INSTITUTO NACIONAL DE CÂNCER
DIREÇÃO GERAL

POLÍTICA DE SEGURANÇA

CIBERNÉTICA

Documento Nº 000.1000.008

Revisão 00

07/07/2025

Autores:

Direção Geral
Serviço de Tecnologia da Informação
Serviço de Controle Interno e Integridade

POLÍTICA DE SEGURANÇA CIBERNÉTICA DO INSTITUTO NACIONAL DE CÂNCER.

Considerando a governança pública como sendo o conjunto de mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade;

Considerando Portaria SGD/MGI Nº 852, de 28 de março de 2023, que em seu texto traz disposições sobre segurança cibernética, também conhecido por cibersegurança, como sendo são ações voltadas para a segurança de operações, visando garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético;

Considerando o art. 17 do Decreto no. 9.203/2017, que determina que a alta administração da administração pública federal deve estabelecer um sistema de gestão de riscos e controles internos.

Considerando a ABNT NBR ISO 27001, que trata de Segurança da Informação;

Considerando a Portaria Inca nº 169, de 23 de fevereiro de 2024, que reformulou o Comitê de Governança, Riscos e Controles do Instituto;

Considerando a necessidade de desenvolver processos e produtos considerando os pilares e as boas práticas de segurança da informação, apoiada na gestão dos riscos cibernéticos como assunto estratégico ao negócio, e fomentar a cultura de segurança entre todos os colaboradores para prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético. do Instituto, e ainda

Considerando que o aperfeiçoamento da governança institucional potencializa a produção e entrega de valor público, a Direção Geral resolve instituir a sua **POLÍTICA DE SEGURANÇA CIBERNÉTICA DO INCA**.

CAPÍTULO I

OBJETIVOS

Art. 1º. O objetivo desta política é definir princípios e diretrizes para proteger e salvaguardar os ativos de informação; nortear a definição de normas e procedimentos específicos de Segurança Cibernética, implementar controles e procedimentos para prevenir, detectar e/ou reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético, e que permitam garantir a confidencialidade, a integridade, autenticidade e a disponibilidade dos dados e dos sistemas de informação utilizados pela Instituição.

CAPÍTULO II

ABRANGÊNCIA

Art. 2º. Esta Política é de observância obrigatória por todos os agentes públicos do INCA, inclusive em períodos de férias, licenças e/ou afastamentos. Incluem-se todos aqueles que se relacionarem com a Instituição, como órgãos e entidades públicas, clientes, fornecedores e prestadores de serviços, bem como aqueles que tenham acesso aos dados ou aos sistemas informatizados por ela utilizados.

CAPÍTULO III

DEFINIÇÕES

Art. 3º Para os efeitos desta Política, entende-se por:

I. Dado(s) e/ou Informação(ões): são todos os dados referentes às atividades desenvolvidas pela Instituição;
II. Agente Público: é todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos entes públicos;

III. Incidente: qualquer ocorrência que realmente ou potencialmente comprometa a confidencialidade, integridade ou disponibilidade de um sistema de informação ou a informação que o sistema processa, armazena ou transmite ou que constitui uma violação ou ameaça iminente de violação de políticas de segurança, procedimentos de segurança ou políticas de uso aceitáveis.;

IV. Riscos cibernéticos: são os riscos de ataques oriundos de malware, técnicas de engenharia social, invasões, ataques de rede, fraudes externas, entre outros, que possam expor Dados, redes e sistemas da Instituição, causando danos financeiros e/ou de reputação consideráveis, podendo, em algumas circunstâncias, prejudicar a continuidade das suas atividades;

V. Segurança da informação: conjunto de conceitos, técnicas e estratégias, as quais visam proteger os ativos de informação;

VI. Comitê de Governança, Integridade, Riscos e Controles Internos (CGRC): instância interna colegiada de natureza propositiva e deliberativa, de caráter permanente, composto por membros da alta administração e presidido pelo Diretor Geral;

VII. Segurança cibernética: conjunto de tecnologias, processos e práticas projetados para proteger redes, computadores, sistemas e dados de ataques, danos ou acesso não autorizado;

VIII. Plano de resposta a incidentes: procedimento estabelecido para que os incidentes de segurança da informação e cibernética sejam identificados e respondidos conforme as diretrizes estabelecidas internamente;

IX. Identificação de eventos de risco: processo de identificação dos eventos que influenciam negativamente o cumprimento dos objetivos, suas causas e consequências;

X. Medida de controle: medida aplicada pela instituição para tratar os riscos, aumentando a probabilidade de que os objetivos e as metas institucionais estabelecidos sejam alcançadas; e

XI. Risco: evento incerto que se ocorrer, afeta negativamente o cumprimento dos objetivos.

CAPÍTULO IV
PRINCÍPIOS

Art. 4º São princípios aplicados ao INCA diretamente relacionados à esta Política:

I - **Confidencialidade**: garantir que a informação esteja acessível somente às pessoas autorizadas.

