SENADO FEDERAL

Secretaria de Gestão da Informação e Documentação

**ATO DA COMISSÃO DIRETORA Nº 15, DE 2024**

*Institui a Política Corporativa de Gestão de Incidentes de Segurança da Informação do Senado Federal – PCGIS.*

**A COMISSÃO DIRETORA DO SENADO FEDERAL**, no uso das competências previstas no inciso I do art. 98 do Regimento Interno e no art. 191 do Regulamento Administrativo, aprovado pelo Ato da Comissão Diretora nº 14, de 2022,

CONSIDERANDO o anexo ao Ato da Comissão Diretora nº 5, de 2015, no qual destaca-se o compromisso de preservar a memória do Senado, material e imaterial, garantindo a proteção e transparência devida, nos termos da lei;

CONSIDERANDO o Ato da Comissão Diretora nº 9, de 2017, que dispõe sobre Política Corporativa de Segurança da Informação do Senado Federal - PCSI e destaca que o Senado Federal recebe, produz, processa, armazena e transmite informações, as quais devem permanecer íntegras, disponíveis e com o seu grau de sigilo resguardado;

CONSIDERANDO o Ato do Presidente nº 10, de 2020, que dispõe sobre a Política Institucional de Proteção de Dados Pessoais e enfatiza que o Senado Federal adotará medidas de segurança técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito;

CONSIDERANDO o Decreto nº 10.222, de 5 de fevereiro de 2020, que institui a Estratégia Nacional de Segurança Cibernética, o qual enfatiza a necessidade de que as organizações identifiquem os pontos mais vulneráveis de seus sistemas, as ameaças cibernéticas mais prováveis, os maiores fatores de risco que requerem a adoção das proteções adequadas, os mecanismos de detecção de ataques, as metodologias de resposta a incidentes e os procedimentos de restauração do ecossistema informático;

CONSIDERANDO o Ato da Comissão Diretora nº 6, de 2022, que dispõe sobre a Política de Preservação Digital de Documentos do Senado Federal (PPDD) e estabelece princípios, dentre os quais se destaca a "Integridade e confiabilidade das informações custodiadas, de modo a garantir a segurança dos documentos e evitar a corrupção e perda de dados";

CONSIDERANDO o Acórdão nº 1768/2022 - TCU - Plenário, que versa sobre o acompanhamento de controles críticos de Segurança Cibernética nas organizações públicas federais, o qual considera que sistemas, serviços e processos devem contar com mecanismos eficientes de identificação e de resposta a incidentes como parte fundamental para o sucesso na resiliência e proteção organizacional;

CONSIDERANDO o Decreto nº 11.856, de 26 de dezembro de 2023, que institui a Política Nacional de Cibersegurança, que tem como objetivo incrementar a resiliência das

organizações públicas e privadas a incidentes e ataques cibernéticos, bem como estimular a adoção de medidas de proteção cibernética e de gestão de riscos para prevenir, evitar, mitigar, diminuir e neutralizar vulnerabilidades, incidentes e ataques cibernéticos, e seus impactos; RESOLVE:

Art. 1º Este Ato institui a Política Corporativa de Gestão de Incidentes de Segurança da Informação do Senado Federal - PCGIS, que compreende princípios, objetivos, diretrizes e responsabilidades para orientar e subsidiar as tomadas de decisão e a estruturação de ações e procedimentos que tangem ao gerenciamento assertivo e tempestivo de incidentes de segurança da informação, a fim de viabilizar e assegurar a disponibilidade, a integridade, a autenticidade e a confidencialidade dos ativos de informação do Senado Federal.

CAPÍTULO I

DAS DISPOSIÇÕES PRELIMINARES

Art. 2º Para os fins deste Ato, são adotadas as definições instituídas pela Portaria GSI/PR nº 93, de 18 de outubro de 2021, que aprova o Glossário de Segurança da Informação.

CAPÍTULO II

DOS PRINCÍPIOS

Art. 3º A PCGIS observará os seguintes princípios:

I - a proteção dos valores organizacionais;

II - a proteção dos ativos de informação custodiados ou pertencentes ao Senado Federal;

III - a melhoria contínua dos processos organizacionais;

IV - a qualidade e tempestividade das informações;

V - a responsabilidade na utilização de recursos públicos;

VI - a transparência e a comunicação;

VII - a preservação da memória e dos bens materiais e imateriais do Senado Federal;

VIII - o alinhamento à gestão de riscos corporativos;

IX - a garantia, nos termos da lei, da disponibilidade, da integridade, da confidencialidade e da autenticidade dos ativos de informação do Senado Federal.

