Escenarios de aprendizaje competitivo a través de uso de elementos lúdicos para entrenamiento en Ciberseguridad

Tesis presentada en satisfacción parcial de los requerimientos para obtener el grado de Maestro en Dirección de Tecnologías de Información

por:

Doig Diaz, Daniel Fernando

Mendoza Blanco, Juan Carlos

Mendoza Pasco, Jorge Luis

Yañez Herrera, Diego Alfredo

Programa de la Maestría en Dirección de Tecnologías de Información

MADTI 17-1

Lima, 08 de julio de 2019

Esta tesis

Escenarios de aprendizaje competitivo a través de uso de elementos lúdicos para entrenamiento en Ciberseguridad

ha sido aprobada.

……..

Fanny Ariza Llado (Jurado)

……..

Ramón Batalla Font (Jurado)

……..

Luis Rolando Madrid Guerra (Jurado)

……..

Richard Moarri Nohra (Asesor)

Universidad ESAN

2019

DEDICATORIAS

Quisiera dedicar esta tesis a mi papa por su eterno apoyo y cariño incondicional y a mi mamá por su amor incansable e inquebrantable. Día a día me enseñan el valor de la bondad y el amor. Siempre encuentro fuerzas en ellos, junto con mis queridos hermano y hermana, para poder salir adelante y buscar crecer como persona. Ellos son la razón de ser de todo lo que hago en mi vida y les agradezco siempre por ello.

De igual manera agradecer a los otros miembros de mi hermosa familia, que siempre me han enseñado que la familia es lo más valioso que Dios nos ha dado.

Daniel Fernando Doig Díaz

La presente tesis de investigación se la dedico a mi futura esposa Karen, por ser siempre mi soporte, inspiración y motivación para continuar esforzándome y lograr alcanzar mis objetivos, que sé que también son los tuyos. Tengo fe que juntos seguiremos alcanzando todas las metas que nos propongamos.

Asimismo, a mis padres, hermanos y suegros, por sus sabios consejos, amor incondicional y ayuda a lo largo de todo este proceso. Sin ustedes no hubiese sido posible llegar hasta este momento.

A mis jefes y amigos, que en el transcurso de este largo camino han sabido apoyarme y brindarme orientación en sus áreas de experiencia.

Por último, a mis amigos del grupo 04 y coautores de la presente tesis debido a que sin su apoyo, confianza y dedicación hubiese sido imposible encontrarnos en este momento. Mis mejores deseos a cada uno de ustedes, tengo la confianza y certeza que lograrán sus metas personales y profesionales.

Juan Carlos Mendoza Blanco

En esta pequeña entrada mi deseo es poder expresar el agradecimiento a todas las personas que nos han contribuido con su apoyo y motivación para lograr esta meta. En ayudarnos a construir este trabajo y presentarlo con orgullo. Agradezco a mi familia, mi padre y mi madre, quienes siempre me han motivado a dar el máximo potencial en cada proyecto, principalmente el académico. A mi pareja, quien ha estado a mi lado brindándome su apoyo y soporte en este tiempo de investigación.

Y a mis compañeros, quienes han dispuesto de su tiempo y esfuerzo para que construyamos juntos este proyecto. También quiero agradecer a las instituciones que nos apoyaron y guiaron para completar nuestros objetivos, la Universidad de Negocio ESAN y mi alma mater, la Universidad de Lima. Dicho todo esto, muchas gracias. Y que procedamos con la frente en alto dejando una marca más en la historia de nuestra profesión.

Diego Alfredo Yañez Herrera

No sería capaz de aceptar este logro si no fuera por el conjunto esfuerzo de mis amigos y familiares que me han apoyado y motivado a conseguir este logro. Me siento agradecido con mis padres por enseñarme que dedicarme al estudio sería un factor importante para mi desarrollo personal y, principalmente, el profesional. Doy gracias al gran equipo de alto rendimiento que formamos como amigos y colegas con mis miembros de equipo.

Y a todo el apoyo de mis amigos quienes dieron de sus experiencias para ayudarme a afrontar los retos con ideas y frases motivadoras. Y me da gusto también agradecer por este logro, y compartirlo con mi pareja, quien ha estado todo el tiempo dándome soporte para yo dar más de mí mismo. Entrego este documento como muestra de las gracias que les tengo, muchas gracias.

Jorge Luis Mendoza Pasco

ÍNDICE DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

DANIEL FERNANDO DOIG DIAZ

Profesional con sólidos conocimientos en procesos back y front office. Conocimiento en procesos de compras, distribución y punto de venta. Con 6 años de experiencia en el sector retail y poseedor de un alto expertise técnico en base de datos, programación y desarrollo de sistemas.

EXPERIENCIA PROFESIONAL

Farmacias Peruanas

La empresa Farmacias Peruanas es una cadena de boticas y farmacias que se encuentra a nivel nacional y es parte del Grupo Intercorp. Brinda a sus clientes productos para la salud y el cuidado personal procurando que su propuesta de valor sea ofrecer siempre los precios más bajos del mercado.

Analista de Sistemas **Setiembre 2014 – Actualidad**

- Encargado de atender requerimientos y servicios
- Brindar soporte y proponer mejoras.
- Participar en proyectos relacionados a los sistemas de Punto de Venta, de Gestión de Almacenes y SAP.
- Encargado de analizar que estos procesos de desarrollen de manera eficiente y poder encontrar las causas de los posibles incidentes que surjan.
- Encargado de coordinar la atención de requerimientos e incidentes con Oracle para el sistema WMS de la empresa.

Agronegocios Génesis

Empresa Agro-Comercializadora que se encarga de la importación de semillas para su venta a los productores de hortalizas locales.

A la vez también brinda servicios para el acondicionamiento de plantines de manera que estos puedan crecer en un vivero en las condiciones de cultivo ideales. También cuenta con un rubro para la producción de material vegetal que se utiliza para el cultivo de la uva.

Analista Programador **Agosto 2012 – Setiembre 2014**

- Analista Programador en Java web, Javascript y PL/SQL para el ERP de la empresa OPENBRAVO. Módulos de Logística, Almacenes, Ventas y Finanzas. Reportes en JasperReports para los diferentes módulos del ERP. Manejo de base de datos Oracle.

HYO System

Empresa que brinda el servicio de Software como Servicio ofreciendo sistemas que permiten la gestión de escuelas con los módulos de matrículas, notas, tesorería, biblioteca entre otros. Esta empresa es la primera en su rubro a nivel nacional.

Analista Programador **Setiembre 2011 – Enero 2012**

- Programación en php, usando el framework zend, y programación en Jquery para los sistemas de gestión de colegios que la empresa ofrece a importantes instituciones educativas.

FORMACION PROFESIONAL

UNIVERSIDAD ESAN 2017 - Actualidad

Maestría en Dirección de Tecnologías de Información

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO 2005 - 2010

Ingeniería de Sistemas.

CIBERTEC 2016 - 2017

Java 8.0 Architect Developer

CIBERTEC 2013 - 2013

Curso Oracle Database 11G: Program with PL/SQL

CIBERTEC 2011 - 2011

Curso para la Certificación internacional OCA y OCP de administración de base de datos Oracle.

JUAN CARLOS MENDOZA BLANCO

Profesional con 8 años de experiencia en TI en el sector financiero y servicios. Con capacidad de comunicación a todo nivel, facilidad de adaptación a cualquier tipo de tecnología y con sólida experiencia en Seguridad de Información, Ciberseguridad y Gestión de Riesgos.

Orientado a superar objetivos organizacionales con innovación, mejora de procesos, competitividad y productividad. Capaz de liderar cambios organizacionales. Habilidades para negociación, superar retos y aportar soluciones de valor agregado y con capacidad de gestionar equipos de trabajo multifuncionales.

EXPERIENCIA PROFESIONAL

Banco de Crédito del Perú

El Banco de Crédito de Perú (BCP) es una empresa del Grupo Credicorp, un grupo empresarial muy importantes en el país, siendo la segunda empresa más grande de este grupo y la que provee la estructura financiera del holding de empresas. El BCP es líder en el segmento de banca privada a nivel nacional y tiene como finalidad atender a los clientes de la banca de consumo, a nivel de personas naturales y jurídicas, en el territorio del Perú.

Gerente Adjunto de Ingeniería de Defensa de Ciberseguridad
Junio 2018 - Actualidad

- Supervisar la respuesta de incidentes de Ciberseguridad.
- Supervisar y apoyar al Centro de Operaciones de Ciberseguridad.
- Identificar y definir los requisitos para las dimensiones de Ciberseguridad de la organización Credicorp.
- Definir los controles apropiados para administrar los riesgos de ciberseguridad y asegurar el cumplimiento de las políticas.
- Brindar apoyo a las unidades de 1ra y 2da línea de defensa.

Sub Gerente de Ingeniería de Defensa de Ciberseguridad
Febrero 2018 – Abril 2018

- Supervisar la respuesta de incidentes de Ciberseguridad.
- Supervisar y apoyar al Centro de Operaciones de Ciberseguridad.
- Identificar y definir los requisitos para las dimensiones de Ciberseguridad de la organización Credicorp.
- Definir los controles apropiados para administrar los riesgos de ciberseguridad y asegurar el cumplimiento de las políticas.
- Brindar apoyo a las unidades de 1ra y 2da línea de defensa.

Sub Gerente de Seguridad en Infraestructura TI **Marzo 2017 - Enero 2018**

- Coordinar, implementar y ejecutar proyectos de Infraestructura de Seguridad Informática.
- Gestión de riesgos de procesos de negocio y plataformas.
- Evaluar efectividad y eficiencia de controles existentes.
- Gestión de Ethical Hacking de la organización y subsidiarias.
- Asistir a las Gerencias de Negocios en nuevas iniciativas.
- Gestión de la SGSI de la organización.

Sub Gerente de Seguridad de Información **Junio 2016 - Febrero 2017**

- Participación en proyectos de gran envergadura.
- Liderazgo de equipos.
- Gestión de riesgos y análisis de seguridad de aplicaciones.
- Gestión de proyectos internos.

Sub Gerente Adjunto de Seguridad de Información **Abril 2015-Mayo 2016**

- Participación en proyectos de mediano impacto.
- Liderazgo de equipos dentro de mi unidad.
- Gestión de la SGSI de la organización.
- Definición de lineamientos y controles de seguridad.
- Gestión de riesgos y análisis de seguridad de aplicaciones.
- Gestión de proyectos internos.

Analista de Seguridad de Información **Marzo 2012-Marzo 2015**

- Análisis de seguridad de aplicaciones.
- Clasificación de Activos de Información.
- Análisis y mantenimiento de roles de accesos.

FORMACION PROFESIONAL

UNIVERSIDAD ESAN 2017 - Actualidad

Maestría en Dirección de Tecnologías de Información

ESCUELA DE POSGRADO CENTRO DE ALTOS ESTUDIOS NACIONALES 2016

Diplomado Internacional en Ciberseguridad

UNIVERSIDAD DE LIMA 2011

Bachiller en Ingeniería de Sistemas

OTROS ESTUDIOS

CISM (Certified Information Security Manager) 2017

JORGE LUIS MENDOZA PASCO

Profesional de tecnología de la información. Las áreas de especialización son virtualización, redes, bases de datos, copias de seguridad, la nube y el almacenamiento. Excelentes habilidades de comunicación. Experiencia a lo largo del ciclo de vida de implementación de sistemas, incluida la estimación de alto nivel y el desarrollo de casos de negocios.

EXPERIENCIA PROFESIONAL

Minera Las Bambas Sa

Empresa dedicada a la extracción de minerales. La operación minera radica en las provincias de Cotabambas y Grau pertenecientes al departamento de Apurímac.

Infrastructure Solution Designer **Enero 2016 - Actualidad**

- Garantizar que los aspectos de infraestructura de las soluciones estén diseñados según los estándares MMG.
- Proporcionar una rigurosa evaluación técnica a todos los proyectos desde el inicio, a través del diseño, construcción, prueba, implementación y transición del servicio.
- Desarrollar el diseño de alto nivel de la solución tecnológica o el diseño detallado de la solución tecnológica, según sea necesario
- Revisar y confirme la aceptación de los resultados del diseño del proveedor, incluida la revisión de la lista de materiales relacionada con la solución, en comparación con los estándares MMG
- Desarrollar declaraciones de trabajo para proveedores de servicios externos. Punto de contacto principal para todas las consultas técnicas / aclaraciones de los proveedores durante el ciclo de vida del proyecto.

Manpower Peru Sa

ManpowerGroup es líder global en soluciones innovadoras de capital humano. ManpowerGroup se encuentra a disposición de empresas grandes y pequeñas en los diferentes sectores de la industria a través de sus marcas: ManpowerGroup Solutions, Experis, Manpower y Right Management.

Consultor IT **Diciembre 2014 – Diciembre 2015**

- Soporte de campo.
- Gestión de pequeños proyectos y órdenes de trabajo para la oficina de Lima.

