Guardianes de la Galaxia: concienciación en Ciberseguridad

Miguel Fernández, Jesús Lizarraga, Iñaki Vélez de Mendizabal, Antton Rodríguez, Urko Zurutuza
Departamento de Electrónica e Informática, Escuela Politécnica Superior
MONDRAGON UNIBERTSITATEA
Goiru Kalea, 2. 20500 Arrasate - Mondragón
mfernandez, jlizarraga, ivelez, arodriguezc, uzurutuza @mondragon.edu

Resumen- En este artículo se presenta una iniciativa de formación denominada "Guardianes de la Galaxia", orientada a concienciar y formar a los participantes en la identificación, detección y prevención de ciberataques de tipo ransomware. Es una iniciativa que, en principio, se ha orientado hacia una audiencia profesional, es decir, personal trabajador de cualquier ámbito de la empresa, pero es aplicable a cualquier tipo de audiencia. Se han definido dos cursos, uno orientado al público en general y un segundo orientado a equipos de intervención frente a incidentes de ciberseguridad. Estos cursos se llevan realizando desde 2022, con más de 7500 personas matriculadas, y en el artículo también se presentan una serie de resultados de las ediciones realizadas hasta el momento.

***Index Terms*- ciberseguridad, formación continua, innovación, ransomware, storytelling, gamificación.**

Tipo de contribución: *Formación e innovación educativa.*

I. INTRODUCCIÓN

La formación continua ha sido siempre una de las actividades principales de Mondragon Goi Eskola Politeknikoa (MGEP), la Escuela de Ingeniería de Mondragon Unibertsitatea (MU), junto con la formación reglada y la investigación. Desde hace algunos años, y debido a la proliferación de ciberataques que están sufriendo, las empresas están demandando formación encaminada a concienciar a su personal trabajador en el ámbito de la ciberseguridad. En este contexto, desde el área de Telemática y Ciberseguridad de MGEP se decidió crear un curso de concienciación sobre ciberataques de tipo ransomware, ya que, actualmente, constituyen uno de los mayores riesgos a los que se enfrentan las organizaciones. Así surgió "Guardianes de la Galaxia", una formación online que utiliza la línea argumental de la película homónima de 2014. Es una formación asíncrona, es decir, los participantes pueden acceder a los contenidos cuando quieran, y se ha utilizado el concepto de "storytelling" usando la línea argumental de la película para intentar dar un mayor atractivo a la formación. También se han utilizado componentes de gamificación (como retos y rankings) para mejorar la participación y la motivación de los participantes. Con este tipo de cursos pretendemos vencer las reticencias hacia las formaciones habituales sobre Ciberseguridad que ya realizamos, como charlas de concienciación o talleres de buenas prácticas, tanto en formato presencial como online, en las que una las principales limitaciones es la audiencia a la que conseguimos llegar.

"Guardianes de la Galaxia" es un proyecto realizado en colaboración con la Corporación MONDRAGON y financiado inicialmente por la Diputación Foral de Guipúzcoa.

II. ANTECEDENTES

El storytelling es el arte de contar historias. Es una técnica utilizada para comunicar mensajes de manera efectiva a través de la estructuración y presentación de relatos convincentes y atractivos. La efectividad del storytelling radica en su capacidad para involucrar a la audiencia emocionalmente, lo que hace que los mensajes sean más memorables, compartibles y persuasivos. La técnica de storytelling es una herramienta especialmente efectiva en el desarrollo de nuevas habilidades académicas y en la motivación de los alumnos, ayuda a los profesores y alumnos a aprender a aplicar eficazmente la tecnología dentro y fuera del aula [1]. La aplicación del storytelling en el ámbito educativo no es algo nuevo, muchas universidades y entidades de formación utilizan esta técnica como un recurso eficaz para enseñar y para aprender [2]. En cuanto a la gamificación, la incorporación de elementos de juego en entornos no lúdicos, es también una técnica que mejora la motivación y la participación de los alumnos, y proporciona a los profesores herramientas para guiar y recompensar a los alumnos. La gamificación puede convertir una experiencia de formación en algo divertido, aunque no es la panacea que se pueda aplicar en cualquier contexto de educación [3].

