RIASPORT

RED ESTATAL DE INVESTIGACIÓN APLICADA SOBRE SEGURIDAD DEPORTIVA

LA SEGURIDAD DEPORTIVA A DEBATE IV

EDITORES

JOANA COSTA
DIMAS PINTO
GABRIEL FLORES ALLENDE
ANA MARÍA MAGAZ GONZÁLEZ
MARTA GARCÍA TASCÓN

EDITORIAL DYKINSON

Ailton Fernando Santana de Oliveira

Aldina Sofia Silva

Ana María Gallardo Guerrero

Ángeles Miranda Martínez

António João Mendes de Jesus Brandão

Ariana Linette Acosta González

Blanca López Catalán

Bruno Avelar-Rosa

Cairo Gabriel Borges Junqueira

Carlos Herrera Pombero

Cristina Pedrosa Leis

Daniel Duclos-Bastías

Darío Pérez Brunicardi

David Alarcón Rubio

Dimas Pinto

Gabriel Flores Allende

Gonçalo Dias

Inês Oliveira Gonçalves

Joana Costa

Joana Rodrigues Carvalho

José Carlos Jaenes Sánchez

Jorge García-Unanue

José Luís Felipe

José Luis Gómez Calvo

Juan Antonio Arjona González

Keyla Andrea Porras Ramírez

Leonor Gallardo-Guerrero

Luis López Catalán

María del Pilar Méndez Sánchez

María José Arenilla Villalba

María José Maciá Andreu

Marta García Tascón

Miguel Nery

Noelia González-Gálvez

Omar Velarde Martínez

Oscar David Bolívar Silva

Pablo Caballero Blanco

Pablo González García

Patricia I. Jaenes-Amarillo

Paulo Pinheiro

Rafael Peñaloza Gómez

Raquel Aparicio-Mera

Raquel Morquecho Sánchez

Raquel Vaquero-Cristóbal

Roberto Silva Piñeiro

Rui Mendes

Sandrielly Lavínia Andrade Santos

LA SEGURIDAD DEPORTIVA A DEBATE IV

Joana Costa

Dimas Pinto

Gabriel Flores Allende

Ana María Magaz González

Marta García Tascón

Editores

DYKINSON

Este libro ha sido sometido a evaluación por parte de nuestro Consejo Editorial.
Para mayor información, véase *www.dykinson.com/quienes_somos*.

La Red "RIASPORT Red estatal de investigación aplicada sobre seguridad deportiva"
ha sido financiada con cargo a la Convocatoria de concesión de ayudas
para la creación de «Redes de Investigación en Ciencias del Deporte»
para el año 2019, con el número de expediente 03/UPB/19
y resolución del día 26 de julio de 2019.
También, con cargo a la Convocatoria de ayudas a
«Redes de Investigación en Ciencias del Deporte» para el año 2021,
con el número de expediente 14/UPB/21
y resolución de 20 de julio de 2021 y,
mediante el expediente 32/UPB/23, resolución de 16 de mayo para el año 2023

Los autores agradecen al Grupo PAIDI MOTIVADO2
(Movimiento, Técnicas de intervención, Valores, Aprendizaje, Deporte y Seguridad)
de la Universidad Pablo de Olavide, Sevilla-España, la financiación para publicar este libro.

Editorial DYKINSON, S.L.
Meléndez Valdés, 61 – 28015 Madrid
Teléfono (+34) 91544 28 46 – (+34) 91544 28 69
e-mail: *info@dykinson.com*
http://www.dykinson.es / http://www.dykinson.com

ISBN: 979-13-7047-062-3
DOI: https://doi.org/10.14679/4784

Maquetación:
Realizada por los autores

ÍNDICE

Bloque II
Aplicación de tecnología en la seguridad en entidades deportivas

Bloque III
Otras perspectivas aplicadas a la seguridad deportiva

Bloque IV
Seguridad deportiva para diferentes usuarios/as

Capítulo 7.
Segurança digital no desporto

Doutor D. Paulo Pinheiro
Cedis, Lisboa, Portugal
Orcid 0000-0002-8912-2244

DOI: https://doi.org/10.14679/4816

1. INTRODUÇÃO

A crescente visibilidade dos eventos desportivos, da prática desportiva e a conectividade digital agudizaram os problemas de garantia da segurança e integridade de todos. Incidentes do passado demonstram que a ausência de adequadas medidas de segurança pode resultar em sérias consequências. Incidentes graves como os de Heysel (1985), Hillsborough (1989) e Kanjuruhan (2022) destacam falhas de segurança em eventos esportivos, resultando em centenas de mortes por superlotação, instalações inseguras, e intervenções inadequadas. Estes incidentes expõem problemas de planeamento, coordenação e segurança das instalações e de acessos.

Atualmente, as tecnologias são utilizadas para ajudar a evitar situações como as referidas. As instalações passaram a dispor de sistemas de controlo de acessos de espetadores, utentes, funcionários e veículos, sistemas de deteção de fumo ou de incêndio, de vídeo vigilância, etc., que funcionam de forma interligada utilizando recursos de armazenamento e processamento de sistemas informáticos.

Por outro lado, as crescentes necessidades administrativas e de gestão das organizações levaram ao armazenamento de dados em bases de dados com

informação sensível que, para estar em conformidade com as normas e legislação, necessita de estar segura.

A necessidade de segurança informática das organizações desportivas não difere de organizações de outras áreas. Contudo, a informação gerada pelas tecnologias usadas quer na esfera individual de atletas e praticantes como das próprias organizações desportivas que suportam atividades e eventos, cria riscos próprios e suscita particular atenção. Os sistemas informáticos, em rede ou isolados, com ligação à internet ou não, que, no seu todo, são o sistema de informação da organização, requerem ações para proteção e segurança de comunicações, hardware, software, dados, processos e pessoas.