Quadrem Peru SAC

Quadrem es una organización de apoyo a la adquisición en la industria minera. Es un proyecto de eMarketplace lanzado en 2000 para respaldar el proceso de compra de la industria minera.

IT Business Services Associate Consultant **Junio 2013 – Septiembre 2014**

- Tareas especializadas en soporte de TI realizadas (1º y 2º nivel de soporte).
- Gestión de incidentes, requisitos y cambios relacionados con la oficina de Lima (sucursal de ingeniería).
- Gestión de pequeños proyectos.

FORMACION PROFESIONAL

UNIVERSIDAD ESAN 2017 - Actualidad

Maestría en Dirección de Tecnologías de Información.

UNIVERSIDAD CATOLICA SANTO TORIBIO DE MOGROVEJO 2012

Ingeniero de Sistemas y Computación.

DIEGO ALFREDO YAÑEZ HERRERA

Con ingenio y dedicación he demostrado grandes aptitudes en las distintas áreas de tecnología. Como ingeniero de sistemas y arquitecto de software, en mis 7 años de experiencia profesional, he logrado poner en marcha varios proyectos de finanzas, marketing y seguridad informática. Me he desarrollado como formador y líder de equipos de alto rendimiento, y gestor de portafolios de proyectos.

EXPERIENCIA PROFESIONAL

Equifax Perú

La empresa financiera dedicada a ofrecer soluciones que facilitan la toma de decisiones manejando el riesgo y maximizando oportunidades de crecimiento en cada etapa del ciclo de negocio a través del desarrollo de valor de la información crediticia.

Gestor de Soluciones TI Sénior **Noviembre 2016 – Actualmente**

- Análisis y diseño de nuevo software.
- Implementación de mejoras a los procesos ETL del negocio.
- Desarrollo de soluciones tecnológicas.
- Líder en proyectos agiles.
- Control de calidad y seguridad de las soluciones implementadas.

Everis

Una consultora multinacional que brinda soluciones de negocio, estrategia, desarrollo y mantenimiento de aplicaciones tecnológicas, y outsourcing. EVERIS forma parte del grupo NTT DATA, la sexta compañía de servicios TI del mundo.

Analista de Soluciones Sénior **Marzo 2014 – Diciembre 2015**

- Análisis y diseño de nuevo software.
- Estimación y planificación de proyectos a corto, mediano y largo plazo.
- Manejo de presupuesto para la organización de planes.
- Líder de equipo de fábrica con cuatro programadores senior y un analista junior.
- Coordinación con el equipo del cliente.

Grupo Delaware

Compañía internacional especializada en consultoría de negocio, integración de sistemas y desarrollo de procesos de negocio. Brinda soluciones a sus clientes para mejorar la relación que estos tienen con sus clientes.

Analista de Sistemas **Abril 2013 – Febrero 2014**

- Análisis y diseño de nuevo software.
- Estimación y planificación de proyectos a corto y mediano plazo.
- Estimación de presupuesto para planes de corto plazo.
- Coordinación con el equipo del cliente.

Programador Sénior **Noviembre 2012 – Marzo 2013**

- Identificar puntos de mejora en las aplicaciones.
- Migrar funcionamiento de sectores del sistema a otros lenguajes.
- Corregir o reconstruir código como parte de mejoras.

Autoridad del Servicio Civil (Servir)

Entidad nacional de servicio civil dedicada a la organización y regulación de leyes a los trabajadores del Perú. Dedicada a organizar la información de todo el país correspondiente a las labores que se realizan y las remuneraciones que estos reciben.

Programador Sénior **Agosto 2012 – Octubre 2012**

- Análisis del sistema de organización provincial.
- Estimación de esfuerzos y presupuesto del sistema.
- Codificación del sistema de organización provincial.
- Líder de equipo de trabajo con tres programadores junior.

Inspira IT Consulting

Empresa multinacional, con presencia en Perú y Chile, que ofrece servicios y soluciones integrales con la finalidad de ayudar a las empresas a optimizar sus procesos de negocios empleando la asistencia de las tecnologías de información.

Programador Junior **Abril 2011 – Enero 2012**

- Desarrollo de aplicaciones de servicios para distintas plataformas.
- Integración de sistemas cliente a través de servicios web.

Avatar

Empresa que provee de consultoría en servicios de estrategia y marketing de productos para compañías de tecnología con la finalidad que alcancen sus objetivos de negocio. Se encargan de lanzar nuevos productos, desarrollar soluciones aptas para un público estratégico e implementar campañas de recursos que dirijan el crecimiento de la compañía.

Programador Junior **Junio 2010 – Marzo 2011**

- Desarrollo de servicios para compañías retail.
- Implementación de un sistema nuevo a partir de un servicio cliente.

FORMACION PROFESIONAL

UNIVERSIDAD ESAN 2017 - Actualidad

Maestría en Dirección de Tecnologías de Información.

UNIVERSIDAD DE LIMA 2013

Ingeniero de Sistemas

UNIVERSIDAD DE LIMA 2012

Bachiller en Ingeniería de Sistemas

RESUMEN EJECUTIVO

En el mercado se extiende una tendencia hacia la digitalización de la información, tanto en empresas como en las personas. Por este motivo, la información personal y corporativa se ven expuestos a varios niveles de acceso, lo que incrementa el riesgo de ser víctimas de un robo de información. Estos riesgos ya no solo se materializan en vulnerabilidades a nivel de hardware y software, sino también por errores humanos, los cuales son aprovechados por los ciberatacantes.

El uso debido de la tecnología que tenemos a nuestro alcance forma parte de la principal defensa contra los ciberataques. Para poder proteger nuestra información personal y de nuestras empresas, debemos ser conscientes de que existen peligros y que no somos ajenos a ellos. Para esto existen buenas prácticas y entrenamientos que facilitan el aprendizaje de técnicas para evitar ser víctimas de ciberataques.

Estas capacitaciones, suelen ser en su mayoría clases de teoría que enseñan conceptos útiles sobre la protección de datos. Pocos son los cursos que enseñan mediante la práctica, y el empleo de herramientas, las cuales suelen ser más complicadas de aprender para un público sin conocimiento técnico. El objetivo de la presente tesis es demostrar que, mediante el empleo de elementos lúdicos se logra reforzar los conceptos básicos de seguridad de la información y obtener un mejor resultado al momento de permitirle al alumno aprender los conceptos y entender como emplearlos en su día a día.

Basados en las principales formas de ciberataque que pueden influir en el día de un empleado cotidiano, hemos identificado las siguientes amenazas más comunes:

- Archivos adjuntos maliciosos.
- Enlaces maliciosos.
- Contraseñas inseguras.
- Dispositivos USB inseguros.
- Phishing dirigidos.

Frente a estas amenazas, la tesis presenta un entrenamiento dinámico con el enfoque lúdico para enseñar medios básicos para que el alumno interactúe y logre identificar y evitar estos tipos de ciberataques, reduciendo la probabilidad de que se materialice el riesgo y permitiéndole reforzar su conducta con la finalidad de asegurar su información.

El entrenamiento propuesto se ejecutó en tres empresas de la ciudad de Lima con la finalidad de corroborar que el aprendizaje de los conceptos se haya llevado con un mejor resultado se realizaron entrevistas, actividades, exámenes y encuestas a los alumnos participantes. Con dicha información y mediante el uso de los indicadores planteados se obtuvo un incremento en el nivel de aprendizaje de cada alumno.

CAPITULO I: INTRODUCCIÓN

1.1. Planteamiento del Problema

La Ciberseguridad, en los últimos años, se ha convertido en un área fundamental y de vital importancia en todas las organizaciones a nivel mundial. Las empresas más atractivas para los ciberatacantes son las entidades que generan, transfieren o almacenan información sensible y/o monetaria debido a que pueden obtener retribución económica por la venta o secuestro de dicha información.

Según diario Gestión, "el Perú es segundo, en ser víctimas de ciberataques a nivel Latinoamérica" (Gil, 2018). Esto nos demuestra que nuestro país no es ajeno a ataques por entes maliciosos y demuestra la necesidad de contar con los mecanismos de seguridad necesarios, tanto en tecnología como en procesos y personas.

Uno de los últimos casos que fueran hechos públicos en Latinoamérica, fue el de Banco de Chile, el cual fue atacado por un grupo de ciberdelincuentes el día 24 de mayo del 2018. En un artículo publicado en la página web diario La Tercera de Chile se informa que "cerca de las 11.00 detectaron que era un virus que se estaba propagando, decidieron desconectar gran parte de las estaciones de trabajo -unas 9.000- para que no siguiera el contagio" (Poblete y Marusic, 2018). Según información de la cadena Reuters "los piratas informáticos habían extraído $ 10 millones de sus fondos, principalmente a Hong Kong" (Iturrieta, Sherwood y Osterman, 2018)

Este tipo de ciberincidente y muchos otros que seguramente aparecerán en un futuro no muy lejano pueden ser mitigados o controlados contando con una adecuada organización, gobierno en ciberseguridad, posicionamiento organizativo, presupuesto, una arquitectura de seguridad bien definida y estructurada a través del uso de tecnologías. Sin embargo, una empresa puede contar con todo lo antes mencionado y de igual forma verse impactada por un ciberincidente si es que dentro de su gobierno de ciberseguridad no tienen contemplado un adecuado programa de concientización a los trabajadores en tópicos de ciberseguridad. Esto refiere a que

la ciberseguridad ya dejo de ser responsabilidad únicamente de los equipos de seguridad y paso a ser responsabilidad de todos los trabajadores de la empresa. Esto genera la necesidad de que toda empresa entrene, concientice y evalué constantemente las capacidades de sus trabajadores de manera efectiva para constatar que se encuentren en la capacidad de identificar y alertar de algún evento sospechoso y/o actividad maliciosa de la que pudieran ser testigos.

En la actualidad, para satisfacer la necesidad de capacitación y/o entrenamiento en temas de ciberseguridad, diferentes empresas e instituciones han invertido recursos en la creación de dinámicas o software basado en los elementos de ludificación para explicar distintos conceptos de ciberseguridad. Esta propuesta está en continuo desarrollo y tiene acogida en países desarrollados como Estados Unidos y Japón donde ya se han realizado investigaciones al respecto. En ese contexto, es necesario evaluar en qué medida el entrenamiento en ciberseguridad utilizado elementos lúdicos es efectivo para una empresa.

1.2. Pregunta de Investigación

¿En qué medida un entrenamiento en ciberseguridad utilizando elementos lúdicos es efectivo para los participantes?

1.3. Objetivos

1.2.1. Objetivo General

Evaluar la efectividad del entrenamiento en ciberseguridad utilizando elementos de ludificación propuesto por los autores.

1.2.2. Objetivos Específicos

- Establecer el estado actual de los programas de entrenamiento en ciberseguridad en las empresas estudiadas.
- Identificar cinco tópicos críticos en Ciberseguridad basados en estudios recientes de fuentes de confianza y tendencias en ataques a nivel mundial.

- Identificar los componentes de ludificación más apropiados para la creación de los escenarios de entrenamiento en Ciberseguridad.

- Evaluar efectividad del entrenamiento en ciberseguridad que utiliza elementos ludificación.

1.4. Justificación

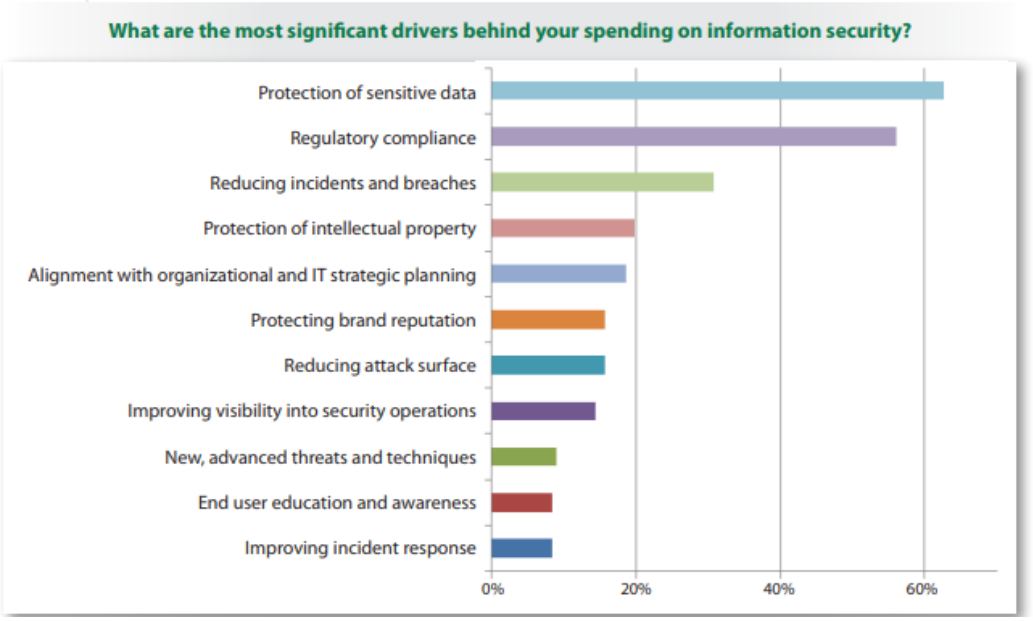
El costo del Cibercrimen se ha incrementado en los últimos años y según el informe "2017 Cybercrime Report" de la compañía CyberSecurity Venture el costo anual ocasionado por el Cibercrimen ascienda de $3 trillones en el año 2015 a $6 trillones de dólares para el año 2021. Así mismo, el reporte de esta misma compañía predice que el gasto anual acumulado de 5 años en Ciberseguridad excederá el $1 trillón de dólares (Morgan, 2017).