II - **Integridade**: garantir a autenticidade da informação e dos seus métodos de processamento.

III - **Disponibilidade**: garantir que a informação esteja disponível às pessoas autorizadas sempre que for necessário acessá-la.

IV - **Autenticidade**: garantir que a informação seja proveniente da fonte original e que não tenha sido alvo de alterações;

V – **Irretratabilidade ou não repúdio**: garantir que o legítimo autor da informação não possa negar sua autoria;

VI - **Conformidade**: garantir que os processos estejam de acordo com os regulamentos, normativos e leis vigentes aplicáveis, de forma a seguir rigorosamente todos os protocolos exigidos na sua área de atuação.

Parágrafo 1º: Considera-se que os ativos de informação são todos aqueles gerados ou desenvolvidos, opt-in e opt-out. Os ativos de informação podem estar presentes em diversas formas, tais como: arquivos digitais, mídias externas, documentos digitalmente assinados, dispositivos móveis, bancos de dados e gravações de áudio.

Parágrafo 2º: Os ativos de informação, independentemente da forma apresentada, compartilhada ou armazenada, devem ser utilizados apenas para a sua finalidade devidamente autorizada, estando sujeitos a monitoramento e auditoria.

Parágrafo 3º: Para todo ativo de informação deve ser atribuído um responsável, que deverá ser devidamente classificado quanto ao seu nível de confidencialidade, de acordo com os critérios estabelecidos em norma

específica, e adequadamente protegido de quaisquer riscos, bem como de ameaças que possam comprometer o Instituto.

CAPÍTULO V
DIRETRIZES GERAIS

Art. 5º Esta política estabelece as seguintes diretrizes gerais:

I. Resguardar a proteção dos dados contra acessos indevidos, bem como contra modificação, destruição ou divulgação não autorizada;
II. Realizar a adequada classificação das informações e garantir a continuidade do processamento, conforme os critérios e princípios indicados nos normativos internos;
III. Garantir que os sistemas e dados sob sua responsabilidade estejam devidamente protegidos e sejam utilizados apenas para o cumprimento de suas atribuições;
IV. Zelar pela integridade da sua infraestrutura tecnológica na qual estão armazenados, processados ou, de qualquer outra forma, tratados os dados, adotando as medidas necessárias para prevenir ameaças lógicas, como vírus, programas nocivos ou outras falhas que possam ocasionar acessos, manipulações ou usos não autorizados a dados internos e confidenciais;
V. Garantir que as intervenções realizadas no ambiente tecnológico, como auditorias, testes de segurança ou outras atividades no ambiente que possam, de alguma forma, impactar os sistemas operacionais ou os processos de negócio, sejam previamente acordadas entre o solicitante e o responsável pelo ambiente;
VI. Atender às leis e normas que regulamentam as suas atividades.

DIRETRIZES ESPECÍFICAS PARA A ÁREA DE GESTÃO DA INFORMAÇÃO

Art. 6º. Além das diretrizes dispostas no art. 5º, visam estabelecer um ambiente salubre para a manipulação de dados e informações:

I. Todas as informações devem ser tratadas de forma ética e sigilosa e de acordo com as leis vigentes e normas internas, evitando-se mau uso e exposição indevida, atentando-se, prioritariamente, às nuances dissertadas pela Lei Geral de Proteção de Dados - LGPD;
II. A informação deve ser utilizada de forma transparente e apenas para a finalidade para a qual foi coletada, coibindo-se qualquer utilização aleatória ou com finalidade externa;
III. O acesso às informações e recursos só deve ser feito se devidamente autorizado pela área de Tecnologia da Informação, em consonância às diretrizes e deliberações oriundas da Direção Geral do Instituto;
IV. A identificação de qualquer agente público deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas em ambiente sistêmico, ou em qualquer documento emitidos pelos meios eletrônicos e cibernético usufruídos pelo INCA;
V. A concessão de acessos deve obedecer ao critério de menor privilégio, no qual os usuários têm acesso somente aos recursos de informação imprescindíveis para o pleno desempenho de suas atividades, devendo, tal mapeamento de atribuições e competência, alinhar-se às responsabilidades atribuídas às definições estratégicas da instituição;
VI. Todo agente público deve reportar os riscos às informações ao Serviço de Tecnologia da Informação;
VII. A área de Tecnologia da Informação deve divulgar amplamente, em consonância às diretrizes redigidas pela Direção da instituição, as responsabilidades sobre Segurança da Informação aos agentes públicos, que devem entender e assegurar estas diretrizes.