Incidentes em organizações desportivas relacionados com falhas de segurança e ataques a estes sistemas são cada vez mais frequentes e podem provocar prejuízos avultados ou mesmo danos com consequências graves para atletas e praticantes, clubes, autoridades desportivas nacionais ou mesmo internacionais. Em 2014, o *New York Times* publicou uma história sobre um ataque cibernético à Agência Mundial Antidoping, que expôs informações médicas privadas e evidências de doping de atletas olímpicos que testaram positivo para drogas proibidas, mas que depois obtiveram o chamado certificado de "exceção de uso terapêutico" (Greenwald, 2017). Nos Jogos Olímpicos de Inverno de 2018, em Pyeongchang, na Coreia do Sul, um ataque cibernético causou a queda do site oficial, impedindo espectadores de obterem bilhetes, e comprometeu a cobertura Wi-Fi durante a cerimónia de abertura (Rascagneres & Mercer, 2018). Em 2020, ocorreu uma violação de perfis no iCloud de atletas do Reino Unido, resultando na exposição online de fotografias e vídeos íntimos (Pinko, 2021). Em Portugal, decorre ainda o processo jurídico do caso em que foram divulgados documentos confidenciais e informações sensíveis através da plataforma Football Leaks, na sequência de acessos ilegítimos e violação de correspondência. E muitos outros poderiam ser citados.

A crescente relevância da segurança em ambientes desportivos reflete a compreensão de que a proteção vai além dos limites do campo de jogo e treino, sendo necessário ter uma visão holística e integrada de todos os pontos-chave necessários para proporcionar maiores níveis de segurança, e esta passa sem dúvida

pela segurança informática. Neste contexto, a segurança informática das organizações, e em particular das organizações desportivas, não pode ser descurada.

Este documento visa abordar as questões de segurança informática no âmbito no desporto, de forma a ajudar as organizações desportivas a protegerem-se contra ameaças e ataques. Neste sentido, apresentamos na seção 2 os fundamentos da segurança informática, e na seção 3 as principais vulnerabilidades e ameaças a que as organizações em geral estão sujeitas. Na seção 4 apresentamos o que tem sido as principais ameaças e ataques a organizações desportivas. Na seção 5 apresentamos legislação relevante, e na seção 6 apresentamos as medidas de segurança que podem ser tomadas. Na seção 7 abordamos o impacto das tecnologias emergentes na cibersegurança, e por fim, na seção 8 apresentamos as conclusões.

2. FUNDAMENTOS DA SEGURANÇA INFORMÁTICA

A segurança informática ou cibersegurança tem o foco específico na proteção de dados, sistemas e redes contra ameaças que comprometem sua operação, privacidade e fiabilidade. A segurança da informação baseia-se em princípios fundamentais que orientam o desenvolvimento de estratégias e tecnologias voltadas à mitigação de riscos e ao fortalecimento da resiliência digital. A segurança da informação destina-se a preservar a confidencialidade, integridade e disponibilidade da informação (ISO/IEC 27000:2018, 2018) (National Institute of Standards and Technology (NIST) et al., 2017). Estes princípios estão na base da construção de sistemas de gestão de segurança da informação (SGSI).

A confidencialidade indica que a informação não pode ser divulgada ou disponibilizada a indivíduos, entidades ou processos não autorizados. Esta propriedade está intimamente relacionada com a Privacidade, que assegura que os indivíduos têm o poder de decidir que informação sua pode ser recolhida e armazenada, por quem e a que fim se destina.

A integridade é a propriedade que caracteriza a precisão e completude da informação. Este conceito abrange a integridade da informação que garante que a mesma apenas é alterada de forma única e autorizada; e a integridade dos sistemas,

que garante que estes executam de forma integra as funções para que foram criados, e que não podem ser manipulados de forma acidental ou deliberada para operar outra função que não aquela para que foram criados.

A disponibilidade refere-se à prontidão do sistema para responder sempre que necessário a utilizadores autorizados. A perda de disponibilidade significa a interrupção do acesso, do uso de informações, ou do uso do sistema de informação.

Conforme refere Stallings (2014), embora estes três conceitos estejam bem definidos no que concerne aos objetivos de segurança, há quem defenda que são necessários conceitos adicionais como a autenticidade, a responsabilização, o não-repúdio, e a confiabilidade.

A autenticidade é a propriedade que garante que uma entidade é quem afirma ser. É a propriedade de ser genuíno, em que a origem pode ser verificada e é de confiança. A responsabilização indica que as ações de uma entidade podem ser rastreadas e apontam univocamente para essa entidade. O não-repúdio é a capacidade de provar a origem da ocorrência de determinado evento ou ação. E a confiabilidade refere-se a obter comportamentos e resultados consistentes e intencionais.

Como parte integrante de um SGSI definem-se os ativos e os controlos. Um ativo é qualquer coisa que tem valor para a organização. Pode ser um ativo primário, como informação, atividades ou processos de negócio; ou pode ser um ativo de suporte aos bens primários, como o hardware, o software, a rede, o site, ou mesmo o pessoal.

Um controlo é uma medida ou um mecanismo implementado para gerir os riscos relacionados com a segurança da informação. Os controlos, que podem ser preventivos, de deteção ou corretivos, têm por objetivo proteger a confidencialidade, a integridade e a disponibilidade dos ativos, garantindo o cumprimento dos requisitos de segurança.

Uma vulnerabilidade é uma fraqueza de um ativo ou de um controlo que pode ser explorado por uma ou mais ameaças. Uma ameaça é uma causa potencial de um incidente indesejado e que pode resultar em danos num sistema ou organização. Um ataque é uma tentativa para destruir, expor, alterar, desativar, roubar ou ganhar acesso não autorizado, ou fazer uso não autorizado de um ativo.

