ser realizadas em caráter emergencial quando da ocorrência de notórios incidentes internos ou externos.

§ 2º. Aos usuários envolvidos em incidentes de malware, ou ao menos considerados suscetíveis a tais incidentes, pode-se revogar em caráter temporário o acesso parcial ou total aos recursos de TI do DNOCS, podendo ser exigidos conscientização e treinamento específicos como requisito para remoção desta revogação temporária.

Art. 15. O DNOCS deve promover a conscientização ou treinamento a todos os usuários sobre como identificar arquivos e programas infectados por malware e a quem relatar uma possível infecção.

Art. 16. O DNOCS deve basear-se em relatórios de eventos de malware ocorridos anteriormente para planejar o programa de conscientização e treinamento de seus colaboradores.

Art. 17. Criar e manter um programa de conscientização, educação e treinamento que aborde temas entendidos como importantes, levando em consideração a política de segurança da informação e suas diretrizes.

Art. 18. O programa de conscientização e treinamento sobre malware do DNOCS deve ser revisado e atualizado de forma periódica.

Art. 19. O DNOCS deve elaborar treinamentos específicos para os diferentes requisitos de segurança da informação inerentes a cada cargo ou função de seus servidores.

Art. 20. O programa de conscientização e treinamento do DNOCS deve considerar o treinamento de novos colaboradores.

Art. 21. O DNOCS deve criar e manter uma forma de avaliação do programa de conscientização e treinamento por meio de feedback dos participantes.

Art. 22. O programa de conscientização e treinamento deve ter como um dos objetivos elucidar os colaboradores sobre as suas responsabilidades no que diz respeito a segurança da informação de ativos de informação do DNOCS.

Art. 23. O programa de conscientização do DNOCS deve observar a importância de elaborar a conscientização e treinamento dos prestadores de serviço de acordo com novas contratações e encerramento de contrato.

Art. 24. O programa de conscientização do DNOCS pode utilizar de ferramentas como salas virtuais e físicas de treinamento, folhetos, cartazes, websites, boletins informativos e eventos específicos para manter o público-alvo, informado e atualizado sobre as diretrizes de proteção contra malware do DNOCS .

Art. 25. O DNOCS deve conscientizar os seus colaboradores quanto a importância de relatar o mais rápido possível uma possível infecção ou evento de segurança da informação.

Art. 26. O DNOCS deve manter e divulgar de forma ampla o canal de comunicação de possíveis eventos de segurança da informação.

CAPÍTULO IV
PREVENÇÃO DE INCIDENTES DE MALWARE

Art. 27. O DNOCS deve adotar medidas que visam mitigar o impacto da exploração de vulnerabilidades por malwares, tais como a indisponibilidade de recursos (redes, aplicações etc) que venham a afetar negativamente a continuidade dos negócios.

Art. 28. O DNOCS deve adotar técnicas de segmentação de rede visando mitigar a propagação ou disseminação de ameaças, tais como malwares, dentro da rede da organização.

Art. 29. O DNOCS deve adotar, quando necessário, infraestrutura como código para a configuração e atualização do ambiente de redes, bem como, implementar protocolos de redes seguros, tais como SSH e HTTPS.

Art. 30. Planos de continuidade de negócios para recuperação de ataques de malware, incluindo backups e softwares necessários, devem ser mantidos pelo DNOCS.

Art. 31. Procedimentos para coletar informações sobre novos malwares, devem ser implementados pelo DNOCS .

Art. 32. Realizar, regularmente e de forma automatizada, backup de todos os dados de sistemas. As cópias de segurança devem ser armazenadas e protegidas em locais adequados, por meio de segurança física ou criptografados. Além disso devem ser executados testes de integridade dos dados e das mídias de armazenamento em período regular.

Art. 33. O DNOCS deve elaborar e manter uma política de senhas que oriente aos usuários utilizarem senhas fortes e autenticação de múltiplo fator para suas contas e dispositivos. Além disso deve-se utilizar senhas exclusivas para todos os ativos institucionais.