CAPÍTULO VI
MECANISMOS DE PROTEÇÃO ADOTADOS PELA INSTITUIÇÃO

Art. 7º: Para cumprimento das diretrizes elencadas no art. 5º, a Instituição, através do Serviço de Tecnologia da Informação, pratica as seguintes ações:

I. Adota procedimentos e controles de segurança dentre os quais: a autenticação, a criptografia, a prevenção e a detecção de intrusão, a

prevenção de vazamento de informações, a realização periódica de testes e varreduras para detecção de vulnerabilidades, a proteção contra softwares maliciosos, o estabelecimento de mecanismos de rastreabilidade, os controles de acesso, segregação de funções, segmentação da rede de computadores e a manutenção de cópias de segurança dos dados e das informações, conforme normativos internos.

II. Controla, monitora, restringe o acesso aos ativos de informação a menor permissão e privilégios possíveis;

III. Aplica os procedimentos e controles, inclusive, no desenvolvimento de sistemas de informação seguros e na adoção de novas tecnologias empregadas em suas atividades.

IV. Possui controles específicos, incluindo os voltados para a rastreabilidade da informação, que buscam garantir a segurança das informações sensíveis.

V. Classifica os incidentes de segurança da informação e cibernética conforme sua relevância e de acordo com a classificação das informações envolvidas;

VI. Realiza o registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da Instituição, que abrangem, inclusive, informações recebidas de empresas prestadoras de serviços;

VII. Estabelece e documenta em normativo interno os critérios que configuram situações de crises, bem como elabora inventário dos cenários de crises cibernéticas relacionados aos incidentes de segurança, considerados nos testes de continuidade e realiza testes anuais para garantir a eficácia dos processos, além de, anualmente, elaborar o seu relatório de resposta a incidentes no ambiente tecnológico;

VIII. Estabelece regras e padrões para assegurar que a informação receba o nível adequado de proteção quanto à sua relevância, conforme normativo interno;

IX. Toda informação possui um proprietário, é classificada e recebe os devidos controles, que garantem sua confidencialidade, condizendo com as boas práticas de mercado e regulamentações vigentes; e

X. Adota mecanismos para disseminação da cultura de segurança cibernética no Instituto, incluindo:
   a) O comprometimento da administração com a melhoria contínua dos procedimentos relacionados com a segurança cibernética;
   b) A prestação de informações a usuários finais sobre precauções na utilização de produtos e serviços.

CAPÍTULO VII
CLASSIFICAÇÃO DA INFORMAÇÃO

Art. 8º: As informações devem ser classificadas de acordo com a confidencialidade e as proteções necessárias, nos seguintes níveis: Restrita, Confidencial, Interna e Pública. Para isso, devem ser consideradas as necessidades da Instituição, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações, usando, em sua totalidade, as definições contidas na Lei Geral de Proteção de Dados e em seus dispositivos, considerando-se:

I. **Pública:** são informações que possuem caráter informativo geral e que são direcionadas ao público em geral;
II. **Interna**: são informações destinadas ao uso interno da instituição e que estão disponíveis para todos os colaboradores da instituição;
III. **Restrita**: são informações disponíveis apenas a colaboradores específicos da instituição, que as necessitem para exercer suas atribuições;
IV. **Confidencial**: são informações sigilosas de caráter estratégico para a instituição e que estão disponíveis somente para a diretoria e pessoas por ela autorizadas

CAPÍTULO VIII
GESTÃO DE ACESSOS

Art. 9º. As concessões, revisões e exclusões de acesso devem utilizar as ferramentas e os processos do INCA, e em consonância com os demais

documentos, políticas e processos da instituição. Os acessos devem ser rastreáveis, a fim de garantir que todas as ações passíveis de auditoria possam identificar individualmente o agente público, prestador de serviço ou qualquer outro terceiro que possua tal acesso, a quem possam ser atribuídas as responsabilidades pelas ações e posturas tomadas.

Parágrafo Único: Para tratamento e condução destas ações, o Instituto dispõe de Política própria, que deve ser consultada e utilizada em caráter acessório e complementar a esta Política.

CAPÍTULO IX
GESTÃO DE RISCOS CIBERNÉTICOS

Art. 10. Os riscos devem ser identificados por meio de um processo estabelecido para análise de vulnerabilidades, ameaças e impactos sobre os ativos cibernéticos e de informação da instituição. Este processo, bem como os cenários de riscos de segurança da informação são escalonados pela área de Tecnologia da Informação, através da elaboração de Plano próprio de gerenciamento, sob sua elaboração e poder de anuência e/ou veto do Comitê de Governança, Riscos e Controles do Instituto.