En MGEP ya teníamos experiencia en iniciativas de este tipo. Con anterioridad, por ejemplo, lanzamos dos ediciones de un MOOC sobre Hacking Ético en el que también utilizábamos los conceptos de gamificación y storytelling [4]. El curso constaba de varios retos tanto individuales como grupales y contaba con un hilo narrativo basado en "La Guerra de las Galaxias". Otro ejemplo es un curso sobre competencias digitales dirigido a personas desempleadas, en el que, tras una primera sesión presencial de presentación, durante una semana los participantes resuelven diversos retos online en equipo y se finaliza el curso con "Escape Room" digital y online. En esta ocasión utilizamos una narrativa basada en la serie "CSI", como se puede observar en la figura 1:

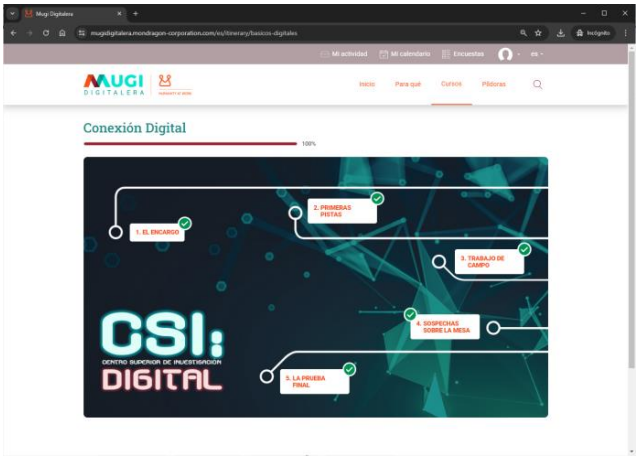

Fig. 1: pantalla de inicio del curso sobre competencias digitales.

Estas y otras experiencias nos han convencido de que estos formatos de formación son percibidos de manera positiva por los participantes y contribuyen a que los indicadores de finalización de los cursos y satisfacción con los mismos sean altos.

Cabe destacar que, aunque utilizamos hilos argumentales de series y películas muy populares, el desconocimiento de los mismos no es una condición excluyente para los participantes en estas actividades. Somos conscientes de que muchos de los participantes en "Guardianes de la Galaxia" no conocen la saga. Sin embargo, esto no es un impedimento para seguir el curso. Utilizamos conceptos argumentales y visuales de la saga como un marco para la presentación y el seguimiento de los contenidos.

III. OBJETIVOS

Esta formación constituye una solución de aprendizaje en la gestión de incidentes de ciberseguridad en entornos corporativos. El objetivo principal de esta formación es concienciar y formar en la gestión de incidentes de ciberseguridad a los usuarios de las empresas ante posibles ataques, y en particular, ante incidentes de ransomware por su impacto. Los objetivos específicos de esta formación son:

- Concienciar a los trabajadores de las empresas de la importancia de la seguridad en la información y del uso seguro de los dispositivos digitales.
- Formar a los trabajadores en cómo prevenir y actuar ante posibles ataques de ransomware en sus dispositivos.

El curso está dirigido a:

- Personal trabajador de empresas con acceso a dispositivos conectados.
- Personal trabajador con conocimientos y uso habitual de dispositivos digitales.
- Personal trabajador con poco tiempo para la formación, y poca motivación y sensibilización por la ciberseguridad.

Uno de los problemas principales a la hora de lanzar acciones de concienciación en las empresas es la falta de tiempo del personal trabajador, que en muchas ocasiones perciben estas acciones como una carga adicional de trabajo o, incluso, una pérdida de tiempo. Por este motivo se optó por un tipo de formación corta en el tiempo y que pudiera ser atractiva y fácil de seguir por los participantes.

IV. DESCRIPCIÓN DE LA PLATAFORMA Y DE LOS CONTENIDOS

La plataforma en la que se ofrecen los contenidos es una plataforma llamada "Mugi Digitalera"[1] (https://mugidigitalera.mondragon-corporation.com), que es un espacio de aprendizaje puesto en marcha por la corporación MONDRAGON, de la que MU y MGEP forman parte. En esta plataforma se ofrecen cursos de distintas temáticas para las empresas y personal trabajador que forman parte de la corporación. Además, para aquellas empresas que soliciten el curso y que no formen parte de la corporación, también está disponible en la plataforma Moodle de MGEP.

