Universidad de Valladolid

TRABAJO FIN DE MÁSTER

MÁSTER EN PROFESOR DE EDUCACIÓN SECUNDARIA OBLIGATORIA Y BACHILLERATO, FORMACIÓN PROFESIONAL Y ENSEÑANZAS DE IDIOMAS

Especialidad de Tecnología e Informática

Gamificación en CyberSeguridad (CyberSecurity Gamification)

Autor:
Dña. Raquel Del Pozo Garrote
Tutor:
Dña. Alma Pisabarro Marrón

Valladolid, 13 de Julio de 2022

Resumen

Este proyecto propone la elaboración de una serie de actividades basadas en gamificación que recogen los contenidos de la asignatura que se ocupa del uso responsable, seguro y crítico de las tecnologías en cuarto de la ESO.

Todas las actividades tienen como objetivo el aprendizaje de las diferentes amenazas a que estamos expuestos así como las distintas herramientas y/o procedimientos con que evitarlas y/o defendernos de ellas.

La metodología que se utiliza es una metodología activa. Es el concepto de acción el que nos lleva a aprender a aprender durante toda la vida. Somos protagonistas junto con los alumnos de éste proceso de enseñanza-aprendizaje.

En la propuesta que aquí se expone, se llevan a cabo retos basados en gamificación que potencian el aprendizaje cooperativo ya que trabajaremos en grupos pequeños donde cada miembro es responsable tanto de su aprendizaje como del aprendizaje de los otros miembros del grupo.

Con este trabajo se intenta fomentar el pensamiento crítico y responsable en nuestros alumnos como ciudadanos activos y participativos en el uso seguro y responsable de Internet y las nuevas tecnologías.

Palabras Clave: amenaza, defensa, gamificación, trabajo colaborativo.

Abstract

This project proposes the elaboration of a series of activities based on gamification that collect the contents of the subject that deals with the responsible, safe and critical use of technologies in the fourth year of ESO.

All activities are aimed at learning about the different threats to which we are exposed as well as the different tools and/or procedures with which to avoid and/or defend ourselves against them.

The methodology used is an active methodology. It is the concept of action that leads us to learn to learn throughout life. We are protagonists together with the students of this teaching-learning process.

In the proposal presented here, challenges based on gamification are carried out that enhance cooperative learning since we will work in small groups where each member is responsible for both their own learning and the learning of the other members of the group.

With this work we try to encourage critical and responsible thinking in our students as active and participatory citizens in the safe and responsible use of the Internet and new technologies.

***KeyWords**: threat, defense, gamification, collaborative work.*

Agradecimientos.

A mi abuela, la maestra, a mi madre, la profesora, a mis herman@s, docentes.

A mi tutora Alma Pisabarro por su ayuda, su empuje y su creatividad. [0]

Índice

Introducción.

Motivación

Es tarea de todos y, especialmente de los docentes, contribuir al completo desarrollo personal, social y laboral de nuestros alumnos.

Por encima de otras implicaciones, “somos responsables de formar a los menores para afrontar los riesgos de Internet” [1]. Procuraremos que hagan un uso responsable y sepan defenderse ante posibles ataques susceptibles de producirse en el uso de medios digitales. El camino pasa por compartir nuestras experiencias y las suyas, a través de este proceso de vida que es la enseñanza-aprendizaje.

La creciente digitalización, el aumento de dispositivos y sistemas IoT e incluso la situación de pandemia vivida no hacen sino proporcionar a los ciberdelincuentes un caldo de cultivo cada vez mayor. Esta situación de vulnerabilidad es, a su vez, una oportunidad para actuar y apostar por el talento en ciberseguridad y conseguir, de éste modo, fortalecer a nuestros alumnos frente a, los cada vez, más sofisticados ciberataques.

Llevaremos a cabo el aprendizaje de las distintas amenazas y defensas cibernéticas a través de la gamificación como eficaz instrumento motivador y generador de aprendizaje. Me sumo al sentir de Ripoll quien en su artículo “Taller de creació de jocs” nos dice que, “aunque el tema ya resulte motivador por sí mismo, uno de los retos de la asignatura es conseguir despertar las ganas de aprender de todo lo que pasa por delante y por sus manos.” [2]. No debemos dejar de lado y recalcar la importancia que adquiere la ciberseguridad en la inclusión, la diversidad y el impulso al talento femenino. [3]

Dado que la propia ciberseguridad implica interactuar con el entorno social, se relaciona de forma natural con el aprendizaje colaborativo, por lo que esta es una de las metodologías seleccionadas para desarrollar esta propuesta.

Objetivos

El objetivo principal de este trabajo es conseguir que el alumnado mejore y adquiera una conciencia crítica y responsable sobre la importancia de la ciberseguridad. Ayudarles a resolver conflictos que puedan surgir en la vida cotidiana y cumplir este cometido mientras se lleva a cabo la labor habitual docente en clase son los propósitos que se persiguen en éste proyecto.

Para conseguir estos objetivos se plantean una serie de actividades gamificadas en forma de retos con la que ayudamos a nuestros alumnos a defenderse con más resiliencia formando equipos que prueben sus defensas mediante ataques simulados y comprendan lo que hace su adversario anticipándose a él como medida de prevención.

Trabajaremos en el segundo ciclo de la ESO, en cuarto curso, un momento importante, crucial y decisorio en la continuidad de sus estudios. Nos ocupamos en particular de la competencia digital entre otras competencias. En el nuevo curriculum se plantean los contenidos "en todas sus dimensiones mediante, por ejemplo, la realización de búsquedas en internet con espíritu crítico, la gestión del espacio personal de aprendizaje, la creación de contenidos digitales de diversa índole, el uso de plataformas digitales para comunicarse y colaborar, la valoración de los riesgos digitales y la adopción de medidas para evitarlos o minimizarlos, o el desarrollo de aplicaciones informáticas".

"El tercer bloque de Seguridad y bienestar digital persigue el desarrollo de actitudes preventivas y correctivas en el alumnado en los tres pilares de la seguridad, el de los equipos, el de los datos y el de las personas, conociendo los riesgos existentes en el mundo digital y adquiriendo estrategias para protegerse de ellos". [4]

La ciberseguridad total no existe, es necesario que el alumno sea capaz de reconocer los riesgos que pueden afectar a su integridad y a la seguridad de los sistemas informáticos y adoptar conductas adecuadas de protección.

El propósito pasa por integrar los aprendizajes que abordaremos en esta actividad con el curso y el resto de las materias. Ello le permitirá continuar sus estudios con éxito o incorporarse, en su caso, al mundo laboral con el grado adecuado de adquisición de la competencia digital.

Como ya se ha determinado con anterioridad, el objetivo principal de éste trabajo es desarrollar una actividad en forma de retos que conciencien a los alumnos y desarrollen su pensamiento crítico y responsable a cerca de las ciberamenazas a que están expuestos.

Alcanzar este objetivo principal nos lleva a abordar otros específicos que surgen en el desarrollo de éste trabajo de forma ineludible, que aunque se escapan del ámbito de este trabajo, si pretendemos hacer una pequeña aportación. Estos son:

- Ayudar al **desarrollo personal y social** de nuestros alumnos

  En el preámbulo de la Ley de protección integral a la infancia y la adolescencia se establece la protección del menor que se extiende a toda la Unión Europea y expresa la protección de los derechos del niño según el Tratado de Lisboa. [5][5]

  El Consejo de Europa garantiza esta protección a través de varios Convenios como el de Lanzarote, Estambul, el Convenio sobre la lucha contra la trata de seres humanos o el Convenio sobre la Ciberdelincuencia.

  Nos hacemos eco de las conclusiones de la Comisión Europea entre las que encontramos que "Necesitamos una estrategia que incluya a todos los niños y nos ayude cuando nos encontremos en situaciones vulnerables, una estrategia que promueva y apoye nuestro derecho a participar en las decisiones que nos afectan. Porque no debería decidirse sin los niños nada que se decida para ellos. Es hora de normalizar la participación de los niños". [6]

- Impulsar el desarrollo de las **competencias clave** en particular la competencia digital que "implica el uso seguro, saludable, sostenible, crítico y responsable de las tecnologías digitales para el aprendizaje, para el trabajo y para la participación en la sociedad, así como la interacción con estas". [7] Esta competencia abarca y se hace extensible a la seguridad, el bienestar, la ciberseguridad o la privacidad.

- **Motivar hacia el aprendizaje** a través de la gamificación.

  Trataremos de hacer vivir una experiencia interesante y cautivadora a nuestros alumnos. De nuevo volvemos la vista hacia el pensamiento de Oriol Ripoll quien apuesta por hacer nacer la motivación de la propia implicación de los alumnos. Según Oriol, "sería un fracaso si después de una actividad (y aún más si es gamificada), los alumnos solo estuviesen mirando la puntuación que han conseguido y dejasen a un lado el proceso que se ha seguido. Por este motivo es importante entender qué elementos podremos usar para permitir la motivación intrínseca, es decir, que la actividad se lleve a cabo porque se quiere hacer y no porque hay una recompensa externa."[2]

- Tomar conciencia del significado de **inclusión y diversidad.**

  La discapacidad forma parte de la persona y está influida por factores intrínsecos y extrínsecos de forma tal que está presente de por vida. Trataremos de integrarla en nuestras aulas para atender así a la inclusión y a la diversidad.

Moreno Rodriguez lo expresa de forma contundente e irrebatible, “a algunos estudiantes, a algunos de nuestros niños, les acompaña una discapacidad que puede estar presente de manera más o menos intensa. Pero esa intensidad dependerá, no solo de los aspectos físicos que componen el contexto escolar, sino de los materiales, las metodologías, los procesos y la implicación del grupo de iguales. Y cuando la accesibilidad se hace transversal a todos estos elementos y se integra de manera adecuada en la vida escolar hablamos de educación inclusiva, de atención a la diversidad y, por supuesto, de las implicaciones didácticas que tiene para el ejercicio profesional del maestro.”[8]

- Contribuir a aumentar la presencia de **mujeres en la tecnología y la ciencia.**

  Es inevitable abordar la escasa presencia de mujeres en la ciencia más cuando voy a convertirme en un referente para ellas. Se trata de un problema complejo que intentaré paliar en mi actividad docente diaria. En este punto me subscribo a las palabras de la Directora General de la UNESCO, Irina Bokoba, quien nos dice, y cito textualmente, “Las niñas se siguen enfrentando a estereotipos y restricciones sociales y culturales, que limitan su acceso a la educación y la financiación para la investigación, impidiéndoles así cursar carreras científicas y desarrollar todo su potencial.”[9]

- Apostar por disminuir el **abandono escolar**.

  Sabemos que es un análisis complejo y que “el abandono escolar está vinculado al desempleo, la exclusión social, la pobreza y una mala salud. Hay muchas razones por las que algunos jóvenes abandonan prematuramente la educación y la formación: problemas personales o familiares, dificultades en el aprendizaje o una situación socioeconómica frágil”. [10]

  Ofrecemos a los alumnos una oportunidad para continuar sus estudios despertando su interés hacia el mundo de la informática. En particular, hacia la seguridad informática, que sabemos que lleva aparejadas expectativas laborales seguras. En caso de no finalizar con éxito este cuarto curso podrían acceder a la Formación Profesional Básica, que “posibilita la progresión en el Sistema Educativo, el desempeño cualificado de una profesión y tiene los mismos efectos laborales que el título de Graduado en Educación Secundaria Obligatoria para el acceso a empleos públicos y privados. Tiene carácter gratuito y una duración de 2 años, 2000 horas de formación teórico-prácticas, de las cuales, como mínimo, 240 deberán desarrollarse en centros de trabajo”. [11]

- Potenciar el uso de **metodologías activas** como son la colaborativa y la gamificación.

