**Documento de Segurança da Informação baseado na ISO 27000**  
**Aplicação: Empresa de eSports – Time Profissional de League of Legends**

**1. Introdução**

A Segurança da Informação é um conjunto de práticas, políticas e processos que visam proteger os ativos de informação de uma organização, garantindo que estejam sempre disponíveis, íntegros, confiáveis e acessíveis apenas a pessoas autorizadas.

Os pilares fundamentais são:

* **Confidencialidade:** Garantir que a informação seja acessível apenas a pessoas autorizadas, impedindo a divulgação não autorizada.
* **Integridade:** Assegurar que os dados não sejam alterados, modificados ou corrompidos de forma indevida ou não autorizada, mantendo sua precisão e completude.
* **Disponibilidade:** Garantir que os sistemas e informações estejam acessíveis e utilizáveis por usuários autorizados quando necessário.
* **Autenticidade:** Confirmar a identidade de usuários, sistemas e a origem das informações, assegurando que são quem ou o que afirmam ser.
* **Vulnerabilidade:** Pontos fracos em sistemas, processos ou na infraestrutura que podem ser explorados por ameaças.
* **Ameaças:** Eventos ou circunstâncias que podem comprometer os ativos de informação, como ataques cibernéticos, falhas humanas, desastres naturais, sabotagem ou vazamentos de dados.

No contexto de uma organização de eSports, como um time profissional de League of Legends (LoL), os ativos de informação são diversos e críticos. Eles incluem:

* **Dados estratégicos do time:** Táticas de jogo, análises de adversários, gravações de scrims (treinos), planos de jogo e dados de desempenho de jogadores.
* **Contratos e dados pessoais de jogadores e staff:** Informações financeiras, dados de identificação, termos contratuais e informações de saúde.
* **Plataformas digitais:** Contas em plataformas de streaming (Twitch, YouTube), redes sociais (Twitter, Instagram), e-mail corporativo e plataformas de comunicação interna (Discord, Slack).
* **Infraestrutura de servidores e redes:** Servidores de jogo, servidores de comunicação, redes locais de treino, dispositivos de rede (roteadores, switches) e serviços em nuvem.
* **Estrutura física:** Gaming office, salas de treino, estúdios de transmissão, data centers locais, equipamentos de informática (computadores, monitores, periféricos) e sistemas de controle de acesso físico.

**2. Aplicação da ISO/IEC 27000 e Ciclo PDCA**

O ciclo PDCA (Plan – Do – Check – Act) é uma metodologia essencial para a gestão contínua e a melhoria do Sistema de Gestão de Segurança da Informação (SGSI), conforme preconizado pela ISO 27001. Ele permite que a organização estabeleça, implemente, monitore, revise e melhore o SGSI de forma sistemática e eficaz.

**2.1 Planejamento da Gestão da SGSI (Plan)**

Nesta fase, a organização estabelece os objetivos de segurança, avalia os riscos e define as políticas e processos necessários para gerenciar a segurança da informação.

* **Definição de Objetivos de Segurança:** Proteger os dados de jogo (táticas, resultados, análises), contratos de jogadores e parceiros, informações financeiras e dados pessoais, garantindo a disponibilidade das plataformas de treino e competição.
* **Mapeamento e Avaliação de Riscos:** Identificação e análise de riscos como ataques DDoS durante competições online, vazamento de táticas de jogo, falhas em equipamentos críticos, roubo de dados de jogadores, sabotagem interna ou externa, e interrupção de serviços essenciais. A ISO 27005 é fundamental nesta etapa.
* **Desenvolvimento de Políticas de Segurança:** Elaboração e aprovação de políticas que guiam a segurança da informação, como a utilização de autenticação multifator (MFA) em todos os sistemas críticos, uso obrigatório de VPN para acesso a sistemas remotos, política de senhas fortes, e controle de acesso a áreas físicas restritas.
* **Definição do Escopo do SGSI:** Delimitação clara dos limites do SGSI, abrangendo tanto a segurança de software (servidores, bancos de dados, sistemas internos, aplicações de comunicação) quanto a segurança da infraestrutura física (espaço de treinos, gaming office, computadores, redes locais, pessoas e processos). A ISO 27003 auxilia no planejamento da implementação do SGSI.