La gran mayoría del presupuesto designado a Ciberseguridad puede o podría ser gastado por las organizaciones para la adquisición de tecnologías de seguridad. Sin embargo, olvidan que ninguna tecnología es infalible y que el error humano es el frente más vulnerable para explotar. Este último ha sido el causante de muchos de los recientes incidentes de ciberseguridad en el mundo.

Pero pese a conocer la debilidad humana a equivocarse, muchas empresas no participan de una enseñanza adecuada para la capacitación de su personal.

En la *Figura 1.1*. se puede apreciar que la educación de empleados se encuentra en la penúltima posición y representaba menos del 10% de inversión de ciberseguridad en el año 2016.

Figura 1.1. *Tendencias del gasto en Seguridad Informática*



Fuente: SANS Institute, 2016.

Elaboración: SANS Institute, 2016

El "2017 Cybercrime Report" también predice que hacia el año 2027 la inversión en entrenamiento de Ciberseguridad para empleados llegará a los $10 billones de dólares, esta predicción nos brinda una sólida referencia que nos permite ratificar que el propósito de nuestra investigación será de gran importancia y relevancia en un corto o mediano plazo para las organizaciones (Morgan, 2017).
Las empresas empiezan a tomar mayor importancia en el desarrollo de su personal, en capacitarlos para prever incidentes y darles las herramientas necesarias para anticiparse al enemigo.

Sin embargo, estas capacitaciones no resultan ser suficiente. Muchas empresas capacitan a sus empleados y prueban sus resultados, para ver que lo enseñado haya sido aprendido. Sin embargo, muchos empleados que han asistido a estas clases no retienen las enseñanzas debido a que el método que se utiliza no influye en ellos.

Y considerar tener un personal más atento, y algo paranoico, es de alto valor para la empresa. Debido que pueden detectar el eslabón que debilite la integridad de la empresa, los tendrá más alertas y preparados para evitar estos incidentes en un futuro. Para esto queremos demostrar que, empleando un método diferente de enseñanza, los empleados retengan estas capacidades con mejores resultados.

Un estudio realizado por IBM en el año 2014 "IBM Security Services 2014 Cyber Security Intelligence Index" indicaba que más del 95% del total de los incidentes que formaron parte de la investigación reconocían al error humano como un factor clave para la materialización del incidente. Estos errores son comúnmente asociados a configuraciones de sistema mal ejecutadas, falta de parches de sistema operativo y/o seguridad, uso de credenciales por defecto o no seguras, ingreso a enlaces o sitios web no seguros o de dudosa reputación, apertura/ejecución de archivos adjuntos no seguros, entre otros.

En el estudio "EY Global Information Security Survey 2018-19" realizado por Ernst & Young Perú (EY) se menciona que la vulnerabilidad con mayor incremento de riesgo de exposición son los empleados descuidados con un 34% en los últimos 12 meses. Asimismo, en el mismo estudio se hace mención que la ciberamenazas conocidas como Phishing y Malware (ambas comúnmente propagadas por ciberdelincuentes mediante el uso de correo electrónico) se encuentran encabezando el top 1 y 2 con 22% y 20% respectivamente del top 10 de más grandes ciberamenazas para las organizaciones.

De materializarse el ciber riesgo mencionado en el párrafo anterior podría significar para una empresa de gran envergadura un costo de $148 por cada registro robado por los ciberdelincuentes y pudiendo alcanzar un costo promedio de $3.86 millones por un ciberincidente que desencadene en fuga de información, estas cifras fueron extraídas del reporte "2018 Cost of a Data Breach Study: Global Overview" publicado por IBM Security y el Ponemon Institute en el año 2018.

Tomando como referencia las cifras mostradas en los párrafos previos, recopilados de diferentes reportes de entidades de gran reputación y confianza, los

autores consideran preliminarmente que el presente tema de tesis “Escenarios de aprendizaje competitivo a través de uso de elementos lúdicos para entrenamiento en Ciberseguridad” genera un gran valor a todo tipo de empresa independientemente del sector al que pertenezcan y la inversión en ciberseguridad, siempre y cuando estas hagan uso de tecnologías de información, cuenten con empleados y manejen información de relevancia para la empresa. Asimismo, consideramos que debido a la criticidad y posible impacto del ciber riesgo, es de suma importancia que las empresas incluyan este tipo de entrenamientos como parte de un plan de mitigación de dicho ciber riesgo.

1.5. Alcance

La presente investigación tiene el siguiente alcance:

- La aplicación de los escenarios propuestos será puesta a prueba en tres (03) empresas privadas ubicadas en la ciudad de Lima.

- El entrenamiento será brindado a diez (10) personas como mínimo por cada sesión realizada en cada una de las empresas elegidas, estas personas serán escogidas aleatoriamente por la empresa.

- Se incluirán escenarios de evaluación en los entrenamientos reales con la finalidad de obtener una evaluación cuantitativa, cualitativa y critica de los participantes.

- El nivel de aceptación de los escenarios y general del programa será evaluado al finalizar las actividades.

1.6. Contribución

Con el presente Plan de Investigación los autores queremos brindarle a la comunidad cuatro (04) aspectos clave resultado de nuestra investigación para que estos sean utilizados de la forma que consideren más adecuada:

- Transmitir y lograr que las organizaciones comprendan y contextualicen la importancia de entrenar constantemente a sus empleados en tópicos de ciberseguridad. Es esencial lograr contextualizar mediante ejemplos, acordes al rubro donde se desempeñen las empresas, el riesgo al que se ven expuestas sus organizaciones por no contar con un programa de entrenamiento en tópicos de ciberseguridad para sus colaboradores.

- Evidenciar que por más complejo, extenso u aburrido que pueda ser un tópico, este puede ser enseñado de forma sencilla y eficiente a través de elementos lúdicos.

- Promover el entrenamiento en tópicos de ciberseguridad empleando las actividades desarrollada por los autores.

- Incentivar y extender el uso de elementos de ludificación para entrenamiento en diferentes clases de tópicos, no solo ciberseguridad.

CAPITULO II: MARCO CONCEPTUAL

2.1. Antecedentes

Titulo:	Competitive Learning Environment for Cyber-Physical System Security Experimentation
Autores:	Rujit Raval, Alison Maskus, Benjamin Saltmiras, Morgan Dunn, Peter J. Hawrylak y John Hale
Año:	2018
Resumen:	En esta investigación se introducen un banco de pruebas que también constituyen un entorno de aprendizaje competitivo en el que los estudiantes pueden explorar y dominar conceptos, técnicas y practicas fundamentales para Sistemas ciber físicos (CPS).
Titulo:	Practical security education on operational technology using gamification method
Autores:	Keiichi Yonemura, Kuniaki Yajima, Ryotaro Komura, Jun Sato y Yoshihiro Takeichi
Año:	2017
Resumen:	Los investigadores evaluaron el uso de la herramienta KIPS (Kaspersky Industrial Protection Simulation) en ambientes de educación en seguridad de tecnología operacional (OT). Al comparar los resultados del entrenamiento de seguridad integral y los resultados del juego de seguridad (KIPS), se revela que los materiales de enseñanza de seguridad del juego reflejan habilidades de seguridad reales y son efectivos para medir el nivel de habilidad
Titulo:	Using simulators to assess knowledge and behavior of “novice” operators of critical infrastructure under cyberattack events
Autores:	Aunshul Rege, Saroj Biswas, Li Bai, Edward Parker y Timothy R. McJunkin
Año:	2017

Resumen:	Este artículo presenta un estudio de caso en el que estudiantes de ECE de la Universidad de Temple utilizaron un simulador interactivo de micro-red, "Grid Game". Este estudio de caso ofrece información sobre la comprensión de los estudiantes de ECE de los principios clave de ingeniería (estabilidad de Microred, sistema de control de generación, inercia del generador, almacenamiento de energía y seguridad de la red) obtenidos mediante el uso del programa simulador.
Titulo:	Using Computer Programming Competition for Cyber Education
Autores:	Oded Margalit
Año:	2016
Resumen:	Esta investigación explora el uso de tareas de programación que serán solucionadas por los participantes como parte del proceso de aprendizaje.
Titulo:	A renewed approach to serious games for cyber security
Autores:	Alexis Le Compte, David Elizondo y Tim Watson
Año:	2015
Resumen:	La investigación presenta un marco para el diseño de juegos serios que tienen como objetivo concientizar sobre la ciberseguridad a personas que tienen poco o ningún conocimiento del tema.
Titulo:	Security & Privacy. Why Cybersecurity Is So Difficult to Get Right
Autores:	JM Olejarz
Año:	2015
Resumen:	Entrevista a Marc van Zadelhoff, VP of IBM Security, sobre las dificultades que enfrentan las empresas frente a los ciberataques y porque es una materia complicada el educar a los empleados a prevenir estos ataques.

Titulo:	2017 Data Breach Investigations Report. 10th edition.
Autores:	Verizon
Año:	2017
Resumen:	Reporte de vulnerabilidades basado en los estudios de múltiples empresas que han reportado en el año casos de incidencias por brechas de seguridad explotadas.
Titulo:	TrendLabs 2017 Annual Security Roundup: The Paradox of Cyberthreats.
Autores:	TrendLabs
Año:	2017
Resumen:	Estudio realizado por TrendLabs para la clasificación y organización de los tipos de ciberataques realizados a nivel mundial. Clasifica los tipos de ataques más importantes y evalúa el impacto que tienen las compañías.

2.2. Marco Teórico

2.1.1. Ciberespacio

El ciberespacio en un contexto amplio podría definirse como el espacio donde se interconectan las redes. Para Refsdal, Solhaug y Stølen: "El ciberespacio es una colección de redes computarizadas incluyendo servicios, sistemas computacionales, procesadores embebidos y controladores, así como información almacenada o en tránsito" (Refsdal, Solhaug y Stølen, 2015).

2.1.2. Ciberseguridad y Ciber riesgos

La ciberseguridad es mucho más que un problema técnico que se delega a los departamentos de tecnologías de la información (TI). Para (Green, 2015) "Ciberseguridad involucra los procesos que las organizaciones necesitan implementar para mitigar los ciber riesgos". Bajo esta definición, la ciberseguridad en un sentido más amplio un conjunto de mecanismos de control hacia los ciber riesgos. A lo largo de esta investigación, se utilizará el término "Ciberseguridad" como sinónimo de "seguridad de la información".

Según (Kostopoulos, 2012) la ciberseguridad debe salvaguardar los siguientes principios:

- Confidencialidad: Todos los datos transmitidos o almacenados son privados, solo pueden ser vistos por las personas autorizadas.

- Integridad: Todos los datos transmitidos o almacenados deben estar libre de error.

- Disponibilidad: Todos los datos transmitidos o almacenados deben estar disponibles para los autorizados.

- No Repudio: Todos los datos transmitidos o almacenados son de indiscutible autenticidad, especialmente cuando están soportados por certificados digitales, firmas digitales u otros identificadores explícitos.

En este contexto, se hace necesario definir también que es un ciber riesgo.

Para Refsdal, Solhaug y Stølen: “Un ciber riesgo es un riesgo causado por una ciber amenaza”. Sin embargo, los autores manifiestan que es importante entender que los Ciber riesgos son originados únicamente por ciber amenazas y no por otro tipo como por ejemplo el riesgo de inundación. Esto significa, en definitiva, que los ciber riesgos pueden ser únicamente llamados como tal si su origen es el ciberespacio (Refsdal, Solhaug y Stølen, 2015).

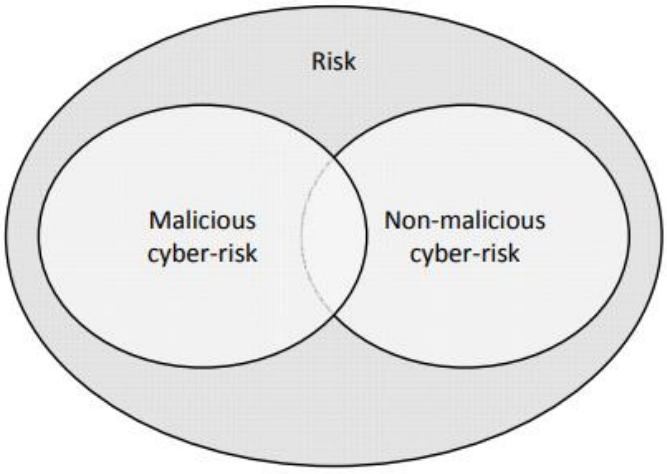
Refsdal, Solhaug y Stølen también establecen dos tipos de riesgos:

- Ciber Riesgos Maliciosos: Aquellos que potencialmente son ejecutados por agentes maliciosos como hackers.