Los contenidos de este curso se han diseñado de acuerdo a los siguientes objetivos de aprendizaje:

Objetivos de conocimiento:

- Detectar el incidente,
- Avisar a la persona correcta y con la celeridad que requiere,
- Aplicar las primeras acciones de contención,
- Realizar o identificar tareas preventivas.

Objetivos actitudinales:

- Ser consciente de la gravedad de estos ataques.
- Responsabilidad por parte del usuario: conseguir que se comporten de manera preventiva y reactiva.

El curso está disponible en 3 idiomas (castellano, euskera e inglés) y consta de 5 secciones, que se identifican con 5 gemas (presentes en la película "Guardianes de la Galaxia"), y cada sección trata sobre un tema diferente relativo a los incidentes de ransomware en las empresas:

- Gema del poder: es una introducción sobre los ataques ransomware, para concienciar al participante de la importancia que tienen este tipo de incidentes hoy en día en las empresas. Se explica qué es un ataque ransomware, las amenazas que supone y las consecuencias de un ataque ransomware.
- Gema de la mente: trata sobre cómo se manifiesta un ataque ransomware. Explica las fases típicas de un ataque: infección, contacto, propagación, cifrado, rescate y recuperación.
- Gema de la realidad: trata sobre los síntomas de un ataque ransomware, para que el participante sepa identificarlos y aporta una serie de recomendaciones para reducir el impacto del ataque.
- Gema del espacio: trata sobre qué hacer ante un ataque ransomware, qué medidas podemos tomar si

[1] Se podría traducir de euskera a castellano como "Digitalízate".

somos conscientes de que estamos siendo víctimas de un ataque de este tipo.
- Gema del tiempo: se centra en qué medidas podemos tomar para prevenir un ataque ransomware.

El objetivo del participante en el curso es lograr las 5 gemas. Para ello, tiene que acceder a los contenidos de cada gema y superar un cuestionario, lo que le brindará el acceso a la siguiente gema. En la figura 2 se muestra el mapa de las gemas, a través del cual el participante accede a las distintas secciones:

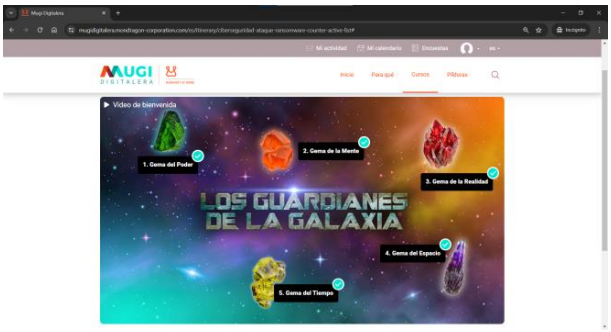

Fig. 2: mapa de navegación del curso.

Todas las secciones tienen la misma estructura:
- Un paquete SCORM, que cuenta a su vez con las siguientes secciones:
  - Introducción.
  - Video explicativo.
  - Sección "Recuerda".
  - Cuestionario.
- Enlaces a noticias o información adicional
- Una infografía resumen del contenido de la sección. Estas infografías son descargables por parte del participante.

En la figura 3, a modo de ejemplo, se observa la distribución de contenidos de la primera gema o sección:

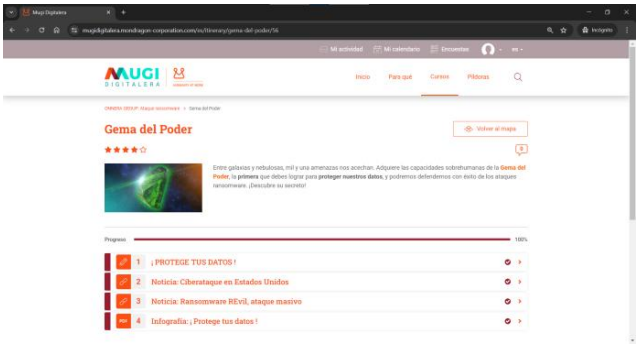

Fig. 3: contenidos de sección.