  Para que el alumnado adquiera los conocimientos científicos y técnicos del curriculum apostamos por aplicar “metodologías de trabajo creativo para desarrollar ideas y soluciones innovadoras y sostenibles que den respuesta a

necesidades o problemas planteados, aportando mejoras significativas con una actitud creativa y emprendedora.” [12]

- Promover lo establecido en el artículo 45 de la L.O. 8/2021, de 4 de junio, de **protección integral a la infancia y la adolescencia frente a la violencia**, donde se establece el uso seguro y responsable de Internet, de la siguiente forma: “Las administraciones públicas desarrollarán campañas de educación, sensibilización y difusión dirigidas a los niños, niñas y adolescentes, familias, educadores y otros profesionales que trabajen habitualmente con personas menores de edad sobre el uso seguro y responsable de Internet y las tecnologías de la información y la comunicación, así como sobre los riesgos derivados de un uso inadecuado que puedan generar fenómenos de violencia sexual contra los niños, niñas y adolescentes como el cyberbullying, el grooming, la ciberviolencia de género o el sexting, así como el acceso y consumo de pornografía entre la población menor de edad.”[13]

- Abordar la **materia de digitalización** del nuevo curriculum de la E.S.O., “El bloque «Seguridad y bienestar digital» se centra en los tres pilares de la seguridad: el de los dispositivos, el de los datos y el de la integridad de las personas. Busca que el alumnado conozca e implemente medidas preventivas para hacer frente a los posibles riesgos y amenazas a los que los dispositivos, los datos y las personas están expuestos en un mundo en el que se interactúa constantemente en entornos digitales. Pone especial énfasis en hacer consciente al alumnado de la importancia de cuidar la identidad, la reputación digital, la privacidad de los datos y la huella digital que se deja en la red. En este bloque también se abordan problemas como los discursos de odio, el ciberacoso, la suplantación de identidades, los contenidos inadecuados y el abuso en los tiempos de conexión, asuntos que pueden suponer amenazas para el bienestar físico y mental del alumnado. Se trata de un bloque de naturaleza eminentemente actitudinal dirigido a promover estrategias que permitan al alumnado tomar conciencia de esta realidad y generar actitudes de prevención y protección, a la par que promover el respeto a los demás.”[4]

Metodología

A continuación, paso a exponer, la metodología utilizada en la elaboración de éste trabajo. La labor de recopilación de información se ha llevado a cabo a través de consultas en Internet de trabajos académicos, libros o revistas especializadas de las que haré mención detallada en el apartado bibliográfico.

El acceso a ésta documentación se ha basado fundamentalmente en el uso de buscadores académicos, portales científicos, publicaciones electrónicas como SciELO (Scientific Electronic Library Online), Dialnet, Google Scholar o Academia.edu entre otros.

La observación del funcionamiento del aula en mi periodo de prácticas y la consecuente determinación de la necesidad de dinamización de la misma es la razón que me ha guiado hacia la elección del uso de gamificación en el aula.

En suma, el método observacional, es el que ha guiado mis pasos en la elaboración de éste trabajo. Observación que he realizado de los alumnos, del profesorado, del centro, tanto dentro como fuera del aula e incluso de mi misma en un sano ejercicio de autoevaluación.

Resumen del contenido

El contenido de éste trabajo se distribuye en tres capítulos, el primero estará dedicado al concepto de gamificación, ya que la actividad se fundamenta en que los alumnos comprendan los distintos ciberataques y las defensas contra ellos a través de un reto en forma de juego.

En el segundo abarcaré la teoría de ciberataques especificando tanto una escueta clasificación de los mismos como las medidas de protección oportunas.

El tercero ocupará la actividad propuesta, entorno, desarrollo y herramienta de evaluación de la misma.

Por último, se determinan las conclusiones y las líneas futuras de actuación.

La memoria concluirá con un glosario de términos relativos a ciberseguridad, referencias utilizadas en la elaboración de la memoria y una serie de anexos teóricos orientativos para el desarrollo de la actividad.

Capítulo 1. Concepto de gamificación vs Juego Serio.

Nos aproximamos al concepto de gamificación [14], cuyo uso desaconseja la R.A.E. a favor de ludificación, con la intención de imbuirnos de acción, de provocar en el alumno la ilusión por saber, de despertar sus sentidos. Como nos dice Oriol Ripoll, "El juego, o la vivencia de éste, tiene el poder de transformar la actitud de un usuario pasivo a un generador activo, y que lo haga voluntariamente".[2]

Del gran número de definiciones u aproximaciones que he encontrado respecto al concepto de gamificación, me quedo, sin lugar a duda, con esta: **"**Gamificar es hacer jugar. La gamificación no se mide por los premios, sino por el disfrute del jugador durante el proceso."[15]

Mi experiencia en el aula, desde que tengo memoria, ha estado bañada por el aburrimiento. Por este motivo me hago eco de las palabras de Mora quien sostiene que "la curiosidad, lo que es diferente y sobresale en el entorno, enciende la emoción. Y con ella, con la emoción, se abren las ventanas de la atención, foco necesario para la creación de conocimiento". [16]

Este trabajo se lleva a cabo en pequeños grupos que realizan un aprendizaje cooperativo. Vygotsky determinaba que durante el juego, aquel que ocurre de manera natural, son los niños quienes controlan su acción y crean una "zona de desarrollo próximo", que es dónde se produce el aprendizaje. [17]

Adoptamos el concepto de aprendizaje cooperativo como "el empleo didáctico de grupos reducidos en los que los alumnos trabajan juntos para maximizar su propio aprendizaje y el de los demás." [18] El juego siempre ha sido un elemento crucial para la socialización, ser parte de un equipo contribuye al aprendizaje cooperativo aunque no debemos creer que la magia opere siempre.

Pasamos a significar determinados elementos del juego que consideramos relevantes a la hora de clarificar el concepto de gamificación.

Un componente importante es el establecimiento de avatares, tanto individuales como de grupo. Son un elemento pedagógico que permite al alumno, al mismo tiempo, ser y no ser, mostrar sus contradicciones y mejorar los sentimientos de autoestima.

El avatar constituye "La representación ideal de uno mismo, es la causante de una sensación de agrado, de una imagen positiva de uno mismo, de una sensación de distanciamiento que son vitales también dentro del proceso de aprendizaje". [19]

Otros factores a tener en cuenta como la estimulante competición, el establecimiento de rankings y los feedback son factores cambiantes y progresivos.

Los espacios, las reglas e incluso el reto planteado permiten crear un escenario de ficción en el que desenvolverse con autonomía.

El error humano es uno de los mayores responsables de los incidentes de seguridad. El error constituye una forma de aprendizaje, de llevar a cabo, a través de su descubrimiento, la competencia de "aprender a aprender".

En suma, "la idea de gamificar propone plantear el proceso de enseñanza-aprendizaje basado en el juego y sus dinámicas, donde los alumnos participantes son los jugadores, los protagonistas del juego y por ende del proceso de enseñanza-aprendizaje, pero deben sentirse implicados, que forman parte del proceso tomando decisiones, asumiendo riesgos, superando retos y recibiendo una retroalimentación inmediata." [20]

Debemos distinguir el concepto de gamificación del de juego serio.

Los "Juegos Serios" o *Serious Games*, según la taxonomía de Sawyer y Smith, "son aquellos juegos diseñados específicamente para potenciar el aprendizaje de unos contenidos didácticos concretos, y no tanto el entretenimiento (ejemplos: *Duolingo*, *Box Elements*, etc.). A diferencia de la gamificación, la duración es corta, por eso son idóneos para adquirir conocimientos y/o habilidades asequibles en un tiempo relativamente corto". [21]

El juego serio abarca todos los elementos de un juego, mientras que, la gamificación consiste en utilizar uno o más de estos elementos.

La gamificación emerge como una técnica, estrategia o metodología ya desde hace años. Está consolidada y un gran número de experiencias de éxito avalan su uso.

Prieto Andreu señala, "en el ámbito educativo, la gamificación se ha ganado un importante espacio de reflexión y análisis, al ser empleada, cada vez más, como técnica o estrategia para motivar al estudiantado en su proceso de aprendizaje". [22]

La gamificación es, por tanto, una poderosa metodología que suma al juego el proceso de enseñanza-aprendizaje de forma más motivadora y atractiva para el alumnado y posibilita de éste modo la construcción de un aprendizaje significativo del mismo modo que propicia el desarrollo de una actitud crítica y responsable y mejora las interacciones sociales.

Capítulo 2. Teoría de Ciberataques

2.1. ¿Qué es un ciberataque?

Son técnicas y/o herramientas con las que los ciberdelicuentes buscarán sacar beneficio de problemas o fallos de seguridad. Encuentran agujeros de seguridad debidos a malas prácticas como son, en el caso de las contraseñas, utilizar la misma contraseña para distintos accesos, o utilizar contraseñas débiles o fáciles de recordar con patrones sencillos, uso de información personal para generarlas o apuntarlas y/o guardarlas en archivos sin cifrar, en webs o en el navegador.

2.2 Tipos de ciberataques:

- **Ataques a contraseñas.**

"Un ataque de fuerza bruta a las contraseñas es en esencia un método en el que el ciberdelincuente prueba a entrar en un sistema muchas veces con diferentes combinaciones de caracteres (alfabéticos, numéricos y especiales) utilizando un *software* específico, esperando que ocurra alguna coincidencia con nuestra contraseña. Los ciberdelincuentes se valen de la mala práctica común de utilizar la misma contraseña en distintos servicios. Además, en ocasiones estas contraseñas "reutilizadas" pueden estar ya comprometidas, ser muy comunes o venir por defecto en los sistemas o aplicaciones, por ejemplo las del tipo "12345" o "admin"."[23]

INCIBE te insta para que pruebes introducir una contraseña que hayas utilizado y comprobaras cuantas veces ha sido utilizada. [24]

- **Ataques por ingeniería social.**

"Cuando hablamos de ingeniería social, nos referimos a los ciberataques en los que se abusa de la buena fe de las personas para que realicen acciones que puedan interesar al ciberdelincuente. Si lo situamos en el contexto de la ciberseguridad, nos referimos a la manipulación psicológica que tiene como finalidad, por ejemplo, que un

usuario haga clic en un enlace, descargue un archivo que infecte su equipo o revele información confidencial, ya sean datos personales, credenciales de acceso, información bancaria, etc."[25]

El *phishing* es la técnica que acapara el mayor número de ataques de ingeniería social.

Para concienciar a los alumnos de la importancia y problemática que llevan este tipo de ataques se podrían poner ejemplos reales como el siguiente. Un hombre víctima de *phishing* al que la rabia le lleva a declarar, "Si me entero de algún nombre, lo encontraré y lo pagará con creces. No confío en la justicia", dice la víctima del fraude. Como prueban las cifras de casos resueltos, es extremadamente improbable que ocurra. [26]

- **Ataques a las conexiones.**

"Los ataques a las conexiones inalámbricas son muy comunes, y los ciberdelincuentes se sirven de diversos software y herramientas con las que saltarse las medidas de seguridad e infectar o tomar control de nuestros dispositivos. Generalmente, este tipo de ataques se basan en interponerse en el intercambio de información entre nosotros y el servicio web, para monitorizar y robar datos personales, bancarios, contraseñas, etc." [27]

Si notas que tu conexión se ralentiza es posible que te hayan hackeado el WiFi, corres peligros que atañen a tu integridad mayores como son el robo de información, la conexión a nuestros dispositivos o la responsabilidad ante acciones ilícitas. Piensa que la configuración del router puede mejorarse así como las opciones de seguridad.

Si apagas tus equipos y la luz del router parpadea, un extraño se ha colado en casa. Recomendaciones de la Oficina de Seguridad del Internauta [28] nos proponen utilizar *Wireless Network Watcher* para detectarlo o *Android ezNetScan*.

- **Ataques por malware.**

Los ataques por malware se sirven de programas maliciosos cuya funcionalidad consiste en llevar a cabo acciones dañinas en un sistema informático y contra nuestra integridad.

Ataques como el ransomware que es uno de los que más afecta a las empresas. De nuevo el INCIBE nos proporciona una guía segura para recuperarnos ante un ataque tan peligroso que pone en jaque a toda nuestra empresa. [29]

2.3. Medidas de protección.

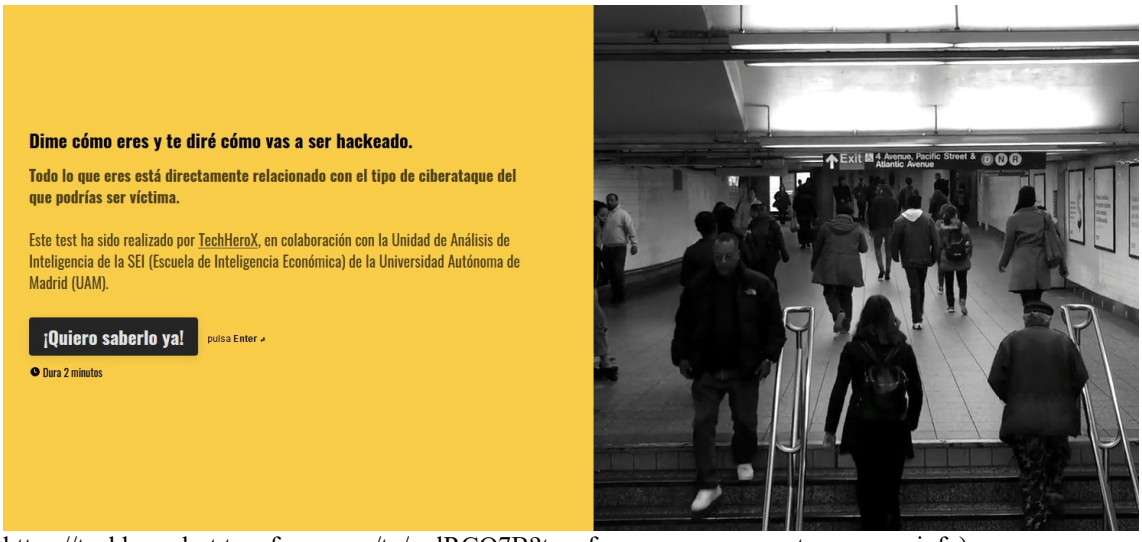
Muchos de estos ataques se ven afectados por el factor humano. Entre otras medidas de protección básicas el INCIBE [30] establece las siguientes,

- Utiliza un antivirus
- Mantén el S.O., navegador y aplicaciones siempre actualizados.
- Utiliza contraseñas robustas y diferentes.
- Desconfía de los adjuntos sospechosos, enlaces o promociones demasiado atractivas.
- Ten cuidado por dónde navegas.
- Descarga sólo de sitios oficiales.
- Evita conectarte a redes públicas o a conexiones inalámbricas desconocidas.
- No compartas tu información personal.
- Haz copias de seguridad.