Art. 34. É dever do DNOCS implementar medidas que detectem o uso de softwares permitidos ou não permitidos.

Art. 35. O DNOCS deve implementar medidas que detectam acessos a sites maliciosos ou suspeitos.

Art. 36. Logs e alertas do software antimalware devem ser armazenados pelo DNOCS em um local seguro e o acesso deve ser restrito para evitar roubo ou vazamento de dados pessoais que tenham sido coletados.

Art. 37. O DNOCS deve especificar tipos de softwares preventivos (antimalware, antivírus, firewall) necessários para cada tipo de host (servidor, laptop, smartphone, pc etc.) e deve listar os requisitos para configuração e atualização deles.

Art. 38. Ameaças para tipos de malware que não exploram vulnerabilidades, como ataques de engenharia social, devem ser mitigados pelo DNOCS.

CAPÍTULO V
CONFIGURAÇÃO E ATUALIZAÇÃO

Art. 39. É dever do DNOCS manter um processo de configuração seguro para ativos corporativos, dispositivos de usuário final incluindo portáteis e móveis, dispositivos não computacionais/IoT, servidores e softwares como sistemas operacionais e aplicações.

Art. 40. O processo de configuração deve ser revisado e atualizado em períodos predefinidos ou quando ocorrer mudanças significativas no DNOCS que possam impactar esta medida de segurança.

Art. 41. O DNOCS deve realizar o gerenciamento de software antimalware, recomendado ser feito de forma centralizada podendo conter agentes do software antimalware em ativos de informação como estação de trabalho e servidores.

Art. 42. É dever do DNOCS configurar e atualizar o software de detecção antimalware regularmente e realizar varredura nos computadores, servidores e mídias de armazenamento eletrônico incluindo:

I. dados recebidos por meio da rede, sistemas ou qualquer mídia de armazenamento eletrônico;

II. e-mails, mensagens instantâneas e downloads.

Art. 43. O DNOCS deve configurar o software antimalware para que ele obtenha as atualizações das bases antimalware de forma automática. Quando isso não puder ser realizado, deve ser devidamente justificado e aprovado pelos responsáveis.

Art. 44. É dever do DNOCS configurar os dispositivos para a não execução e reprodução automática de mídias removíveis.

Art. 45. O DNOCS deve configurar os softwares antimalware para realizar a varredura automática de mídias removíveis quando inseridas nos dispositivos.

Art. 46. Devem ser configuradas, pelo DNOCS, as funcionalidades "anti-exploits" que estejam disponíveis nos sistemas operacionais e a implementadas as ferramentas que possam ser configuradas para aplicar proteções sobre um conjunto mais amplo de aplicações e executáveis.

Art. 47. O DNOCS deve realizar o gerenciamento de controle de acesso em ativos que se conectam remotamente à organização, considerando, mas não se limitando a:

I. Determinar a quantidade de acessos às soluções utilizando recursos de softwares e de rede;

II. Possuir processos de configuração segura de ativos remotos;

III. Certificar-se que os sistemas operacionais, software antimalware e demais aplicações estejam sempre atualizados.

Art. 48. O DNOCS pode utilizar software antimalware com função holística que tenha a capacidade de monitorar e identificar os comportamentos atípicos de seus ativos de informação.

Art. 49. É dever do DNOCS realizar a atualização de sistemas operacionais e softwares por meio de gestão automatizada de patches.

Art. 50. O DNOCS deve configurar o software antimalware no servidor de e-mail para realizar a varredura de anexos e implementar um ambiente virtual controlado para realizar a verificação e abertura de anexos, tais como uma sandbox.

Art. 51. É dever do DNOCS remover ou alterar contas locais e senhas padrão de sistemas operacionais e softwares para evitar acessos não autorizados.