El contenido principal de cada sección lo constituye el video del paquete SCORM. Se trata de vídeos de corta duración en los que se presentan los conceptos fundamentales que tiene que adquirir el alumno (figura 4).

Cuando el participante completa la formación, obtiene un certificado de realización del curso.

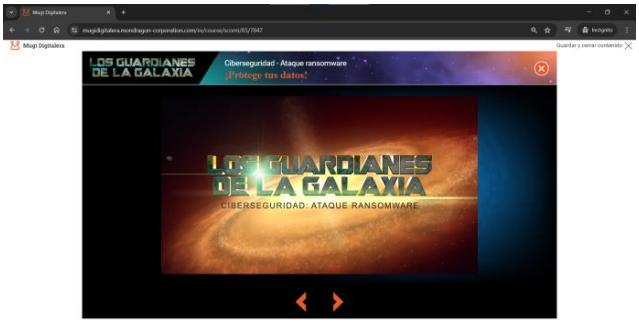

Fig. 4: ejemplo de paquete SCORM presente en el curso.

Además del curso orientado a usuarios, también se ha desarrollado un curso dirigido a poner en marcha y a formar equipos de intervención en incidentes de ciberseguridad. Los objetivos de este segundo curso son detectar los incidentes, priorizar la gravedad y los criterios establecidos para detectar el incidente, analizar la incidencia y desarrollar la solución. Este curso también sigue las directrices comentadas hasta ahora. Los contenidos están disponibles en la plataforma online y se utiliza el concepto de storytelling de "Guardianes de la Galaxia" como hilo argumental. Está dividido en 6 gemas o secciones:
- Xandar: ¿Cómo se manifiesta un ataque ransomware?
- Preventia: Prevención. ¿Cómo podemos prevenir un ataque ransomware y cómo podemos minimizar sus riesgos?
- Sakaar: Preparación. ¿Estamos preparados en la empresa para hacer frente a un ataque ransomware?
- The eye: Detección, análisis, identificación. ¿Estamos sufriendo un ataque ransomware?
- Vormir: Contención, erradicación, recuperación. ¿Qué debemos hacer?
- Jotunheim: Postincidente. ¿Cómo mejoramos?"

Este curso se imparte en formato presencial, con clases magistrales guiadas por un profesor de MGEP. Por ello, el formato de los contenidos está orientado a este tipo de sesiones: presentaciones propias para impartir las clases, documentos de distintas fuentes, etc.

V. METODOLOGÍA DE APRENDIZAJE

Las características fundamentales de la metodología diseñada para el curso de formación y concienciación dirigido a personal trabajador son:
- Aprendizaje gamificado: se utiliza el concepto de gamificación en el sentido de que los participantes compiten entre ellos durante la realización del curso y se genera una clasificación.
- Storytelling basado en la película "Guardianes de la galaxia": para lograr un hilo narrativo que de cohesión a la formación, se ha diseñado una narración del curso basada en la película.
- Contenidos en video de corta duración: los conceptos fundamentales de cada sección son presentados en videos de pocos minutos de duración.

- Cuestionarios para avanzar: los participantes deben superar un cuestionario en cada sección para avanzar en el curso.
- Aprendizaje autónomo, no tutorizado: los participantes pueden acceder cuando quieran a los contenidos disponibles en la plataforma.
- Acceso a recursos de aprendizaje a través de una plataforma digital.

Se ha optado por diseñar una metodología con estas características con el objetivo de vencer las posibles reticencias del personal trabajador de las empresas a la hora de recibir una formación de este tipo y favorecer que los participantes completen el curso. En concreto, la gamificación, como ya se ha comentado, es una técnica de aprendizaje que traslada la mecánica de los juegos al ámbito educativo-profesional con el fin de conseguir mejores resultados, ya sea para absorber mejor algunos conocimientos, mejorar alguna habilidad, o bien recompensar acciones concretas, entre otros muchos objetivos.

Este tipo de aprendizaje no es algo nuevo, y ha ganado terreno en las metodologías de formación debido a su carácter lúdico, que facilita la interiorización de conocimientos de una forma más divertida, generando una experiencia positiva en el participante.