2.4. Dime cómo eres y te diré cómo vas a ser hackeado.

Es importante que los alumnos entiendan que la ciberseguridad es un problema que nos afecta a todos, a ellos también. Una forma de hacerles conscientes de los peligros a los que se exponen es mostrarles sus debilidades particulares. Para ello nos hacemos partícipes de la investigación reciente de María Laura Mosqueda, CEO y fundadora de TechHeroX en relación al *hacking* psicológico.

En la siguiente imagen, se muestra un test ofrecido por la empresa TechHeroX, [31] cuya realización nos permitirá determinar el perfil que nos define como posibles víctimas de fraude.



(Fuente: https://techheroxbot.typeform.com/to/pplRCO7B?typeform-source=www.tecnonews.info)

Empoderar a nuestros alumnos y, del mismo modo, a nosotros mismos pasa por el autoconocimiento. No es probable que podamos cambiar pero si comprendernos para ser menos vulnerables ante las amenazas.

Nos acercamos a una definición formal del *psicohacking* a través de la Oficina de Seguridad del Internauta que la define como "la disciplina que engloba los principios de Psicología, Sociología y Antropología que explota la Ingeniería Social y en los que fundamenta su éxito y efectividad. El también llamado *hacking* psicológico, incluye el estudio de los nuevos paradigmas y comportamientos sociales generados por la inmediatez, alcance y potencial repercusión en nuestras vidas del uso de las nuevas tecnologías."[32]

Desde TechHeroX explican que es importante entender cómo funcionan los atajos de nuestro cerebro, pues son muchos los sesgos cognitivos que nos llevan a juicios incorrectos y convertirnos en víctimas de ciberdelitos. [33]

Un *coach*, como Gonzalo Alvarez Marañón [34], nos ayuda a entender las decisiones irracionales que tomamos en ciberseguridad y cómo superar los errores de pensamiento que sesgan nuestros juicios. Sesgos, entre otros, que nos llevan a tener pensamientos tales como "eso no me va a pasar a mí nunca" o "esto me suena seguro que es verdad" o "yo tengo razón" o "la primera impresión es la que cuenta".

No debemos permitir que ningún elemento distractor nos aleje del objetivo que no es otro que la seguridad de nuestros alumnos. En este punto nos sumamos al parecer de la directora de la unidad de análisis de inteligencia de la SEI (UAM), Eugenia Hernández Sanchez, en su comparecencia ante el Congreso de los Diputados en junio del 2021: "En los entornos *Humint,* la llamada inteligencia obtenida por fuentes humanas, se plantea que pese al desarrollo exponencial de la tecnología y su impacto en todos los entornos de nuestra existencia, el centro de nuestro trabajo son los seres humanos, un elemento esencial que nunca se fue, y la máxima de Protágoras, que el hombre es la medida de todas las cosas, no ha caducado."[35]

Capítulo 3. Actividades Propuestas

La actividad propuesta está inspirada en el tradicional juego de mesa "*The Clue"* adaptándolo al tema de la ciberseguridad. Se ha optado por éste juego debido a la similitud existente entre conceptos básicos de seguridad como son las pistas, la existencia de un asesino o ciberdelicuente en este caso y el proceso de descubrimiento del delito o amenaza.

Cada actividad consiste en una partida del juego. Podrán realizarse en número y tiempo o frecuencia en forma variable, siempre y cuando se lleven a cabo conformes a las exigencias del curriculum y al desarrollo del curso en particular. Por tanto es una actividad flexible, como hemos dicho, fácilmente adaptable al curriculum.

3.1. Entorno.

La actividad se desarrollará en el segundo ciclo de la Educación Secundaria Obligatoria, en cuarto curso. Estará orientada a la asignatura específica Tecnologías de la Información y la Comunicación.

El número aproximado de alumnos por aula es de 25. Se crearán por tanto 5 grupos de 5 alumnos.

La propuesta forma parte del Bloque 4. Seguridad Informática.

La materia de esta asignatura se organiza en seis bloques de contenidos. El Bloque 4 que se centra en el estudio de la Seguridad Informática.

3.2. Temporalización.

Bloque 4. Seguridad Informática			
Sesiones 50' dos por semana		**Contenidos Teóricos**	**Actividad**
MES Enero	**Sesión 1**	Actividad para valorar el conocimiento previo de los alumnos sobre Seguridad Informática.	Debate en el Aula Caso 1. Chiringuito **"Si tiras la toalla que sea en la playa".** Caso 2. Empresa **"No hay mal que cien años dure ni pena que el chocolate no cure".** Caso 3. **No siempre tengo la razón pero nunca me equivoco.**
MES Febrero	**Sesión 2**	Amenazas en la Red. Navegación segura.	*Kahoot*. ***Cyber* T.I.A. *Exam***
	Sesión 3	Conceptos sobre violencia sexual en la red.	Sopa de Letras. **Violencia en la red**
	Sesión 4	Seguridad en Redes. Análisis de ficheros. Esteganografía.	WebQuest. **Mami que será lo que esconde el pato.**
	Sesión 5	Repaso de Contenidos trabajados en sesiones anteriores.	Actividad Final. **Buscando en la basura.**
	Sesión 6	Evaluación	Presentación Actividad Final

Los objetivos para este bloque 4 los establece el curriculum y nos hacemos eco de ellos: "Actualmente casi todos los ordenadores y dispositivos electrónicos se encuentran conectados en red, facilitando la transmisión de información y el acceso a un sinfín de recursos, sin embargo, esta interconexión ha generado problemas en la seguridad de los sistemas de información tanto en el entorno laboral como en el doméstico. Reconocer estos riesgos y adoptar las medidas adecuadas de seguridad activa y pasiva que posibiliten la protección de datos e intercambio seguro de información es fundamental para un desarrollo normal de nuestras actividades con ellos."[7]

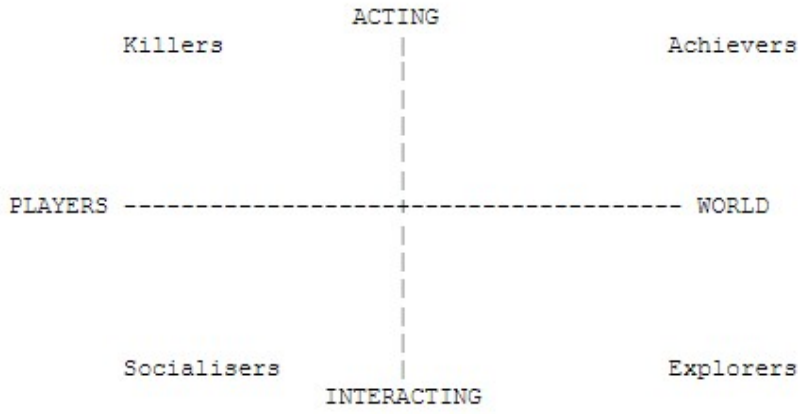
Del mismo modo el nuevo borrador del curriculum [4], establece la ordenación y las enseñanzas mínimas de la Educación Secundaria Obligatoria, y propone el concepto de Seguridad y bienestar digital como aquel que abarca:

- Seguridad de dispositivos: medidas preventivas y correctivas para hacer frente a riesgos, amenazas y ataques a dispositivos.
- Seguridad y protección de datos: identidad, reputación digital, privacidad y huella digital. Medidas preventivas en la configuración de redes sociales y la gestión de identidades virtuales.
- Seguridad en la salud física y mental. Riesgos y amenazas al bienestar personal. Opciones de respuesta y prácticas de uso saludable. Situaciones de violencia y de riesgo en la red (ciberacoso, sextorsión, acceso a contenidos inadecuados, dependencia tecnológica, etc.).

La propuesta de actividad está pensada para llevarse a cabo en la Sesión 5, al finalizar el bloque 4, y antes de comenzar el siguiente bloque de contenidos.

3.3. Jugadores

Es importante tener en cuenta a nuestros alumnos, sus características específicas como jugadores. Nos hacemos eco aquí de la clasificación establecida por Richard Bartle [36] según la personalidad y comportamiento serán:



(Fuente: Imagen tomada de Richard Bartle. MUSE LTD Cochester, Essex, UK https://www.researchgate.net/publication/247190693_Hearts_clubs_diamonds_spades_Players_who_suit_MUDs.)

Ganadores *(Killers)*, son ganadores, necesitan ser los mejores y conseguir el primer puesto.

Aventureros *(Achievers)*, son aventureros y se mueven guiados por un afán de superación personal.

Socializadores *(Socialisers)*, usan el juego para comunicarse con otros, jugar es compartir y hacer amigos.

Exploradores *(Explorers)*, intentan descubrir y experimentar con el juego en sí mismo.

Tendremos en cuenta sus características al distribuir a nuestros alumnos en los distintos grupos para que éstos resulten heterogéneos y propiciar, de este modo, la atención a la inclusión y diversidad. Como hemos mencionado y dado el número aproximado de alumnos por aula, se formarán cinco equipos de cinco alumnos.

3.4. Mini Actividades

Estas actividades que planteamos como complementarias podrán realizarse en los últimos minutos de las sesiones de trabajo, siempre que el desarrollo de la clase lo permita. Tienen como objetivo afianzar conocimientos y crear un clima distendido en el aula.

Las distintas recompensas obtenidas tras la evaluación no serán acumulables.

3.4.1. *Kahoot.*

Nombre de la Actividad: *Cyber* T.I.A. *Exam*

Descripción. El alumno contestará a las preguntas del *Kahoot.*

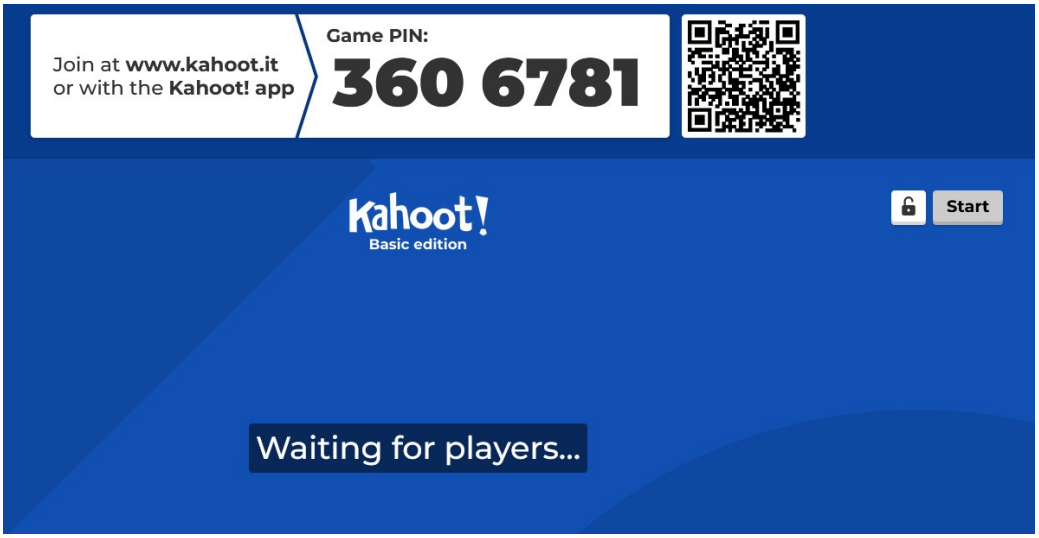
Duración.10’ cada caso.

Técnica didáctica. Trabajo individual. Repaso de contenidos de seguridad informática. Se presentan las definiciones y se pide el concepto. Solo habrá una respuesta correcta entre cuatro opciones posibles.

Evaluación. La realizará el profesor por observación valorando los resultados. Tomará buena cuenta de la misma en su cuaderno de bitácora. En cualquier caso, los tres alumnos que consigan acceder al pódium obtendrán una recompensa que consistirá en un punto de la nota final.