Interessa realçar adicionalmente o conceito de criptoanálise. Para garantir maiores níveis de segurança no armazenamento e transmissão de dados, usam-se cifras. Estas cifras são protocoladas entre o originador e o destinatário, de forma a impedir que os dados sejam acessíveis por terceiros. A criptoanálise é o estudo e utilização de técnicas para decifrar uma mensagem, sem qualquer conhecimento dos detalhes da cifra. A criptoanálise procura contrariar a criptografia que estuda esquemas de cifrar dados de modo que possam ser armazenados e transmitidos de forma segura.

3. VULNERABILIDADES, AMEAÇAS E ATAQUES

A segurança da informação enfrenta desafios cada vez maiores num cenário digital em constante evolução, com vulnerabilidades, ameaças e ataques que se adaptam rapidamente. Para auxiliar na criação de estratégias preventivas e reativas de defesa, organizações como a *International Standard Organization* (ISO) e o *National Institute of Standards and Technology* (NIST) propõem classificações para organizar e abordar essas vulnerabilidades e ameaças. Neste documento seguimos uma classificação baseada na ISO.

3.1. Vulnerabilidades

Uma primeira grande vulnerabilidade surge ao nível processual quando a organização não tem uma política de segurança que indique como gerir dados, acessos e lidar com incidentes, ou, existindo, não prevê um sistema de melhoria continua do sistema de segurança, e/ou não contempla uma gestão do risco que permita identificar, priorizar e mitigar riscos relevantes.

A forma como a organização monta o seu sistema de informação pode revelar vulnerabilidades. Se o sistema de informação está *OnPremises,* ou seja, implementado

dentro da própria organização, podem surgir vulnerabilidades relacionadas com as infraestruturas físicas, nomeadamente no acesso físico não controlado a servidores, a equipamentos de rede ou outros ativos críticos. Se por outro lado a organização utiliza serviços na nuvem, configurações inadequadas podem expor dados sensíveis. Atualmente é comum as organizações disporem de sistemas mistos, pelo que ambos os tipos de vulnerabilidade devem ser considerados.

De um ponto de vista técnico, as vulnerabilidades podem surgir de configurações incorretas de sistemas (níveis de permissão excessivo, falta de encriptação, portos abertos desnecessariamente, etc.), de redes mal segmentadas, e de utilização de software, algoritmos e protocolos obsoletos cujas falhas de segurança já foram detetadas e exploradas anteriormente. Também a falta de planos de backup eficazes, bem como os respetivos planos de recuperação e/ou de redundância, tornam os sistemas mais vulneráveis a ataques e desastres.

As vulnerabilidades relacionadas com a gestão de identidades e acessos, e as vulnerabilidades humanas acabam por estar relacionadas, dado que as primeiras viabilizam mais facilmente ataques nas segundas. As vulnerabilidades relacionadas com a gestão de identidades e acessos dizem respeito a permitir usar credenciais fáceis de adivinhar, não implementar sistemas de autenticação multifator (combinação de mais do que um sistema de identificação como por exemplo indicar um endereço de email e senha de acesso, confirmado com indicação de código enviado por SMS), e/ou deixar contas de antigos colaboradores ativas.

As vulnerabilidades humanas referem-se às tentativas de logro ou manipulação de funcionários e utilizadores que os levem a revelar informações confidenciais, e à comum falta de consciencialização e formação sobre configurações dos dispositivos e práticas seguras de utilização dos sistemas de informação. Funcionários, subcontratados ou outros utilizadores internos à organização, insatisfeitos e mal-intencionados, podem explorar os seus privilégios de acesso para prejudicar o sistema informático e consequentemente a organização.

A falta de colaboração entre as organizações, governos e outros atores, quer por falta de partilha de dados sobre ameaças ou incidentes ocorridos, quer na intervenção contra ameaças globais é apontada como outra vulnerabilidade.

A. Ameaças e Ataques

As preocupações atuais enquadram-se essencialmente em cinco tipos de ameaça:

i. ataques de engenharia social, que consistem na aplicação de truques, psicológicos ou físicos, sobre utilizadores legítimos de sistemas computacionais, de forma a obter-se conhecimento e informação que permita acesso a esse sistema (Mamede, 2006); Este tipo de ameaça pode ser levado a cabo por ataques de *Phishing*, *Pretexting*, etc.
ii. proliferação de software malicioso (*malware*), definido como software ou *firmware* criado com a intenção de executar processos não autorizados que irão ter um impacto adverso na confidencialidade, integridade ou disponibilidade do sistema (National Institute of Standards and Technology (NIST) et al., 2017). A Tabela 1 identifica alguns tipos de software malicioso.

Tabela 1. Tipos de malware

Malware	**Descrição**
Virus	Software que se anexa a ficheiros ou programas e se propaga quando são abertos ou partilhados.
Worm	É diferente do vírus porque não necessita de um ficheiro hospedeiro. Replicam-se automaticamente consumindo recursos de rede.
Trojans	Software disfarçado de software legítimo que permite o acesso de hackers.
Spyware	Monitoriza as atividades do utilizador, recolhendo informações, como dados pessoais, senhas e outro tipo de informação sem o seu consentimento.
Adware	Apresenta publicidade indesejada e pode redirecionar o utilizador para outros sites de publicidade.
Ransomware	Este tipo de *malware* criptografa a informação do sistema vítima e exige um resgate, normalmente em criptomoeda, para desencriptar de novo a informação.
Keyloggers	Software que regista tudo o que o utilizador introduz no teclado, incluindo senhas de acesso.
Bots	*Malware* que permite que os dispositivos infetados sejam controlados remotamente por um atacante.

iii. ataques à privacidade, na perspetiva de aceder e/ou roubar informações pessoais. Este tipo de ataque pode envolver técnicas de engenharia social, software malicioso, tentativas de adivinhar as senhas, interceção de comunicações, redireccionamento para sites maliciosos, ou outras.

iv. *hacking*, definido como a tentativa e acesso não autorizado a dados, a sistemas, redes ou outros dispositivos digitais. Para atingir os seus objetivos, os hackers podem provocar negação do serviço, explorar vulnerabilidades de aplicações, injetar código malicioso, etc.
Apesar deste tipo de atividade estar conotada com atos maliciosos com o intuito de roubar dados, causar danos ou interromper atividades, existem atividades de *hacking*, designado *hacking* ético, que visa testar sistemas de segurança para melhorar a proteção contra ataques;

v. Los ataques do dia-zero correspondem à exploração de vulnerabilidades de software, sistemas ou dispositivos que ainda não foram detetadas. Designa-se por dia-zero exatamente porque os programadores ou produtores têm zero dias para corrigir a falha antes que a mesma venha a ser explorada. A probabilidade de sucesso destes ataques é maior porque não há defesas identificadas e as defesas existentes não os conseguem identificar e impedir.