El modelo de juego realmente funciona porque consigue motivar a los participantes, desarrollando un mayor compromiso de las personas, e incentivando el ánimo de superación. Se utilizan una serie de técnicas extrapoladas de los juegos. En este curso se han utilizado técnicas como la acumulación de puntos y el escalado de niveles.

El curso se ha diseñado en base a dos formatos:

- Formato de autoconsumo.
- Formato dinamizado.

Cada empresa tiene la opción de decidir el tipo de formato que va a elegir para la formación a personal trabajador. En ambos casos se hace uso de los contenidos que están disponibles en la plataforma online del curso. En la figura 5 se muestran las características de los dos formatos o modelos de impartición:

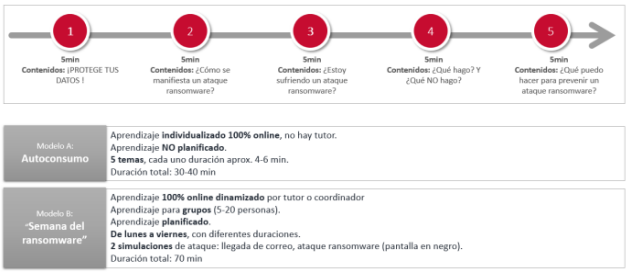

Fig. 5: modelos de impartición.

Como se ha comentado anteriormente, los participantes tienen que ir superando secuencialmente las distintas secciones del curso, no pueden acceder a una sección hasta que no han superado con éxito el cuestionario de la sección anterior. Además, en los contenidos se incluye un documento con el protocolo de actuación definido por la empresa para los usuarios (a qué teléfono tienen que llamar o con quién tienen que contactar, por ejemplo).

En el formato de autoconsumo el aprendizaje es totalmente individualizado y online. El participante es matriculado en el curso y accede a los contenidos cuando quiere, no existe la figura del tutor o dinamizador. No hay una planificación del aprendizaje en cuanto a sesiones o tiempos. Únicamente se define una fecha límite en la que los participantes deben completar la formación.

Cómo ya se ha comentado, el curso tiene 5 secciones, y se estima que el tiempo que tiene que dedicar el participante es de unos 30 o 40 minutos. En este modelo de formación el participante accede exclusivamente a los contenidos que están definidos en la plataforma, no se realizan actividades externas a la plataforma, como las simulaciones de ataque que se realizan en el formato dinamizado.

Aunque en este modelo no existe la figura del tutor o dinamizador, sí que es recomendable que una persona de la empresa analice el ranking para ver la evolución de los usuarios y decidir si debe realizar alguna acción de motivación.

En el formato dinamizado, existe la figura de un tutor o dinamizador. Este dinamizador es una persona de la propia empresa con conocimientos de informática y ciberseguridad, que previamente ha sido formado por MGEP para realizar esta tarea (1 hora de formación). En esta variante, la formación se realiza en grupos de 5 a 20 personas, pudiéndose planificar varios grupos en el tiempo. Cada grupo puede realizar la formación en una semana, de lunes a viernes.

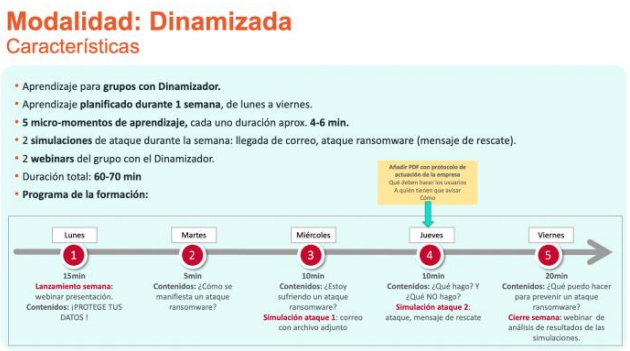

Fig. 6: modelo dinamizado.