Documentación didáctica.

Kahoot es una herramienta didáctica para reforzar el aprendizaje en la que el alumno es concursante de un juego. Los alumnos eligen un alias o nombre de usuario y contestan a una serie de preguntas por medio del móvil. Se utilizará el modo de juego individual.



(Fuente: https://create.kahoot.it/share/ciberseguridad/815e5b75-0bb9-4c71-b8a5-07843d9789d3)

3.4.2. Esteganografía.

Nombre de la Actividad: Mami que será lo que esconde el pato.

Descripción. El alumno selecciona una imagen y la abre con *SilentEye* [37], aplicación diseñada para un uso sencillo de esteganografía. El alumno esconde mensajes en imágenes o sonidos. Para ello utiliza la función *Encode* y almacena la password.

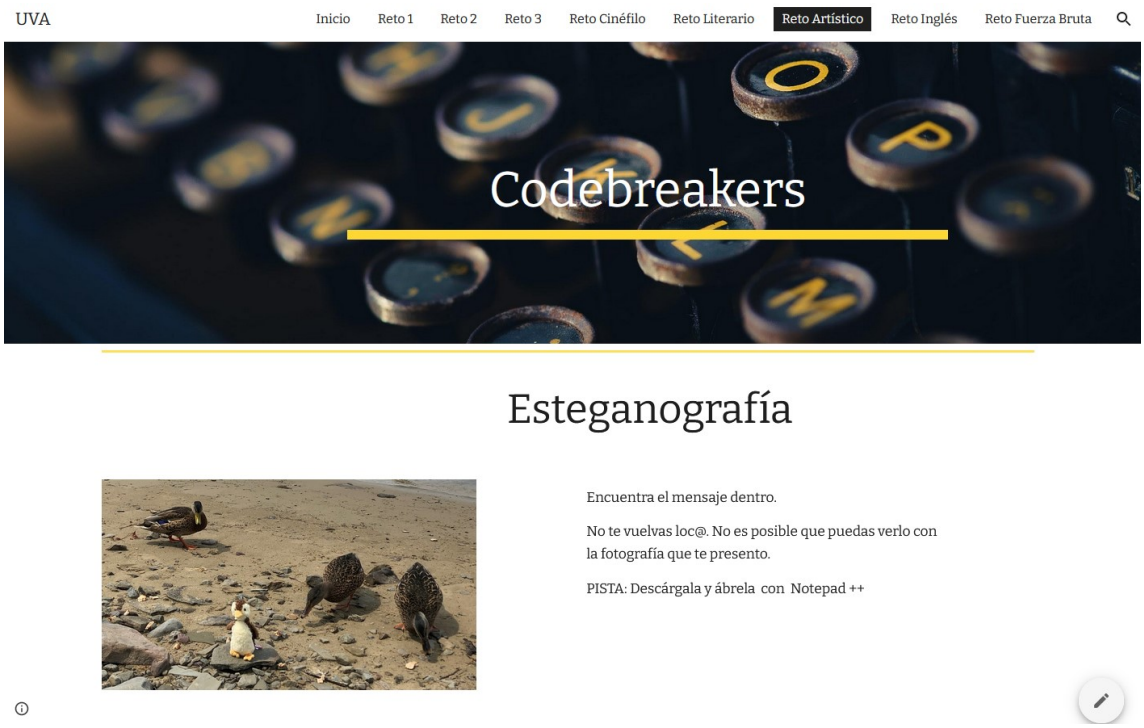
Otra opción de juego es encontrar la password en la imagen del pato.

Duración. 15'

Técnica didáctica. Se trata de un trabajo individual que nos acerca a la forma de investigación que se realiza en informática forense.

Evaluación. El primer alumno en realizar con éxito la actividad será el segundo en elegir avatar en la actividad final.

Documentación didáctica. Acercamos al alumno al concepto de la esteganografía como el estudio y aplicación de técnicas que permiten ocultar mensajes u objetos.



(Fuente: https://sites.google.com/view/retocodebreakers/inicio)

3.4.3. Sopa de Letras.

Nombre de la Actividad: Violencia en la red

Descripción. Los alumnos buscarán en la sopa de letras conceptos que definan distintas formas de violencia en la red

Duración.10'.

Técnica didáctica. Trabajo individual. Repaso de conceptos realizado de forma individual por el alumno.

Evaluación. La realizará el profesor. Recogerá las sopas de letras después del tiempo asignado. Tomará buena cuenta de la misma en su cuaderno de bitácora. El primero en resolverla será el tercero en elegir avatar.

Documentación didáctica.

Trataremos de que los alumnos tengan presentes las distintas formas de violencia sexual. A través del nombre se alcanza el concepto. Es una forma de repaso de contenidos. Más allá del juego es importante que el alumno comprenda el gran número

de formas de violencia sexual que existen y que esto le haga adoptar una actitud crítica y responsable en situaciones reales que pudieran producirse.

C	A	N	S	W	H	N	J	C	R	J	D	K	E
N	I	Q	G	N	L	S	T	J	B	S	W	X	B
N	U	B	T	H	C	V	P	W	L	C	M	P	Q
T	C	G	E	Z	C	J	S	O	F	B	A	G	N
P	X	N	H	R	L	B	B	C	G	Z	Z	P	N
D	H	K	E	D	B	K	B	N	A	U	V	I	G
B	G	I	K	B	X	U	I	N	X	E	U	E	T
R	Z	Y	S	E	O	M	L	A	B	P	K	R	F
E	A	F	S	H	O	H	Y	L	N	Z	T	A	C
A	L	Y	S	O	I	B	B	U	Y	E	Y	R	V
J	R	P	R	Z	D	N	W	J	N	I	L	K	G
O	I	G	J	W	Y	M	G	B	K	Q	N	D	V
F	H	F	S	E	X	T	I	N	G	K	E	G	N
H	A	P	P	Y	S	L	A	P	P	I	N	G	V

ENCUENTRA ESTAS PALABRAS

SEXTING
CIBERBULLYING
HAPPYSLAPPING
GROOMING
PHISHING

(Fuente: https://puzzel.org/es/features/crear-sopa-de-letras)

3.4.4. Debate en el Aula.

Nombre de la Actividad:

- Caso 1. Chiringuito "Si tiras la toalla que sea en la playa".
- Caso 2. Empresa "No hay mal que cien años dure ni pena que el chocolate no cure".
- Caso 3. No siempre tengo la razón pero nunca me equivoco.

Descripción. Un alumno por iniciativa propia leerá el caso y libremente la clase entera participará en un debate abierto.

Duración.15' cada caso.

Técnica didáctica. Lectura de un caso que abrirá un debate con planteamiento de preguntas por parte del profesor

Evaluación. La realizará el profesor por observación valorando tanto la participación como la información aportada. Tomará buena cuenta de la misma en su cuaderno de bitácora. La recompensa para los alumnos que participen con acierto en el debate será de un punto en la nota final.

Documentación didáctica.

Son casos reales o no que ayudarán a nuestros alumnos a formarse en ciberseguridad y evitar así ser víctimas de fraudes y/o ataques cibernéticos. Estos se plantearan en el aula con la intención de abrir un debate. Se trata de que los alumnos tomen conciencia de la importancia de mantener a los equipos protegidos y sean capaces de buscar soluciones. Los objetivos de la actividad son tanto comprender la importancia de la protección de equipos frente a posibles ataques como conocer las posibles soluciones a tomar frente a un ataque informático. La dinámica pasa por la lectura del caso, seguida de un debate o discusión de la lectura e intervenciones del profesor, en caso necesario, planteando preguntas.

CASO 1. Chiringuito si tiras la toalla que sea en la playa.

María está trabajando en el pequeño negocio familiar de hostelería, se trata de un chiringuito veraniego. Tiene 16 años y le encantan las redes sociales, Instagram, Twitter, Facebook. Se ha puesto al frente de la contabilidad de la empresa. Está esperando un pedido que repone cada semana. Hace un par de días que pagó. Está empezando a ponerse nerviosa. Lleva poco tiempo haciéndose cargo de la contabilidad y esto le provoca falta de seguridad. Además le comunicaban un cambio de banco. Para colmo, aún no ha llegado la mercancía y su madre lleva preguntándole desde mediados de semana qué está pasando. Llama a su proveedor y éste le dice que no han cambiado de banco, que debe ser un error. ¿Que puede haber pasado?

(Fuente: INCIBE. Protege tu empresa Protege tu empresa | INCIBE)

CASO 2. No hay mal que cien años dure ni pena que el chocolate no cure.

Sonia es Responsable del Departamento de Calidad de una empresa de chocolate. Su equipo está compuesto por veinte compañeros. Ella no tiene formación en ciberseguridad, siempre se le ha resistido el ordenador, lo suyo es el chocolate. Un día recibe una llamada de soporte informático. Solo la llamada predispone a Sonia hacia un estado de nerviosismo por la inseguridad que le produce la falta de formación en este tema. El operador de soporte informático es muy amable y le explica detalladamente el motivo de su llamada, han detectado un software malicioso y quiere ayudarle para solucionar el problema. El operador necesita conectarse en remoto al equipo informático y pide a Sonia que autorice la conexión. ¿Que podría pasar?

CASO 3. No siempre tengo la razón pero nunca me equivoco.

Elena se siente segura. Ha instalado un poderoso antivirus y está protegida contra cualquier tipo de *malware*. Y se hace oír, "A mí no me va a pasar nada malo". Pero el malware evoluciona y se hace cada vez más fuerte y sofisticado. Una mañana, pendiente de un paquete, recibe un correo con un adjunto. Tiene mucha prisa y lo abre. Se ejecutan macros asociadas al mismo y ya no hay vuelta atrás. ¿Qué ha pasado? ¿Qué puede hacer ahora? ¿Y cómo habría podido evitarlo?

3.5. Actividad Final

3.5.1. Dinámicas

A continuación abordamos el planteamiento del juego de forma genérica. Se trata del nivel conceptual más alto de la gamificación, las dinámicas, que abarcan la narrativa, progresión, emociones, limitaciones y relaciones entre otros aspectos.

El profesor actuará como ciberdelincuente dejando pistas y/o falsas pistas en los distintos escenarios para que los grupos de alumnos, convertidos en investigadores puedan localizar el ataque perpetrado y proponer una posible defensa contra el mismo así como localizar el escenario dónde se produjo la amenaza.

Se trabajará de forma cooperativa en grupos de alumnos. El establecimiento de los grupos será llevado a cabo por el profesor garantizando que se trate de grupos heterogéneos.

A cada grupo le corresponde, al comienzo del juego, un escenario y un ataque. Con lo cual cada equipo deshecha su propio escenario y ataque como solución al ciberataque.

El trabajo en grupo y la competitividad genera que los alumnos tengan consideración individual respecto al grupo.

Se crea un hilo argumental en torno al juego que propone una liga de detectives especializados en ciberseguridad. Estos detectives disponen de características propias que constituyen sus fortalezas y que actuarán como defensas frente a posibles ataques cibernéticos.

Se convierte en ganador el equipo que descubre el escenario, el tipo de ataque y una posible defensa contra éste ataque.

Se desplazarán a los distintos escenarios e intentarán localizar pistas que les lleven a determinar el ataque perpetrado. Se descargarán y estudiarán los códigos QR que encuentren. Una vez localizado el ataque y el escenario realizarán una labor de investigación para determinar posibles defensas a utilizar contra el mismo.

“Los motivos para aprender deben dejar de ser pasivos, es decir, dejar de mantener al estudiante en estado de espectador; por el contrario, se debe partir, en lo posible, del interés por aquello que va a enseñarse y ese interés se debe mantener de modo amplio y diversificado durante la enseñanza». [38]

Se tratará de un ataque de Ingeniería Social. Los principios sobre los que se sustenta la ingeniería social son: reciprocidad, urgencia, consistencia, confianza, autoridad y validación social.

Estos principios están presentes en la relación que existe entre el docente y los alumnos. Para llevarla a cabo el docente adquirirá el rol de “malo”. Utilizará su posición

para hacerse con información privilegiada, esto es, con la clave secreta de los equipos de trabajo. [39]

En ésta actividad se trabajará sobre el uso de contraseñas seguras y la importancia que tienen. El alumno, sin que intervenga el profesor, deberá utilizar algún medio de protección para proteger su clave secreta. Asimismo se esperará que los alumnos propongan otros métodos de protección de la información como técnicas de encriptación de los datos.

Cuando tengamos pruebas de que se ha producido un delito informático debemos informar al profesor. Si somos conscientes del ataque del profesor también debemos declararlo. A partir de aquí los grupos elaborarán un informe pericial con las medidas que debiera haber tomado el equipo para evitarlo y las acciones a tomar una vez producido el incidente.