CAPÍTULO X
AÇÕES DE PROTEÇÃO E PREVENÇÃO DE RISCOS CIBERNÉTICOS

Art. 11. Para pleno funcionamento e efetividade da segurança cibernética, devem ser tomadas as seguintes ações de proteção e prevenção de riscos:

I. Manutenção de inventários de hardware e software;
II. Verificação com frequência se há na Instituição computadores não autorizados ou software não licenciado;
III. Manutenção dos sistemas operacionais e software atualizados;
IV. Realização frequente de testes de invasão externa;

V. Realização de análises de vulnerabilidade na estrutura tecnológica do INCA frequentemente ou em situações que houver mudança significativas;

VI. Realização de teste do plano de resposta a incidentes com simulação de cenários.

VII. Verificação dos logs dos colaboradores;

VIII. Alteração periódica de senha de acesso dos Colaboradores;

IX. Segregação de acessos.

X. Solicitar para os fornecedores testes e eficácia dos processos utilizados para evitar e revelar as principais vulnerabilidades dos sistemas que estão sob a responsabilidades deles, o que permitirá efetuar as correções devidas a tempo de evitar ou mitigar um ataque real;

XI. Estabelecimento de normas para uso seguro da internet, e-mails e dispositivos móveis.

XII. Aplicação do princípio do menor privilégio (conceder acesso apenas ao necessário)

XIII. Uso de autenticação multifator (MFA) em sistemas críticos.

XIV. Uso de antivírus e soluções de EDR/XDR para proteção avançada.

XV. Backup frequente e testado regularmente para garantir recuperação rápida.

XVI. Programas contínuos de educação em segurança cibernética para funcionários.

XVII. Testes de *phishing* para avaliar vulnerabilidades humanas.

CAPÍTULO XI
TIPOS DE RISCOS CIBERNÉTICOS

Art. 12. A Segurança cibernética se constitui da preservação das propriedades da informação, notadamente sua confidencialidade, integridade, autenticidade e disponibilidade, permitindo o uso e o compartilhamento da informação de forma controlada, bem como do monitoramento e tratamento de incidentes provenientes de ataques cibernéticos.

Art. 13. São riscos de ataques cibernéticos todos aqueles oriundos de malware, de técnicas de engenharia social, de invasões, de ataques de rede (DDoS e Botnets), e de fraudes externas, desprotegendo dados, redes e sistemas da Instituição causando danos consideráveis. Dentre os muitos existentes, destacamos os seguintes:

I - Malwares: software invasivo ou código de computador projetado para infectar, danificar ou obter acesso a sistemas de computador

Tipos de Malware:

a) **Vírus**: software que causa danos a máquina, rede, softwares e banco de dados;
b) **Cavalo de Troia**: aparece dentro de outro software e cria uma porta para a invasão do computador;
c) **Spyware**: software malicioso para coletar e monitorar o uso de informações;
d) **Ransomware**: software malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido.

II - **Engenharia Social**: técnica empregada com o objetivo de induzir os usuários a enviarem dados confidenciais, infectar seus computadores com malware ou abrir links para sites infectados, sendo a capacidade de conseguir acesso a informações confidenciais e dados sigilosos por meio de técnicas de persuasão, tendo os seguintes tipos:

a) ***Pharming***: direciona o usuário para um site fraudulento, sem o seu conhecimento;
b) ***Phishing***: links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais;
c) ***Vishing***: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais;

d) ***Smishing***: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais;
e) **Acesso pessoal**: pessoas localizadas em lugares públicos como bares, cafés e restaurantes que captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.

III - **Fraudes externas e invasões**: Realização de operações por fraudadores, utilizando-se de ataques em contas bancárias, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

IV - **Ataques DDoS e Botnets**: Ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição; no caso dos Botnets, o ataque vem de um grande número de computadores infectados utilizados para criar e enviar spam ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços.

CAPITULO XII
INCIDENTES DE SEGURANÇA

Art. 14. Conforme a Lei Geral de Proteção de Dados (LGPD) conceitua-se como qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular de dados pessoais.

AVALIAÇÃO DA RELEVÂNCIA DOS INCIDENTES DE SEGURANÇA

Art. 15. Os parâmetros a serem utilizados na avaliação da relevância dos incidentes deverão considerar a frequência e o impacto dos cenários de incidentes que impliquem em danos ou perigo de dano à confiabilidade, à integridade, à disponibilidade, à segurança e ao sigilo dos dados e dos

sistemas de informação utilizados, que tenham ou possam ter a capacidade de causar interrupção ou comprometer o pleno funcionamento das atividades da instituição.

