Política de Segurança da Informação do Observatório Global de Integridade Esportiva (GSIO)

GLOBAL SPORTS INTEGRITY OBSERVATORY

Data da Última Atualização: 02 de Outubro de 2024.

1. Introdução:

O Observatório Global de Integridade Esportiva (GSIO) reconhece a importância fundamental da segurança da informação para o cumprimento de sua missão de promover a integridade no esporte. Esta Política de Segurança da Informação (PSI) estabelece as diretrizes e os controles para garantir a confidencialidade, integridade e disponibilidade das informações tratadas pelo GSIO e pelas entidades certificadas, protegendo-as contra ameaças internas e externas e assegurando a conformidade com as leis, regulamentos e melhores práticas do setor, incluindo a ISO 27001 e outras normas relevantes.

2. Objetivo:

Esta PSI tem como objetivo principal:

- Proteger os ativos de informação do GSIO e das entidades certificadas contra acessos não autorizados, uso indevido, divulgação, alteração ou destruição.
- Garantir a confidencialidade das informações sensíveis e confidenciais.
- Preservar a integridade dos dados, assegurando sua exatidão e confiabilidade.
- Assegurar a disponibilidade das informações para os usuários autorizados quando necessário.
- Promover uma cultura de segurança da informação entre todas as partes envolvidas.
- Atender aos requisitos legais, regulatórios e contratuais aplicáveis.

3. Escopo:

Esta PSI se aplica a todos os membros, colaboradores, parceiros, consultores, fornecedores e entidades certificadas do GSIO, bem como a todos os ativos de informação da organização, incluindo:

- Sistemas de informação, aplicativos e softwares.
- Infraestrutura de rede e servidores.
- Dispositivos móveis e estações de trabalho.
- Documentos físicos e digitais.
- Dados armazenados em nuvem.

4. Gestão de Acessos:

4.1. **Princípio do Menor Privilégio:** O acesso aos sistemas e informações será concedido com base no princípio do menor privilégio, ou seja, apenas o acesso mínimo necessário para o desempenho das funções será autorizado.

4.2. **Autenticação e Autorização:**

- **Autenticação Multifator (MFA):** Será exigida a autenticação multifator para acesso a sistemas críticos e informações sensíveis.
- **Gestão de Identidades e Acessos (IAM):** Será implementado um sistema de IAM para controlar e gerenciar as identidades digitais e os acessos dos usuários.
- **Contas Individuais:** Contas de acesso compartilhadas são estritamente proibidas. Cada usuário deverá possuir uma conta individual com credenciais únicas.
- **Revisão Periódica de Acessos:** Os acessos serão revisados periodicamente para identificar e revogar permissões desnecessárias ou inativas.

4.3. **Segurança Física:**

- **Controle de Acesso Físico:** O acesso a áreas sensíveis, como data centers e salas de servidores, será restrito a pessoal autorizado, utilizando-se controles de acesso como cartões de acesso, biometria e vigilância por câmeras.
- **Proteção Ambiental:** Os ambientes que abrigam equipamentos críticos deverão ser protegidos contra incêndio, inundação, variações extremas de temperatura e outros riscos ambientais.
- **Segurança de Dispositivos:** Dispositivos móveis e laptops deverão ser protegidos com senhas fortes, criptografia de disco e softwares de segurança.

5. Segurança Lógica:

5.1. **Criptografia:** Dados sensíveis, tanto em repouso quanto em trânsito, serão protegidos por meio de algoritmos de criptografia robustos e reconhecidos pelo mercado.

5.2. **Gestão de Vulnerabilidades:**

- **Varreduras de Vulnerabilidades:** Serão realizadas varreduras regulares de vulnerabilidades em sistemas, aplicativos e infraestrutura de rede.
- **Testes de Penetração:** Testes de penetração periódicos serão conduzidos por profissionais qualificados para simular ataques e identificar potenciais falhas de segurança.

- **Correção de Vulnerabilidades:** As vulnerabilidades identificadas serão corrigidas de forma prioritária, seguindo um processo de gestão de patches.

5.3. **Proteção Contra Malware:** Soluções antimalware atualizadas serão instaladas em todos os dispositivos da organização.

5.4. **Firewall e Segmentação de Rede:** A infraestrutura de rede será protegida por firewalls e segmentada para isolar sistemas críticos e limitar o impacto de possíveis incidentes.

5.5. **Segurança em Nuvem:** Quando aplicável, serão adotadas as melhores práticas de segurança em nuvem, seguindo as recomendações dos provedores de serviços em nuvem e as normas de segurança relevantes.

6. Prevenção e Resposta a Incidentes:

6.1. **Prevenção:**

- **Conscientização e Treinamento:** Serão realizados treinamentos regulares sobre segurança da informação para todos os colaboradores e parceiros.
- **Política de Senhas:** Serão estabelecidas diretrizes para a criação e gestão de senhas fortes e únicas.
- **Controles de Segurança:** Serão implementados controles preventivos, como firewalls, sistemas de detecção de intrusão (IDS/IPS) e antivírus.

6.2. **Resposta a Incidentes:**

- **Plano de Resposta a Incidentes (PRI):** O GSIO manterá um PRI documentado, que descreve os procedimentos a serem seguidos em caso de incidentes de segurança.
- **Equipe de Resposta a Incidentes (CSIRT/CERT):** Será designada uma equipe responsável por coordenar a resposta a incidentes.
- **Notificação de Incidentes:** Incidentes de segurança que envolvam dados pessoais serão notificados à ANPD e aos titulares dos dados, conforme exigido pela LGPD.

7. Continuidade de Negócios e Recuperação de Desastres:

O GSIO manterá um Plano de Continuidade de Negócios (PCN) e um Plano de Recuperação de Desastres (PRD) para garantir a continuidade das operações em caso de interrupções causadas por incidentes de segurança ou outros eventos.

8. Conformidade Legal e Regulamentar:

O GSIO se compromete a cumprir todas as leis, regulamentos e normas aplicáveis à segurança da informação, incluindo a LGPD, o Marco Civil da Internet e outras legislações pertinentes.

9. Revisão e Atualização:

Esta PSI será revisada e atualizada periodicamente para garantir sua efetividade e aderência às melhores práticas e à legislação vigente.

10. Glossário:

- **Ativo de Informação:** Qualquer informação que tenha valor para a organização.
- **Autenticação Multifator (MFA):** Método de verificação que combina duas ou mais credenciais para acessar um sistema.
- **Backup:** Cópia de segurança dos dados para recuperação em caso de perda ou corrompimento.
- **Criptografia:** Processo de conversão de dados em um formato ilegível para proteger informações sensíveis.
- **Firewall:** Sistema que monitora e controla o tráfego de rede para impedir acessos não autorizados.
- **Patch de Segurança:** Atualização de software projetada para corrigir vulnerabilidades conhecidas.
- **IAM (Identity and Access Management):** Gestão de Identidades e Acessos.
- **IDS/IPS (Intrusion Detection/Prevention System):** Sistema de Detecção/Prevenção de Intrusão.
- **PCN (Plano de Continuidade de Negócios):** Plano de Continuidade de Negócios.
- **PRD (Plano de Recuperação de Desastres):** Plano de Recuperação de Desastres.

11. Contato:

Dúvidas ou incidentes relacionados a esta política devem ser comunicados imediatamente à equipe de segurança do GSIO através do email: seg-info@gsio-br.org.