3.5.2. Mecánicas.

En adelante se exponen las mecánicas del juego, es el segundo nivel e incluye elementos que hacen que la acción progrese como son las reglas, desafíos, elección, competición, cooperación y *feedback*.

Las reglas del juego son susceptibles de mejora, bajo propuesta del alumnado, en la realización de retos posteriores.

Se establece un tiempo límite para descubrir el reto. Finalizado el cual los grupos realizarán sus acusaciones ante el profesor, en primera instancia, mediante la entrega de un informe pericial.

Con posterioridad se determinará un día en el que los grupos harán pública ante el resto de alumnos su apuesta final para lo cual podrán elaborar una presentación.

Para resolver este misterio, debes seleccionar un delito informático o amenaza cibernética, una ubicación y una propuesta de defensa. Solo se permite una acusación en el juego.

Si tu acusación es cierta y eres el primero en proponerla ante el profesor ganas la partida.

No hay límite en el número de posibles amenazas que pueda haber en un solo escenario aunque una sola será una amenaza real ya que como hemos dicho habrá pistas falsas que no constituyan alarmas reales.

Si encuentras una pista no puedes moverla de lugar para que todos los grupos tengan las mismas opciones.

Se proporcionara al grupo una hoja de trabajo. Se podrá utilizar ésta u otra que consideren y elaboren los propios grupos de trabajo. En ella se determinarán los posibles escenarios y ataques. En los escenarios se identificarán los activos vulnerables de ser atacados.

3.5.3. Componentes.

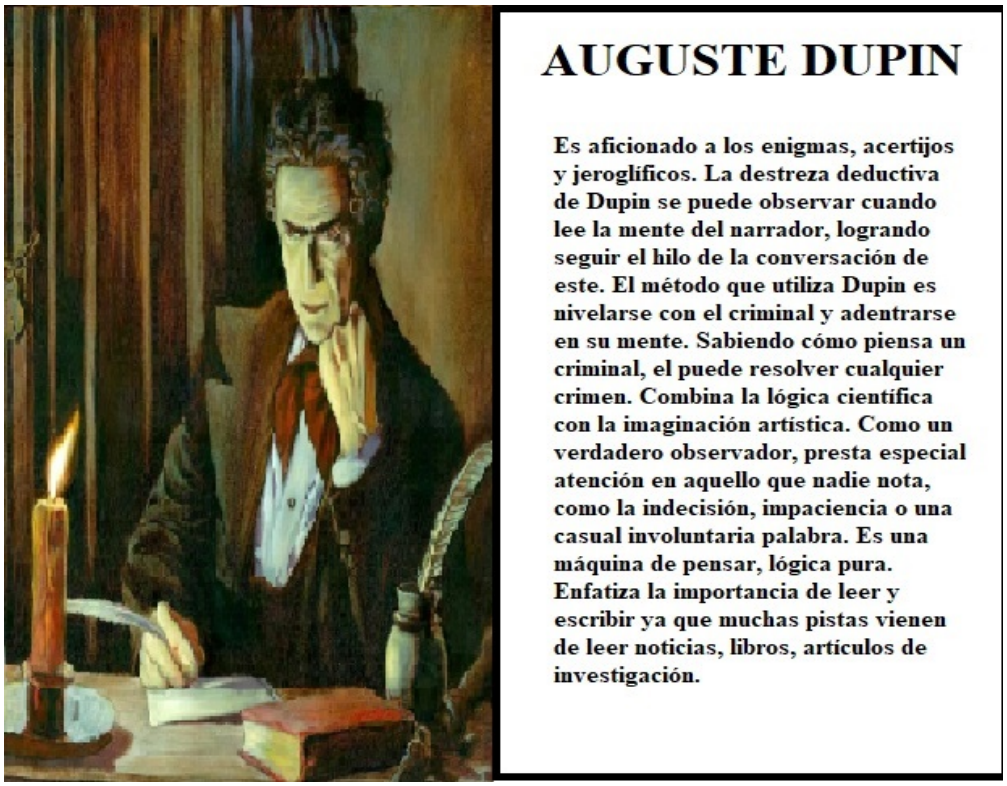
Los componentes conforman el nivel básico y representan los elementos tangibles como son los avatares, premios, logros, trofeos, escudos, puntos, niveles y posibles clasificaciones.

Marcamos un hilo argumental en el desarrollo del juego que será la investigación cibercriminal. Nuestros personajes y/o avatares son investigadores que serán quienes lleven a cabo un proyecto orientado a la búsqueda de conocimiento y al esclarecimiento de hechos y de relaciones.

Proponemos que sean los propios alumnos quienes establezcan sus avatares. Aun así, en el imaginario del juego, realizamos una propuesta como sugerencia.

A modo de ejemplo presentamos los siguientes personajes asociándolos con los perfiles de los jugadores, ganador, aventurero, socializador y explorador.

Auguste Lupin es explorador. Quiere descubrir y aprender cualquier cosa nueva o desconocida.



Miss Marple es ganadora. Busca competir con otros jugadores.

Sherlock Holmes es aventurero. Tiene como objetivo resolver retos con éxito y conseguir una recompensa por ello.

Morgana posee un perfil socializador. Sienten atracción por los aspectos sociales por encima del mismo juego.

Las defensas se traducen en códigos QR que irán adheridos al dorso de las fichas de los personajes.

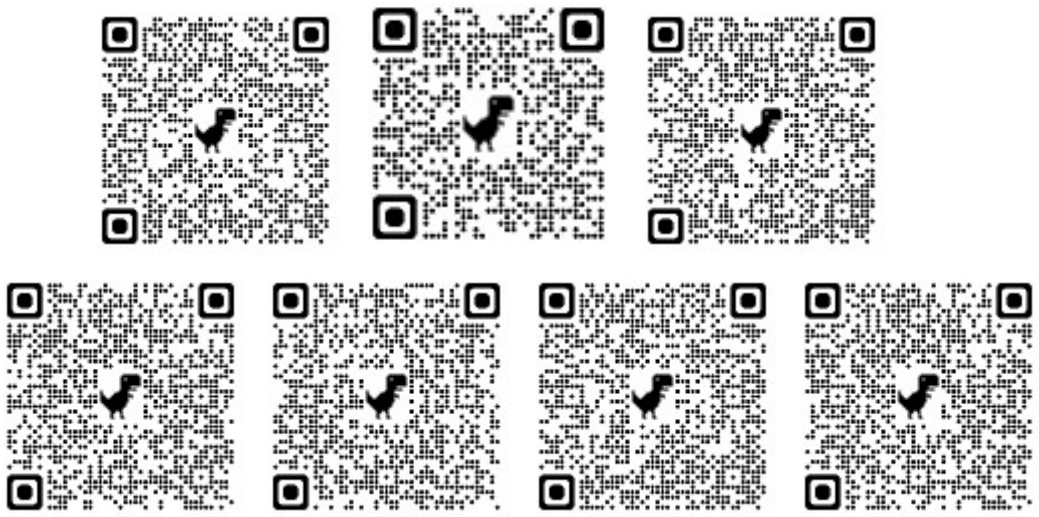
El propio navegador nos genera de forma automática estos QR que presentamos como ejemplo.

Códigos QR defensas:

(Fuente: creados desde el navegador Google Chrome)

En cuanto a los posibles escenarios proponemos los propios espacios del centro educativo como son la biblioteca, la cafetería, el auditórium, el laboratorio y la propia aula dónde se desarrollan las clases.

Al igual que hicimos con los personajes, en éste caso, los escenarios llevan adosados en el dorso posibles amenazas, ataques o vulnerabilidades que pueden perpetrase en su espacio en forma de códigos QR. En éste caso se ubicarán en el propio espacio. Los espacios podrán poseer ninguna, una o más amenazas posibles.



(Fuente: creados desde el navegador Google Chrome)

CLUE HOJA DE TRABAJO

Ataques	Defensas	Escenarios	Activos
Fuga de Información	Configuración del Router	Biblioteca	Pendrive
Ingeniería Social	Uso de constantes biométricas	Cafetería	Compañero de Grupo
Ataques a Contraseñas	No compartir información personal	Laboratorio	Pc de Laboratorio
Ataques a Conexiones Inalámbricas	Mantener actualizaciones	Aula	Compañero de Clase

(Fuente: elaboración propia con editor texto Open Office)

Se publicará en un panel en clase la clasificación o ranking de equipos. La recompensa que recibe el alumno es el logro personal, la reputación y el ranking de grupos.

Respecto al nombre de los equipos proponemos algunos nombres divertidos como Las lupas, Los Secretos, Los Orejas, Las TIAS o La Agencia Mystery INC.

3.5.4. Actividad Final.

Ficha de la Actividad:

Nombre de la Actividad. Buscando en la basura.

Descripción. La información que se proporcionará a los alumnos es la siguiente:

En tu clase se ha producido un incidente de seguridad. Depende de ti averiguar qué tipo de ataque, amenaza o vulnerabilidad se ha producido y en qué espacio. Desplázate a los distintos escenarios para averiguar que ha ocurrido. En caso de que detectes el incidente alerta a los miembros de su grupo. Te recuerdo que cada uno de vosotros poseéis una clave secreta y que deberás utilizar algún mecanismo de seguridad para mantener tu clave secreta a salvo.

Duración. Dos sesiones de trabajo en el aula con una duración de 50' cada una de ellas. La primera sesión se dedicará a la búsqueda de información y resolución del caso. Se elaborará un informe en casa y la segunda sesión estará dedicada a la presentación del informe en el aula.

Técnica didáctica: Trabajo individual y Cooperativo.

Los alumnos trabajarán de forma cooperativa. Sugerimos a los grupos para realizar ésta cooperación estas fases estableciendo así un paralelismo con las fases de un plan para la gestión de incidentes. [39]

Fase inicial: detección del incidente/alerta a los miembros del grupo
Fase de lanzamiento: reunión del grupo/informe inicial de situación/coordinación y primeras acciones
Fase de auditoría: elaboración de informe preliminar
Fase de evaluación: reunión del grupo/presentación del informe/determinación de acciones/tareas y planificación.
Fase de mitigación: ejecución de todas las acciones del plan
Fase de seguimiento: valoración de los resultados/ gestión de otras consecuencias/aplicación de medidas y mejoras.

Evaluación. La realizarán los propios alumnos en una evaluación entre pares para lo cual se les entregará una rúbrica a cada uno de ellos. La rúbrica se encuentra en el apartado de este trabajo "Propuesta de Evaluación Final".

Documentación didáctica.

Se dejarán pistas reales y falsas en los distintos escenarios. Estas podrán consistir en un trozo de papel con información dejado en papeleras en los pasillos del centro o en el propio aula. Un *pendrive* olvidado en un equipo del laboratorio. O incluso una conversación en la cafetería del centro. Tal vez un mensaje en una red social. Un correo electrónico con información falsa o real.

Una de las formas de ingeniería social que se utilizará se trata de una forma poco elegante que recibe el nombre de *"Dumpster Diving"* o búsqueda en la basura. La basura puede ser una auténtica mina de oro. O bien haremos uso de *Pretext* o *Vishing*.

La información respecto a las amenazas o ataques y a las defensas se encuentra en los códigos QR que tendrán los propios alumnos adosados y que se encontraran en los espacios en los que se desarrolla esta actividad.

3.6. Consecución de Objetivos Propuestos.

Dado que se trata de una propuesta completamente teórica, que no se ha llevado a la práctica, no se puede tener constancia cierta del cumplimiento de sus objetivos. Aun así vamos a dilucidar de qué forma vamos a procurar llevarlos a cabo.

Respecto al objetivo principal, desarrollar una actividad en forma de reto que conciencie a los alumnos y desarrolle su pensamiento crítico y responsable a cerca de las ciberamenazas, está elaborado en el cuerpo del trabajo. Esta actividad se plantea al final de una unidad didáctica que abarca el tratamiento de la seguridad informática. Con lo que se parte de conocimientos teóricos base integrados con actividades complementarias propuestas al final de cada sesión de la unidad didáctica. Sobre ésta base teórica se da la oportunidad al alumno de ir más allá y plantearse una crítica constructiva.

El objetivo del desarrollo personal y social de nuestros alumnos. Apostamos por la participación del alumno en el establecimiento del avatar y sus características. Este es efectivo en cuanto lo siente como una extensión de su identidad o de su ideal. Su elección incrementa la autonomía y la percepción de competencia que se hace tomando conciencia de grupo respecto al resto.

Según establece el Ministerio de Educación, el aprendizaje basado en competencias viene dado por la transversalidad, el dinamismo y el carácter integral que hemos procurado integrar en éste trabajo. En particular, en la competencia digital, se desarrollan las destrezas relacionadas con seguridad informática, los derechos y los riesgos en el mundo digital.