- Ciber Riesgos No Maliciosos: Aquellos que potencialmente son resultado de acciones accidentales.

Es importante destacar que los Ciber riesgos también podrían existir bajo la combinación de ambos, según el diagrama de Venn en la *Figura 2.1.:*

Figura 2.1. *Ciber riesgos maliciosos y no maliciosos*



Fuente: Refsdal, Solhaug y Stølen, 2015.
Elaboración: Refsdal, Solhaug y Stølen.

Es relevante también considerar cuales son las categorías de riesgo. Para (Kendrick, 2010); las categorías son las siguientes:

- Riesgo en comunicaciones: En esta categoría podemos encontrar que las tecnologías en mayor riesgo son el correo electrónico, mensajería instantánea (IM), VoIP y redes de comunicaciones.

- Riesgo de Seguridad de la Información: En esta categoría encontramos la mayor cantidad de miembros. Mencionamos los que consideramos los más relevantes para la investigación, como son dispositivos de almacenamiento, sitios web, contraseñas y malware.
- Riesgos de Continuidad del Negocio: Se mencionan aquí como ejemplos principales los ataques perpetrados por hackers, infiltración de virus y ataques de spam.

- Riesgo en Outsourcing de Tecnologías de la Información: Encontramos aquí como principal servicio afectado el "software como servicio" (SaaS). Los riesgos principales en esta categoría son la interrupción de servicios, disponibilidad de la información, infección de virus, reducción en la protección del perímetro, entre otros.

- Redes Sociales: La popularidad de las redes sociales en la actualidad es indiscutible. Para los autores esto implica riesgos para las organizaciones como compartir información sensible, infiltración de virus en sistemas compartidos, transferencia insegura de datos, suplantación de identidad.

2.1.3. Ciberamenaza o amenaza cibernética

Un concepto de Ciberamenaza propuesto por De la Corte y Blanco: "La noción de ciberamenaza suele definirse mediante la adaptación del concepto general de amenaza cuando es realizada a través de internet" (De la Corte y Blanco, 2014). Ciertamente la mayor cantidad de ciberamenazas son distribuidas o realizadas a través de internet; sin embargo, hoy en día es igual de

común encontrar ciberamenazas dentro de dispositivos de almacenamiento extraíbles USB.

Las ciberamenazas relevantes para esta investigación son las siguientes:

A. **Malware:** "Malware es un conjunto de instrucciones que se ejecutan en su computador y hacen que su sistema haga lo que un atacante quiere que haga" (Skoudis y Zeltser, 2004). El ejemplo más común de malware es un virus de computador.

   Para (Ackerman, 2017) hay 7 tipos de malware, cada uno con características únicas:

   - Virus: Programa malicioso que al ejecutarse se propaga infectando otros programas o archivos.
   - Gusano (worm): Este tipo de malware puede replicarse sin necesidad de un programa huésped. Se propagan sin necesidad de interacción humana.

   - Caballo de Troya (Trojan Horse): Es un programa malicioso que es diseñado para parecer legítimo, de manera que los usuarios no sospechen su verdadero propósito.

   - Spyware: Diseñado para colectar información confidencial (como nombre de usuario y contraseñas) dentro de un computador.

   - Ransomware: Este programa malicioso infecta el computador de un usuario y encripta cierta información. Luego los creadores de dicho programa exigen el pago de dinero a cambio de desencriptar la información.

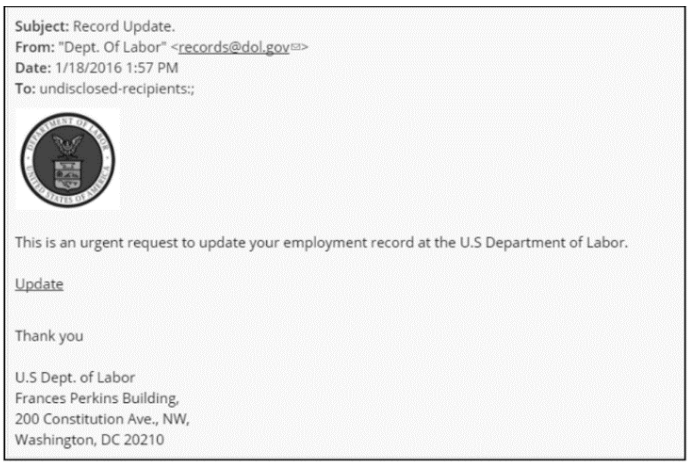
- Rootkit: Está diseñado para obtener acceso a secciones privilegiadas del sistema de un computador. Una vez dentro, mantiene escondido a sí mismo y a otros programas maliciosos para evitar la detección.

- Backdoor: También conocido como Troyano de acceso remoto, este programa malicioso crea una "puerta trasera" cuyo propósito es evitar la autenticación y autorización regular. De esta manera el programa malicioso permite el acceso de un atacante remoto, quien no necesita pasar por ninguna autenticación y/o autorización.

B. Ingeniería Social (Phishing): "Método no técnico utilizado por los cibercriminales para obtener información, realizar fraudes u obtener acceso ilegítimo a los equipos de las víctimas. La Ingeniería Social se basa en la interacción humana y está impulsada por personas que usan el engaño con el fin de violar los procedimientos de seguridad que normalmente deberían haber seguido" (ESET, 2016).

Un ejemplo de este método es el correo enviado por un atacante simulando ser legítimo (de parte de un banco o el gobierno), como se puede apreciar en la *Figura 2.2.*

Figura 2.2. *Email simulando comunicación del Gobierno USA.*



Fuente: Oskaya y Aslaner., 2019.

Elaboración: Oskaya y Aslaner.

La ilustración muestra, por ejemplo, como los cibercriminales utilizan todos los elementos a su alcance (iconografía, direcciones reales y dominios) para simular que el Departamento de Trabajo del Gobierno de los Estados Unidos requiere actualizar el registro de empleado.

Nótese, además, el enlace embebido en el correo electrónico que hacerle clic, enviará al destinatario a una página predefinida por el cibercriminal. Dentro de esta página, muy probablemente solicitará información personal (incluyendo código de empleado o alguna credencial) para luego utilizar esta información en un ataque más elaborado.

2.1.4. Ciberataque o ataque cibernético

"Acción criminal organizada o premeditada de uno o más agentes que usan los servicios o aplicaciones del ciberespacio o son el objetivo de la misma o donde el ciberespacio es fuente o herramienta de comisión de un crimen." (Superintendencia Financiera de Colombia, 2018).

Para (Niemelä, 2016), un ciberataque consta de 5 etapas:

- Reconocimiento: En esta fase, el atacante recopila información sobre su objetivo la cual incluye (pero no está limitada a) información de empleados, clientes, proveedores, sistemas en uso, procedimientos, entre otros. Se recopila también información de cualquiera de los activos en línea (páginas web, blogs, redes sociales, entre otras) que pudieran proporcionar información. Esto provee a los atacantes de una imagen preliminar de la compañía que desean atacar.

- Escaneo: Con la imagen preliminar, se inicia el escaneo de puerto y/o análisis de vulnerabilidades. Con el escaneo de puertos el atacante identifica que puertos están abiertos en la red (todos los computadores dentro de una red tienen el mismo número de puertos numerados desde el 0 hasta 65535) y muchos de esos puertos ya están asignados a servicios estándar, por ejemplo, el puerto 80 para WWW. Una vez identificados

los puertos y el servicio que hace uso de estos, es posible identificar las vulnerabilidades del software.

- Aprovechamiento: En esta etapa se utilizan métodos como phishing para obtener información confidencial como el nombre de usuario y la contraseña. El autor hace mención también a los ataques de denegación de servicios distribuidos (DDoS) y hombre en medio (man-in-the-middle). El primero se ejecuta generando millones de solicitudes incompletas a un servicio (muchos casos Web) que se identificó en las fases previas y que ocasionan el colapso de este. El segundo, se ejecuta al tomar control de algún servicio (por ejemplo, Resolución de Nombres o DNS por sus siglas en inglés) o equipo de comunicaciones intermedio (un router) que redireccione a la víctima a un sitio predefinido por el cibercriminal.

- Mantener acceso: Una vez en control, el cibercriminal se asegura que el acceso al servicio o equipo afectado permanezca disponible. Para esto, utiliza herramientas como backdoors, caballos de troya y rootkits.

- Cubrir pistas: Luego de un ataque, el cibercriminal eliminará los rastros de sus actividades. El autor menciona algunas técnicas como borrar el historial, cambiar fecha/hora del sistema, encriptación, esteganografía u otros que permitan ocultar información o acciones ejecutadas por el cibercriminal.

2.1.5. Ciberincidente o incidente de seguridad

Podemos definir a un incidente de seguridad como “un evento o conjunto de eventos que pueden provocar la interrupción de los servicios ofrecidos por un sistema informático e incluso la perdida de información” (Chicano, 2015).

El Gobierno español, a través de la Guía de Seguridad de las TIC CCN-STIC 817, nos proporciona una clasificación apropiada de los ciberataques atendiendo al vector de ataque utilizado:

Tabla 2.1. *Clasificación de los Ciberincidentes*

Clase de Ciberincidente	Descripción	Tipo de Ciberincidente
Código Dañino	Software que se infiltra o vulnera un ordenador u otro dispositivo de red, sin el conocimiento de la persona a cargo de este dispositivo.	Virus. Gusanos. Troyanos. Spyware. Rootkit. Ransomware. Herramienta para Acceso Remoto.
Disponibilidad	Ataques cuya finalidad es dejar fuera de servicio los sistemas, y de esta manera causar daños en la productividad o en la imagen de las instituciones afectadas.	Denegación [Distribuida] del Servicio. DoS/DDoS. Fallo (Hardware/Software). Error humano. Sabotaje.
Obtención de información	Ataques dirigidos a recaudar información fundamental que permita sacar provecho de esto para nuevos ataques.	Identificación de activos y vulnerabilidades (escaneo). Sniffing. Ingeniería social. Phishing.
Intrusiones	Ataques dirigidos a la explotación de vulnerabilidades y de esta manera poder infiltrarse en los sistemas de las organizaciones.	Compromiso de cuenta de usuario. Defacement (desfiguración). Cross-Site Scripting (XSS). Cross-Site Request Forgery (CSRF). Falsificación de petición entre sitios cruzados. Inyección SQL. Spear Phishing. Pharming. Ataque de fuerza bruta. Inyección de Ficheros Remota. Explotación de vulnerabilidad software/hardware Acceso no autorizado a red.

Clase de Ciberincidente	Descripción	Tipo de Ciberincidente
Compromiso de la información	Incidentes relacionados con el acceso y fuga (Confidencialidad), modificación o borrado (Integridad) de información no pública.	Acceso no autorizado a información. Modificación y borrado no autorizada de información. Publicación no autorizada de información. Exfiltración de información.
Fraude	Incidentes relacionados con suplantación de identidad.	Suplantación / Spoofing. Uso de recursos no autorizado. Uso ilegítimo de credenciales. Violaciones de derechos de propiedad intelectual o industrial.
Contenido abusivo	Ataques dirigidos a dañar la imagen de la organización o a utilizar sus medios electrónicos para actos ilícitos.	Acoso/extorsión/ mensajes ofensivos Pederastia/ racismo/ apología de la violencia/delito, etc.
Política de seguridad	Incidentes relacionados por violaciones de usuarios de las políticas de seguridad de la organización.	Abuso de privilegios por usuarios. Acceso a servicios no autorizados. Sistema desactualizado. Otros.
Otros	Otros incidentes.	

Fuente: Gobierno de España.

Elaboración: Autores de la tesis.

2.1.6. Gamificación o ludificación

Es la actividad de combinar factores de juegos, como estrategias, reglas o recompensas, dentro de un ámbito no relacionado con los juegos. Es que, Según Gallego, Molina y Lorens "Gamificar es aplicar estrategias (pensamientos y mecánicas) de juegos en contextos no jugables, ajenos a los juegos, con el fin de

que las personas adopten ciertos comportamientos" (Gallego, F.; Molina, F.; Llorens, F.; 2014).

En otra definición Teixes, 2015define la gamificación como “la aplicación de recursos de los juegos (diseño, dinámicas, elementos, etc.) en contextos no lúdicos para modificar comportamientos de los individuos mediante accesiones sobre su motivación” (Teixes, 2015).