A Tabela 2 apresenta uma lista de técnicas de ataque que podem ser levadas a cabo na exploração das vulnerabilidades referidas.

Por outro lado, a utilização cada vez maior de aplicações web abre a porta a uma nova série de vulnerabilidades e ameaças. O *Open Web Application Security Project* (OWASP) (2024), uma iniciativa sem fins lucrativos que visa melhorar a segurança do software, em especial das aplicações web, atualiza periodicamente uma lista dos dez maiores riscos a que estas aplicações estão sujeitas. O *Top Ten* de 2021 é apresentado na Tabela 3 (OWASP Project, 2021).

Tabela 2. Técnicas de ataque

Técnica	Descrição
Phishing *Voice phishing* *SMS phishing*	Envio de mensagens fraudulentas para levar os utilizadores a revelar informações pessoais ou a clicar em links maliciosos por email, por telefone ou por SMS
Pretexting	Criação de um cenário falso, como p.e. ser um funcionário de suporte técnico ou bancário, para levar a vítima a fornecer informações privadas
Quid Pro Quo	É oferecido um serviço em troca de informações confidenciais
Tailgating	Acesso a áreas restritas seguindo alguém que tem a devida autorização de acesso
Dumpster Diving	Procurar informações confidenciais no lixo da vítima
Deny of service	Sobrecarga de servidores ou redes de forma a impedir a sua disponibilidade
Brute force attack	Tentativas repetidas que exploram todas as possibilidades para adivinhar senhas de acesso ou chaves criptográficas para obter acesso não autorizado
Identity theft	Uso de informações roubadas para obter acesso a informação não autorizada ou com o intuito de cometer fraude
Credential stuffing	Obtenção de credenciais válidas num sítio e reutilização noutros sítios
Password spraying	Combinação de uma lista de senhas de acesso comuns em ataques de força bruta contra vários sítios
Man-in-the-middle	Interceção de comunicação para roubar informações confidenciais
DNS spoofing	Redirecionamento para sites maliciosos semelhantes a sites legítimos, onde são solicitadas informações que podem ser usadas posteriormente para aceder a sistemas ou contas bancárias

Tabela 3. OWASP Top Ten

Vulnerabilidade	Descrição
Broken Access Control	Falhas no controlo de acesso permitem que utilizadores não autorizados acedam a recursos ou funções a que não estão autorizados
Cryptographic Failures	Problemas relacionados com a implementação ou uso inadequado de algoritmos criptográficos
Injection	Vulnerabilidades que permitem a injeção de código malicioso através da aplicação
Insecure Design	Falha no design das aplicações que não contemplam a implementação de medidas de segurança nas etapas iniciais de desenvolvimento
Security Misconfiguration	Configurações mal geridas ou inseguras
Vulnerable and Outdated Components	Utilização de bibliotecas, *frameworks* e software obsoleto, com vulnerabilidades conhecidas
Identification and Authentication Failures	Problemas de autenticação e de gestão de identidades, como a utilização de passwords fracas ou *tokens* de sessão mal protegidos
Software and Data Integrity Failures	Falhas relacionadas com a integridade do software, como a ausência de verificações de assinatura em atualizações
Security Logging and Monitoring Failures	Falha ou inexistência de monitorização e registos de segurança que dificultam a deteção e resposta a incidentes
Server-Side Request Forgery	O servidor web é levado a solicitar dados a outros sistemas em nome do atacante

4. AMEAÇAS E ATAQUES A ORGANIZAÇÕES DESPORTIVAS

As organizações desportivas têm atualmente grande atividade online, e a grande maioria detém informação pessoal dos seus atletas, praticantes e funcionários. Os ataques cibernéticos a estas organizações podem gerar impactos variados, desde fraudes milionárias envolvidas na venda de produtos, serviços ou bilhetes online, até a exposição de dados pessoais sensíveis que podem levar à aplicação de multas por incumprimento da legislação vigente decorrentes do manejo inadequado de informações pessoais e sensíveis. Na Europa, a penalização por incumprimento ou violação do Regulamento Geral de Proteção de Dados Pessoais (RGPD)

contempla a aplicação de multas que iniciam em dez milhões de euros ou 2% da faturação anual (o que for maior).

Os ataques cibernéticos contra organizações desportivas são comuns. Numa sondagem realizada pelo *National Cyber Security Centre* (NCSC) no Reino Unido (2019), 70% das organizações entrevistadas relataram pelo menos um ataque por ano, e 30% registaram acima de cinco incidentes nos últimos 12 meses. Aproximadamente 30% desses incidentes provocaram um dano financeiro médio de 10000 libras por incidente. Este número é significativamente maior do que a média verificada em organizações de outros setores de atividade.

A Tabela 4 mostra a percentagem de organizações que foram alvo de cada tipo de ataque.