Art. 52. O DNOCS deve desativar ou remover serviços desnecessários, principalmente os serviços de rede, pois são vetores adicionais que um malware utiliza para se propagar.

Art. 53. Deve ser configurado, pelo DNOCS, o servidor de e-mail para proibir o envio e recebimento de certos tipos de arquivos, como executáveis e scripts.

CAPÍTULO VI
DETECÇÃO E ANÁLISE DE MALWARE

Art. 54. O DNOCS deve realizar verificação e validação regular de softwares, sistemas críticos e de dados de sistemas em busca de arquivos desconhecidos que não tenham sido aprovados ou alterações não autorizadas.

Art. 55. Deve ser divulgado amplamente, pelo DNOCS, comunicados sobre ameaças e procedimentos que os usuários devem realizar ao detectar possíveis anormalidades nos ativos de informação.

Art. 56. É dever do DNOCS isolar o ambiente ou os ativos de informação suspeitos,

infectados e os que podem ser potencialmente comprometidos para análise e identificação de malware.

Art. 57 O DNOCS precisa investigar todo incidente onde haja suspeita de que a origem possa ser um malware, para verificar se essa é de fato a causa subjacente.

Art. 58. O DNOCS deve identificar quais ativos de informação estão infectados por malware, para que assim, todos estes ativos consigam ser analisados e, consequentemente, ações específicas de contenção, erradicação e recuperação sejam realizadas.

Art. 59. É dever do DNOCS garantir que toda a identificação de infecção por malware seja realizada por meio de ferramentas automatizadas.

Art. 60. É dever do DNOCS classificar e nomear cuidadosamente os seus ativos de informação, de forma a tornar a detecção de malware mais eficaz.

Art. 61. O DNOCS deve determinar quais tipos de informações de identificação do ativo de informação são necessárias (IP, Sistema Operacional, localização física do ativo de informação), bem como quais fontes de dados dos sistemas de detecção serão utilizadas.

Art. 62. O DNOCS deve utilizar ferramentas de detecção do malware como SIEM, IDS, IPS, para identificar as características de ação do malware.

Art. 63. O DNOCS deve pesquisar informações sobre malware em fornecedores de antivírus, tais como:

I. Categoria do malware (por exemplo, worm, trojan, vírus);

II. Serviços, portas, protocolos que são explorados pelo malware;

III. Como o malware impacta o ativo de informação infectado;

IV. Vulnerabilidades que são exploradas pelo malware;

V. Como o malware se propaga nos ativos de informação;

VI. Como realizar a contenção e remoção do malware.

Art. 64. O DNOCS pode utilizar sniffers de pacotes para realizar a busca ativa de um malware específico.

Art. 65. A equipe de segurança da informação do DNOCS deve analisar o comportamento do malware de forma ativa (ao executar o malware em um ambiente controlado) ou de forma forense (analisando as evidências de ações do malware no ativo de informação infectado).

Art. 66. Caso a análise de malware seja por meio de ambiente controlado, o DNOCS deve estabelecer um sistema de testes isolado, sem acesso à sua rede corporativa e operacional.

Art. 67. O sistema de testes deve ser estabelecido em um sistema operacional virtualizado do DNOCS , que após a realização da análise de comportamento do malware, deverá ser apagado.

Art. 68. O sistema de testes deve incluir ferramentas de identificação e detecção de malware atualizadas.

Art. 69. O DNOCS pode utilizar da análise de logs para analisar o comportamento de um malware.

Art. 70. Implementar ferramenta de análise de tráfego baseado em rede, como o sistema de prevenção de intrusão, buscando pacotes suspeitos, fluxos incomuns na rede e assinaturas de ataque, visando interromper a atividade potencialmente maliciosa.

