Carolus XIII

Royo y Imperad

A.S. 325

* *

No.1 de 2025

Um Ato Relativo à Proteção de Segredos Oficiais contra Divulgação Inapropriada e Prejudicial.

Sanção concedida no dia 31 de janeiro, 2025

SARHOLM

Maya seo donir plisir eun Seito Majis Imperial y Stefanica, pur Seito Majis y pul y pur tel consei y sazion eui tel Parlarmente eui tel Rozirre, comaria tel segeoare:

1. Título Curto Este Ato será conhecido como o Ato de Segredos Oficiais de 325 AS, em resumo.

2. Preâmbulo Em reconhecimento à necessidade de salvaguardar a segurança, soberania e integridade da nação, este Ato estabelece a estrutura para a proteção de informações classificadas críticas para o bem público. Ele delineia as responsabilidades de indivíduos e instituições na preservação de segredos de estado, impedindo divulgações não autorizadas e garantindo o manuseio adequado de materiais sensíveis. Por meio dessas medidas, o Ato busca defender os interesses nacionais, promover a confiança na governança e fortalecer a defesa da nação contra ameaças internas e externas.

2. Autoridade de Classificação Todos os documentos e informações publicados pela *His Imperial Majesty's Stationery* receberão classificações de segurança conjuntamente a critério do Primeiro Ministro de Nova Saróvia e da Agência de Inteligência e Segurança da Coroa, com base no dano potencial à segurança nacional, impacto nas relações internacionais e domésticas de Nova Saróvia, risco à privacidade de qualquer indivíduo e o efeito em operações militares ou civis.

As decisões de classificação devem ser registradas com justificativa básica, bem como revisadas quando necessário; e tornadas públicas aos departamentos relevantes.

3. Níveis e Classificações Haverá quatro tipos de autorizações de segurança - Irrestrita, Protegida, Secreta e Grã-Secreta. Elas serão as classificações oficiais de segurança nacional e estão sujeitas a um memorando de entendimento entre todos os estados e o Governo Saroviano.

Uma classificação de segurança (Protegida, Secreta e GS) só é aplicada a informações (ou ativos que contêm informações, como servidores, canais, conversas DM) se exigir proteção porque o impacto do comprometimento das informações ou ativos seria alto, extremo ou catastrófico.

Irrestrita se aplicará a todos os documentos, canais e informações que são publicados livremente pela *His Imperial Majesty's Stationery*, e não precisam ser explicitamente classificados como Irrestritos, mas podem ser. Protegido significa que a divulgação não autorizada causará danos ao interesse nacional, organizações ou indivíduos. Secreto significa que a divulgação não autorizada causará danos sérios ao interesse nacional, organizações ou indivíduos.

Grã-Secreta significa que a divulgação não autorizada causará danos excepcionalmente graves ao interesse nacional, organizações ou indivíduos. Todos os documentos e conversas escritas entre Ministros, incluindo DMs, discussões de Gabinete, chamadas de voz são automaticamente considerados de GS.

4. Autorizações de Segurança Uma autorização de segurança deve ser uma declaração de garantia de que uma pessoa é elegível e, até onde pode ser determinado no momento em que a autorização é emitida, adequada para ocupar uma posição de confiança que lhe dá acesso a informações, recursos e atividades do Governo Saroviano classificadas como de segurança.

É um julgamento pontual que deve ser acompanhado por um gerenciamento de segurança contínuo daqueles que possuem autorizações para garantir que eles permaneçam adequados. Indivíduos que exigem acesso contínuo a informações, recursos e atividades confidenciais de segurança do Governo Saroviano devem possuir uma autorização de segurança, compatível com sua classificação de segurança. O nível de autorização de segurança exigido não é baseado na patente, antiguidade ou status da pessoa, mas no acesso necessário para desempenhar sua posição identificada.

Uma autorização de segurança ativa é patrocinada e mantida pela Agência de Inteligência e Segurança da Coroa. Todos os Oficiais Comissionados das Forças Armadas Imperiais Sarovianas e todos os Lordes-Tenentes, Membros do Parlamento Provincial e Membros do Parlamento Imperial recebem automaticamente autorização Protegida após o recebimento de seu pergaminho de comissionamento ou seu Juramento de Fidelidade. Membros de Comitês Parlamentares podem receber autorização Secreta para seu comitê específico.