CAPÍTULO III

DOS OBJETIVOS

Art. 4º São objetivos da PCGIS:

I - apoiar as unidades organizacionais do Senado Federal no que tange à condução dos procedimentos adequados e as responsabilidades envolvidas no âmbito da gestão de incidentes de segurança da informação;

II - estabelecer diretrizes para a estruturação de planos de gerenciamento de incidentes de segurança da informação;

III - colaborar para a identificação e avaliação de incidentes de segurança da informação, bem como para a adoção das medidas cabíveis relativas à contenção, erradicação e recuperação;

IV - comunicar às partes interessadas pertinentes, em conformidade com as diretrizes estabelecidas, procedimentos e dispositivos legais vigentes acerca da ocorrência e desenvolvimento dos eventos e incidentes de segurança da informação;

V - mitigar danos totais causados por incidentes de segurança da informação que não puderam ser evitados, bem como a sua reincidência;

VI - coadunar o Senado Federal com as leis, normas, regulamentos e outros dispositivos legais vigentes acerca do tratamento de incidentes de segurança da informação;

VII - promover atividades relacionadas a uma cultura corporativa colaborativa de prevenção e resposta a incidentes de segurança da informação;

VIII - promover melhoria contínua dos processos e procedimentos no que tange às melhores práticas existentes para gestão de incidentes de segurança da informação.

CAPÍTULO IV

DAS DIRETRIZES

**Seção I**

**Da Gestão de Incidentes de Segurança da Informação**

Art. 5º A gestão de incidentes de segurança da informação no Senado Federal será composta por atividades preventivas a fim de limitar o número de incidentes que ocorrerão, mediante a seleção e implementação de um conjunto de controles de segurança

adequados e respaldados nos resultados das avaliações de risco realizadas no Senado Federal.

Parágrafo único. Dentre as atividades de prevenção que devem ser realizadas, incluem-se:

I - estabelecer, documentar e implementar planos, processos e procedimentos para tratamento, resposta e recuperação frente aos variados tipos de incidentes de segurança da informação existentes;

II - instrumentalizar o ambiente digital do Senado Federal com processos e ferramentas destinadas a detectar atividades maliciosas relativas aos ativos de informação do Senado Federal;

III - educar os colaboradores sobre os riscos cibernéticos existentes, seus possíveis impactos, atitudes necessárias para sua devida prevenção e mitigação e sobre ações adequadas de resposta a eventos e incidentes de segurança da informação;

IV - utilizar-se de atividades de inteligência contra ameaças cibernéticas para identificar proativamente potenciais atividades maliciosas;

V - estabelecer ferramentas e procedimentos para coletas de dados, de evidências e condução de análises de forense digital relacionadas a incidentes de segurança.

**Seção II**

**Do Gerenciamento de Incidentes de Segurança da Informação**

Art. 6º O gerenciamento de incidentes de segurança da informação no Senado Federal deve ser composto por ações que proporcionem a implementação operacional dos procedimentos, das atividades e dos processos planejados para lidar com quaisquer sinais que possam indicar a ocorrência de um evento ou incidente de segurança da informação que possa comprometer um ativo de informação do Senado Federal.

Parágrafo único. A estruturação das atividades de gerenciamento deverá compreender ao menos as seguintes etapas:

I - detecção;

II - análise;

III - comunicação;

IV - contenção, erradicação e recuperação;

V - atividades pós-incidente.

§ 1º As etapas mencionadas e as atividades correlatas devem estar preparadas para serem conduzidas de maneira iterativa e concorrente, uma vez que evoluem continuamente até que o incidente de segurança da informação seja resolvido.

§ 2º O gerenciamento de um incidente de segurança da informação é considerado completo quando, a depender das características do incidente, ocorra ao menos uma das seguintes condições:

I - um evento de segurança da informação não se materializa em um incidente real;

II - o incidente é confirmado e a confidencialidade, integridade, autenticidade e disponibilidade dos ativos de informação afetados são restaurados ao estado em que se encontravam antes da ocorrência do incidente;

III - as atividades pós-incidente são conduzidas conforme a necessidade e oportunidade das ações.