Tabela 4. Tipos de ataque a organizações desportivas (extraído de (National Cyber Security Centre, 2019)

Falhas de acesso	Desligar de websites ou serviços online	8%
	Perda de acesso temporário a ficheiros ou redes	12%
	Negação de serviço distribuída	14%
Violação de dados e sistemas	Perda permanente de ficheiros	4%
	Sistemas corrompidos ou danificados	8%
	Dados pessoais alterados, destruídos ou roubados	8%
	Acesso não autorizado ou hacking a sistemas de negócio	12%
	Malware: ransomware/spyware/virus	39%
Fraude e *Phishing*	Hacking ou tentativa de hacking de contas bancárias	5%
	Impersonalização de contas de email de organizações	30%
	Pessoal direcionado para websites fraudulentos	61%
	Emails, SMS e chamadas telefónicas fraudulentas	75%

O relatório do NCSC aponta o que considera serem as três principais ameaças às organizações desportivas: o comprometimento das contas de email da organização usadas posteriormente em fraudes relacionadas com pagamentos ou roubo de dados, as fraudes facilitadas pela tecnologia (mandatos, faturação,

bilhética, etc.), e o *ransomware*. Este último, embora menos frequente que os anteriores e correspondendo apenas a 25% dos ataques que envolvem *malware*, tem normalmente impactos desastrosos.

Interessa também compreender quais os atores e a sua motivação por trás dos ataques conduzidos às organizações desportivas. O *NCC Group* e o *PHOENIX Sport & Media Group* identificaram atores e respetivas motivações que podem representar ameaças a organizações desportivas (NCC Group et al., 2023).

i. Organizações rivais: espionagem com o objetivo de obter segredos ou estratégias, roubar propriedade intelectual ou obter detalhes sobre compra ou venda de jogadores;
ii. Crime organizado: eventual utilização de *ransomware* para sequestrar sistemas e/ou dados em troca de avultadas somas de dinheiro, obter informação relevante para melhorar a probabilidade das apostas ou para ganhar vantagem para a combinação de resultados, ou até para executar fraudes financeiras relacionadas com a venda de bilhetes, serviços ou produtos;
iii. Nações hostis: motivações geopolíticas podem incluir ataques à reputação de clubes, organizações ou nações, comprometimento da integridade de registos médicos, ou sequestro de dados para enganar ou perturbar a atividade;
iv. Funcionários descontentes: ameaças internas de funcionários descontentes com o objetivo de ganho financeiro ou o de provocar danos reputacionais à organização;
v. *Cyber Bullies* ou *Trolls*: pessoas que utilizam redes sociais, jogos online, etc., para assediar, assustar, enfurecer ou envergonhar atletas ou outras pessoas, utilizando linguagem ofensiva com características como o racismo, homofobia e misoginia;
vi. Atacantes ocasionais ou aprendizes de hacker: agem tipicamente por prazer, curiosidade ou apenas para ganharem notoriedade junto dos seus pares provocando por vezes graves fugas de informação ou de dados para o público;

vii. *Hacktivistas*: hackers que atuam para desacreditarem atletas, clubes, organizações ou nações com base em controversas relacionadas com a hospedagem de eventos desportivos, crenças, atitudes relativas à igualdade, etc.;
viii. Jogadores organizados: têm como principal motivação ganharem vantagem relativamente às apostas que efetuam.

5. LEGISLAÇÃO

Considerar a legislação ao planear e implementar um sistema de gestão de segurança da informação (SGSI) é crucial para garantir a conformidade legal, proteger a organização contra sanções financeiras e danos reputacionais, e salvaguardar os direitos dos indivíduos cujos dados são tratados; além disso, assegura que o SGSI atenda aos requisitos de proteção de dados e cibersegurança, promovendo confiança junto a clientes, parceiros e reguladores, enquanto mitiga riscos de vulnerabilidades legais e operacionais.

Em linha com este raciocínio, as organizações desportivas devem ter em consideração alguns regulamentos fundamentais. O Regulamento Geral de Proteção de Dados (RGPD) (2016/679) (EUR-Lex, 2016b), que entrou em vigor em maio de 2018, estabelece normas para a proteção de dados pessoais na União Europeia (UE) com vista a garantir a privacidade e a segurança dos dados pessoais dos seus cidadãos, impondo obrigações às organizações que recolhem e processam esses dados.

Este regulamento apresenta como principais ideias a necessidade de requerer o consentimento explícito para o tratamento de dados pessoais, e dar ao cidadão o direito ao esquecimento, o acesso e à portabilidade dos dados que lhe dizem respeito. Estão associados os princípios de privacidade por defeito (*Privacy by Default*) e privacidade desde a conceção (*Privacy by Design*) que significam respetivamente, que as configurações de privacidade devem estar ativadas automaticamente sem necessidade de intervenção do utilizador, e que todas as medidas técnicas e organizacionais para proteger os dados pessoais devem ser consideradas e integradas no sistema desde o início da sua implementação.

Pelo RGPD as organizações são obrigadas a notificar violações de dados às entidades competentes num prazo de até 72 horas e impõe sanções pesadas às organizações incumpridoras que podem ascender a 20 milhões de euros ou 4% do volume de negócios.

O Regulamento ePrivacy (2002/58/EC) (EUR-Lex, 2017) regula a confidencialidade e a proteção dos dados em comunicações eletrónicas, cobrindo áreas como o uso de cookies, metadados, marketing digital e confidencialidade das comunicações. Complementa o RGPD ao focar especificamente nos direitos de privacidade em comunicações digitais, garantindo que os dados tratados por serviços de telecomunicações e plataformas online respeitam os princípios de consentimento e transparência, especialmente no que diz respeito ao rastreamento e armazenamento de informações no dispositivo dos utilizadores.

A Diretiva 2016/1148 de Segurança das Redes e da Informação (SRI ou NIS em inglês) (EUR-Lex, 2016a) estabelece medidas para alcançar um elevado nível de segurança das redes e sistemas de informação em toda a União Europeia, exigindo que os estados-membros adotem estratégias nacionais de cibersegurança, designem autoridades competentes e equipas de resposta a incidentes de segurança informática.

A Diretiva 2022/2555 (SRI2 ou NIS2 em inglês) veio ampliar o âmbito de aplicação da SRI original através da exigência da implementação de medidas e avaliação regular de riscos. Aplica-se a mais setores de atividade classificando as entidades como "essenciais" e "importantes" e impondo requisitos de segurança e supervisão mais rigorosa. A definição de entidades "essenciais" passou a incluir a administração local detentora e gestora de um grande número de instalações desportivas.