5. Agências de Verificação Autorizadas

O ISC, por ordem da Agência de Inteligência e Segurança da Coroa, conduzirá a verificação de segurança para entidades do Governo Saroviano, a menos que a entidade tenha sido autorizada a conduzir a verificação de segurança para seu próprio pessoal. O ISC deve conduzir a verificação de segurança de forma consistente com este Ato. O termo "analista de verificação" denota uma pessoa dentro do CISA que analisa as avaliações de verificação estabelecidas pelo ISC.

O Rosecuizo, ou um delegado de verificação de segurança, é formalmente autorizado a tomar decisões sobre o resultado de um processo de verificação (ou seja, conceder, negar, conceder condicionalmente, revogar ou cancelar uma autorização de segurança).

6. Elegibilidade para uma Autorização de Segurança

Para ser elegível para uma autorização de segurança do Governo Saroviano, um indivíduo que não obtém automaticamente sua autorização por meio de sua ocupação deve ser um cidadão Saroviano por um mínimo de três anos Stefanic e ser patrocinado para verificação por um indivíduo autorizado. A Agência de Inteligência e Segurança da Coroa pode considerar um histórico como "segurança não verificável", recusando-lhes permanentemente a autorização de segurança.

A Agência de Inteligência e Segurança da Coroa avaliará os Sarovianos sujeitos à verificação de segurança com base nas seguintes características:

a) Honestidade e integridade.
b) Maturidade e julgamento.
c) Estabilidade e confiabilidade.
d) Tolerância e aceitação.
e) Lealdade e comprometimento com Sarovia, seus valores e seu sistema democrático de governo; e
f) Vulnerabilidade a influência imprópria ou coerção.

7. Requisitos de Divulgação

Os sujeitos da autorização devem fornecer consentimento informado explícito para compartilhar as informações necessárias. No mínimo e sob um juramento de verdade, os sarovianos sujeitos à verificação de segurança devem, se necessário, fornecer ao ISC, que fornecerá preocupações à CISA, com:

a) Atividade no Discord nos últimos seis (6) anos Stefanicos; incluindo
b) Outros servidores Discord;
c) Vínculos com potências estrangeiras;
d) Amizades ou relacionamentos significativos feitos em outros servidores ou organizações;
e) Afiliações relevantes em qualquer outra associação nacional nos últimos 12 anos Stefanic,
f) Funções em qualquer comunidade online;
g) Amizades com autoridades estrangeiras; e
h) Rivalidades ou conflitos com estados neutros, amigáveis ou inimigos.

8. Requisitos de Verificação

O ISC verificará essas divulgações por meio de uma revisão manual do histórico acessível do Discord e fornecerá à Agência de Segurança e Inteligência da Coroa seu veredito. A Polícia Imperial Saroviana também pode entrevistar qualquer indivíduo mencionado nessas divulgações.

9. Violações

Violações menores serão definidas como omissões não intencionais de informações não críticas dentro das divulgações; atrasos em relatar alterações (menos de 14 dias de atraso); compartilhamento acidental de informações protegidas com pessoas não autorizadas; falha de comunicação sobre funções ou relacionamentos do servidor que não afetam a segurança e compartilhamento de informações protegidas com pessoas não autorizadas.

Violações graves serão definidas como qualquer declaração falsa intencional para agências de verificação; qualquer omissão de afiliações a nações estrangeiras, funções de liderança em outras comunidades, conflitos conhecidos com indivíduos liberados, incidentes de segurança anteriores; compartilhamento de informações secretas ou ultrasecretas com pessoas não autorizadas; padrão de violações menores repetidas (3 ou mais em 6 meses); falha em relatar violações de segurança conhecidas por terceiros; ocultação ativa de informações relevantes; qualquer violação das disposições definidas nesta Lei.