**Seção III**

**Da Detecção**

Art. 7º A etapa de detecção consiste na recepção da notificação de um evento de segurança da informação ou da identificação de sinais de sua ocorrência, que podem ser resultado da exploração de uma vulnerabilidade de segurança ou resultado de uma atividade não intencional.

Parágrafo único. Dentre os meios para detecção de um incidente de segurança da informação, incluem-se:

I - a percepção de sinais e indicadores da ocorrência de incidentes pelos membros da CETIR conforme disposto no art. 20;

II - a notificação de colaboradores internos e externos por meio de canais disponibilizados;

III - os alertas e notificações gerados por ativos de informação.

Art. 8º Na detecção ou recepção da notificação de um evento de segurança da informação, deve-se utilizar das diretrizes e dos procedimentos definidos pelo Senado Federal para análise e deliberação acerca da necessidade e oportunidade do prosseguimento das atividades para a etapa de análise.

Art. 9º A qualquer momento poderá ser solicitado que o notificante forneça informações adicionais que possam ser necessárias à continuação do gerenciamento do incidente de segurança informação.

**Seção IV**

**Da Análise**

Art. 10. A etapa de análise consiste na realização de atividades com o objetivo de avaliar se um evento de segurança da informação se caracteriza ou não em um incidente de segurança da informação real.

Parágrafo único. Se for verificado que um evento de segurança da informação não se transformou em um incidente de segurança da informação, atividades adicionais na etapa pós-incidente deverão ser realizadas caso sejam identificadas necessidades de melhoria em algum procedimento realizado anteriormente.

Art. 11. No ato da confirmação da ocorrência de um incidente de segurança da informação, os colaboradores responsáveis deverão ser designados e envolvidos adequadamente nas atividades decorrentes.

§ 1º Durante toda a análise e gerenciamento do incidente de segurança da informação deve-se documentar a investigação realizada por meio de procedimentos estabelecidos que propiciem de maneira assertiva a coleta e armazenamento de informações e evidências acerca do incidente.

§ 2º O incidente deverá ter o seu escopo e estado atual identificados para se determinar a abrangência, os ativos afetados e se ainda está em andamento.

§ 3º Para incidentes em curso, deve-se iniciar prontamente as etapas de contenção e erradicação a fim de minimizar danos e prejuízos aos ativos de informação do Senado Federal.

§ 4º O incidente deverá ser classificado e priorizado considerando ao menos os seguintes critérios:

I - as características e tipificação do incidente;

II - como o incidente impactará os processos suportados pelos sistemas de informação afetados;

III - como o incidente impactará a confidencialidade, integridade e disponibilidade das informações afetadas;

IV - a quantidade de tempo e recursos que devem ser gastos na recuperação do incidente;

V - os riscos ao Senado Federal.

§ 5º Os critérios relativos à classificação do incidente serão definidos em ato específico.
Art. 12. No momento em que se possua dados suficientes acerca da natureza, classificação e priorização do incidente de segurança da informação, deve-se iniciar prontamente as atividades necessárias e oportunas para contenção, erradicação e recuperação do incidente.

**Seção V**

**Da Comunicação**

Art. 13. Durante todo o gerenciamento do incidente de segurança da informação, deve-se observar as diretrizes, procedimentos e dispositivos legais vigentes que disponham sobre a necessidade, periodicidade e forma das atividades de comunicação que deverão ser realizadas acerca da ocorrência e desenvolvimento dos eventos e incidentes.

Parágrafo único. A depender da natureza e características do incidente, as partes interessadas a serem comunicadas incluem:

I - os colaboradores internos ou externos;

II -as unidades administrativas do Senado Federal;

III - outros órgãos governamentais;

IV - as equipes de tratamento de incidentes de outros órgãos;

V - as autoridades policiais competentes, nos termos do disposto no item 8.5.1 da Norma Complementar 08, Instrução Normativa 01-DSIC/GSIPR, de 19 de agosto de 2010;

VI - a sociedade.

**Seção VI**

**Da Contenção, Erradicação e Recuperação**

Art. 14. A etapa de contenção consiste na realização de atividades para mitigar a causa raiz do incidente de segurança da informação, a fim de limitar impactos causados como a indisponibilidade de sistemas, até que seja possível prosseguir para sua devida erradicação e recuperação.