Los autores Hamari y Koivisto publicaron en 2013 su estudio *Social “Motivations to Use Gamification: An Empirical Study of Gamifying Exercise”*, donde explicaban las diferencias entre la gamificación y los juegos convencionales:

A. La gamificación tiene como principal objetivo influir en el comportamiento de las personas, independientemente de otros objetivos secundarios como el disfrute de las personas durante la realización de la actividad del juego.

B. La gamificación produce y crea experiencias, crea sentimientos de dominio y autonomía en las personas dando lugar a un considerable cambio del comportamiento en éstas. Los videojuegos tan solo crean experiencias hedonistas por el medio audiovisual.

La diferencia que existe entre la gamificación y los juegos educativos en las aulas es que la primera muestra un espacio de juego más atractivo que motiva a los jugadores mientras que la segunda no (Kapp, 2012). A lo largo de esta investigación, se utilizará ludificación o gamificación como sinónimos.

2.1.7. Juego

En este punto se hace necesario proporcionar una definición de Juego. Según (McGonigal, 2011) un juego tiene 4 rasgos principales:

- Meta: Que es el resultado especifico que los jugadores trabajaran para conseguir.

- Reglas: Son las limitaciones de como los participantes pueden llegar a la meta. Al remover o limitar las formas obvias de llegar al resultado, se fuerza a los jugadores a explorar estrategias nuevas.

- Sistema de retroalimentación: muestra a los participantes que tan cerca estuvieron de llegar a la meta. Puede tomar muchas formas, las más conocidas son puntos, niveles, barra de progreso, entre otros. La retroalimentación muestra a los jugadores que la meta es alcanzable y sirve como motivación para continuar jugando.

- Participación Voluntaria: Requiere que todos los que participen, se encuentren de acuerdo con la meta, las reglas y la retroalimentación. La libertad de entrar o salir del juego asegura que los jugadores experimenten la actividad como segura y placentera.

Para el autor, elementos como interactividad, gráficos, narrativa, recompensa, competencia, ambientes virtuales la idea de "ganar" son comunes en los juegos, pero no lo definen como tal. Por tanto, los 4 rasgos arriba mencionados son la esencia de cualquier juego.

2.1.8. Los elementos de juego en la gamificación

Según (Kapp 2012) algunas de las características de la gamificación, muchas de ellas similares a lo expuesto por (Zichermann y Cunningham 2011):

- Base del juego: en esta parte es donde se puede dar el aprendizaje de la misma manera como se puede dar el entretenimiento por la acción misma de estar participando en un juego y de tener un reto que superar.

- Mecánica: La incorporación de premios, distinciones que gana la persona. Buscando incentivar la superación.

- Estética: El uso de imágenes atractivas para las personas que participan en el juego.

- Idea del juego: El objetivo que se pretende conseguir. Como en esta parte participan procesos mentales en el subconsciente de los jugadores se logra que se puedan adquirir habilidades nuevas.

- Conexión juego-jugador: Se lograr un compromiso entre los jugadores y el juego.

- Jugadores: Existen diferentes perfiles. Por la existente diversidad, Kapp diferencia a los jugadores motivados que participan activamente en el proceso de creación, y los que no.

- Motivación: La predisposición psicológica de la persona a participar es fundamental. Se debe resaltar respecto a la motivación en la gamificación es que no debe ser demasiado simple, de manera que no llame la atención, ni demasiado compleja, de manera que pueda desalentar a las personas a participar.

- Promover el aprendizaje: la gamificación utiliza técnicas psicológicas para desarrollar el aprendizaje a través del juego. Técnicas tales como la asignación de puntos y el feedback correctivo.

Resolución de problemas: Se puede entender como el objetivo final del jugador, es decir, llegar a la meta, resolver el problema, anular a su enemigo en combate, superar los obstáculos, etc.

2.1.9. Teoría del Flujo

Csikszentmihalyi citado por Fernandez y Arias, 2017 sostiene que el "flujo" es un estado de condición mental en la cual la persona está completamente integrada con lo que hace. Este flujo está integrado por 7 componentes core que se dividen en 2 categorías (condiciones y características):

Tabla 2.2. *Condiciones del Flujo*

Condiciones del Flujo	Explicación
Tareas Claras.	Las personas entienden lo que deben hacer.
Retroalimentación.	Las personas reciben una inmediata y clara retroalimentación de lo que funciona y de lo que falla.
Concentración.	La persona no es distraída y puede atender completamente la tarea.
Un objetivo alcanzable y balanceado.	El objetivo es retador y se cuenta con las habilidades para lograrlo.

Fuente: Fernández y Arias, 2017.

Elaboración: Autores de la tesis.

Tabla 2.3. *Características del Flujo*

Características del Flujo	Explicación
Control.	Las personas saben que sus acciones tienen impacto directo sobre las tareas y ellas pueden controlar el resultado.
Disminución de la conciencia de uno mismo.	La completa atención sobre la tarea deja poco espacio para la autoconciencia o la duda. Frecuentemente descrito como ser parte de la actividad.
Sentido del tiempo alterado.	La percepción del tiempo es distorsionada. El tiempo pasa rápidamente y de manera inadvertida.

Fuente: Fernández Zamora, 2017.

Elaboración: Autores de la tesis.

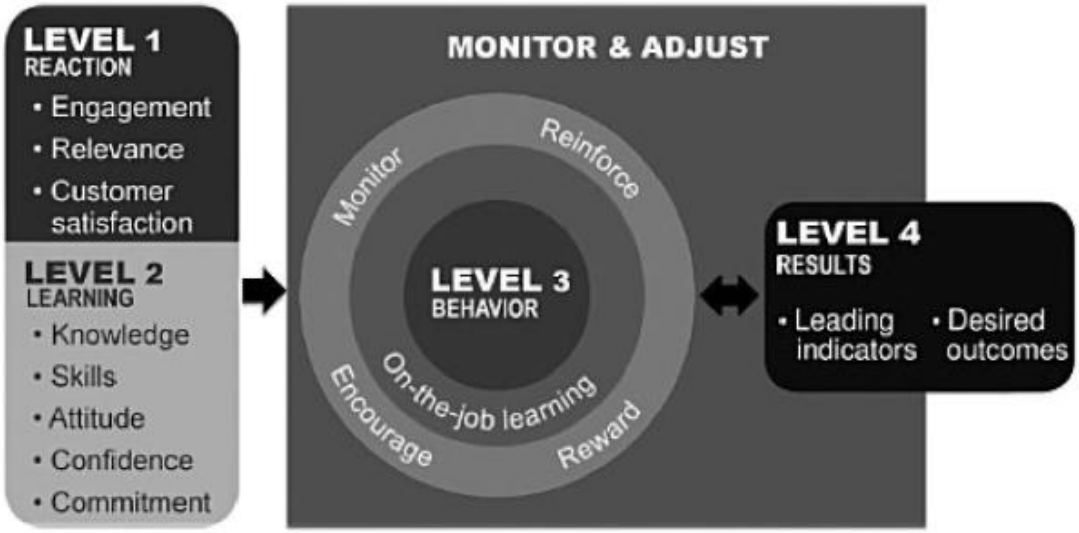
Es importante considerar esta teoría para poder entender cómo es que la gamificación, puede ayudarnos a incrementar la calidad del proceso de enseñanza-aprendizaje y cuáles son las características que deben tomarse en cuenta y cumplirse para lograr alcanzar este fin.

2.1.10. El Modelo de cuatro niveles de evaluación formativa de Kirkpatrick

En 1959, Donald Kirkpatrick estableció un modelo de evaluación para la formación dentro de las empresas. Este modelo propone 4 niveles: reacción, aprendizaje, conducta y resultados.

En la *Figura 2.3.* se muestra un resumen de los 4 niveles propuestos en el modelo actualizado (Kirkpatrick y Kirkpatric, 2016):

Figura 2.3. *Resumen de los 4 niveles de modelo Kirkpatrick y Kirkpatric*



Fuente: Kirkpatrick y Kipatrick, 2016.
Elaboración: Kirkpatrick y Kipatrick

Con el objetivo de medir la efectividad, nos centraremos en los 2 primeros niveles debido a que en palabras de los autores "Niveles 1 y 2 en el nuevo modelo Kirkpatrick proveen datos relacionados a la efectividad del entrenamiento" (Kirkpatrick y Kirkpatrick, 2016). Según Kirkpatrick y Kirkpatric, 2016:

- Nivel 1: Este nivel se refiere a medida en que los participantes encuentran el entrenamiento favorable y relevante para su trabajo diario. Este es uno de los niveles más evaluados. Dentro del nivel 1 se encuentran 3 componentes:

    - Satisfacción del participante: Los autores consideran mejor evaluar la satisfacción del cliente usándolo para identificar y eliminar cualquier barrera al aprendizaje durante el entrenamiento.

- Relevancia: Se refiere al grado en el que los participantes tendrán la oportunidad de usar lo que aprendieron en su trabajo diario.

- Compromiso: Referido al grado en el que los participantes están envueltos y contribuyendo a las actividades de aprendizaje.

- Nivel 2: Se refiere al grado en el que los participantes adquieren los conocimientos, habilidades, actitudes, confianza e involucramiento deseado. Dentro del nivel 2, hay 5 componentes:

    - Conocimientos: Es el grado en el cual los participantes conocen cierta información.

    - Habilidades: Es el grado en el cual los participantes saben cómo ejecutar cierta tarea.

    - Actitudes: Es el grado en el cual los participantes del entrenamiento creen que lo que han aprendido será valioso usarlo para su trabajo.

    - Confianza: Es el grado en el cual los participantes creen que podrán ejecutar lo que aprendieron en el entrenamiento.

    - Involucramiento: Es el grado en el cual los participantes tienen la intención de aplicar lo que aprendieron en su trabajo.

CAPITULO III: MARCO CONTEXTUAL

3.1. Contexto Global

La gamificación tiene su origen en la industria de los medios digitales, el primero documento el cual hace referencia a esto es del 2008, pero fue recién en el 2010 donde el término cobro fuerza en la literatura. Los países que más publicaciones científicas hacen respecto a este tema son Estados Unidos, Reino Unido, Alemania, Australia y España (Gazabón et al, 2016).

Los estudios sobre la gamificación aplicada a la educación sugieren que los profesionales que primero la adoptaron provienen de campos como las Ciencias de la Computación o las Tecnologías de la Información (Dicheva et al, 2015).

Otros estudios establecen que la mayoría de los estudios sobre gamificación aplicados a la educación se han publicado en conferencias y está enfocado a niveles superiores de educación (de Sousa Borges et al, 2014).

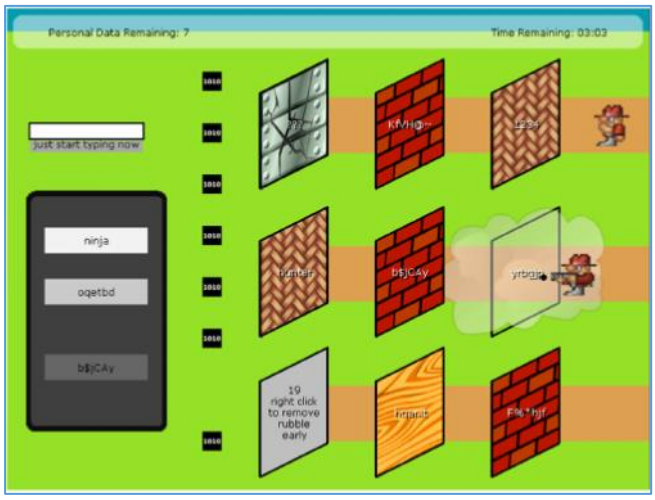
La enseñanza de Ciberseguridad haciendo uso de la gamificación ha tenido éxito en diferentes partes del mundo. En la universidad de Amritapuri en la India, por ejemplo, se ha empleado diferentes elementos de juego para explicar diferentes conceptos de Ciberseguridad a través de dinámicas que incluye la competencia entre equipos para atacarse y defenderse entre sí, logrando tener éxito en el proceso de enseñanza (Boopathi, Sreejith y Bithin, 2015).

En las academias de servicios militares de Estados Unidos se incluyen competencia en Ciberseguridad como un requisito en la educación. A comienzos del 2004 la academia militar en West Point incorporó “Captura la bandera” en un contexto civil e introdujo esto en algunas universidades, incluyendo la Universidad de Washington. Estas universidades incorporaron esto para la certificación en Ciberseguridad y era una experiencia anual primordial para sus estudiantes (Fink, 2013).

El departamento de defensa de los Estados Unidos y la Fundación Nacional para la Ciencia de Estados Unidos han usado de una manera más directa la gamificación para la enseñanza de la Ciberseguridad. Ha diseñado el juego “Fuerza Bruta”, cuyo objetivo principal es enseñar hábitos de generación de buenas contraseñas (seguras) a los usuarios del juego. Los jugadores deben defender su información personal de los ladrones de información.

El juego está diseñado de manera simple, de manera que los jugadores vayan aprendiendo gradualmente a medida que se van familiarizando con el juego y los conceptos de contraseñas seguras. (Thornton et al, 2014).