**2.2 Implantação (Do)**

Esta fase envolve a implementação das políticas, processos e controles de segurança definidos na fase de Planejamento.

* **Controles de Software:**
  + Implementação de firewalls robustos e sistemas de detecção/prevenção de intrusões.
  + Instalação e manutenção de soluções antivírus e antimalware atualizadas em todos os dispositivos.
  + Configuração de sistemas de monitoramento de logs e eventos para análise proativa de ameaças.
  + Aplicação de políticas de senhas complexas e uso de MFA para contas críticas (e-mails, plataformas de jogo, sistemas financeiros, redes sociais).
* **Controles de Infraestrutura Física e Pessoas:**
  + Implantação de sistemas de controle de acesso biométrico ou por cartão ao gaming office e áreas restritas (salas de servidor, salas de treino estratégico).
  + Instalação de sistemas de vigilância por câmeras com monitoramento contínuo e gravação.
  + Elaboração e implementação de políticas de etiquetagem, inventário e descarte seguro de equipamentos.
  + Programas de treinamento e conscientização em segurança da informação para todos os colaboradores (jogadores, staff técnico, administrativo), abordando engenharia social, phishing e boas práticas de higiene digital.
  + Implementação de políticas claras para visitantes e prestadores de serviço.

**2.3 Checagem (Check)**

Nesta fase, a organização monitora, mede e revisa o desempenho do SGSI em relação aos objetivos e controles estabelecidos.

* **Auditorias Internas:** Realização de auditorias periódicas para verificar a conformidade com as políticas de segurança, revisar logs de acesso aos sistemas, inspecionar a integridade dos backups e analisar relatórios de incidentes de segurança.
* **Testes Periódicos:** Condução de testes de penetração em sistemas e aplicações, varreduras de vulnerabilidades, e testes de intrusão física simulada para avaliar a eficácia dos controles de acesso e segurança física.
* **Monitoramento Contínuo:** Análise em tempo real de vulnerabilidades, monitoramento de tráfego de rede para detecção de anomalias (como ataques DDoS), e revisão constante das atualizações de segurança e configurações de sistemas. A ISO 27004 fornece diretrizes para a medição do desempenho da segurança da informação.
* **Revisão da Gestão:** Avaliações regulares pela alta gerência para analisar o desempenho do SGSI, resultados das auditorias e adequação aos objetivos de negócio.

**2.4 Ações de Melhoria Contínua e Revisão (Act)**

Com base nos resultados da fase de Checagem, a organização toma ações corretivas e preventivas para melhorar continuamente o SGSI.

* **Aplicação de Melhorias:** Implementação de correções e aprimoramentos identificados nas auditorias, testes e revisões, abordando vulnerabilidades e não conformidades.
* **Treinamento Contínuo:** Capacitação e reciclagem periódica de jogadores e equipe administrativa sobre novas ameaças, políticas de segurança atualizadas e melhores práticas.
* **Atualização da Política:** Revisão e atualização das políticas, procedimentos e controles de segurança para incluir novos riscos, tecnologias ou requisitos regulatórios.
* **Revisão Anual do SGSI:** Realização de uma revisão completa do SGSI para garantir sua contínua adequação, suficiência e eficácia, assegurando a aderência às normas ISO e a evolução da maturidade de segurança da organização.

**3. Aplicação em Duas Versões: Software vs. Infraestrutura Física e Pessoas**

Para garantir uma segurança abrangente, o SGSI da organização de eSports deve ser abordado sob duas perspectivas distintas, mas interligadas: a segurança em software e a segurança da infraestrutura física e das pessoas.

**3.1 Segurança da Informação em Software (Sistemas e Dados Digitais)**

Esta versão foca na proteção dos ativos de informação que residem em formato digital, sistemas, redes e aplicações.