Violações menores serão decididas pela Agência de Segurança e Inteligência da Coroa, que pode instruir ou delegar instruções ao infrator de que ele foi sancionado. As sanções serão:

a) A primeira infração constituirá uma advertência por escrito;
b) A segunda infração constituirá a suspensão da autorização por um período de 2 anos Stefanic; e
c) A terceira infração será tratada como violação grave.

Violações menores serão decididas pela Crown Intelligence and Security Agency e aprovadas pelo Tribunal, que pode instruir ou delegar instruções ao infrator de que ele foi sancionado se for considerado culpado. As sanções podem ser:

a) Revogação imediata e de autorização;
b) Proibição mínima de 12 anos Stefanic de reaplicação;
c) Aviso público de revogação de autorização;
d) Perda de cargos governamentais atuais onde legalmente aplicável;
e) Proibição de serviço governamental por 24 anos Stefanic;
f) Multa de 50.000 Saros; e

g) Uma revisão por violações de acusações criminais sob o Código de Direito Mathievas, Seções 6 e 8, ou outros, se aplicável.

10. Divulgação Acidental

Omissões não intencionais que são auto-relatadas antes da descoberta, ou corrigidas dentro de 7 dias, ou não relacionadas a questões críticas de segurança podem ser tratadas como questões administrativas em vez de violações, a critério da agência de verificação.

Se qualquer informação que esteja acima de Unrestricted for acidentalmente divulgada, a pessoa que descobrir a divulgação deve:

a) Pare de compartilhar imediatamente;
b) Reporte à CISA em 24 horas; e
c) Documente todos que possam ter visto.

11. Compartilhamento de Informações

As informações só podem ser compartilhadas entre pessoas com autorizações de segurança no mesmo nível ou superior, e somente se ambas as partes tiverem uma necessidade legítima de saber. O compartilhamento de informações com indivíduos que não podem ser justificados como uma necessidade legítima de saber pode ser processado como uma sanção maior ou menor.

12. Compartilhamento de Emergência

Em caso de emergência, que deve ser definida como qualquer ameaça imediata à segurança ou interesses nacionais; incidentes de segurança em andamento, situações diplomáticas críticas, necessidade marcial ou uma ameaça à segurança pessoal, membros do Gabinete, Estado-Maior ou Almirantado da Marinha com acesso Top Secret podem compartilhar informações classificadas com indivíduos não qualificados para possuir essas informações. O compartilhador das informações deve, dentro de sessenta minutos do compartilhamento dessas informações, relatar isso ao Primeiro-Ministro, com uma justificativa detalhada para a emergência, todas e quaisquer medidas tomadas para limitar a exposição e um plano para controlar novos vazamentos de informações. Esses relatórios serão revisados pela Crown Intelligence and Security Agency, que determinará se a emergência foi justificada e se o indivíduo tomou todas as medidas razoáveis para garantir o limite de exposição das informações.

13. Medidas de Controle de Informações

Qualquer informação compartilhada que exija controles e procedimentos de manuseio específicos deve ser claramente marcada como Protegida, Secreta ou Top Secret.

14. Processo de Apelação

Para acesso temporário, a informação deve ser prefixada com "*TEMP ACCESS*" e incluir instruções de manuseio e uma data de expiração. Ao receber informações classificadas, os destinatários devem acusar o recebimento e confirmar explicitamente sua compreensão de quaisquer restrições. Os destinatários são proibidos de compartilhar novamente as informações sem obter nova autorização, devem remover ou restringir o acesso quando o período de compartilhamento expirar e são obrigados a relatar qualquer acesso não autorizado imediatamente.

As negações de liberação podem ser apeladas dentro de 14 dias por:

a) Enviar explicação por escrito;
b) Fornecer novas informações; e

c) Solicitar depoimento do patrocinador.

Os recursos serão revisados somente pela CISA.

15. Manutenção da Folga

Todos os detentores de autorização, uma vez por mês, serão abordados por um membro de uma agência de verificação para coletar qualquer informação sobre novas associações de servidores, relacionamentos com autoridades estrangeiras, conflitos pessoais, funções governamentais e qualquer outra informação adicional.