Figura 3.1. *Juego “Fuerza Bruta”*

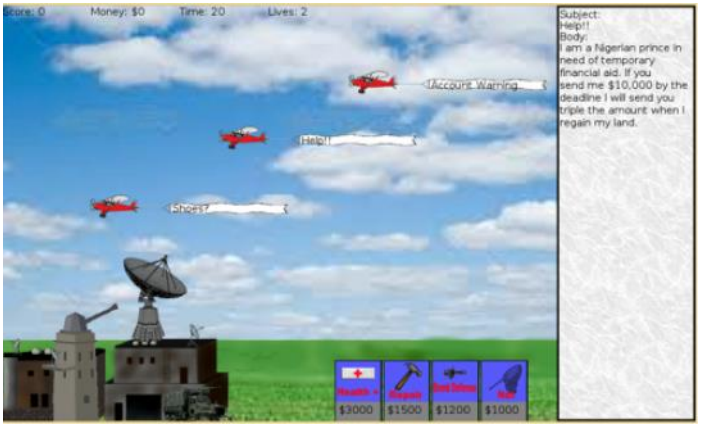


Fuente: Thornton, D, 2014.
Elaboración: Thornton, D.

Además, también han creado el juego “Mensaje Recibido”, cuyo objetivo es informar a los usuarios sobre que es phishing y cómo evitarlo. El juego consiste en un aeroplano base el cual debe ser defendido de aviones enemigos.

El usuario debe decidir si el mensaje enviado por los aviones es un buen mensaje o un mal mensaje, y luego que el usuario tome una decisión el juego explicará si la decisión tomada fue la correcta y porque ese mensaje es seguro o no.

Figura 3.2. *Juego "Mensaje Recibido"*



Fuente: Thornton, D, 2014.

Elaboración: Thornton, D.

De todo esto podemos inferir que el concepto de Gamificación aplicado a la Ciberseguridad no es del todo nuevo. Además, debemos considerar la existencia de diversas soluciones de entrenamiento en Ciberseguridad para trabajadores que emplean la gamificación (Adams y Makramalla, 2015):

Tabla 3.4. *Soluciones de Entrenamiento en Ciberseguridad*

Solución	Concientización	Estrategia Defensiva	Estrategia Ofensiva
CounterMeasure	Conocimiento Básico	Ninguno.	Autenticación y bypass de contraseñas.
CyberCiege	Conocimiento Básico. Evaluación General.	Prevención de ataques de penetración.	Ninguno.
CyberNexs	Ninguno.	Prevención de ataques de penetración. Evaluación de Sistemas.	Captura la bandera.
CyberProyect	Conocimiento Básico. Evaluación General.	Ninguno.	Ninguno.
NetWars	Evaluación de habilidades.	Evaluación de Sistemas. Prevención de ataques de penetración.	Escenarios de penetración de sistemas.
Micro Games	Conocimiento Básico. Evaluación General.	Detección de ataques de penetración. Gestión de contraseñas.	Ninguno.

Fuente: Adams, M., 2015.

Elaboración: Autores de la tesis

De esto se desprende el hecho, que es válido el empleo de la gamificación para la enseñanza de la Ciberseguridad, por ser algo que ya se ha aplicado antes y que ha sido considerado por importantes instituciones a nivel mundial como una opción importante para la enseñanza de diversos conceptos en Ciberseguridad.

En la Universidad de Granada, se utilizó la gamificación en el Master de Economía, para los cursos de Gestión de la cadena de suministros y Gestión de operaciones. Para ello, utilizaron componentes (puntos de experiencia, niveles, tablas de clasificación), mecánicas (recompensas, retroalimentación, competición, cooperación, retos) y dinámicas (emociones, relaciones, narrativa) de gamificación. Se pudo obtener como resultado que la gamificación cuando se aplica al proceso de estudio debería mejorar significativamente la motivación, experiencia de aprendizaje, participación, retención y la proactividad de los estudiantes. (Fernández y Arias, 2017).

Es importante conocer esta información porque nos permite saber de antemano los efectos positivos que puede producir el empleo de la gamificación para producir un proceso de aprendizaje adecuado, en diversos niveles de enseñanza.

3.2. Contexto Regional y Casos

En la región Latinoamericana también se ha empleado la gamificación para aplicarlo al proceso de enseñanza. En una escuela técnica Bolivia, se utilizó la gamificación en una plataforma virtual para fomentar el compromiso de maestros en una escuela técnica. Mediante el uso de logros, puntos, reconocimientos, barras de progreso, entre otros. Esto como parte del proyecto “Construyendo en RED” llevado a cabo por la Universidad la Salle por solicitud de la cooperación suiza en Bolivia (Valda y Arteaga, 2015).

En una publicación del Banco Interamericano de Desarrollo (BID) Rivas, 2016 considera a la gamificación como una tendencia educativa y nos comenta diferentes casos de éxito que han surgido para América Latina.

- Mate Marote, en Argentina. Es un programa de estimulación cognitiva para niños haciendo uso de programas digitales. Tiene como objetivo mejorar la atención y la flexibilidad mental.

- Kokori, en Chile. Es un videojuego que tiene como finalidad enseñar de manera didáctica acerca de biología celular, haciendo uso de cómics, guías didácticas y series animadas.

- Qranio, en Brasil. Es un juego que hace preguntas sobre diferentes categorías educativas y permite la interacción con otros jugadores. Además de poder ganar monedas en base a ciertos méritos.

- Creápolis, en Argentina. Permite la creación de mundos en 2 y 3 dimensiones donde los jugadores desarrollan su creatividad, al mismo tiempo que aprenden y colaboran con otras personas.

- Ncite, en México. Permite realizar prácticas profesionales a adolescentes con el objetivo que encuentren su orientación vocacional en una determinada área de estudio.

3.3. Contexto Local

3.3.1. Macroentorno

El desarrollo de nuevas tecnologías ha dado lugar a mejores formas de aprendizaje y mayor libertad para abordar maneras creativas de realizar el proceso de enseñanza. Esto influye en las instituciones que buscan maneras innovadoras de realizar sus procesos.

La gamificación representa una tendencia y una oportunidad para las empresas y organizaciones que quieran capacitar a su personal, y confiar en que de esta manera se lograran los objetivos de las capacitaciones.

3.3.2. Microentorno

En nuestra realidad nacional cada vez se hace más notorio la necesidad de capacitar al personal de las empresas e instituciones en temas de Ciberseguridad. Las grandes empresas cada vez reconocen más la importancia de contar con un área dedicada a estos temas.

En esta realidad también las instituciones educativas han comenzado a reconocer los beneficios que podría significar el empleo de la gamificación en la enseñanza en diferentes campos y en diferentes niveles de enseñanza. Se ha popularizado el empleo de "Kahoot!", un programa que permite realizar cuestionarios interactivos y que presenta elementos de gamificación, para poder evaluar el conocimiento de los participantes en diversas instituciones educativas.

CAPITULO IV: METODOLOGÍA DE INVESTIGACIÓN

4.1. Diseño de Investigación

La presente investigación es de tipo cuantitativa, no experimental, transeccional, descriptivo, según lo expuesto por Hernández, Fernández y Baptista (2010):

- Cuantitativa, debido que este estudio estará basado en mediciones numéricas.
- No experimental, debido a que no se manipularán las variables. Sólo se observará su comportamiento.
- Transeccional, debido a que la recolección de datos se hará en un mismo tiempo y no se evaluará su evolución a través de este.
- Descriptivo, puesto que se investigará la incidencia y los valores que se manifiestan en las variables.

4.2. Hipótesis

Basado en la pregunta de investigación ¿En qué medida un entrenamiento en ciberseguridad utilizando elementos lúdicos es efectivo para los participantes?, se plantea la siguiente hipótesis:

La efectividad del entrenamiento propuesto en ciberseguridad utilizando elementos lúdicos es alta (>61%).

4.3. Población y Muestra

La población considerada para este estudio las pequeñas (20 a 250 trabajadores) medianas (251 a 1000 trabajadores) y grandes (más de 1000 trabajadores) empresas

con sede en Lima Metropolitana, de los rubros servicios y retail. Se utilizará una muestra aleatoria de (10) empleados como mínimo en (03) empresas. Es importante mencionar que, debido a las restricciones de tiempo y presupuesto, los autores han optado por una muestra no probabilística.

No se considera el género, edad o nivel socio económico, ni tampoco el nivel trabajo dentro de la organización o el departamento/área al cual pertenecen los participantes debido a que los riesgos de ciberseguridad, por lo general, pueden aparecer sin importar estas variables.

4.4. Instrumentos de Medición

Para la presente investigación se han considerado los siguientes instrumentos de medición según lo expuesto por Hernández, Fernández y Baptista (2010):

- Cuestionarios aplicados a los participantes (inicio).
- Cuestionarios sobre tópicos de ciberseguridad (final).
- Escala de Likert.

Antes de iniciar con el entrenamiento, aplicaremos una encuesta a los participantes para obtener información de cada uno de ellos. Adicionalmente, entrevistaremos a los responsables de la seguridad en las empresas estudiadas para conocer los métodos o programas de entrenamiento en ciberseguridad utilizados actualmente (si hubiera).

Durante el curso, se observará el comportamiento de los participantes a través y se registrará los resultados usando la escala de Likert de 5 niveles.

Al terminar de dictar el curso, se empleará una herramienta lúdica, donde el grupo participará de un cuestionario preguntas cerradas de opciones múltiples pero presentadas al grupo. Cada participante responderá con sus propios conocimientos obtenidos, pero se les evaluará de forma individual y fomentando la competencia.

Tomando en cuenta el modelo de Kirkpatrick, la operacionalización de variables es como se muestra en la Tabla 3.5:

Tabla 3.5. *Operacionalización de Variables*

Variable	Conceptualización	Dimensiones	Indicadores	Escala	Valor Final
Efectividad del entrenamiento de ciberseguridad	Grado en el que se mide la reacción y aprendizaje de los participantes del entrenamiento	Reacción	Nivel de Compromiso	De Intervalos (5 Puntos)	Muy Alto:>81% Alto:>61%, <81% Medio: >41%, <61% Bajo: <21%, <41% Muy Bajo: <21%
			Nivel de Relevancia		
			Nivel de Satisfacción del participante		
		Aprendizaje	Nivel de Conocimiento		
			Nivel de Habilidades		
			Nivel de Actitudes		
			Nivel de Confianza		
			Nivel de Involucramiento		

Fuente: Autores de la tesis.

Elaboración: Autores de la tesis.

4.5. Descripción de Procedimientos

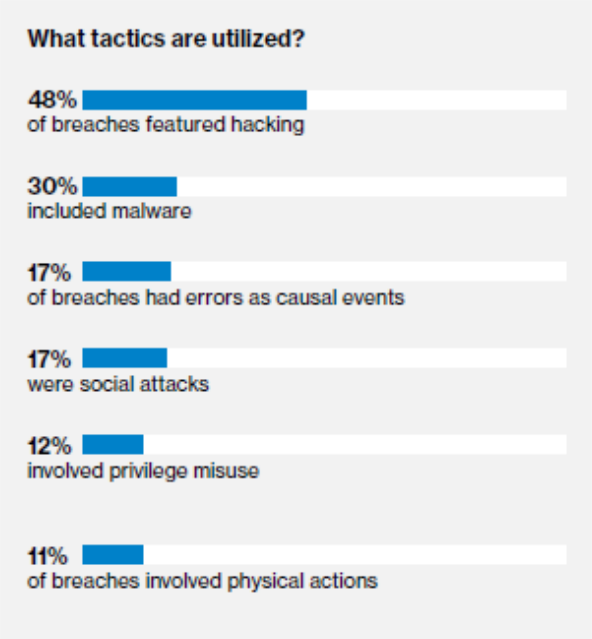
Se han seleccionado 5 tópicos de ciberseguridad para la elaboración del entrenamiento:

- Tópico 01: ¿Cómo evitar archivos adjuntos maliciosos?
- Tópico 02: ¿Cómo evitar enlaces maliciosos?
- Tópico 03: ¿Cómo proteger tus contraseñas?
- Tópico 04: Dispositivos USB seguros
- Tópico 05: Precauciones contra el Phishing dirigido

Estos tópicos fueron elegidos en base a los resultados de los estudios de entidades como "2018 Data Breach Investigations Report 11th Edition" de Verizon y "2017 Cost of Cybercrime Study" de Accenture, en los cuales explican los factores que aprovechan los ciberatacantes para lograr robar data en las organizaciones. Los mencionados tópicos también fueron escogidos debido a la sencillez de enseñanza que representaban desde la perspectiva lúdica y se limitaron únicamente a cinco tópicos debido al tiempo disponible para la elaboración de la presente tesis.
El estudio de Verizon muestra los siguientes resultados:

- El 48% de brechas de seguridad son perpetuadas debido a técnicas de hacking que pueden ser desde el ataque y explotación de una vulnerabilidad en una aplicación web hasta vulnerar contraseñas de usuarios finales debido al uso de credenciales no seguras (Ilustración 7).
- El 30% de brechas de seguridad incluyen el uso de malwares. En su mayoría los malware son propagados mediante dispositivos de almacenamiento USB, correo electrónico (Phishing) y/o debido a que los usuarios acceden a sitios inseguros o de dudosa reputación para descargar y/o instalar contenido (Ilustración 7).
- El 17% de las brechas de seguridad han utilizado ataques sociales dentro de los cuales encontramos al phishing (Ilustración 7).