* **Normas ISO Relevantes:**
  + **ISO 27001:** Define os requisitos para o estabelecimento, implementação, manutenção e melhoria contínua de um SGSI, sendo a base para a gestão de riscos e controles de sistemas, dados e redes.
  + **ISO 27002:** Fornece um código de prática para controles de segurança da informação, com orientações detalhadas sobre gestão de acesso, criptografia, segurança de rede, aquisição, desenvolvimento e manutenção de sistemas, e gestão de incidentes.
  + **ISO 27003:** Oferece diretrizes para a implementação de um SGSI, auxiliando no planejamento e execução dos controles de segurança digital.
  + **ISO 27004:** Trata da medição do desempenho da segurança da informação, com foco em métricas para tempo de resposta a incidentes de software, taxa de detecção de vulnerabilidades e eficácia dos controles de acesso lógico.
  + **ISO 27005:** Foca na gestão de riscos de segurança da informação, essencial para a análise de riscos de ataques online (phishing, malware, ataques DDoS, vazamento de senhas) e a mitigação proativa.
  + **ISO 27701:** Extensão da ISO 27001 e 27002, com requisitos específicos para a gestão da privacidade da informação (PIMS), garantindo a conformidade com regulamentações de proteção de dados como LGPD e GDPR no tratamento de dados pessoais de jogadores, fãs e colaboradores.
* **Exemplos Práticos:**
  + Proteção robusta de credenciais de contas em plataformas de jogos (Riot Games, Steam) com autenticação multifator e senhas exclusivas.
  + Uso de redes privadas virtuais (VPNs) dedicadas e criptografadas para todas as sessões de scrims e treinos remotos, protegendo contra interceptação de dados e ataques man-in-the-middle.
  + Políticas de atualização rigorosas para patches de segurança em sistemas operacionais, aplicações e servidores de jogo, para corrigir vulnerabilidades conhecidas.
  + Implementação de firewalls de aplicação web (WAF) para proteger plataformas de streaming e sites contra ataques cibernéticos.
  + Segregação de redes para ambientes de treino, competição e administração, limitando o impacto de possíveis incidentes.

**3.2 Segurança da Informação em Infraestrutura Física e Pessoas**

Esta versão aborda a proteção dos ativos físicos da organização, das instalações e dos aspectos relacionados ao comportamento humano e aos processos.

* **Normas ISO Relevantes:**
  + **ISO 27001:** Aplica-se aos controles físicos (como segurança do perímetro e áreas de segurança física) e à gestão de segurança de pessoal.
  + **ISO 27002:** Oferece um código de prática para controles de segurança física e ambiental (acesso físico, segurança de equipamentos, proteção contra desastres naturais) e segurança de recursos humanos (antes, durante e após o emprego).
  + **ISO 27003:** Auxilia no planejamento da implementação do SGSI, incluindo a definição de procedimentos para controle de acesso físico, planos de evacuação e políticas para visitantes e fornecedores.
  + **ISO 27004:** Para métricas de desempenho de segurança física, como a quantidade de incidentes físicos relatados, o tempo médio de resposta a alarmes ou a taxa de conformidade com as políticas de controle de acesso.
  + **ISO 27005:** Essencial para a análise de riscos físicos, como roubo de equipamentos, espionagem, vandalismo, incêndios, inundações e acesso não autorizado a instalações.
  + **ISO 27701:** Aplica-se à proteção de dados pessoais em formato físico (documentos impressos, contratos) e à gestão de privacidade em relação ao pessoal (dados de funcionários, jogadores), garantindo a conformidade legal.
* **Exemplos Práticos:**
  + Instalação de catracas eletrônicas, leitores biométricos ou sistemas de cartão de acesso para controlar a entrada e saída do gaming office e áreas restritas.
  + Configuração de salas de treino estratégico com acesso altamente restrito, limitando a entrada apenas à equipe técnica e aos jogadores envolvidos, e com monitoramento por CFTV.
  + Desenvolvimento e comunicação de procedimentos de evacuação claros e treinamento de brigada de incêndio para a equipe.
  + Uso de cofres à prova de fogo e armários seguros para guardar documentos e contratos impressos (como contratos de jogadores, acordos de patrocínio).
  + Implementação de políticas de "mesa limpa e tela limpa" para evitar a exposição inadvertida de informações confidenciais.
  + Realização de inventário detalhado e periódico de todos os equipamentos do gaming office, incluindo números de série e localização.