Como se muestra en la figura 6, el curso comienza con una primera sesión (por ejemplo, un lunes) dinamizada por el tutor, que recomendamos que sea presencial, aunque también se puede realizar en formato webinar. En esta sesión inicial el tutor presenta la plataforma y la dinámica del curso. El resto de la semana los participantes van accediendo a los contenidos y progresando en el curso. En la última sesión (por ejemplo, el viernes), también de manera presencial o webinar, el tutor puede cerrar el curso y comentar los resultados del mismo.

En el modelo dinamizado, durante la semana el tutor lanzará dos acciones de ataque simuladas a las personas que están recibiendo la formación. El tutor debe planificar y gestionar las simulaciones y hacer seguimiento de las acciones de los usuarios.

Para realizar las simulaciones se puede utilizar la plataforma de simulacros de phishing que tenga la empresa. Si la empresa no dispone de plataforma de simulacros de phishing es MGEP quien configura y lanza las simulaciones desde su propia plataforma (esto requiere de una configuración en el servidor de correo y DNS de la empresa).

El día 3 (miércoles) se lanza una simulación de ataque consistente en un correo con un fichero adjunto. El objetivo es comprobar que los participantes han entendido las amenazas a

las que se enfrentan y saben actuar adecuadamente. Se monitoriza quienes abren el documento adjunto (figura 7):

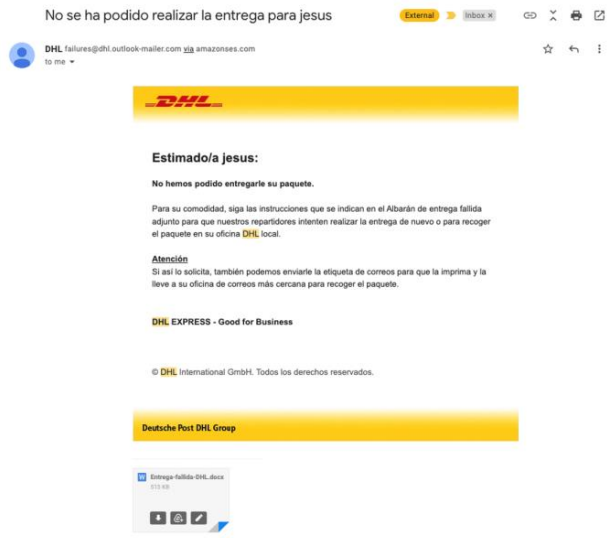

Fig. 7: ejemplo de simulación de phishing.

El día 4 (jueves) se envía un mensaje con un mensaje de rescate de ransomware. El objetivo es comprobar que el participante sabe identificar este tipo de mensajes y sigue el protocolo establecido por la empresa.

Fig. 8: ejemplo de simulación de ataque.

En el caso del curso orientado a equipos de intervención, la metodología de impartición se basa en clases magistrales impartidas por profesores de MGEP, que forman parte del equipo de trabajo de esta propuesta. Se planifican dos sesiones síncronas.

En la primera sesión se imparten las secciones 1, 2 y 3 del curso. Esta sesión está dirigida al personal técnico del equipo de intervención, es decir: personal trabajador que forma parte del equipo de intervención y que disponen de conocimientos técnicos tanto de informática como de ciberseguridad.

En la segunda sesión se imparten las secciones 4, 5 y 6 del curso, y está dirigida a todos los miembros del equipo de intervención. Es decir, en esta sesión estarán presentes también los miembros con perfiles de gestión y dirección, además del personal técnico. Esta segunda sesión está más centrada en aspectos de gestión de los incidentes de ciberseguridad, y no tanto en los aspectos técnicos (figura 9).

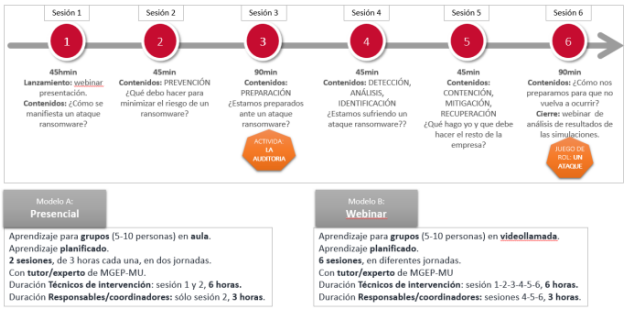

Fig. 9: planificación del curso para equipos de intervención.