Ao contrário da SRI que deixava a cargo dos estados-membros as sanções e penalizações a aplicar, a SRI2 estabelece multas dissuasivas com valores máximos de até 10 milhões de euros ou 2% do volume de negócios global.

6. MEDIDAS DE SEGURANÇA

Não existem regulamentações, avaliações e/ou medidas de segurança específicas para o setor do desporto. Desta forma, as organizações desportivas devem adotar os processos e medidas de segurança que garantam a proteção do seu sistema de informação e o cumprimento da legislação.

Segundo Mamede (2006) a segurança na organização deve constituir-se como um processo cuja execução a capacita na proteção da sua infraestrutura e no controlo de acesso à sua informação. A definição e implementação do processo de segurança na organização deve incluir os passos de desenvolvimento da política de segurança organizacional, especificações de implementação, formação, levantamento da situação atual, implementação de medidas corretivas, e manutenção da estratégia de segurança.

Veiga (2024) refere que o planeamento de uma estratégia de cibersegurança repercute-se em múltiplos vetores, os quais devem ser vertidos nas opções táticas iniciais e no modo como estas poderão evoluir ao longo do ciclo de funcionamento da empresa e/ou ciclo de vida dos vários produtos e serviços que fazem parte do seu portfólio.

A ISO disponibiliza uma família de normas ISO/IEC 27000 que promove uma visão holística da segurança da informação visando as pessoas, as politicas e a tecnologia. Este conjunto de normas tem por principais objetivos:

i. Permitir às organizações implementar práticas que garantam a confidencialidade, integridade e disponibilidade da informação, pretegendo-a contra acessos não autorizados, alterações indevidas e indisponibilidade;
ii. Estabelecer os requisitos para criar um SGSI através de uma abordagem sistemática e baseada na gestão do risco para gerir a segurança da informação;
iii. Integrar a gestão da segurança com os processos de negócio de forma a que as medidas de segurança sejam proporcionais às necessidades e aos objetivos da organização;

iv. Disponibilizar um quadro de suporte ao cumprimento dos requisitos legais e contratuais relacionados com a proteção de dados e cibersegurança;
v. Orientar na identificação, análise e mitigação dos riscos de seguir, priorizando recursos e propcurando minimizar os impactos de potenciais incidentes;
vi. Promovendo a monitorização, revisão e atualização continua das políticas e processos de segurança para garantir a resiliência diante de ameaças e mudanças tecnológicas.

As medidas de segurança são especificadas em detalhe na ISO/IEC 27001 e os seus controlos descritos no anexo A e complementados pela ISO/IEC 27002. Contudo, destacam-se algumas das medidas de segurança mais relevantes.

Em primeiro lugar é necessário definir e criar uma política de segurança alinhada com os objetivos da organização. É fundamental sensibilizar e envolver a administração, definir as funções e responsabilidades, e criar uma equipa para supervisionar a segurança da informação. Esta política deve ser revista periodicamente quer para se ajustar a mudanças internas na organização, quer para refletir as alterações no ambiente externo e a novas ameaças.

A gestão dos acessos é fundamental para limitar a exposição de informações sensíveis. O acesso à informação deve estar em linha com o princípio do privilégio mínimo, garantindo que cada utilizador, sistema ou processo tenha apenas os acessos estritamente necessários para realizar as suas funções ou tarefas. Este princípio deve ser complementado pela utilização de autenticação multifator, pela utilização de senhas de acesso fortes, e pelo registo das atividades no sistema.

A segurança física e ambiental deve ser assegurada através da implementação de controlos de segurança física que protejam os ativos contra ameaças e acessos não autorizados, desastres naturais ou mesmo vandalismo.

Do ponto de vista tecnológico e de operações, a norma destaca a importância da utilização de controlos para proteção dos sistemas através da implementação de *firewalls*, da utilização de criptografía, e atualizações regulares do software

utilizado. É também fundamental uma política de backups eficiente, bem como um plano de resposta e recuperação para assegurar a continuidade do negócio em casos de interrupção do serviço.

Como parte dos controlos, as organizações devem gerir os riscos associados a fornecedores e parceiros incluindo a avaliação de contratos, auditorias de conformidade e a garantia de que terceiros seguem as mesmas normas de segurança exigidas pela organização. Apesar de ser parte integrante da norma, esta supervisão dos terceiros assume especial importância quando a organização utiliza em parte ou no seu todo a computação na nuvem. É também fundamental assegurar que os parceiros que prestam serviços de software na nuvem (*Software as a Service* – SaaS) estão a proteger devidamente os seus dados e informação.

Por fim, uma das partes mais importantes no SGSI diz respeito às pessoas. Os colaboradores devem estar cientes e envolvidos na segurança. A norma incentiva a realização de programas regulares de consciencialização para ensinar boas práticas de segurança, políticas organizacionais e como identificar ameaças de engenharia social e *phishing*.

Embora não se tratando de um controlo, a norma apresenta a gestão do risco como forma de orientar a aplicação de controlos específicos para mitigar ou tratar os riscos identificados. O Centro Nacional de Cibersegurança (CNCS, 2022) o processo de gestão dos riscos é um exercício estruturado, no qual a organização identifica possíveis ameaças que possam explorar as vulnerabilidades dos ativos, bem como quais os niveis de risco associado, avaliando-se a probabilidade de ocorrência de possiveis impactos.

7. TENDÊNCIAS

A evolução tecnológica tem impulsionado avanços significativos em diversos setores, mas também trouxe novos desafios no campo da cibersegurança. Veiga (2024) refere que nos próximos anos o uso das tecnologias digitais virá a ter um crescimento ainda mais acelerado, motivado pela contínua redução de custos e à miniaturização, e como consequência novos problemas de segurança irão surgir. A massificação do teletrabalho requer a implementação de novas soluções, desde

o acesso por VPN ao acesso a aplicações, e até o controlo de acesso a determinados dados tem de ser repensado para esta nova realidade. Também o uso de dispositivos com ligação à internet (IoT) cada vez mais massificado requer soluções seguras para garantir a segurança digital e a privacidade dos dados.