Art. 71. O DNOCS deve utilizar tecnologias de inspeção e filtragem de conteúdo, tais como as especificadas a seguir:

I. Ferramenta de filtragem de spam;

II. Ferramenta de filtragem e inspeção de conteúdo da web;

III. Listas negras de sites maliciosos.

Art. 72. O DNOCS deve utilizar métodos de arquitetura defensiva, tais como:

I. Proteção de BIOS;

II. SandBox.

CAPÍTULO VII
REMEDIAÇÃO - CONTENÇÃO E ERRADICAÇÃO

Seção I
Da Contenção

Art. 73. As estratégias de contenção devem apoiar os responsáveis pelo tratamento de incidentes na seleção da combinação apropriada de métodos, com base nas características de uma situação específica.

Art. 74. Os usuários devem receber instruções sobre como identificar infecções e quais medidas tomar se um host for infectado, tais instruções incluem e não se limitam a:

I. Ligar para o suporte técnico;

II. Desconectar o host da rede;

III. Desligar o host.

Art. 75. O malware identificado deve ser removido dos ativos do DNOCS.

Art. 76. Softwares não autorizados devem ser removidos dos ativos do DNOCS ou receber uma exceção documentada.

Art. 77. Todas as exceções devem ser anotadas no inventário de software e no registro de exceções.

Art. 78. O DNOCS deve ter mecanismos alternativos para distribuir informações aos usuários, como enviar mensagens para todas as caixas de correio de voz do DNOCS , afixar cartazes nas áreas de trabalho e distribuir instruções nas entradas dos edifícios e escritórios.

Art. 79. O DNOCS deve identificar e implementar métodos para fornecer utilitários e atualizações de software aos usuários que deverão ajudar na contenção.

Art. 80. É prudente que o DNOCS utilize tecnologias automatizadas para prevenir e detectar infecções, o que irá ajudar a conter muitos incidentes causados por malwares. Essas tecnologias incluem softwares, tais como antivírus, filtragem de conteúdo e prevenção de intrusões.

Art. 81. O DNOCS deve estar preparado para usar outras ferramentas de segurança para conter o malware até que as assinaturas antivírus possam realizar a contenção de forma eficaz.

Art. 82. Se o DNOCS receber assinaturas atualizadas, é prudente testá-las pelo menos antes da implantação, para garantir que a atualização em si não cause um impacto negativo.

Art. 83. O DNOCS pode adotar vários métodos de detecção automatizados que não sejam software antivírus, tais como os seguintes:

I. Filtragem de conteúdo;

II. Software IPS baseado em rede;

III. Lista negra executável.

Art. 84. Manter lista das portas TCP e UDP utilizadas por cada serviço, para que possa suportar a desativação de serviços de rede.

Art. 85. Manter uma lista de dependências entre os principais serviços para que a equipe de resposta a incidentes esteja ciente deles ao tomarem decisões de contenção.

Art. 86. O DNOCS pode parar serviços que estiverem com vulnerabilidades e oferecer outros alternativos com funcionalidades semelhantes aos usuários.

Art. 87. A Equipe de Resposta e Tratamento de Incidentes deve considerar bloquear todo o

acesso ao host externo (por endereço IP ou nome de domínio, conforme apropriado), se os hosts infectados tentarem estabelecer conexões com um host externo para baixar malwares, como por exemplo rootkits.

Art. 88. Se hosts infectados tentarem espalhar um malware, o DNOCS poderá bloquear o tráfego de rede dos endereços IP dos hosts para controlar a situação enquanto os hosts infectados são fisicamente localizados e limpos.

Art. 89. O DNOCS deve projetar e implementar suas redes para tornar a contenção, através da perda de conectividade, mais fácil e menos perturbadora, isso poderá incluir:

I. Colocar servidores e estações de trabalho em sub-redes separadas;

II. Uso de redes locais virtuais (VLAN) separadas para hosts infectados;

Art. 90. A Equipe de Resposta e Tratamento de Incidentes deve selecionar uma combinação de métodos de contenção que, provavelmente, serão eficazes na contenção do atual incidente, ao mesmo tempo em que limita os danos aos hosts e reduz o impacto que os métodos de contenção podem ter sobre outros hosts.