**4. Checklist de Segurança da Informação**

Este check-list oferece uma lista de verificação para auxiliar na auditoria e monitoramento contínuo da segurança da informação em ambas as esferas.

**4.1 Check-list de Software (Sistemas e Dados Digitais)**

1. Verificar se os logs de todos os sistemas críticos (servidores, firewalls, aplicações) estão sendo gravados, armazenados com segurança e revisados periodicamente.
2. Confirmar que todos os dispositivos (PCs de jogadores, notebooks de staff, servidores) possuem soluções antivírus/antimalware atualizadas e funcionando corretamente.
3. Garantir o uso obrigatório de Autenticação Multifator (MFA) em todas as contas consideradas críticas (e-mail corporativo, acesso a servidores, plataformas de streaming, contas de jogos e sistemas administrativos).
4. Monitorar ativamente possíveis ataques DDoS durante períodos de competições ou eventos importantes, com planos de mitigação pré-definidos.
5. Revisar e exigir a atualização de senhas e credenciais de acesso a sistemas administrativos, servidores e plataformas críticas a cada 90 dias, no máximo.
6. Verificar se há um plano de resposta a incidentes de segurança cibernética testado e atualizado.
7. Validar a política de descarte seguro de dados digitais em equipamentos ou mídias.

**4.2 Check-list de Infraestrutura Física e Pessoas**

1. Verificar o funcionamento adequado e a gravação contínua das câmeras de segurança (CFTV) e dos sistemas de alarme de intrusão e incêndio.
2. Conferir se o controle de acesso biométrico/por cartão ao prédio e às áreas restritas está ativo, funcionando corretamente e com as permissões atualizadas.
3. Validar se há uma política clara de visitantes e prestadores de serviço, incluindo registro de entrada/saída e acompanhamento.
4. Garantir que todos os colaboradores (jogadores, staff) receberam treinamento inicial e reciclagens periódicas em segurança da informação, incluindo conscientização sobre ameaças físicas e comportamentais.
5. Conferir a integridade, validade e localização dos extintores de incêndio e a sinalização adequada das rotas de evacuação de emergência.
6. Realizar inventário atualizado de todos os equipamentos do gaming office, garantindo que estejam devidamente etiquetados e protegidos contra roubo.
7. Confirmar o descarte seguro de documentos e mídias físicas confidenciais (destruição por fragmentação, incineração).
8. Garantir que os equipamentos críticos (servidores, roteadores principais) estejam fisicamente protegidos em racks ou salas com acesso restrito e controle ambiental.
9. Verificar se há um plano de contingência para falhas de energia e outros desastres naturais.

**5. Conclusão**

A implementação e a gestão de um Sistema de Gestão de Segurança da Informação (SGSI) baseado na família de normas ISO 27000 é um imperativo estratégico para uma empresa de eSports como um time profissional de League of Legends. A segurança vai muito além da proteção digital, abrangendo a salvaguarda da infraestrutura física, a capacitação do capital humano e a preservação da reputação da marca.

Ao adotar o ciclo PDCA, a organização estabelece um framework robusto que permite uma melhoria contínua em segurança. Este processo iterativo minimiza os riscos de forma proativa, garantindo a integridade, a disponibilidade e a confidencialidade das informações críticas. A aderência às diretrizes das ISOs 27001, 27002, 27003, 27004, 27005 e 27701 assegura uma abordagem holística e em conformidade com as melhores práticas internacionais.

Com um SGSI bem implementado e mantido, o time profissional de League of Legends não apenas protege seus ativos mais valiosos – desde táticas de jogo até dados pessoais de jogadores –, mas também consolida sua posição competitiva e a confiança de patrocinadores, jogadores e sua crescente base de fãs. A segurança da informação torna-se, assim, um diferencial competitivo e um pilar fundamental para o sucesso e a longevidade da organização no cenário global dos eSports.