§ 1º As atividades de mitigação do impacto deverão observar as características do incidente e poderão incluir, dentre outras atividades necessárias:

I - o isolamento de sistemas e redes;

II - a restrição de acesso a sistemas, informações ou a quaisquer outros recursos de TI como equipamentos e os locais físicos relacionados;

III - a aplicação de atualizações de emergência;

IV - o bloqueio de acesso de contas;

V - o monitoramento intensificado dos ativos de informação do Senado Federal.

§ 2º As atividades de mitigação do impacto a serem realizadas devem ainda levar em conta aspectos que possam:

I - comprometer os serviços mantidos e fornecidos pelo Senado Federal, bem como a confidencialidade, integridade, autenticidade e disponibilidade das suas informações;

II - comprometer a duração, os recursos necessários e a eficácia das atividades a serem realizadas para contenção e erradicação;

III - prejudicar a coleta e a preservação de documentações e evidências acerca do incidente;

IV - prejudicar a imagem e reputação institucional do Senado Federal perante a sociedade.

Art. 15. A etapa de erradicação consiste na realização de ações para remover quaisquer elementos maliciosos presentes no ambiente cibernético bem como para corrigir as vulnerabilidades que possam ter causado o incidente de segurança da informação.

§ 1º As atividades de erradicação devem levar em conta aspectos e práticas que garantam a preservação da documentação produzida e das evidências coletadas acerca do incidente.

§ 2º As atividades de erradicação devem levar em conta a confidencialidade, integridade, autenticidade e disponibilidade dos ativos de informação mantidos e fornecidos pelo Senado Federal. § 3º As atividades de erradicação deverão levar em conta as características do incidente e poderão incluir, dentre outras atividades necessárias:

I - a correção e tratamento de vulnerabilidades;

II - a remoção de malware;

III - a reconfiguração de sistemas e hardware;

IV - a remediação de equipamentos;

V - a reinstalação de softwares e hardware.

Art. 16. A etapa de recuperação consiste na realização de atividades para certificar-se de que todos os elementos nocivos ao ambiente cibernético do Senado Federal foram identificados e erradicados e que os ativos de informação afetados foram restaurados a um estado seguro e operacional.

§ 1º As atividades de recuperação realizadas deverão sobretudo levar em conta, quando existentes, processos de gestão da continuidade de negócios, planos de contingência de sistemas, planos e políticas de backups ou outros normativos correlatos estabelecidos pelo Senado Federal.

§ 2º As atividades de recuperação também deverão levar em conta as características do incidente e poderão incluir, dentre outras atividades que vierem a ser necessárias:

I - a restauração de dados e sistemas a partir de backups;

II - a reconstrução de sistemas;

III - a comunicação adequada aos colaboradores;

IV - a mitigação e recuperação de impactos financeiros e reputacionais.

Art. 17. Nos casos de incidentes em que os ativos de informação tenham a sua integridade, confidencialidade ou disponibilidade comprometidos em larga escala ou por longo período, ou da ocorrência de extenso dano material ou de imagem ao Senado Federal, deverá ser instaurado um Comitê de Crises Cibernéticas composto por membros da CETIR, conforme disposto no art. 20, e pelos titulares da Diretoria-Geral, da Secretaria de Tecnologia da Informação, do Comitê de Segurança da Informação e das áreas afetadas;

Parágrafo único. O Comitê atuará em estado de convocação permanente, enquanto durar a crise, podendo reunir-se a qualquer horário para, sem prejuízo de outras atividades que vierem a ser necessárias:

I - analisar e avaliar os riscos aos quais o ambiente tecnológico do Senado Federal está exposto e elencar os ativos de informação mais críticos;

II - deliberar acerca da priorização e concentração de recursos humanos, tecnológicos e financeiros na condução das atividades de contenção, erradicação e recuperação, de acordo com a criticidade dos ativos envolvidos e com os objetivos estratégicos do Senado Federal;

III - avaliar a necessidade de recursos adicionais para apoiar as atividades de resposta;

IV - definir estratégias adequadas de comunicação com a imprensa e a sociedade.