Art. 91. O DNOCS deve apoiar decisões de contenção sólidas, tendo políticas que estabeleçam claramente quem tem autoridade para tomar decisões importantes de contenção e sob que circunstâncias (por exemplo, desconectar sub-redes da Internet).

Seção II
Da Erradicação

Art. 92. Nos casos em que a destruição do malware é possível, as ferramentas mais comuns para erradicação que o DNOCS normalmente são: software antivírus, software de controle de acesso à rede e outras ferramentas projetadas para remover malware e corrigir vulnerabilidades.

Art. 93. O DNOCS pode utilizar métodos automatizados de erradicação, como acionar verificações de antivírus remotamente.

Art. 94. O DNOCS deve fornecer instruções e atualizações de software aos usuários além de assistência durante o processo de erradicação de malwares.

Art. 95. O DNOCS pode manter áreas de suporte técnico formais ou informais nas principais instalações para aumentar a eficácia e eficiência na erradicação de malwares.

Art. 96. Durante incidentes graves, integrantes da equipe de TI podem ser realocados temporariamente de outras funções para ajudar nos esforços de erradicação.

Art. 97. O DNOCS deve estar preparado para reconstruir hosts rapidamente, conforme necessário, quando ocorrerem incidentes de malware.

Art. 98. Em vez de realizar ações típicas de erradicação, o DNOCS deve reconstruir qualquer hospedeiro que apresente alguma das seguintes características de incidente:

I. Um ou mais invasores obtiveram acesso de nível de administrador ao host;

II. O acesso não autorizado de nível de administrador ao host estava disponível para qualquer pessoa através de um backdoor, através de um compartilhamento desprotegido criado por um worm ou por outros meios;

III. Os arquivos do sistema foram substituídos por um cavalo-de-troia, backdoor, rootkit, ferramentas de ataque ou outros meios;

IV. O host fica instável ou não funciona corretamente depois que o malware foi erradicado por software antivírus ou outros programas ou técnicas. Isso indica que o malware não foi completamente erradicado ou que causou danos a arquivos ou configurações importantes do sistema ou de aplicativos;

V. Há dúvidas sobre a natureza e a extensão da infecção ou sobre qualquer acesso não autorizado obtido por causa da infecção.

Art. 99. A Equipe de Resposta e Tratamento de Incidentes deve realizar, periodicamente, atividades de identificação de hospedeiros que ainda estão infectados e estimar o sucesso da erradicação.

Art. 100. O DNOCS deve se esforçar para reduzir o número suspeito de máquinas infectadas e vulneráveis a níveis suficientemente baixos, para que, se todas elas estiverem conectadas a rede de uma só vez e todas as máquinas vulneráveis estiverem infectadas, o impacto geral das infecções seja o menor possível.

CAPÍTULO VIII
DA RECUPERAÇÃO

Art. 101. O DNOCS deve observar dois aspectos principais da recuperação de incidentes de malware, que são:

I. Restaurar a funcionalidade e os dados dos hosts infectados; e

II. Remover medidas de contenção temporárias.

Art. 102. Para incidentes de malware que são muito mais prejudiciais, como cavalos de Tróia, rootkits ou backdoors, que corrompem milhares de arquivos de sistema e de dados ou destroem discos rígidos, muitas vezes é melhor reconstruir primeiro o host e depois proteger o host para que ele não fique mais vulnerável à ameaça de malware.

Art. 103. O DNOCS deve considerar cuidadosamente os possíveis cenários de pior caso, como uma nova ameaça de malware que exija a reconstrução de uma grande porcentagem de suas estações de trabalho, e determinar como os hosts seriam recuperados nesses casos, isto pode incluir:

I. Identificação de quem executaria as tarefas de recuperação;

II. Estimativa de quantas horas de trabalho seriam necessárias e quanto tempo de calendário decorreria;

III. Determinação de como os esforços de recuperação deveriam ser priorizados.

Art. 104. O DNOCS deve determinar quando remover medidas de contenção temporárias.