La motivación del alumnado está servida en el juego en sí mismo ya que se asocia inevitablemente con diversión. En cuanto a la temática elegida, están especialmente expuestos y conocen la existencia de riesgos debido al uso que hacen de las tecnologías y redes sociales. Buscan su seguridad y son conscientes de la preocupación por su seguridad de las familias, del centro educativo y de la sociedad en general.

El aprendizaje, otro de los objetivos que previsiblemente se alcanzarán, viene dado por la curiosidad. El planteamiento de misterios ayuda a garantizar esa química. Siendo curiosos nuestros alumnos en esa búsqueda de pistas mejorarán su atención, su memoria, su capacidad de deducción lógica, afrontarán mejor sus problemas, se harán preguntas, serán creativos, en suma, aprenderán.

En cuanto a la inclusión y la diversidad, se atenderán en la creación de grupos, tarea que llevará a cabo el docente y que serán, en la medida de lo posible, heterogéneos. La presentación de avatares también procurará abarcar la diversidad. Diversidad cultural, de género, de identidad sexual, de capacidades, socioeconómica o cualquier otra índole.

Respecto a fomentar el interés de las mujeres por la tecnología se llevará a cabo no realizando distinciones en el trato, no menospreciando ideas o pensamientos y haciendo visibles las fortalezas de todos y cada uno de los alumnos. La tecnología no está reñida con el género, al igual que la ciencia, y hay que hacerlo patente a través del respeto.

Un objetivo secundario que abordo con mucho interés es intentar paliar el abandono escolar a través de ésta iniciativa que trata un tema, el de la seguridad informática, que tiene un futuro asegurado. Recientemente la familia de Formación Profesional de Castilla y León ha incorporado un nuevo título: Ciberseguridad en entornos de las tecnologías de operación, éste es sólo un ejemplo de la apertura hacia la ciberseguridad que tanto en el mundo de la Educación como en el laboral está llevando a cabo. Sabemos que detrás del abandono escolar, tema muy complejo para ser tratado aquí a fondo, uno de los elementos que subyace de fondo es el problema económico. Ofrecer un futuro laboral a nuestros alumnos y a sus familias podría servir de ayuda.

El uso de metodologías activas es evidente en la gamificación. Opción cada vez más elegida por nuestros docentes dado el éxito de sus resultados.

En cuanto a la protección frente a la violencia esperamos que tomen conciencia de ella especialmente recordando conceptos tanto en la actividad principal como en las actividades complementarias como el *Kahoot* o la sopa de letras. Es necesario que conozcan la violencia, no sólo los conceptos, como *sexting* o *grooming* sino fundamentalmente como protegerse frente a ellas y lo llevamos a cabo a través de una de las principales defensas especificadas en la actividad, la protección de la intimidad. Hacemos ver a los alumnos que el más preciado activo son ellos mismos.

Por último incorporamos la materia de digitalización del nuevo borrador del curriculum de la ESO como un ejercicio de aprendizaje continuo llevado a cabo en ésta vorágine que constituye aprender a aprender a lo largo de la vida.

3.7. Propuesta de Evaluación de la Actividad Final.

Planteamos una evaluación de la presentación final del informe pericial elaborado por los distintos grupos. Presentamos una posible rúbrica en la que suponemos seis grupos de trabajo.

Esta evaluación se realizará al finalizar el reto y durante las presentaciones de los equipos.

CRITERIOS DE EVALUACIÓN	**%**	**G1**	**G2**	**G3**	**G4**	**G 5**	**G6**
1. Soporte de la Entrega (Objetivos, Justificación, Contextualiza, Metodologías, Conclusiones, Estructura, Índice, Apartados, Conclusiones, Claridad, estética, Bibliografía)	25%						
2. Contenidos (Actividades, Herramientas, Evaluación, Redacción, Coherente al Objetivo, Temporalización)	50%						
3. Presentación (Material de Apoyo, Muletillas, Lenguaje verbal, Volumen, Velocidad)	25%						
NOTA GRUPO (100%)	100%						

GRUPOS	**G1**	**G2**	**G3**	**G4**	**G5**	**G6**
Mejor Trabajo						

Nombre del alumno evaluador:

Incorporamos una adaptación al instrumento de evaluación de la experiencia gamificada del laboratorio de innovación educativa GALEA [40] para determinar cómo es percibido el reto propuesto por los estudiantes.

Evaluación de distintos aspectos de la actividad que se realizará de forma anónima.

<table>
<tr><td colspan="3">EVALUACIÓN DE LA ACTIVIDAD GAMIFICADA</td></tr>
<tr><td colspan="3">Fecha:</td></tr>
<tr><td colspan="3">RETO:</td></tr>
<tr><td colspan="3">Asignatura:</td></tr>
<tr><td colspan="3">Profesor:</td></tr>
<tr><td colspan="3">Evaluación General de la Actividad</td></tr>
<tr><td colspan="3">Calificar cada aspecto considerando 1=Deficiente, 2=Insuficiente, 3=Aceptable, 4=Bueno y 5=Excelente</td></tr>
<tr><td colspan="2">Dimensión</td><td>Calificación</td></tr>
<tr><td colspan="2">Interés por el contenido del reto</td><td></td></tr>
<tr><td colspan="2">Metodología utilizada (trabajo en grupo)</td><td></td></tr>
<tr><td colspan="2">Pistas (interesantes, adecuadas, suficientes)</td><td></td></tr>
<tr><td colspan="2">Tiempo</td><td></td></tr>
<tr><td rowspan="2">¿Repetirías una experiencia similar?</td><td>SI</td><td>NO</td></tr>
<tr><td></td><td></td></tr>
<tr><td colspan="3">¿Cómo mejorarías esta experiencia?</td></tr>
</table>

Conclusiones

Este trabajo tiene como motor de cambio un sueño, parafraseando a César Bona quien afirma respecto a su libro "nace para vislumbrar algunas de las escuelas que existen en nuestro país que no siguen el sistema educativo actual, para demostrar que otra educación no es un sueño sino una realidad". [41]

La mayor parte de los recursos utilizados en la elaboración de este trabajo se han tomado del Instituto de Ciberseguridad (INCIBE), cuya sede está ubicada en León, en la Comunidad de Castilla y León.

Tuve noticia de su existencia casi inmediatamente a su aparición, en 2006, entonces se denominaba INTECO, y encontré entre sus páginas herramientas de seguridad gratuitas, actualizadas, recomendadas y consejos de seguridad. Yo entonces trabajaba como Técnico de Soporte Informático y me resultaron de gran utilidad. La seguridad de una empresa depende en gran medida del comportamiento seguro de las personas que trabajan en ella. Por éste motivo, y ya entonces, di a conocer a mis usuarios este referente que es INCIBE, para que hicieran tanto profesional como personalmente un buen uso de la tecnología.

En 2012 el instituto INCIBE focalizó su actividad en ciberseguridad. Se ha desarrollado mucho desde entonces hasta convertirse en referente mundial.

En nuestro caso, no tratamos con usuarios sino con alumnos. Son menores, más vulnerables y despiertan, aún más, la necesidad de protección.

Me produce una enorme satisfacción hacer visible la problemática asociada al uso de la tecnología en cuanto a los riesgos a los que estamos sometidos todos y en especial los menores.

Quizás mi interés por la seguridad se haya fraguado durante los años que trabaje como técnico de soporte. Trabajando he visto la evolución de las amenazas en todas sus formas y quizás por ello me resulte una situación más alarmante aún que a quien ha nacido con ellas.

El futuro está en sus manos y llenárselas de herramientas y fundamentalmente de una actitud responsable y crítica es fundamental para su pleno desarrollo. Las amenazas, las vulnerabilidades cambiarán de nombre y forma, se volverán mucho más sofisticadas, pero será su actitud la que les ayude a enfrentarse a lo que el futuro les depare.

Líneas Futuras

En el caso de la gamificación, el futuro ya está aquí y avalado por un elevado número de experiencias. La mayor parte de éstas son accesibles y están publicadas en Internet.

Consideramos aquí el juego como base del proceso fundamental de enseñanza-aprendizaje que es, en resumen, el viaje que llevamos a cabo junto con nuestros alumnos a lo largo del curso.

Más allá de lo propuesto, siempre queda la opción de "darle la vuelta a la tortilla", activar la metodología de clase invertida en esa búsqueda constante que es la mejora educativa.

Hemos formulado en el trabajo una primera partida y se plantea como propuesta futura que los propios alumnos diseñen una nueva partida del juego, que se conviertan en creadores o diseñadores de juegos en el aula propiciando la estrategia de *flipped classroom* o clase invertida ya mencionada.

La ciberseguridad nos atañe a todos y por ello, y con el fin de involucrar a la comunidad educativa del centro proponemos la creación de una liga de ciberseguridad en el propio centro escolar. Promover contactos con alumnos y profesores en otros centros con proyectos similares dentro y/o fuera de la ciudad, provincia, comunidad autónoma o incluso con comunidades en otros países.

Siempre, como docente, es una obligación placentera motivar al alumno hacia la lectura. A través de la elección de avatares intentaré que conozcan y se interesen por la literatura, en esta ocasión, la de misterio.

Otra realidad crea la necesidad de utilizar un entorno virtual en el aula-laboratorio para poder poner en práctica determinados retos. Entre los incidentes que pueden proponerse están los siguientes:

- **Infecciones por código malicioso de sistemas**, equipos de trabajo o dispositivos móviles. Este tipo de incidentes, en su mayoría iniciados a través de correo electrónico, páginas web comprometidos o maliciosos, SMS o redes sociales, también pueden provocar que los recursos infectados entren a formar parte de una *botnet*.
- **Intrusiones o intentos de intrusión provocadas por explotación de vulnerabilidades**, ataques mediante *exploits* y vulneración de credenciales, lo que conlleva el compromiso de cuentas con o sin privilegios de administrador y el compromiso de aplicaciones o servicios. Si el servicio comprometido es la página web, puede dar lugar a incidentes como una suplantación de identidad o distribución de malware, entre otros. Aquí también pueden incluirse incidentes de robo por acceso no autorizado a instalaciones físicas.

- **Fallos de disponibilidad a través de ataques DoS** (denegación de servicio) que pueden afectar a diferentes recursos de la organización (redes, servidores, equipos de trabajo, etc.) e imposibilitar el normal funcionamiento de los mismos. Este tipo de incidentes incluyen también los provocados por sabotajes o ataques físicos a los recursos o infraestructuras, así como otro tipo de interrupciones de origen externo no intencionadas.
- **Compromiso de la información como resultado del acceso no autorizado** a la misma o de su modificación (por ejemplo, mediante cifrado por *ransomware*). Este tipo de incidentes incluyen además aquellos en los que el resultado es el borrado, pérdida o fuga de datos, y pueden estar provocados de forma intencionada (a través del robo o compromiso de credenciales) o por fallo de los dispositivos que los almacenan.
- **Fraude provocado principalmente a través de la suplantación de entidades legítimas**, con el objetivo de engañar a los usuarios para obtener un beneficio económico, o por ataques de *phishing*, para la obtención de credenciales privadas de acceso a medios de pago.