Figura 4.1. *Tácticas utilizadas por atacantes*

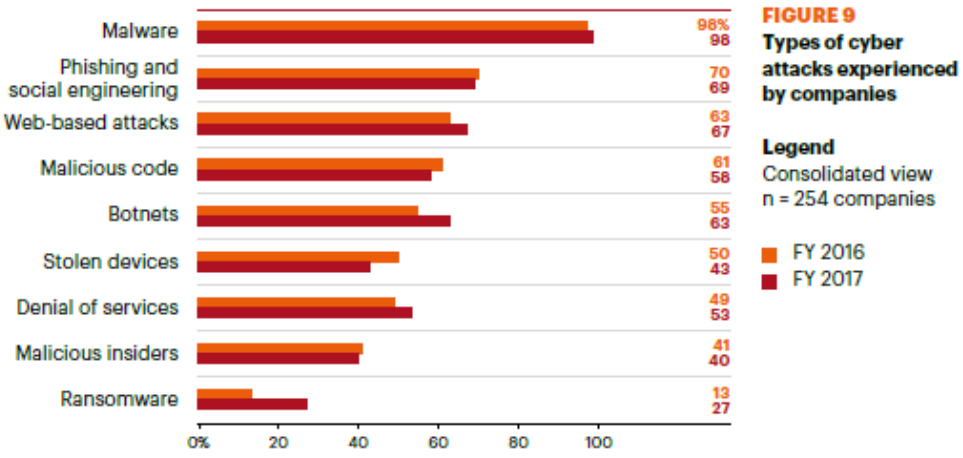


Fuente: 2018 Data Breach Investigations Report 11th Edition.

Elaboración: Verizon.

Resultados muy similares identificamos en el estudio de Accenture (Ilustración 8) en el cual tenemos en las dos primeras posiciones a ciberataques como malware y phishing e ingeniería social.

Figura 4.2. *Tipos de ciberataques experimentados por Compañías*



Fuente: 2017 Cost of Cybercrime Study, Accenture.

Elaboración: Accenture.

Elegidos los 5 tópicos, el entrenamiento ha sido dividido en 5 actividades de 15 minutos cada una:

Actividad #1: Correo Peligroso

Figura 4.3. *Esquema de la Actividad Correo Peligroso*

Fuente: Autores de la Tesis.
Elaboración: Autores de la Tesis.

Base del juego

El desarrollo de esta actividad requiere los siguientes elementos:

- Un tutor.
- Hasta 10 participantes
- Hojas A4 - Impresión email riesgoso en cada hoja.
- Varios plumones para resaltar (de preferencia 4).
- Un aula con escritorios por alumno o con mesas para ciertos números de participantes.

- 20 pegatinas de logro.

Mecánica

Formados en equipos de 5 personas, cada equipo recibirá una hoja impresa con un correo electrónico y un plumón para resaltar. Deberán en grupo discutir y resaltar todos los elementos que puedan identificar qué puedan resultar peligrosos o sospechosos. Al finalizar el tiempo estimado por el tutor, los grupos revisarán con el tutor empleando la presentación del correo si cumplieron o no con identificar todos los riesgos.

Estética

Se emplearán pegatinas de logros para aquellas personas que participen y ganen el desafío.

Idea del juego

Empleando este ejercicio, los participantes podrán identificar y discutir con cada miembro de su grupo sobre los riesgos potenciales que puede tener un correo malverso. Y esto reforzará el conocimiento que ya tenían los más experimentados y les dará aportes para aprender a los que son nuevos en el tema.

Conexión juego-jugador

El juego en equipos motivará a cada grupo a competir entre sí.

Jugadores

- Perfil experimentado: Son aquellos jugadores que tienen cierto nivel de conocimiento sobre el tópico, y dependiendo del ejercicio pueden aportar con valor o esperar otros estén al nivel de su conocimiento.

- Perfil novato: Son aquellos jugadores que no tienen conocimiento en el tema, son los más dispuestos a aprender y a escuchar lo que otros puedan ofrecer.

Motivación

El factor clave de este ejercicio es la competitividad de grupos de pocas personas, dándoles a todos la oportunidad de opinar dentro de sus grupos y superar colectivamente al otro grupo.

Promover el aprendizaje

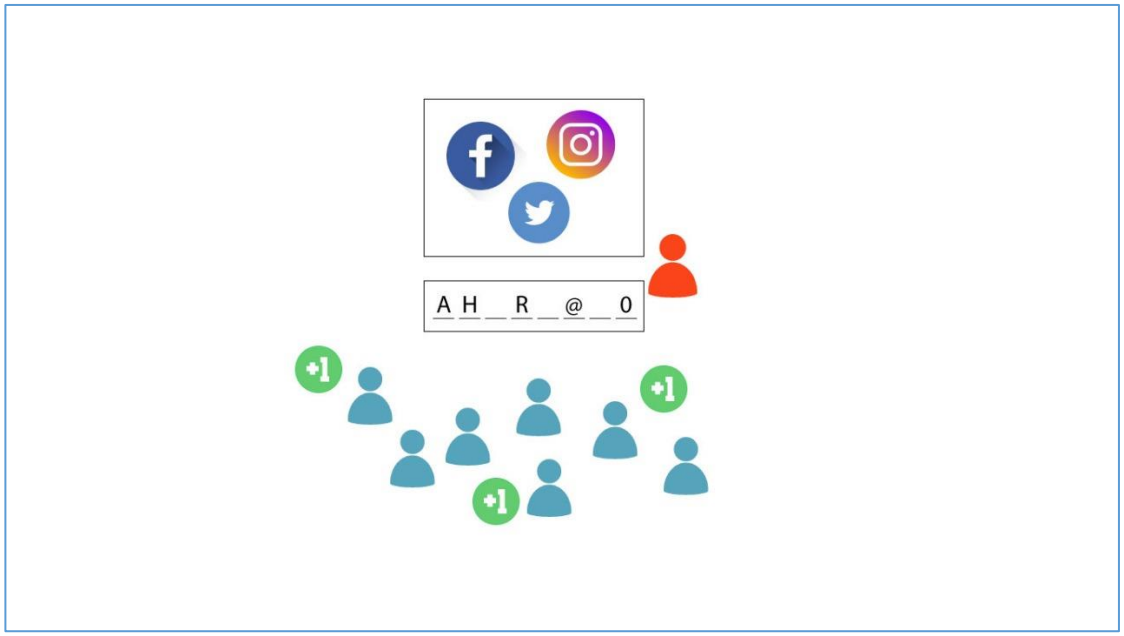
El objetivo del ejercicio es que puedan lograr identificar los puntos riesgosos de un email. Con la práctica podrán reconocerlos inmediatamente.

Resolución de problemas

Lo importante es superar el obstáculo de que no somos invulnerables, ver cómo cada grupo compara sus resultados esperando haber identificado cada riesgo hace que ellos mismos se vuelvan más agudos en su forma de interpretar un correo electrónico.

Actividad #2: Usuario Ahorcado

Figura 4.4. *Esquema de la Actividad Usuario Ahorcado*



Fuente: Autores de la Tesis.

Elaboración: Autores de la Tesis.

Base del juego

El desarrollo de esta actividad requiere los siguientes elementos:

- Un tutor
- 10 participantes.
- Tiza para pizarra o proyector.
- Un aula con escritorios por alumno o con mesas para ciertos números de participantes.
- 20 pegatinas de logro.

Mecánica

El tutor armara un ahorcado de ocho letras en la pizarra. Y pondrá en pantalla varias imágenes que contienen información pública de una persona.

Los participantes podrán levantar la mano y tomando la atención del tutor dictarán cual valor podría tener cada letra. Si un alumno, descubre la palabra clave puede levantar la mano y participar en contarla a la clase. Si acierta, gana un reconocimiento.

Se repite el proceso una vez más, pero esta vez utilizando una contraseña más segura.

Estética

Se emplearán pegatinas de logros para aquellas personas que participen y ganen el desafío.

Idea del juego

En el ejercicio, los participantes identificarán los puntos vulnerables en la información que ellos mismos exponen que podrían poner en riesgo sus contraseñas sencillas. Enseñándoles como reforzar una contraseña, permitirá al grupo identificar como mejorar la creación y cuidado de sus contraseñas en el futuro.

Conexión juego-jugador

El juego de forma individual motivará a cada persona a responder rápidamente, pero más que cantidad de intentos buscará ser asertivo.

Jugadores

- Perfil investigador: Son aquellos jugadores que identifican las respuestas correctas, visualizando las más complejas posibilidades.

- Perfil casual: Son aquellos jugadores que buscan acertar en su respuesta, pero no toman mucho tiempo en pensar su respuesta antes de decirla.
- Perfil nublado: Son aquellos jugadores que frente a la decisión de descubrir algo, no logran ver la solución.

Motivación

El factor clave de este ejercicio es la competitividad abierta, dándoles espacio a los más activos y pensadores.

Promover el aprendizaje

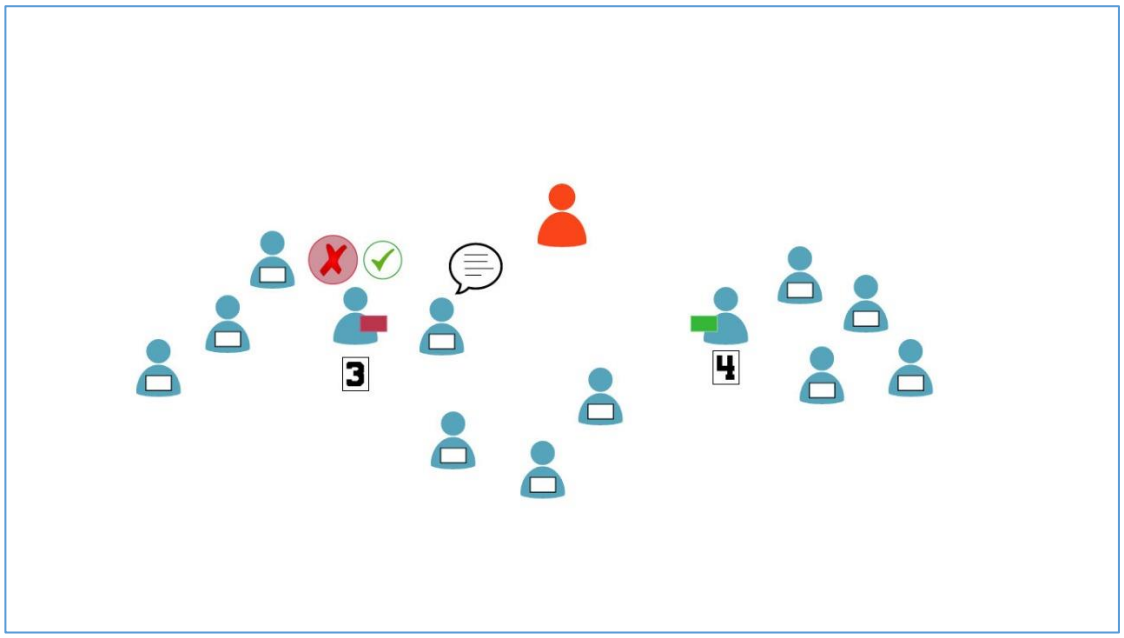
Enseñándoles como reforzar sencillamente una contraseña, permitirá al grupo identificar como mejorar la creación de contraseñas en el futuro.

Resolución de problemas

Lo importante del ejercicio es tratar de filtrar rápidamente las respuestas que no son obvias y ponerse en la posición de atacante malintencionado.

Actividad #3: Enlaces Prohibidos

Figura 4.5. *Esquema de la Actividad Enlaces Prohibidos*



Fuente: Autores de la Tesis.

Elaboración: Autores de la Tesis.

Base del juegoEl desarrollo de esta actividad requiere los siguientes elementos:

- Un tutor
- 10 participantes.
- Tarjetas con direcciones URL (8) o la palabra Firewall (2) en verde y rojo.
- Un aula con escritorios por alumno o con mesas para ciertos números de participantes.
- 20 pegatinas de logro.

Mecánica

Formados en equipos de 5 personas, cada equipo recibirá 5 tarjetas. Estas tarjetas vienen de 2 tipos, firewall (1) o enlace de internet (4). Los miembros firewall se pondrán frente al salón y serán los jueces de decisión para filtrar los enlaces permitidos de los prohibidos. Los jueces decidirán como agrupar a sus miembros de grupo: Delante de el

sin SON URLs NO permitidas o detrás suyo si son permitidas. Al finalizar, la repartición de participantes se decidirá qué equipo acertó más URLs.