Art.16. Para avaliação quanto ao grau de relevância do incidente e impactos aos sistemas interno e/ou externo, apresenta-se a seguinte classificação:

a) altamente críticos: são aqueles que podem comprometer desmedidamente a segurança cibernética da informação, obstruir a realização operacional e de difícil ação mitigadora, considerando-se, sendo as ocorrências desse nível, como incidentes relevantes;
b) medianamente críticos: remetem aos incidentes que podem comprometer, de forma conhecida e controlada, a segurança cibernética da informação, e apresentar uma ação saneadora já conhecida pela instituição, considerando-se, as ocorrências desse nível, como incidentes relevantes;
c) reduzidamente críticos: tangenciam àqueles eventos que fragilizam levianamente a segurança cibernética da informação, e requerem ações saneadoras palatáveis.

Parágrafo Único: Todos os incidentes passam por um processo de tratamento e comunicação, onde são registradas as informações pertinentes aos incidentes como causa, impacto e classificação (conforme classificação acima), de acordo com o procedimento operacional interno

PROCEDIMENTOS E CONTROLES

Art. 17. A instituição adota os seguintes procedimentos e controles para prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético:

I- Autenticação: Para garantir a segurança dos acessos a instituição adota regras de autenticação para o sistema operacional e banco de dados, os quais utilizam dados e chaves armazenadas no banco de dados para efetuar o

acesso. Sendo que o chamado de consulta do login do usuário pelo sistema é feito em ambiente criptografado por chaves SSL.
Acessos com a exigência de autenticação:

- Sistema de e-mail;
- Consulta a base de dados (em todos os canais);
- Sistema ERP;
- Diretórios e arquivos na rede de computadores.

Obs. Cada sistema tem sua composição de senha e criptografia

II- Criptografia: O sistema de comunicação e transmissão de dados da instituição é criptografado.

III- Prevenção e detecção de intrusão: O sistema de prevenção e detecção de intrusão utilizado pela instituição é o Firewall, que possui regras de detecção de ataques DDOS, e também o monitoramento dos registros das tentativas de acessos e de conexão.

IV- Prevenção de vazamento de informações: O Banco de dados da instituição é mantido em rede interna apartado do ambiente do sistema operacional, e mantido atrás de camadas de segurança, com os softwares de monitoramento mantendo o sistema operacional seguro e estável. Ao sinal de indício de instabilidade ou tentativa de comprometer algo no sistema, recebemos um alerta que prontamente é atendido na ocorrência.

V- Proteção contra software malicioso: A instituição possui em todas suas unidades de trabalho, assim como no servidor web, o Antivírus Trend Vision One Já o servidor do sistema operacional e do banco de dados é baseado em Microsoft, só é adicionado softwares e aplicações homologadas pelas distribuições ou pela comunidade, sendo analisado minuciosamente para que não haja brechas.

VI- Mecanismos de rastreabilidade para informações sensíveis: Os sistemas contêm locais fixos onde são imputados os dados originados da instituição. Esses dados competem única e exclusivamente na origem, baseado nos

produtos e políticas da instituição. Locais onde estão armazenados estão contidos em relatórios de uso interno.

V- Controles de acesso: O sistema dispõe de mecanismos de log, e fornece rastreabilidade dos acessos. As telas de sistema são segregadas de acordo com as funções estabelecidas aos usuários.

VI- Backup dos dados e das informações: Esta instituição possui um método definido para execução de cópias de segurança, o qual é executado de forma a garantir continuidade caso necessário o reestabelecimento dos dados. **Diariamente** é feito uma cópia da base de dados e armazenado em uma pasta dentro do servidor, em um determinado horário e software, que se encarrega de efetuar uma cópia de segurança para uma ilha de backup, onde é armazenado por tempo determinado conforme legislação.

VII- Registro e controle dos efeitos de incidentes relevantes: Os incidentes são registrados com o seu devido código de prioridade conforme definido no Plano de Ação e Resposta a Incidentes, onde é descrita a forma como devem ser registrados e tratados os incidentes de segurança, sendo que nos processos e ocorrências, caso os responsáveis verifiquem grau de importância, devem notificar responsáveis e envolvidos, e observar outros itens obrigatórios ou de interesse, além de atualizar rotinas e processos de documentos como a própria política, manuais e outros que a instituição defina como necessário.