Las sesiones pueden impartirse presencialmente o en formato de video llamada (online), en función de las necesidades de la empresa. Además de los contenidos de la plataforma, se realizan otras actividades de distintos tipos (una autoevaluación y un juego de rol). El juego de rol consiste en la simulación de un ataque ransomware, en el que cada participante asume un rol dentro de la organización y entre todos deben actuar para pararlo y resolverlo de la mejor forma posible.

En esta simulación el profesor va mostrando a los participantes distintas situaciones que se van presentando a medida que avanza el ataque y los asistentes deberán tomar decisiones e indicar cuales serían las acciones a llevar a cabo. Para cada una de las fases del incidente se da al grupo un tiempo limitado para proponer acciones creando situaciones de estrés similares a las de un incidente real. A título de ejemplo podemos ver a continuación unos de los primeros escenarios que se presentan: "¿por dónde empezamos?" en la figura 10.

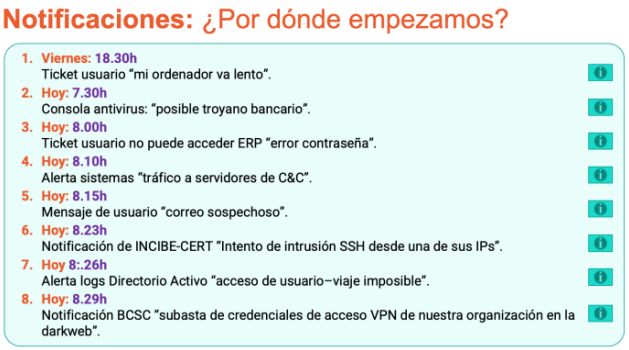

Fig. 10: juego de rol, simulación de un ataque.

VI. PLAN DE APOYO Y ACOMPAÑAMIENTO

Para cada modelo de aprendizaje, se han definido y desarrollado diferentes recursos y acciones de apoyo y acompañamiento a gestores, tutores y expertos de las empresas.

Para el formato de autoconsumo, se ha elaborado una guía para los responsables de esta formación en las empresas, que normalmente son los responsables de formación, como gestores de la acción formativa, y algún técnico de TI como experto en la materia. La guía describe el proceso de

aprendizaje y las acciones que tanto el responsable de formación como el experto deberán realizar durante el proceso de aprendizaje.

Para el formato dinamizado, en la guía comentada en el párrafo anterior, se ha añadido información para los expertos de TI sobre cómo ejecutar las acciones de simulación de ataques ransomware. Además, cada empresa cuenta con el soporte de profesores expertos de MGEP.

La formación de los equipos de intervención es una formación tutorizada por profesores de MGEP, que trabajan con los expertos y gestores de la empresa para planificar la formación, así como para, antes de una formación, analizar la situación y protocolos que la empresa pueda disponer ante ataques de ciberseguridad y en concreto ante ataques ransomware. El apoyo y tutorización se realiza tanto en el modelo presencial como webinar, siguiendo también la metodología aplicada de gamificación.

VII. RESULTADOS

El curso estaba listo para ofertarse a las empresas desde el año 2022. Hasta este momento, como se muestra en la Tabla I, se han realizado 43 ediciones del curso, en el que han participado 31 empresas, ya que algunas empresas han solicitado dos o más ediciones del curso. El total de participantes matriculados en los cursos ha sido de 7569 personas, de las cuales 4261 han iniciado la formación, lo que supone solamente un 56% del total de personas matriculadas. Sin embargo, el número de participantes que han terminado el curso es de 4141 personas, lo que supone el 54% del total de personas matriculadas, y el 97% de las personas que han iniciado el curso.

Tabla I
DATOS DE CURSOS Y PARTICIPACIÓN

Cursos realizados	Empresas que han participado	Número total de participantes	Participantes que han iniciado la formación	Participantes que han terminado la formación
43	31	7569	4261	4141

En el caso de los cursos dirigidos a equipos de intervención, se han realizado 15 cursos con una media de participantes de 7 personas, con un alto grado de satisfacción entre los asistentes. Hay que recordar que el curso dirigido a equipos de intervención no sólo forma a los participantes, sino que, en la mayoría de las ocasiones, sirve también para crear el propio equipo de intervención y los procedimientos de actuación frente a incidentes de ciberseguridad.

