

# CYBERTOWN 2D: Xogo dixital sobre Ciberseguridade



Alberto Pampín Pérez  
Universidade de Santiago de  
Compostela (USC)  
alberto.pampin@rai.usc.es

REVISTAGALEGA  
DE EDUCACIÓN  
PUBLICACIÓN DE NOVA ESCOLA GALEGA

ISSN: 1132-8932  
Páx. 62 - 63

A aparición de Internet cambiou por completo as nosas vidas, producindo grandes avances nos eidos da investigación, a saúde e por suposto a educación. Aínda que os avances son sempre positivos, o seu uso masivo deu lugar á aparición dos que empregan esta ferramenta con fins maliciosos. Os ciberataques como o *phishing* ou o *ransomware* e a fraude *on-line* non fan máis que aumentar, tal e como demostran os alarmantes resultados do balance realizado polo Instituto Nacional de Ciberseguridade de España (INCIBE, 2022a). Malia que moitos usuarios e usuarias cren que os riscos que os axegan na Internet están asociados aos coñecidos *hackers*, a verdade é que moitas veces son eles mesmos os que se poñen en perigo mediante prácticas de risco como o *sexting*, que a miúdo remata coa difusión de contido íntimo, o *revenge porn* e o *cyberbullying*. Estas prácticas teñen especial importancia na adolescencia, xa que se trata dunha etapa con importantes cambios no plano psicolóxico, biolóxico e interpersonal (Steinberg, 2008). Sumado a isto, cómpre destacar os cada vez máis comúns problemas de adición ás TIC. Un estudo levado a cabo pola Fundación Barrié (2022) mostrou que un 95,7% dos dez mil adolescentes enquisados ten o seu propio *smartphone* con conexión a Internet e que o 78,8% está rexistrado en 3 ou máis redes sociais (YouTube, Instagram, TikTok...), nas que o 10,5% pasa 5 horas diarias.

Dende a Administración pública estase tratando de remediar esta situación mediante campañas de concienciación e outros recursos, así como incluíndo no currículo básico da LOMLOE contidos de Ciberseguridade dentro da Competencia Dixital. Mais... que efectividade están a ter estas medidas entre o profesorado, familias e alumnado de Educación Secundaria Obrigatoria? Coñecen os riscos máis básicos e as campañas e servizos sobre Ciberseguridade que a Administración pon á súa disposición? Co fin de avaliar estas circunstancias, elaborouse e adminístrouse un cuestionario *on-line* entre os meses de xaneiro e marzo de 2023. En total participaron 1120 persoas, as cales se agruparon en 4 perfís tal e como se amosa na Fig. 1.

Os resultados obtidos dan respostas rotundas ás cuestións presentadas ante-

riormente. Na Fig. 2 pódese observar como o *smishing*, o risco máis común na actualidade, é un misterio para todos os perfís. Ademais, a falsa crenza de que calquera páxina web que teña un cadeado (🔒 HTTPS) é segura está amplamente entendida - *Si, así é, é un mito! Se acabas de descubri-lo lendo este artigo... Xenial! Xa serviu para algo.* En canto á efectividade dos esforzos da Administración por difundir as súas campañas e servizos, a Figura 3 demostra que aínda queda moito traballo por facer. Finalmente, dos 1120 participantes, tan só 92 souberon identificar que o número telefónico 017 corresponde á liña de axuda en Ciberseguridade do INCIBE.

Os resultados do cuestionario avalan a preocupante situación que vivimos, mais resignarse e aceptar que as cousas son así nunca é unha solución. Polo tanto, decidiuse desenvolver un recurso que permitise á cidadanía, en especial ao alumnado de Secundaria, mellorar as súas competencias en Ciberseguridade e que axudase a dar a coñecer os recursos, campañas e institucións existentes. Con esa finalidade nace CYBERTOWN 2D (<http://bit.ly/cybertown-2d>), un xogo 2D con estilo Pixel Art que evoca aos primeiros xogos da franquía Pokémon. Para o seu desenvolvemento partiuse dos aspectos positivos e puntos a mellorar dos recursos interactivos que a Administración lanzou nos últimos anos, facendo especial fincapé no aspecto didáctico. Mediante a técnica do *storytelling* trátanse tres casos reais; o primeiro deles sobre *smishing* e fraude en Internet, o segundo sobre compras *on-line*

seguras e o último sobre *sexting* e a importancia da privacidade na Rede para evitar a difusión de contido de carácter íntimo. CYBERTOWN 2D busca concienciar sobre estas situacións e proporcionar ferramentas que permitan identificar e evitar estes riscos, así como outras que axuden a remediar os erros que se cheguen a cometer. O recurso da a posibilidade de expandir a información proporcionada a través de ligazóns a recursos nos sitios web do INCIBE, a Oficina de Seguridade do Internauta (OSI) —que depende do INCIBE— e a Axencia Española de Protección de Datos (AEPD).