VIII- Gestão de prestadores de serviço: Os contratos com prestadores de serviço deverão conter cláusulas de confidencialidade e responsabilidades entre as partes, assim como cláusulas que garantam que os profissionais das empresas prestadoras de serviços a terceiros:

- Tenham conhecimento e cumpram esta política;
- Zelem e protejam o sigilo das informações da instituição;
- Cumpram as normas legais que regulamentam a propriedade intelectual e a proteção de dados e a normas vigentes relacionadas à segurança cibernética e afins;

- Utilizem os dados da instituição ou os sistemas por ela utilizados, bem como os ambientes físico e tecnológico da instituição, apenas para as finalidades objeto do contrato de prestação de serviço;
- Notifiquem imediatamente qualquer violação desta Política ou outras normas.

PLANO DE AÇÃO E DE RESPOSTA A INCIDENTES (documento a parte)

Art. 18. O Plano de Ação e de Resposta a Incidentes Cibernéticos abordará detalhadamente os cenários de incidentes a serem avaliados nos testes de continuidade, considerando a avaliação de risco dos incidentes por níveis de impacto com os seguintes objetivos:

I. Identificar os incidentes de segurança;
II. Registrar os eventos que acarretaram problemas de segurança/continuidade;
III. Direcionar medidas paliativas a incidentes ocorridos;
IV. Criar evidências e registros para medidas corretivas;
V. Acionar o plano de continuidade dos negócios;
VI. Reportar os incidentes de segurança;
VII. Adotar iniciativas para compartilhamento de informações sobre incidentes relevantes com outras instituições.

Parágrafo único: Em razão das especificidades acima, devem ser identificados por meio de um processo estabelecido pela área de Tecnologia da Informação, através de Plano próprio de gerenciamento, sob sua elaboração.

Figura1 Fonte: Guia de resposta a incidentes da SGD (Secretaria de Governo Digital).

Preparação: a entidade deve criar e treinar equipes para atuar na resposta a incidentes, além de limitar o número de incidentes, selecionando e implementando controles com base em avaliações de risco.

Detecção e análise de incidentes: a entidade deve adotar meios para detecção de incidentes e analisar tais eventos, buscando documentar, priorizar e notificar; esta fase também pode ser executada em conjunto com a fase posterior.

Contenção, erradicação e recuperação: fase em que são implementadas ações para contenção, erradicação e recuperação do incidente; aqui, também são identificadas as origens de ataques e coletadas as evidências.

Atividades pós-incidente: a entidade deve realizar atividades para melhorar o tratamento de novos incidentes.

TRATAMENTO DE INCIDENTES

Art.19. Os incidentes são interrupções de sistema tecnológico não planejado que afetam total ou parcialmente as atividades da instituição e podem acontecer nas seguintes situações (rol não taxativo):

Art.20. As ocorrências de incidentes devem ser avaliadas com relação a gravidade da situação, os motivos que levaram aos acontecimentos desses incidentes e as consequências para o INCA. O SETI em análise conjunta com a Direção Geral deverá realizar as seguintes ações após a avaliação dos incidentes:

INCIDENTE	POSSÍVEIS CAUSAS A S
Interrupção de energia elétrica	Fatores externos inerentes à rede ou à localidade e Fatores internos que comprometem a rede interr Sobrecarga da rede atu
Superaquecimento de ativos	Falha no sistema de climati
Indisponibilidade de dados	Servidores instáveis e Backup indisponível ou
Falha na rede de internet	Obstrução do sinal por fatores externos, como fal Mau funcionamento de recursos internos
Ataques cibernéticos a servidores	Falha no firewall e demais Furto de senhas e demais cr
Incêndio	Casos fort

I. Avaliar o impacto do incidente;
II. Redirecionar os contatos como as linhas de telefones para os celulares, instruir o provedor de telefonia a desviar linhas de dados, entre outros;
III. Avaliar a relevância, em caso de sabotagem ou terrorismo a fim de decidir pelo registro de boletim de ocorrência ou outras providencias caso seja necessário;
IV. Comunicar tempestivamente às chefias competentes, as ocorrências de incidentes relevantes e as interrupções de serviços relevantes que configurem uma situação de crise.

Art.21. Após o incidente ter sido resolvido com a contingência da segurança cibernética e demais equipes chaves notificadas, as áreas devem verificar se os dados estão faltando ou foram corrompidos ou outros problemas. Caso seja identificado que houve perda de informações ou dados, a equipe de contingência deve analisar quais as ações que podem voltar a operar normalmente, bem como a reconstrução de sistemas, mudanças e medidas de prevenção.

RELATÓRIO DE PLANO DE AÇÃO E RESPOSTA A INCIDENTES

Art. 22. Deverá ser emitido anualmente um relatório do Plano de ação e respostas a incidentes. Os referidos relatórios devem ser aprovados pelo Comitê de Governança, Riscos e Controles e apresentado pelo responsável pela segurança cibernética. O relatório deverá conter, no mínimo, as seguintes informações:

I. Resumo dos resultados alcançados na implementação de rotinas, procedimentos e tecnologias utilizados na prevenção e na resposta a incidentes;
II. As ocorrências de incidentes relevantes ocorrido no período relacionado referente ao ambiente cibernético.