Segundo o relatório de Tecnologias Emergentes do Centro Nacional de Cibersegurança Português (2023), cinco áreas específicas apresentam riscos crescentes e potenciais vulnerabilidades que exigem atenção: a computação na nuvem, a Internet das Coisas (IoT), a inteligência artificial, as redes 5G e a tecnologia quântica. Estas tecnologias, ao mesmo tempo que oferecem oportunidades disruptivas e inovadoras, ampliam as superfícies de ataque e introduzem complexidades que podem comprometer a segurança e a privacidade das informações, tornando essencial o desenvolvimento de estratégias robustas e adaptativas para mitigar tais riscos.

A computação em nuvem disponibiliza recursos e serviços pela internet, permitindo escalabilidade e redução de custos, em modelos como nuvens públicas, privadas e híbridas. Apesar das suas vantagens, surgem preocupações de segurança, privacidade e conformidade com os regulamentos e legislação, especialmente devido à localização dos servidores e dados. Os principais riscos associados à computação na nuvem incluem o comprometimento de dados, ataques à integridade dos serviços, e dependência de fornecedores. Estes riscos são agravados pela falta de governança e/ou de profissionais capacitados. Para mitigar estes desafios é necessário adotar uma estratégia alinhada com os objetivos organizacionais que inclua uma gestão de riscos robusta e a conformidade com a legislação.

A IoT é um ecossistema de dispositivos interconectados que utiliza sensores, atuadores, redes móveis, computação em nuvem e inteligência artificial para automatizar processos em áreas como saúde, transporte e cidades inteligentes. A IoT enfrenta desafios de segurança devido à diversidade tecnológica, e às vulnerabilidades resultantes da utilização de software *open-source*. Como consequência, há um aumento da superfície de ataque, especialmente em dispositivos remotos ou domésticos. Os riscos envolvem transmissão insegura de dados, exfiltração de informações sensíveis e comprometimento de serviços

críticos. Para mitigar estes perigos, são necessárias práticas de desenvolvimento seguro, rastreamento de vulnerabilidades e certificação de dispositivos, garantindo-se assim maior proteção e confiança nestes sistemas.

A Inteligência Artificial (IA) utiliza grandes volumes de dados e tecnologias como o *machine learning* para criar aplicações que aprendem e tomam decisões inteligentes. É usada em áreas que vão desde a automação à cibersegurança. A utilização desta tecnologia representa riscos de segurança e podem surgir vulnerabilidades relacionadas com a manipulação maliciosa de modelos, automação de ataques.

A auditoria destes sistemas pode também revelar-se de difícil aplicação motivada pela opacidade de alguns sistemas. Os perigos da utilização da IA podem ser a obtenção de resultados imprevisíveis, uso de *malware* inteligente e exploração de vulnerabilidades. Para mitigar esses riscos, é essencial combinar IA com discernimento humano, adotar técnicas auditáveis e abordar questões éticas e sociais relacionadas à IA.

O 5G é a quinta geração de redes móveis, de grandes velocidades e baixa latência, foi projetada para melhorar a conectividade e impulsionar serviços para empresas e a sociedade. A arquitetura complexa do 5G, que inclui virtualização, IoT e plataformas programáveis, amplia a superfície de ataque expondo infraestruturas críticas a vulnerabilidades cibernéticas e físicas. Além disso, os riscos são agravados pela dependência de fornecedores específicos, exigindo-se análises rigorosas do perfil de segurança dos produtos para mitigar interrupções de serviço e ataques.

A computação quântica baseia-se em princípios diferentes da computação clássica, o que permite resolver rapidamente problemas matemáticos extremamente complexos, como a factorização e o logaritmo discreto, que são a base dos atuais sistemas de criptografia de chave pública. Embora esta tecnologia traga avanços promissores em áreas como a saúde, representa, contudo, uma séria ameaça à segurança digital, pois poderá tornar obsoletos protocolos criptográficos cruciais para a proteção de dados. Para mitigar esses riscos, será essencial implementar sistemas de segurança que combinem tecnologias clássicas e

quânticas, garantindo múltiplas camadas de proteção em redes e no armazenamento de dados.

8. CONCLUSÕES

Como demonstram incidentes passados, a segurança informática é fundamental para garantir a continuidade e a resiliência das organizações desportivas, tendo em atenção a crescente digitalização e dependência tecnológica. Assim, neste documento começamos por apresentar conceitos de segurança informática, com destaque para os seus três pilares, a confidencialidade, a integridade e a disponibilidade. Foram identificadas as principais vulnerabilidades a ter em conta na proteção do sistema de informação, bem como as principais ameaças e técnicas utilizadas em ataques.

Embora a segurança informática seja importante em todas as organizações, os riscos e incidentes nas organizações desportivas tem vindo a aumentar face à grande exposição mediática e aos valores envolvidos, nomeadamente em grandes eventos desportivos.

Os principais incidentes têm ocorrido ao nível do comprometimento de contas de email, em fraudes relacionadas com a bilhética e faturação, e ataques de *ransomware*, normalmente explorados por atores com interesses variados.

Os regulamentos como o RGPD, o ePrivacy e o SRI proporcionam uma estrutura legislativa fundamental e algumas orientações no sentido da segurança informática. No entanto é imperativo que as organizações desportivas adotem medidas práticas de segurança como políticas de segurança robustas, gestão eficaz de acessos ao sistema, disponham de segurança física e ambiental adequadas, e assegurem o envolvimento e consciencialização dos colaboradores. A implementação de medidas de segurança aplicáveis referidas nas Normas ISO/IEC 27000 é um possível caminho a seguir na constituição de um SGSI robusto.