Este recurso foi presentado nun centro de Educación Secundaria onde o alumnado do primeiro curso dedicou dúas sesións de cincuenta minutos a xogar e avaliar dita experiencia. A súa valoración foi moi positiva: CYBERTOWN 2D logrou captar a súa atención dende o primeiro momento, ensinándolles a identificar os riscos máis comúns e dándolles a coñecer outras ferramentas coas que defenderse na Rede. Entre os aspectos mellor valorados cómpre destacar a inclusión de casos reais, a explicación das causas e consecuencias de cada risco e o emprego dunha linguaxe fácil de comprender.

A Ciberseguridade representa un dos maiores problemas da sociedade actual. Malia os grandes esforzos da Administración por protexer e formar a cidadanía, aínda queda moito por facer, polo que resulta indispensable seguir traballando e desenvolvendo recursos efectivos como CYBERTOWN 2D. ■

## REFERENCIAS

- FUNDACIÓN BARRIÉ. (2022). *Adolescencia, Tecnología, Salud y Convivencia*. <https://fundacionbarrie.org/prevencion-estudio>
- INSTITUTO NACIONAL DE CIBERSEGURIDAD. (2022a). *Balance de Ciberseguridad*. [https://www.incibe.es/sites/default/files/paginas/que-hacemos/balance\\_ciberseguridad\\_2022\\_incibe.pdf](https://www.incibe.es/sites/default/files/paginas/que-hacemos/balance_ciberseguridad_2022_incibe.pdf)
- STEINBERG, L. (2008). A social neuroscience perspective on adolescent risk-taking. *Developmental Review*, 28, 78-106. <https://doi.org/10.1016/j.dr.2007.08.002>

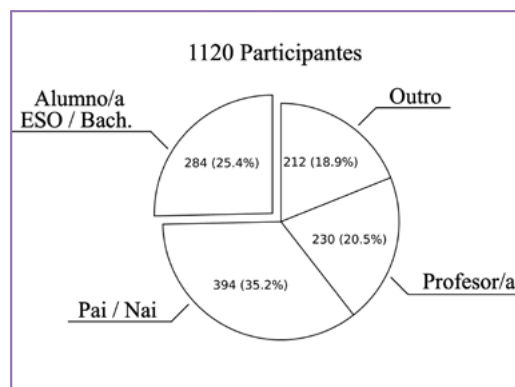


Fig. 1. Diagrama sectorial da participación no cuestionario

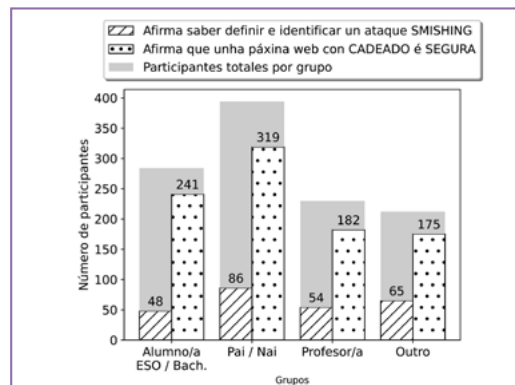


Fig. 2. Coñecemento sobre ataques na rede

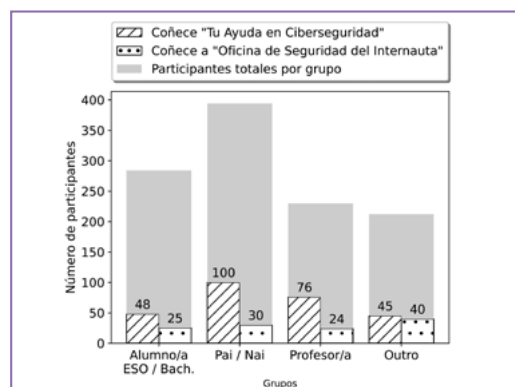


Fig. 3. Coñecemento sobre ciberseguridade



Fig. 4. Interfaz de Cybertown 2D