Art. 105. A Equipe de Resposta e Tratamento de Incidentes deve esforçar-se para manter medidas de contenção em vigor até que o número estimado de hospedeiros infectados e de hospedeiros vulneráveis à infecção seja suficientemente baixo, de modo que os possíveis incidentes subsequentes tenham poucas consequências.

Art. 106. A Equipe de Resposta e Tratamento de Incidentes também deve considerar medidas de contenção alternativas que possam manter adequadamente a contenção do incidente e, ao mesmo tempo, causar menor impacto nas funções normais do DNOCS.

Art. 107. A Equipe de Resposta e Tratamento de Incidentes deve avaliar os riscos de restaurar o(s) serviço(s).

Art. 108. O Comitê de Governança Digital deve, em última análise, ser responsável por determinar o que deve ser feito, com base nas recomendações da equipe de resposta a incidentes e na compreensão da gestão sobre o impacto no DNOCS da manutenção das medidas de contenção.

CAPÍTULO IX
RELATÓRIOS E LIÇÕES APRENDIDAS

Art. 111. Todos os alertas de alta gravidade confirmados devem ser relatados ao Diretor Geral.

Art. 112. Os usuários devem ser treinados para reportar malwares descobertos ao Serviço de Tecnologia da Informação.

Art. 113. Possíveis resultados de atividades de lições aprendidas para incidentes de malware podem ser os seguintes:

I. Mudanças na política de segurança;

II. Mudanças no Programa de Conscientização;

III. Reconfiguração de software;

IV. Implantação de software de detecção de malware;

V. Reconfiguração do software de detecção de malware;

CAPÍTULO IX
DISPOSIÇÕES FINAIS

Art. 114. Reforçar o compromisso do DNOCS com a segurança da informação, incluindo a proteção contra malware, destacando a importância de todas as pessoas envolvidas seguirem a política estabelecida.

Art. 115. Enfatizar a responsabilidade de cada colaborador em aderir às práticas de segurança da informação estabelecidas e relatar qualquer atividade suspeita o mais rápido possível.

Art. 116. Promover uma cultura de segurança da informação em todo DNOCS , incentivando a colaboração e a comunicação aberta sobre ameaças de malware e melhores práticas de segurança.

Art. 117. Garantir o apoio contínuo da alta administração para a implementação e execução eficaz da Política de Defesas Contra Malware, alocando recursos adequados e priorizando a segurança cibernética como uma preocupação organizacional.

Art. 118. Avaliar periodicamente o impacto da Política de Defesas Contra Malware na segurança geral do DNOCS , identificando áreas de sucesso e oportunidades de melhoria.

Art. 119. Considerar a comunicação da Política de Defesas Contra Malware para partes externas, como fornecedores e parceiros, para promover a conscientização e colaboração na proteção contra ameaças.

Art. 120. Integrar a Política de Defesas Contra Malware aos planos de continuidade do negócio, garantindo que o DNOCS se capacite para lidar com interrupções causadas por ataques de malware e outros incidentes de segurança da informação.

Anexo II

Não conformidade

As sanções por descumprimento podem incluir, mas não se limitam a um ou mais dos seguintes:

1. Revogação em caráter temporário do acesso parcial ou total aos recursos de TI do DNOCS;

2. Processo Administrativo disciplinar de acordo com a legislação aplicável;

3. Exoneração ou desligamento;

4. Ação judicial de acordo com as leis aplicáveis e acordos contratuais.

Anexo III

Concordância

Li e entendi a Política de Defesas Contra Malware do DNOCS . Entendo que caso venha a

violar as diretrizes estabelecidas nesta Política, posso enfrentar ações legais ou disciplinares de acordo com as leis aplicáveis ou normas internas do DNOCS.

_____

Nome do Servidor/Empregado

_____

Assinatura do Servidor/Data