Referencias

[0] Marrón, A. M. P., & Vivaracho, C. E. (2018). Gamificación en el aula: gincana de programación. *ReVisión*, *11*(1), 8

[1] INCIBE. (2022). *Internet Segura For Kids*. https://www.is4k.es/

[2] Ripoll, O. (2016). *Gamificación en aulas universitarias. "Taller de creació de jocs", una asignatura gamificada"*. (J. L. Contreras, Ruth S., Eguia (ed.); Instituto).

https://bdigital.uvhm.edu.mx/wp-content/uploads/2020/06/gamificacion-aulas-universitarias.pdf

[3] INCIBE. (2021). *Mujeres Ciber*. https://www.incibe.es/mujeresciber

[4] JCYL. Consejería de Educación. (2022). *Borrador Curriculum ESO*. https://www.educa.jcyl.es/es/informacion/sistema-educativo/educacion-secundaria-obligatoria/educacion-secundaria-obligatoria-borrador-curriculo

[5] Comisión Europea. (2020). Tratado de Lisboa. *Tratado de Lisboa*. https://doi.org/10.2307/j.ctv10qqzzp

[6] Comité, A. L., Social, E. Y., & Al, E. Y. (2021). Estrategia de la UE sobre los Derechos de los Niños. https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A52010DC0636

[7] Ministerio de Educación y Formación Profesional. Real Decreto 217/2022, de 29 de marzo, por el que se establece la ordenación y las enseñanzas mínimas de la Educación Secundaria Obligatoria. *BOE*, *76*, de *30 de marzo de 2022, 41571-471789.* https://www.boe.es/buscar/pdf/2022/BOE-A-2022-4975-consolidado.pdf

[8] Moreno Rodriguez, Ricardo, Tejada Cruz, A. (2018). Atención a la Diversidad e Inclusión Educativa: Implicaciones Didácticas. In *Atención a la diversidad e inclusión educativa: implicaciones didácticas: Vol. Vol. 15*. https://sid-inico.usal.es/idocs/F8/FDO27377/iAccessibility_15.pdf

[9] UNESCO. Director-General, 2009-2017 (Bokova, I. G. . (2017). *Mensaje de la Sra. Irina Bokova, Directora General de la UNESCO, con motivo del Día Internacional de las Mujeres y las Niñas en la Ciencia, 11 de febrero de 2017*. https://unesdoc.unesco.org/ark:/48223/pf0000247047_spa

[10] Unión Europea. Educación. . *Abandono Escolar*. https://education.ec.europa.eu/es/education-levels/school-education/school-education-initiatives/early-school-leaving

[11] JCYL. Consejería de Educación. *Formación Profesional. Grado Básico.* https://www.educa.jcyl.es/fp/es/normativa-publicaciones/normativa-formacion-profesional-basica

[12] educagob. Portal del Sistema Educativo Español (2022). *Tecnología y Digitalización*. https://educagob.educacionyfp.gob.es/curriculo/nuevo-curriculo/menu-curriculos-basicos/ed-secundaria-obligatoria/materias/tecno-digitali/desarrollo.html

[13] Departamento: Jefatura del Estado. (2021). Ley Orgánica 8/2021 de 4 de junio de protección integral a la infancia y la adolescencia frente a la violencia. *Boletín Oficial Del Estado (BOE)*, 1–75. https://www.boe.es/buscar/pdf/2021/BOE-A-2021-9347-consolidado.pdf

[14] Real Academia Española. *R.A.E. Observatorio de palabras. Gamificación.* https://www.rae.es/observatorio-de-palabras/gamificacion

[15] Ripoll, O. (2014). *Gamificar significa hacer jugar*. https://lab.cccb.org/es/gamificar-significa-hacer-jugar/

[16] Mora, F. (2021). *Neuroeducación. Solo se puede aprender aquello que se ama.* (Alianza Ed).

[17] Vygotsky, L. S. (2009). El desarrollo de los procesos psicológicos superiores (Mind in society: The development of Higher Psychological Processes). *Critica. Edición de bolsillo*.

[18] Johnson, David W, Johnson, Roger T, Holubec, E. J. (1994). *El aprendizaje cooperativo en el aula* (Paidós Editorial).

[19] Foncubierta, José Manuel, Rodrigúez, C. (2014). Didáctica de la gamificación en la clase de español. *@Editorial Edinumen*. https://edinumen.es/

[20] Fernández-Rio, J., & Flores Aguilar, G. (n.d.). Capítulo 1. Fundamentación teórica de la Gamificación. In *Gamificando en la Educación Física. De la teoría a la práctica en educación primaria y secundaria.* (Universidad de Oviedo).

https://idus.us.es/bitstream/handle/11441/128643/Fundamentaci%c3%b3n%20te%c3%b3rica%20de%20la%20Gamificaci%c3%b3n.pdf?sequence=1&isAllowed=y

[21] Sawyer, B., & Smith, P. (2008). *Serious Games Taxonomy*. https://thedigitalentertainmentalliance.files.wordpress.com/2011/08/serious-games-taxonomy.pdf

[22] Prieto Andreu, J. M. (2020). Una revisión sistemática sobre gamificación, motivación y aprendizaje en universitarios. *Teoría de La Educación. Revista Interuniversitaria*, *32*(1), 73–99. https://doi.org/10.14201/teri.20625

[23] INCIBE. *Con estos ataques nos roban las contrasenas, aprende a evitarlos*. https://www.incibe.es/protege-tu-empresa/blog/sabes-funciona-ciberataque-utiliza-ingenieria-social

[24] Hunt, T. (n.d.). *Passwords @ haveibeenpwned.com*. https://haveibeenpwned.com/Passwords

[25] INCIBE. (n.d.). *sabes-funciona-ciberataque-utiliza-ingeniería-social @ www.incibe.es*. https://www.incibe.es/protege-tu-empresa/blog/sabes-funciona-ciberataque-utiliza-ingenieria-social

[26] Colomé, E. P. J. P. (2022, January 22). *Así-es-un-fraude-online-paso-a-paso.* https://elpais.com/tecnologia/2022-01-22/asi-es-un-fraude-online-paso-a-paso-queria-romperle-las-piernas-solo-que-no-era-quien-decia-ser.html

[27] OSI. (n.d.). *Guía de Ciberataques*. https://www.osi.es/es/guia-ciberataques

[28] OSI. (n.d.). *Protege tu WiFi*. https://www.osi.es/es/protege-tu-wifi

[29] INCIBE. *Ataque de ransomware*. https://www.incibe.es/protege-tu-empresa/blog/ataque-ransomware-puedo-recuperar-mi-informacion

[30] OSI. (n.d.). *Guía de Ciberataques*. https://www.osi.es/es/guia-ciberataques

[31] TechHeroX y Unidad de Análisis de Inteligencia de la SEI de la UAM. (n.d.). *pplRCO7B @ techheroxbot.typeform.com*. https://techheroxbot.typeform.com/to/pplRCO7B?typeform-source=www.tecnonews.info

[32] OSI. (2018, March 14). *¿Qué es el psicohacking?* https://www.osi.es/es/actualidad/blog/2018/03/14/psickohacking

[33] *Turning education*. (2022). TechHeroX. https://www.techherox.com/

[34] Alvarez Marañón, G. A. (2019) *Decisiones Irracionales en Ciberseguridad: Supera los errores de pensamiento que sesgan tus juicios*. ElevenPaths, Telefónica Cyber Security Unit.

[35] CONGRESO DE LOS DIPUTADOS. (2012). Cortes Generales Cortes Generales. *Diario De Sesiones*, *SESION PLE*, 1–57. https://www.congreso.es/public_oficiales/L14/CONG/DS/CO/DSCD-14-CO-427.PDF

[36] Bartle, R. (1996). *Hearts, clubs, diamonds, spades: Players who suit MUDs*. https://www.researchgate.net/publication/247190693_Hearts_clubs_diamonds_spades_Players_who_suit_MUDs

[37] *SilentEye*. https://achorein.github.io/silenteye/

[38] Bruner, J. (1984). Desarrollo cognitivo y educación. Capítulo X. In *Desarrollo cognitivo y educación.* (Ediciones Morata, S.L.).

[39] Incibe. (2016). *Cómo gestionar una fuga de información*. https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestion_fuga_informacion_0.pdf

[40] Lobo-Rueda, M. A., Paba-Medina, M. C., & Torres-Barreto, M. L. (2020). Análisis descriptivo de experiencias gamificadas para enseñanza y aprendizaje en educación superior en ingeniería. *Revista Espacios*, *41*(Nº 16), Pág. 21. https://www.revistaespacios.com/a20v41n16/a20v41n16p21.pdf

[41] Bona, C. (2017). Las escuelas que cambian el mundo. *Educatio Siglo XXI*, *35*(1), 165–172. http://revistas.um.es/educatio

Glosario de términos de ciberseguridad

Este glosario recoge los términos relativos a la ciberseguridad que aparecen en el trabajo. Se ha tomado como referencia la guía glosario de ciberseguridad de 2021 elaborada por el INCIBE en su mayor parte junto con la Wikipedia cuyas definiciones se han traspuesto como sigue.

Activo de Información. Es cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización, pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones. Es susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización

Amenaza. Circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. Una amenaza puede tener causas naturales, ser accidental o intencionada. Si esta circunstancia desfavorable acontece a la vez que existe una vulnerabilidad o debilidad de los sistemas o aprovechando su existencia, puede derivar en un incidente de seguridad.

Bastionado (**Defensa**). Proceso que trata de reducir las vulnerabilidades y agujeros de seguridad presentes en un sistema, creando un entorno lo más seguro posible siguiendo los principios de: mínima superficie de exposición, mínimos privilegios y defensa en profundidad. Entre las acciones que se realizan para alcanzar este propósito destacan la eliminación de recursos, servicios o programas que no se utilizan, baja de usuarios o cambio de las credenciales o configuraciones establecidas por defecto.

Botnet. Botnet es un término que hace referencia a un conjunto o red de *robots informáticos* o *bots*, que se ejecutan de manera autónoma y automática. El artífice de la botnet puede controlar todos los ordenadores/servidores infectados de forma remota.

Ciberataque.Intento deliberado de un ciberdelincuente de obtener acceso a un sistema informático sin autorización sirviéndose de diferentes técnicas y vulnerabilidades para la realización de actividades con fines maliciosos, como el robo de información, extorsión del propietario o simplemente daños al sistema.

Ciberdelincuente. Persona que realiza actividades delictivas en la red contra personas o sistemas informáticos, pudiendo provocar daños económicos o reputaciones mediante robo, filtrado de información, deterioro de software o hardware, fraude y extorsión. Casi siempre están orientados a la obtención de fines económicos.

Contraseña. Forma de autentificación de un usuario, a través de una clave secreta, para controlar el acceso a algún recurso o herramienta. En caso de que no se proporcione la clave correcta no se permitirá el acceso a dichos elementos.

Cyberbullying. El ciberacoso (derivado del término en inglés *cyberbullying*), también denominado acoso virtual, es el uso de medios digitales para molestar o acosar a una persona o grupo de personas mediante ataques personales, divulgación de información personal o falsa entre otros medios. Los actos de ciberagresión poseen unas características concretas que son el anonimato del agresor, su velocidad y su alcance.

El ciberacoso puede causar daños psicológicos muy graves y, de igual manera, de esto va a depender la reprensión legal que tendrá el acosador.

Puede constituir un delito penal. El ciberacoso implica un daño recurrente y repetitivo infligido a través de los medios electrónicos. Según R. B. Standler, el acoso pretende causar angustia emocional, preocupación y no persigue fines lícitos en su elección de comunicaciones.

Esteganografía. La esteganografía (del griego στεγανος *steganos*, "cubierto" u "oculto", y γραφος *graphos*, "escritura") trata el estudio y aplicación de técnicas que permiten ocultar mensajes u objetos, dentro de otros, llamados portadores, para que no se perciba su existencia. Es decir, procura ocultar mensajes dentro de otros objetos y de esta forma establecer un canal encubierto de comunicación, de modo que el propio acto de la comunicación pase inadvertido para observadores que tienen acceso a ese canal.

Exploit. Es una palabra inglesa que significa *explotar* o *aprovechar*, y que en el ámbito de la informática es un fragmento de *software*, fragmento de datos o secuencia de comandos o acciones, utilizada con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo.

Firewall. Sistema de seguridad compuesto o bien de programas (*software*) o de dispositivos *hardware* situados en los puntos limítrofes de una red que tienen el objetivo de permitir y limitar, el flujo de tráfico entre los diferentes ámbitos que protege sobre la base de un conjunto de normas y otros criterios. La funcionalidad básica de un cortafuego es asegurar que todas las comunicaciones entre la red e Internet se realicen conforme a las políticas de seguridad de la organización o corporación. Estos sistemas suelen poseer características de privacidad y autentificación.

Grooming. Un engaño pederasta, más conocido por el anglicismo *grooming* (del verbo *to groom*, que alude a conductas de acercamiento o preparación para un determinado fin) o ciberacoso es una serie de conductas y acciones emprendidas por adultos, a través de Internet, con el objetivo deliberado de ganarse la amistad de menores de edad, creando una conexión emocional con los mismos, con el fin de ganarse su confianza y poder abusar sexualmente de ellos. En algunos casos se puede buscar la introducción del menor al mundo de la prostitución infantil o la producción de material pornográfico. Las víctimas pueden ser tanto chicas como chicos.

Happy slapping. El término *happy slapping* (bofetada feliz, en español) nació en Reino Unido en 2005. Aunque este nombre parece inocente a primera vista, tras él se esconde un fenómeno que se ha ido extendiendo en España durante los últimos años por imitación: el de grabar una agresión y colgarla en la red. Así, el *happy slapping* consiste en la grabación de una agresión física, verbal o sexual y su difusión online mediante las

tecnologías digitales (páginas, blogs, chats, redes sociales, etc.). Lo más común es que esta violencia se difunda por alguna red social y, en ocasiones, puede hacerse viral.

Ingeniería Social. La ingeniería social es la práctica ilegítima de obtener información confidencial a través de la manipulación de usuarios legítimos. Es un conjunto de técnicas que pueden usar ciertas personas para obtener información, acceso o permisos en sistemas de información que les permitan realizar daños a la persona u organismo comprometidos y es utilizado en diversas formas de estafas y suplantación de identidad. El principio que sustenta la ingeniería social es el de que, en cualquier sistema, los usuarios son el «eslabón débil».