**Seção VII**

**Das Atividades Pós-Incidente**

Art. 18. Na etapa pós-incidente deve-se realizar atividades para verificar e certificar que:

I - as atividades de contenção, erradicação e recuperação atingiram os objetivos esperados;

II - as evidências necessárias acerca do incidente foram devidamente coletadas e armazenadas;

III - a documentação necessária acerca dos fatos relativos ao incidente foi devidamente produzida;

IV - as partes interessadas pertinentes ao incidente foram comunicadas adequadamente.

Art. 19. Ao final das atividades e considerando a necessidade e oportunidade das ações, deverão ser conduzidas atividades de revisão e análise das atividades realizadas durante o decorrer do incidente a fim de se identificar pontos de melhoria necessários.

§ 1º Os pontos de melhoria, a depender das características e natureza do incidente, podem incluir:

I - a modificação de políticas, planos e processos;

II - a inclusão, remoção ou modificação de papéis e responsabilidades;

III - a inclusão, remoção, modificação ou atualização de ativos de informação;

IV - a realização de atividades de conscientização e treinamento.

§ 2º As melhorias identificadas deverão ser incorporadas aos ativos de informação e às etapas adequadas do processo de gerenciamento de incidentes de segurança da informação observando-se a devida necessidade e oportunidade das ações.

CAPÍTULO V

DA ORGANIZAÇÃO DE PREVENÇÃO, TRATAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICO NO SENADO FEDERAL

Art. 20. Fica criada a Comissão para Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - CETIR, vinculada ao Comitê de Segurança da Informação - CSI, cujo regulamento será definido em Ato da Diretoria-Geral do Senado Federal.

Parágrafo único. Compete à CETIR:

I - planejar, coordenar e executar atividades de tratamento e resposta a incidentes em redes computacionais, preservando os ativos informacionais e de infraestrutura do Senado Federal;

II - manter relacionamento técnico com o sistema público de prevenção, tratamento e resposta a incidentes cibernéticos, notadamente o CTIR Gov - Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo.

Art. 21. Compete aos colaboradores internos, externos e às demais unidades administrativas do Senado Federal relatar qualquer suspeita de evento ou incidente de segurança da informação, seguindo as diretrizes e procedimentos disponibilizados.

Art. 22. Compete a todas as áreas do Senado Federal, no âmbito de suas atribuições, garantir que recursos adequados, incluindo financeiros, tecnológicos e de recursos humanos sejam alocados para implementar e manter a capacidade de gestão de incidentes de segurança da informação.

Art. 23. Compete à Secretaria de Tecnologia da Informação (Prodasen):

I - fornecer liderança eficaz em situações críticas, apoiando a equipe de resposta a incidentes de segurança da informação e tomando decisões operacionais para minimizar os impactos causados;

II - facilitar a colaboração entre diferentes departamentos e setores para garantir uma resposta eficaz a incidentes de segurança da informação, incluindo comunicação transparente e coordenação de esforços.

Art. 24. Compete ao Comitê de Segurança da Informação (CSI):

I - garantir que a gestão de incidentes de segurança da informação seja integrada às práticas gerais de governança de TI e segurança no Senado Federal.

CAPÍTULO VI

DAS DISPOSIÇÕES FINAIS

Art. 25. A PCGIS deverá ser revista e atualizada, sempre que necessário, com vistas a se manter em consonância com os objetivos da organização, com as melhores práticas, dispositivos legais, regulamentos e demais aspectos relativos à gestão de incidentes de segurança da informação.

Art. 26. Os casos omissos serão analisados pelo Comitê de Segurança da Informação, que poderá propor normas complementares à Diretoria-Geral sempre que necessário.

Art. 27. Este Ato entra em vigor na data de sua publicação.

Sala de Reuniões, 17 de dezembro de 2024. Senador **Rodrigo Pacheco** - Presidente, Senador **Veneziano Vital do Rêgo** - 1º Vice-Presidente, Senador **Rodrigo Cunha** - 2º Vice-Presidente, Senador **Rogério Carvalho** - 1º Secretário, Senador **Weverton** - 2º Secretário, Senador **Chico Rodrigues** - 3º Secretário, Senador **Styvenson Valentim** - 4º Secretário, Senadora **Ivete da Silveira** - 2ª Suplente, Senador **Dr. Hiran** - 3º Suplente.

*Publicado:*
*- Boletim Administrativo do Senado Federal, nº 9583, seção 1, de 19 de dezembro de 2024, p. 12.*