VIII. CONCLUSIONES

La principal conclusión que obtenemos después de 2 años y varias ediciones del curso orientado a usuarios es que, efectivamente, el enfoque del curso es apropiado para que los participantes sigan y terminen el curso, logrando así los objetivos de conocimiento planteados. La introducción de la gamificación y, sobre todo, del storytelling en la formación hace que ésta sea más atractiva y fácil de seguir. El alto porcentaje de usuarios que han terminado el curso con éxito (un 97% de las personas que lo han iniciado) así lo demuestra. El porcentaje de abandono es casi residual. También concluimos que es recomendable que este tipo de formaciones sean cortas en el tiempo y con contenidos muy dirigidos hacia los resultados de aprendizaje (concienciación en ciberseguridad, prevención y actuación frente a incidentes de ransomware), a modo de "píldoras de conocimiento".

La principal barrera a superar es logar un mayor número de personas que, habiendo sido matriculadas en el curso, lo inicien. Hay un 44% de personas que no han iniciado el curso, un indicador que es claramente mejorable. Esto sucede sobre todo en los cursos que siguen el formato de autoconsumo, en el que los participantes tienen total libertad para seguir los contenidos cuando quieran. Lógicamente, en los cursos que siguen el formato dinamizado, en el que hay un mayor seguimiento y la presencia de un dinamizador, la participación es mucho mayor.

En cuanto a la valoración del curso por parte de los participantes que lo han completado, al finalizar el mismo completaban una encuesta de satisfacción muy sencilla. Como resultados globales, un 88.9% de los participantes recomendaría el curso a otros compañeros, y la valoración general del curso es de un 4.6 sobre 5. Aunque son datos positivos, pensamos que ésta es una de las debilidades de este estudio, ya que sería deseable contar con más datos para realizar una evaluación cualitativa profunda del impacto del aprendizaje. Una de las líneas futuras para próximas actividades de este tipo es contar desde el diseño de las formaciones con una metodología estadística de recogida y análisis de datos.

Otro ámbito en el que deberíamos avanzar es el tipo de reconocimiento que reciben los participantes en este tipo de formaciones. Hasta la fecha, al completar el curso los participantes reciben un diploma acreditativo emitido por la universidad. Puede ser interesante avanzar en el reconocimiento de los conocimientos y habilidades adquiridas a través de un sistema de microcredenciales universitarias, que son "credenciales derivadas de formaciones breves (menos de 15 créditos ECTS), focalizadas en la adquisición de conocimientos, habilidades o competencias específicos, de formato flexible y adaptable a las diversas necesidades y limitaciones de disponibilidad del alumnado adulto, incluyendo el uso de la modalidad virtual o semivirtual, y con una estructura modular por la que cada formación puede tener sentido de forma independiente, y al mismo tiempo, acumularse y combinarse en credenciales más amplias, en el marco de un itinerario formativo personalizado.[1]" Este enfoque también puede ser interesante si estas microcredenciales son reconocidas por la industria y pueden mejorar las perspectivas laborales de los estudiantes al demostrar su dominio de habilidades específicas.

[1] https://www.universidades.gob.es/plan-microcreds/

Referencias

[1] Halah Ahmed Alismail: ”Integrate Digital Storytelling in Education”, Journal of Education and Practice, Vol.6, No.9, 2015.

[2] Bernard Robin: ”The Power of Digital Storytelling to Support Teaching and Learning”, Digital Education Review, No.30, 2016.

[3] Joey Lee, Jessica Hammer: ”Gamification in Education: What, How, Why Bother?”, Academic Exchange Quarterly, Vo.15, No.2, 2011.

[4] Miguel Fernández, Iñaki Arenaza, Iñaki Garitano, Jesús Lizarraga, Mikel Iturbe: ”MOOC sobre Hacking ético de MONDRAGON UNIBERTSITATEA - #moocHackingMU”, Jornadas Nacionales de Investigación en Ciberseguridad (JNIC 2016), Granada, 2016.

.