CAPÍTULO XIII
DAS RESPONSABILIDADES

Art. 23. Ao **COMITÊ DE GOVERNANÇA, RISCOS E CONTROLES** compete:

I. Ser o responsável pela aprovação da Política de Segurança Cibernética, devendo ser revisada e atualizada de maneira que demonstre o compromisso da Alta Administração com a construção de um ambiente capaz de se proteger dentro do ambiente cibernético;
II. Manter a correção de eventuais deficiências da estrutura simplificada de gerenciamento de riscos que possam ser identificadas, assegura a observância por todos de, no mínimo a cada dois anos aprovar e revisar as políticas institucionais;
III. Prover recursos para a implementação, manutenção e melhoria da gestão de segurança cibernética;

Art. 24 Ao **SERVIÇO DE TECNOLOGIA DA INFORMAÇÃO** compete:

I. Elaborar o Plano de Gerenciamento de Riscos Cibernéticos e conduzir seu processo de gestão;

II. Conduzir a gestão de incidentes de segurança cibernética, incluindo as investigações para determinação de causas e responsáveis e a comunicação dos fatos ocorridos;

III. Conduzir a definição controles para tratamento de riscos, vulnerabilidades, ameaças e não conformidades identificadas;

IV. Propor projetos e iniciativas para melhoria do nível de segurança das informações;

V. Identificar com a equipe técnica as violações de segurança cibernética, estabelecendo ações sistemáticas de detecção, tratamento e prevenção de incidentes, ameaças e vulnerabilidades nos ambientes físicos e lógicos, objetivando a mitigação dos riscos cibernéticos;

VI. Ser o responsável pela elaboração do Plano de ação de incidentes cibernéticos;

VII. Assegurar que todos da equipe tenham acesso, conhecimento e implementação pratica desta política e demais normas e padrões de segurança de cibernética;

VIII. Assegurar que o acesso a dados e informações pela equipe seja somente o necessário ao desempenho de suas funções, atribuições e para cumprimento das operações e atividades em nível institucional.

Art.25 Ao **GESTOR DE SEGURANÇA** compete:

I- O Gestor de Segurança da Informação é a figura responsável por coordenar, supervisionar e implementar os controles, processos e diretrizes relacionados à segurança cibernética e à proteção das informações;

II- O Gestor de Segurança Cibernética atua como um elo estratégico entre a alta gerência e as equipes operacionais, assegurando que a segurança da informação seja uma prioridade contínua e um processo integrado às operações de negócio;

III- Liderar a criação, implementação e revisão contínua da Política de Segurança Cibernética, assegurando sua conformidade com as normas e legislações vigentes;

IV- Supervisionar planos de resposta a incidentes de segurança, garantindo a detecção, contenção, erradicação e recuperação eficazes, além da análise pós-incidente para melhoria contínua;

V- Promover a cultura de segurança cibernética em toda a organização, desenvolvendo e aplicando programas de treinamento para colaboradores sobre as políticas, boas práticas e as ameaças atuais; e

VI- Supervisionar a implementação de controles de acesso, a segurança de sistemas, redes e aplicações, e o monitoramento contínuo para detectar e prevenir atividades maliciosas.

Art.26 Ao **ENCARREGADO DE DADOS** compete:

I. Assegurar que as operações de tratamento de dados pessoais na organização estejam em plena conformidade com as diretrizes da LGPD e outras regulamentações de privacidade de dados;

II. Servir como principal ponto de contato e comunicação com os titulares dos dados para qualquer solicitação ou esclarecimento relacionado aos seus dados pessoais, bem como com a ANPD em caso de fiscalizações ou incidentes;

III. Fornecer orientação à instituição e aos colaboradores sobre as práticas de proteção de dados pessoais, incluindo a aplicação da LGPD e outras normas de privacidade;

IV. Gerenciar e coordenar o atendimento às solicitações dos titulares dos dados, como acesso, correção, exclusão e portabilidade de dados pessoais;

V. Colaborar com o Gestor de Segurança na avaliação e comunicação de incidentes de segurança que envolvam dados pessoais à ANPD e aos titulares dos dados, quando aplicável, conforme os requisitos da LGPD;

VI. Participar ativamente na promoção da cultura de privacidade e proteção de dados dentro da organização, complementando os esforços de conscientização em segurança cibernética;

Art.27 A **TODOS OS AGENTES PÚBLICOS** que trabalham no INCA compete:

I. Todo do componente da estrutura organizacional e agente público, independente do cargo, função ou local de trabalho, é responsável pela segurança das informações e deve cumprir as determinações desta política, normas e padrões de segurança cibernética;

II. O atendimento a esta política é ato de boa conduta e integridade, e integra a cultura institucionalizada em seu Código vigente, que deve ser igualmente atendido e respeitado por todos;

III. Todos os membros abrangidos por esta Política respondem civil, penal e administrativamente, isolada e/ou concomitantemente pelo exercício irregular de suas atribuições e têm o dever de dar ciência ao Comitê de Governança, Riscos e Controles para apuração de informação concernente à prática de crimes ou improbidade de que tenha conhecimento, ainda que em decorrência do exercício de cargo, emprego ou função pública;

IV. Quando for constatada irregularidade que configure dano à Administração, adotar-se-ão as providências necessárias para a apuração das infrações administrativas, observadas a segregação de funções e a necessidade de individualização das condutas, para a apuração dos ilícitos de sua competência.

CAPÍTULO XIV
DAS DISPOSIÇÕES FINAIS

Art. 28. Ao aprovar esta Política de Segurança Cibernética, o Comitê de Governança, Riscos e Controles da instituição firma um compromisso com a melhoria contínua dos procedimentos relacionados com a segurança cibernética, buscando sempre se manter em conformidade com as normas e regulamentos aplicáveis, guiada pelos princípios, diretrizes e práticas aqui adotadas para assegurar a confidencialidade, a integridade e a disponibilidade dos dados da instituição ou dos sistemas de informação por ela utilizados.

Art. 29. O Instituto incentiva e exige que violações, suspeitas ou indícios de descumprimento das disposições desta Política, da Política de *Compliance* e Integridade ou do Código de Conduta e Integridade, assim como dos demais

normativos ou da legislação aplicável, sejam oportunamente comunicadas por meio do Canal de Denúncias – Ouvidoria do INCA e Fala.BR, que tem a garantia da confidencialidade e de não retaliação ao manifestante.

Art. 30. A POLÍTICA DE SEGURANÇA CIBERNÉTICA poderá ser revista por iniciativa da Direção Geral a qualquer tempo, caso mudanças no ambiente interno e/ou externo o justificarem.

Art. 31. O Diretor é autorizado a expedir os atos necessários à regulamentação desta Política e a dirimir os casos omissos.

Art. 32. Todas as políticas, códigos e normas internas estão à disposição do público interno por meio da intranet. Para as informações destinadas ao público externo, são feitas publicações no site do Instituto, na internet, a exemplo dos Relatórios Anuais de Gestão, Agenda do Diretor, Atas das Reuniões do Comitê de Governança, Riscos e Controles e Divulgação de fatos relevantes.

Art. 33. Esta Política entra em vigor na data de sua publicação.

CAPÍTULO XV
REFERÊNCIAS

Referencial Básico de Governança Organizacional para Organizações Públicas do TCU – 3ª Edição, ano 2020;

Lei Nº 12.527, de 18 DE NOVEMBRO DE 2011, que regula o acesso a informações.

ABNT NBR ISO 27001, que trata de Segurança da Informação

Portaria SGD/MGI Nº 852, de 28 de março de 2023, que dispõe sobre o Programa de Privacidade e Segurança da Informação – PPSI

Decreto Nº 11.529 de 16 de maio de 2023, que institui o SITAI - Sistema de Integridade, Transparência e Acesso à Informação da Administração Pública Federal e a Política de Transparência e Acesso à Informação da Administração Pública Federal;

Portaria GM/MS Nº 5.763, de 25 de novembro de 2024, institui o Programa de Integridade do Ministério da Saúde – IntegriSAÚDE, e traz o conjunto de princípios, normas, procedimentos e mecanismos de prevenção, detecção e remediação de práticas de corrupção e fraude, de irregularidades, ilícitos e outros desvios éticos e de conduta, de violação ou desrespeito a direitos, valores e princípios que impactem a confiança, a credibilidade e a reputação institucional;

Decreto Nº 9.203, de 22 de novembro de 2017, dispõe sobre a POLÍTICA DE GOVERNANÇA da administração pública federal direta, indireta e fundacional;

Instrução Normativa Conjunta/CGU Nº 01 de 10 de maio de 2016, dispõe sobre GOVERNANÇA, CONTROLES INTERNOS E GESTÃO DE RISCOS no âmbito do Poder Executivo Federal;

Portaria INCA nº 169, de 23 de fevereiro de 2024, que atualizou o Comitê de Governança, Riscos e Controles Internos do Instituto;

Política de *Compliance* e Integridade do INCA, junho 2025.