Referimos as tecnologias emergentes como a computação em nuvem, a IoT, a inteligência artificial e a computação quântica, cuja utilização predispõe a novas

vulnerabilidades e consequentemente grandes desafios em termos de cibersegurança.

Acompanhando os benefícios significativos que estas tecnologias trazem, o aumento da superfície de ataque é inevitável exigindo uma abordagem proativa e integrada para mitigar os riscos associados.

Para garantir e preservar a reputação do desporto e proporcionar experiências positivas e seguras para atletas, participantes e espectadores, as organizações desportivas precisam de adotar uma abordagem estratégica em relação à cibersegurança reconhecendo-a como um investimento contínuo e enquadrado com os seus objetivos de negócio. Apenas com uma colaboração efetiva entre pessoas, processos e tecnologia será possível enfrentar os desafios presentes e futuros, proteger os seus ativos digitais, e manter a confiança do público e dos parceiros.

BIBLIOGRAFIA

Centro Nacional de Cibersegurança (CNCS). (2022). *Guia para Gestão dos Riscos em matérias de Segurança da Informação e Cibersegurança*. 1–55. https://www.cncs.gov.pt/docs/guia-de-gestao-dos-riscos11.pdf

Centro Nacional de Cibersegurança (CNCS), Aguiar, R. L., Antunes, M., Barraca, J. P., Bartolomeu, P., Corujo, D., Cunha, V., Direito, R., Gomes, D., Marcuzzo, L. da C., Martins, R., Mateus, P., Pinto, A. N., & Silva, N. (2023). *Relatório- Tecnologias Emergentes*.

EUR-Lex. (2016a). Diretiva relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União Europeia (SRI ou NIS).

EUR-Lex. (2016b). *Regulamento Geral sobre a Proteção de Dados (RGPD)*. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679

EUR-Lex. (2017). *Regulamento relativo à privacidade e às comunicações eletrónicas (ePrivacy)*. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52017PC0010

Greenwald, M. (2017). *Cybersecurity in Sports Questions of Privacy and Ethics*. *December*, 1–14. http://www.cs.tufts.edu/comp/116/archive/fall2017/mgreenwald.pdf

ISO/IEC 27000:2018. (2018). *ISO/IEC 2018*. https://www.iso.org/standard/73906.html

Mamede, H. S. (2006). Segurança Informática nas Organizações (FCA).

National Cyber Security Centre. (2019). *The Cyber Threat to Sports Organisations*. 1–27.

National Institute of Standards and Technology (NIST), Nieles, M., Dempsey, K., & Pillitteri, V. Y. (2017). NIST 800-12 Rev. 1 - An introduction to information security evaluation. *National Institute of Standards and Technology*. https://doi.org/https://doi.org/10.6028/NIST.SP.800-12r1

NCC Group, Phoenix Sports and Media Group, & University of Oxford. (2023). *The Hidden Opponent: Cyber Threats in Sport*. 1–23.

OWASP Project. (2021). *OWASP Top Ten*. https://owasp.org/www-project-top-ten/

OWASP Project. (2024). *OWASP*. https://owasp.org/

Pinko, E. (2021). A new dimension of risks in sports: the cyber domain. *Strategies for Policy in Science and Education-Strategii Na Obrazovatelnata i Nauchnata Politika*, *29*(4s), 9–17. https://doi.org/10.53656/str2021-4s-1-risk

Rascagneres, P., & Mercer, W. (2018). Who wasn't responsible for Olympic Destroyer. *Virus Bulletin Conference (VB2018)*, *October*, 1–8.

Stallings, W. (2014). *Cryptography and Network Security* (6th ed.). PEARSON.

TUVRheinland. (2024). *ISO 27001 Segurança da Informação*. https://www.tuv.com/portugal/pt/certificação-de-acordo-com-a-iso-27001.html

Veiga, P. (2024). *Cibersegurança*. Fundação Francisco Manueal dos Santos.

La seguridad en el deporte se ha convertido en un gran reto para las sociedades contemporáneas, debido a la creciente complejidad de las organizaciones deportivas y a la interconexión entre sectores diversos con el mercado deportivo. En este escenario, garantizar entornos deportivos seguros, éticos e inclusivos es hoy una prioridad ineludible. La edición de este IV libro reúne las reflexiones y aportaciones de investigadores, gestores, juristas, técnicos y responsables institucionales que analizan, desde una perspectiva científica y multidisciplinar, los principales riesgos y desafíos que afectan al ecosistema deportivo actual.

A lo largo de sus capítulos se abordan cuestiones clave hoy en día como la protección de la infancia y la juventud, la prevención de lesiones y accidentes, la seguridad en instalaciones deportivas, la integridad de las competiciones, la violencia y la discriminación, así como los nuevos retos derivados de la digitalización, entre otras. Estas contribuciones evidencian que la seguridad deportiva no depende de una única disciplina o actor, sino de la cooperación entre la comunidad científica de diferentes disciplinas e instituciones públicas, organizaciones deportivas, profesionales del sector, y practicantes consumidores deportivos.

Este volumen también pone de relieve la importancia de la buena gobernanza, la formación especializada y el desarrollo de marcos normativos sólidos que permitan anticipar riesgos y fortalecer la cultura de prevención. A través de experiencias, estudios y buenas prácticas internacionales, la obra ofrece herramientas útiles para responsables de políticas públicas, gestores deportivos, educadores y profesionales comprometidos con la mejora del sistema deportivo.

Más allá del análisis de problemas, esta cuarta entrega sobre seguridad deportiva, propone una visión constructiva del deporte como espacio de educación, inclusión y desarrollo social. Una llamada de RIASPORT al compromiso colectivo para consolidar entornos deportivos más seguros, responsables y sostenibles, en los que la integridad, los derechos fundamentales y el bienestar de las personas ocupen siempre el centro de la acción deportiva.