Malware. Es un tipo de software que tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un sistema de información. Palabra que nace de la unión de los términos en inglés de software malintencionado: malicious software. Dentro de esta definición tiene cabida un amplio elenco de programas maliciosos: virus, gusanos, troyanos, *backdoors*, *spyware*, etc. La nota común a todos estos programas es su carácter dañino o lesivo.

Phishing. Técnica o tipo de ataque en el que alguien suplanta a una entidad/servicio mediante un correo electrónico o mensaje instantáneo para conseguir las credenciales o información de la tarjeta de crédito de un usuario. Ese correo/mensaje suele tener un enlace (o fichero que contiene ese enlace) a un sitio web que suplanta al legítimo y que usan para engañarlo.

Pretextos. El pretexto es la creación de un escenario inventado para llevar a la víctima a revelar información personal o a actuar de una forma que sería poco común en circunstancias normales. Una mentira elaborada implica a menudo una investigación previa de la víctima para conseguir la información necesaria, y así llevar a cabo la suplantación (por ejemplo, la fecha de nacimiento, el número de la Seguridad Social, datos bancarios, etc.) y hacerle creer que es legítimo. El pretexto también se puede utilizar para suplantar a compañeros de trabajo, a la policía, al banco, a autoridades fiscales o cualquier otra persona que podría haber percibido el derecho a la información en la mente de la víctima. El "*pretexter*" simplemente debe preparar respuestas a preguntas que se puede plantear la víctima. En algunos casos, todo lo que necesita es una voz que inspire autoridad, un tono serio y la capacidad de improvisar para crear un escenario pre textual.

Redes Sociales. Uno de los factores más peligrosos, es la creciente tendencia por parte de los usuarios, principalmente los más jóvenes, a colocar información personal y sensible en forma constante. Desde imágenes de toda su familia, los lugares que frecuentan, gustos personales y relaciones amorosas. Las redes sociales proveen de mucha información a un delincuente para que realice un ataque, como para robar tu identidad o en el menor de los casos ser convincente para tener empatía.

Ransomware. *Malware* cuya funcionalidad es «secuestrar» un dispositivo (en sus inicios) o la información que contiene de forma que si la víctima no paga el rescate, no podrá acceder a ella.

Resiliencia. Capacidad de una organización de resistir ante una situación adversa, como por ejemplo, un incidente de ciberseguridad. La resiliencia empresarial debería ir acompañada de un plan de contingencia y continuidad para hacer frente a posibles situaciones de crisis en la empresa.

Router. Es un dispositivo que distribuye tráfico de red entre dos o más diferentes redes. Un *router* está conectado al menos a dos redes, generalmente LAN o WAN y el tráfico que recibe procedente de una red lo redirige hacia la(s) otra(s) red(es). En términos domésticos un router es el dispositivo que proporciona el proveedor de servicios de telefonía (o ISP) y que permite conectar nuestra LAN doméstica con la red del IS. El router comprueba las direcciones de destino de los paquetes de información y decide por qué ruta serán enviados, para determinar el mejor camino emplean cabeceras y tablas de comparación.

***Sexting*.** Sexteo (contracción de sexo y texteo, del inglés *sexting*) es un término que se refiere al envío de mensajes sexuales, eróticos o pornográficos, por medio de teléfonos móviles. Inicialmente hacía referencia únicamente al envío de SMS de naturaleza sexual, pero después comenzó a aludir también al envío de material pornográfico (fotos y vídeos) a través de móviles y ordenadores.

Vishing. El *vishing* consiste en realizar llamadas telefónicas encubiertas bajo encuestas con las que también se podría sacar información personal de forma que la víctima no sospeche. Por este motivo debemos tener cuidado y no proporcionar información personal aunque se trate de nuestra compañía de móvil, electricidad o agua (entre otras), ya que podría ser un *hacker* que haya elegido casualmente la nuestra.

Vulnerabilidad. Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos (normalmente mediante un programa que se denomina *exploit*). Cuando se descubre el desarrollador del software o hardware lo solucionará publicando una actualización de seguridad del producto.

Wifi. Una red wifi es una red de dispositivos inalámbricos interconectados entre sí y generalmente también conectados a Internet a través de un punto de acceso inalámbrico. Se trata por tanto de una red LAN que no utiliza un cable físico para el envío de la información. Tecnología de interconexión de dispositivos electrónicos de forma inalámbrica, que funciona en base al estándar 802.11, que regula las transmisiones inalámbricas. Esta ausencia de cable físico quiere decir que se pierda la confidencialidad de la información transmitida. Por esta razón se hace necesario el cifrado de los contenidos transmitidos a través de una red wifi. Preferiblemente se deben utilizar como sistemas de cifrado: • WPA2 • WPA3.

Código QR (del inglés Quick Response code, «código de respuesta rápida») es la evolución del código de barras. Es un módulo para almacenar información en una matriz de puntos o en un código de barras bidimensional. La matriz se lee en el dispositivo móvil por un lector específico (lector de QR) y de forma inmediata nos lleva a una aplicación en Internet, un mapa de localización, un correo electrónico, una página web o un perfil en una red social. Fue creado en 1994 por la compañía japonesa Denso

Wave, subsidiaria de Toyota. Presenta tres cuadrados en las esquinas que permiten detectar la posición del código al lector. El objetivo de los creadores (un equipo de dos personas en Denso Wave, dirigido por Masahiro Hara) fue que el código permitiera que su contenido se leyera a alta velocidad. Los códigos QR son muy comunes en Japón, donde es el código bidimensional más popular.

Anexos

Anexo 1. Documento sobre el concepto de seguridad informática y seguridad de la información.

Cuando hablamos de **seguridad de la información** estamos indicando que dicha información tiene una relevancia **especial** en un contexto determinado y que, por tanto, hay que **proteger**.

La Seguridad de la Información se puede definir como **conjunto de medidas técnicas, organizativas y legales** que permiten a la organización asegurar la confidencialidad, integridad y disponibilidad (**CIA**) de su sistema de información.

"La seguridad informática consiste en la implantación de un conjunto de medidas técnicas destinadas a preservar la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio." (ISO/IEC 27001)

Como vemos el término seguridad de la información es más amplio ya que engloba otros aspectos relacionados con la seguridad más allá de los puramente tecnológicos.

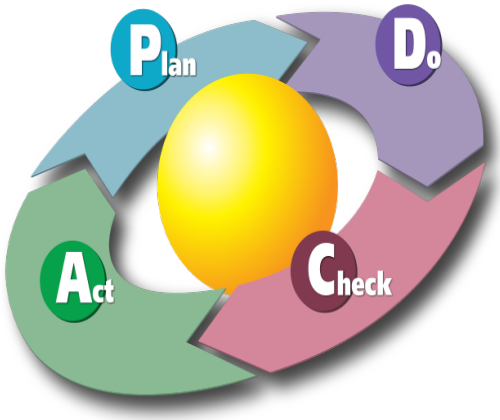
La organización debe plantearse un **S**istema de **G**estión de la Seguridad de la **I**nformación.

El objetivo de un SGSI es proteger la información y para ello lo primero que debe hacer es identificar los **activos de información** que deben ser protegidos y en qué grado:

Hardware: elementos físicos. **Software:** elementos lógicos **Datos:** información manejada por el hardware y el software **Otros:** fungibles, **personas**, infraestructuras,..

De los **riesgos** se desprende que los problemas de seguridad **nunca se eliminan** en su totalidad.

Un SGSI siempre cumple cuatro niveles repetitivos que comienzan por Planificar y terminan en Actuar, consiguiendo así mejorar la seguridad. **PLAN – DO – CHECK – ACT**



PLANIFICAR (Plan): consiste en establecer el contexto en el se crean las políticas de seguridad, se hace el análisis de riesgos, se hace la selección de controles y el estado de aplicabilidad

HACER (Do): consiste en implementar el sistema de gestión de seguridad de la información, implementar el plan de riesgos e implementar los controles .

VERIFICAR (Check): consiste en monitorizar las actividades y hacer auditorías internas.

ACTUAR (Act): consiste en ejecutar tareas de mantenimiento, propuestas de mejora, acciones preventivas y acciones correctivas.

ANEXO 2 *¿Quieres ser de la CIA ?*

Cuando se habla de seguridad de la información, es importante conocer el término **CIA (Confidencialidad, Integridad, Disponibilidad)**, que presenta los principios básicos de la seguridad de la información.

Tenemos que recordar que ningún sistema de seguridad es completamente seguro, siempre debemos tener claro que un sistema es mucho más vulnerable de lo que pensamos. Es necesario que tengamos en cuenta las causas de los riesgos y la posibilidad de que ocurran fallos. Una vez que tenemos esto claro podemos tomar las medidas necesarias para tener un sistema para conseguir un sistema menos **vulnerable**.

A continuación aclaramos cada uno de los puntos que forman la CIA:

Confidencialidad

La confidencialidad implica que la información es accesible únicamente por el **personal autorizado**. Es lo que se conoce como ***need-to-know.*** Con este término se hace referencia a que la información solo debe ponerse en conocimiento de las personas, entidades o sistemas autorizados para su acceso. Ejemplos de falta de confidencialidad, son el robo de información confidencial por parte de un atacante a través de Internet, la divulgación no autorizada a través de las **redes sociales** de información confidencial o el acceso por parte de un empleado a información crítica de la compañía ubicada en carpetas sin permisos asignados, a la que no debería tener *acceso.*

Integridad

Cuando hablamos de integridad en seguridad de la información nos referimos a cómo los datos se mantienen intactos libre de modificaciones o alteraciones por terceros, bien por accidente o intencional. Una manera de proteger los datos es cifrando la información mediante un método de autenticidad como una contraseña o mediante huella digital.

Ejemplos de ataques contra la integridad de la información son la alteración malintencionada en los ficheros del sistema informático mediante la explotación de una vulnerabilidad, o la modificación de un informe de ventas por un empleado malintencionado o por error humano.

Availability(Disponibilidad)

Es un pilar fundamental de la seguridad de la información, nada hacemos teniendo segura e integra nuestra información, si no va a estar disponible cuando el usuario o sistema necesite realizar una consulta.

Para cumplir con la última condición tenemos que tener claro cuál será el flujo de datos que debemos manejar, para conocer donde se debe almacenar dicha información, qué tipo de servicio debemos contratar, etc.

Algunos ejemplos de falta de disponibilidad de la información son: cuando nos es imposible acceder al correo electrónico corporativo debido a un error de configuración, o bien, cuando se sufre ***un ataque de denegación de servicio***, en el que el sistema «cae» impidiendo accesos legítimos. Ambos tienen implicaciones serias para la seguridad de la información.

Ningún sistema de seguridad es completamente seguro, es mucho más vulnerable de lo que pensamos

La seguridad de la información es un elemento fundamental cuando la actividad de la empresa se realiza mediante la ***web***.

La seguridad de la información contempla la protección de la infraestructura y los dispositivos, también la información y la integridad física y moral de los usuarios que la proveen. Se han creado diversos mecanismos, como la *encriptación de datos*, la creación de **firewalls**, detectores de ***hackers***, simuladores de ataques informáticos, etc.
Hoy en día, existen diferentes empresas que se dedican a proveer de seguridad a otras empresas.Estos son algunos de los requisitos que debe cumplir la organización que presta estos servicios y de qué elementos se compone su sistema de seguridad.
Se provee de servicios de integración de seguridad y tecnología de la información divididos en tres áreas.

- Los servicios gestionados de seguridad, desde los que se administran y monitorean los sistemas de seguridad las **24 horas del día**.
- Los servicios profesionales, que apoyan **la consultoría de análisis de vulnerabilidades, las pruebas de penetración, la implantación de normativas y estándares.**
- El área de tecnología e ingeniería, para **diseñar, integrar y soportar soluciones tecnológicas de seguridad.**

Si los clientes no cuentan con la infraestructura de seguridad necesaria, se le entregan las herramientas requeridas, como puede ser **firewalls**, ***detectores de intrusos***, **anti spam**, etc.
Te propongo este enlace para aprender herramientas de seguridad a través del juego https://cybergamesuk.com/
La seguridad tiene como objetivo resguardar la confidencialidad, integridad y disponibilidad de la información, por lo tanto, se tiene que aplicar de forma efectiva en toda la cadena. Los sistemas tradicionales de seguridad no son muy efectivos en entornos modernos de mucha movilidad, por lo cual se plantean arquitecturas basadas en **cloud computing**, siendo más efectivas, simples y económicas.
Todas las organizaciones deben velar por resguardar la seguridad de la información crítica. No hacerlo puede costarle muy caro en caso de que se produzca un **incidente.**
Lo importante es que **los riesgos de seguridad de la información sean gestionados**.

El estándar internacional ISO 27001, junto con todas las normas que componen su familia, generan todos los requisitos necesarios para poder implementar un Sistema de Gestión de Seguridad de la Información de una forma rápida y sencilla.