Estética

Se emplearán pegatinas de logros para aquellas personas que participen y ganen el desafío.

Idea del juego

Con las URL peligrosas, lo importante es identificar los puntos clave que la conforman y que riesgos pueden existir en cada enlace. Capacitarlos a reconocer que sitios web son seguros y como los enlaces que nos llegan pueden ser utilizados para atacarnos, pero más que todo como prevenir los problemas.

Conexión juego-jugador

El juego en equipos motivará a cada grupo a competir entre sí. Los motivará a realizar la tarea de búsqueda con velocidad y rápidamente decidir si algo es favorable o no.

Jugadores

- Perfil razonamiento veloz: Son aquellos jugadores que tienden a decidir rápidamente si algo les es favorable o no basados en las reglas del juego, sin necesidad de pensar si es asertivo o no.

- Perfil razonamiento lento: Son aquellos jugadores que tienen a tomar más tiempo en decidir si algo les es favorable o no, pero enfocados en tomar el tiempo necesario para identificar lo más favorable.

Motivación

El factor clave de este ejercicio es la competitividad de grupos y el razonamiento individual de cada alumno.

Promover el aprendizaje

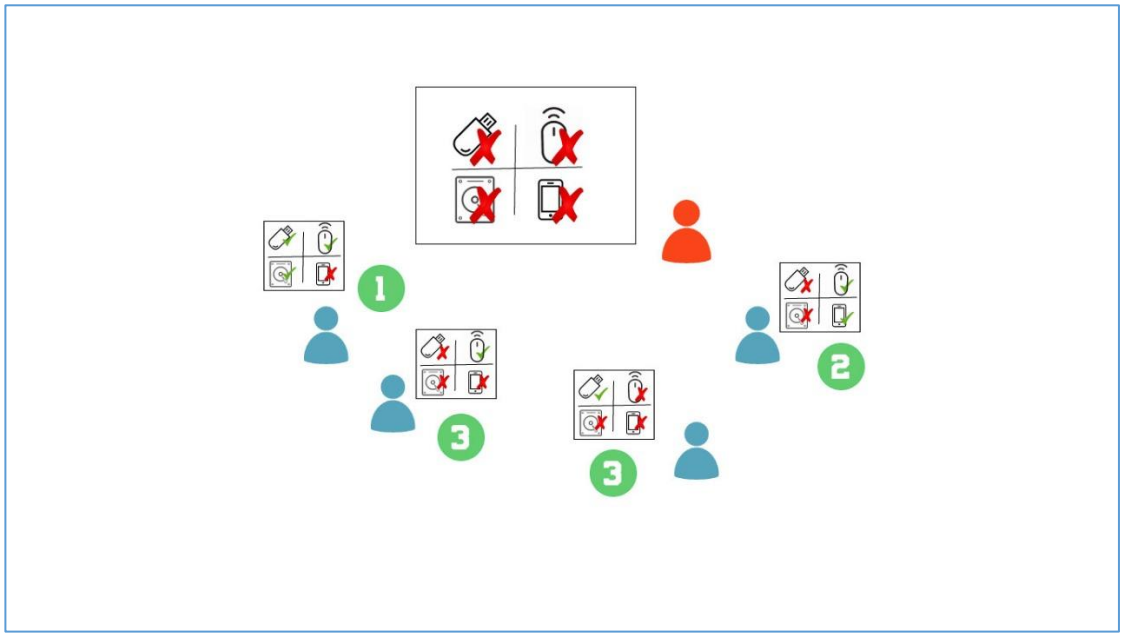
Como objetivo del juego es permitir a los participantes conversar e interpretar rápidamente que factores peligrosos pueden existir en una dirección URL del enlace que recibieron.

Resolución de problemas

Ningún grupo está a salvo, ninguna herramienta filtrará todos los enlaces prohibidos. Durante el ejercicio verán que existen varias posibilidades de perder si se confían y eligen una URL que no les conviene. Esto generará conflicto de decisión y debe llevarse la indecisión para un camino más favorable.

Actividad #4: Invasión en Puertos

Figura 4.6. *Esquema de la Actividad Invasión de Puertos*



Fuente: Autores de la Tesis.

Elaboración: Autores de la Tesis.

Base del juego

El desarrollo de esta actividad requiere los siguientes elementos:

- Un tutor

- 10 participantes.
- Hojas impresas con los collages.
- Lapiceros de tinta.
- 20 pegatinas de logro.

Mecánica

Cada jugador, alumno, recibirá una hoja con el collage de figuras con los dispositivos USB más vulnerables. Cada alumno podrá marcar los dispositivos que considera vulnerables a ataques. Luego de entregar sus resultados, se verá quien acertó en los correctos. Los participantes que coincidan en la totalidad de aciertos ganarán un reconocimiento.

Estética

Se emplearán pegatinas de logros para aquellas personas que participen y ganen el desafío.

Idea del juego

Los dispositivos USB son en todo su aspecto peligrosos. Así su objetivo sea de brindar utilidad, suelen ser dispositivos peligrosos. Por lo tanto, todos los dispositivos que se encuentran ilustrados son de carácter peligrosos.

Conexión juego-jugador

El juego en equipos motivará a cada alumno a competir entre sí. Los motivará a realizar la tarea de búsqueda con certeza y juicio al decidir si algo es vulnerable o no.

Jugadores

- Perfil razonamiento veloz: Son aquellos jugadores que tienden a reconocer rápidamente si algo les es vulnerable o no basados en sus experiencias.

- Perfil razonamiento lento: Son aquellos jugadores que tienen a tomar más tiempo en decidir si algo es vulnerable o no, pero enfocados en tomar el tiempo necesario para identificar lo más favorable.

Motivación

El factor clave de este ejercicio es el buscar el asertividad en las respuestas. Los participantes buscarán las respuestas en sus propias experiencias, lo cual demostrará que tan experimentados en la materia son.

Promover el aprendizaje

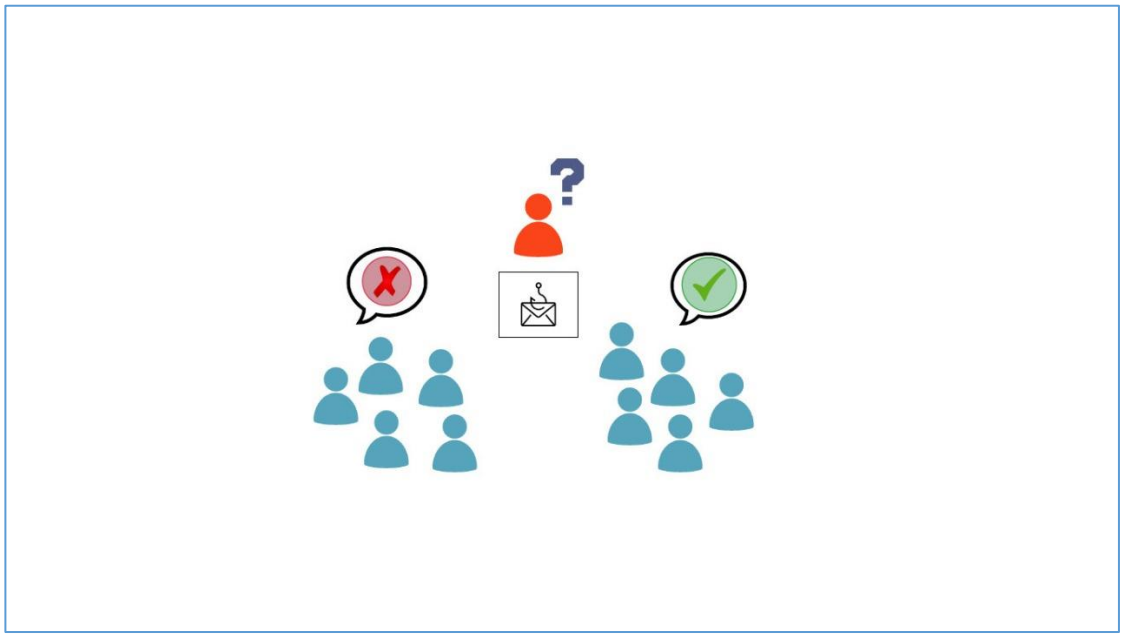
Como objetivo del juego es permitir a los participantes reflexionar e interpretar sus experiencias con dispositivos USB.

Resolución de problemas

Como la premisa es que todos los dispositivos son vulnerables, los participantes tienen que reconocer que los peligros existen en su día a día. Podrán tomar sus precauciones al adquirir algún dispositivo de esta índole.

Actividad #5: Reto de Phishing

Figura 4.7. *Esquema de la Actividad Reto de Phishing*



Fuente: Autores de la Tesis.

Elaboración: Autores de la Tesis.

Base del juego

El desarrollo de esta actividad requiere los siguientes elementos:

- Un tutor
- 10 participantes.
- Tarjetas con ejemplos de phishing.
- Tiza para pizarra o plumón para pizarra acrílica.
- Un pizarrón (tiza o pizarra)
- 20 pegatinas de logro.

Mecánica

Formados en grupos de 5, el tutor pasará a mezclar las tarjetas, dejando la explicación y respuesta de cada una de estas al lado que sólo él mira. El tutor presentará la otra casa al grupo participante y ellos deben decidir en 30 segundos si el ejemplo es de phishing o no. Si aciertan, pasan a la siguiente tarjeta; caso contrario, pierden una vida y pasan a la siguiente tarjeta. Si se les acaban las vidas (3 por equipo), pierden el juego.

Existe una posibilidad de usar pistas, una pista por tarjeta, esta brinda información adicional que no se visualiza a simple vista.

Estética

Se emplearán pegatinas de logros para aquellas personas que participen y ganen el desafío.

Idea del juego

En el ejercicio, los participantes identificarán los puntos vulnerables en la información que ellos reciben en correos. Además, les permitirá acostumbrarse a reconocer factores de peligro en cualquier notificación que reciban.

Conexión juego-jugador

El juego en equipos motivará a cada grupo a competir entre sí. Los motivará a realizar la tarea de búsqueda con velocidad y rápidamente decidir si algo es favorable o no para su equipo.

Jugadores

- Perfil experimentado: Son aquellos jugadores que tienen cierto nivel de conocimiento sobre el tópico, y dependiendo del ejercicio pueden aportar con valor o esperar otros estén al nivel de su conocimiento.
- Perfil novato: Son aquellos jugadores que no tienen conocimiento en el tema, son los más dispuestos a aprender y a escuchar lo que otros puedan ofrecer. En algunos casos, existen aquellos que consultan más ante cualquier duda.

Motivación

El factor clave de este ejercicio es la competitividad abierta, dándoles espacio a los más activos y pensadores, a proponer sus ideas de forma veloz y asertiva.

Promover el aprendizaje

El objetivo del ejercicio es que puedan lograr identificar los puntos riesgosos de un correo electrónico o algún mensaje dirigido a obtener nuestra información. Con la práctica podrán identificar los factores que más ocurren, y con la reflexión al final, el grupo podrá comparar con el tutor en clase que puntos les hicieron falta.

Resolución de problemas

Lo importante del ejercicio es tratar de filtrar rápidamente las respuestas que son obvias y mantenerse el mayor tiempo posible vivo. Esto les ayudará a ver más ejemplos de phishing con lo cual van a estar más prevenidos en sus vidas.

Al finalizar cada actividad, el tutor dará una reflexión sobre que aprendieron, compartiendo con ellos una conversación abierta y resolviendo las dudas que pudieron haber quedado en el aire.

Al terminar el temario, se les pedirá participen de un cuestionario utilizando una herramienta lúdica Kahoot!. El objetivo de esta herramienta es presentar el mismo cuestionario que el grupo de control, pero permitiéndoles ser evaluados de forma competitiva. Los resultados son presentados durante el cuestionario para motivar a cada alumno a responder rápido y asertivamente.

CAPITULO V: ANÁLISIS DE RESULTADOS

Con el fin de lograr los objetivos de esta investigación, a continuación, se presenta la información obtenida.

5.1. Estado de los programas de entrenamiento en Ciberseguridad actuales.

La investigación ha sido enfocada en Lima Metropolitana, y basada en las visitas y acercamiento con las tres (03) empresas que forman parte del grupo de estudio. Por motivos de confidencialidad no es posible indicar el nombre de dichas empresas, pero estas pertenecen al sector retail y se encuentran categorizadas como pequeñas y medianas empresas.

Se utilizó el modelo propuesto por el Instituto SANS para evaluar preliminarmente la madurez de los programas. De acuerdo con la información recopilada, en dichas empresas se identificó lo siguiente:

- El 100% de las empresas consultadas no cuentan con un plan debidamente formalizado donde se aborde el alcance del programa de entrenamiento en ciberseguridad, los principales riesgos humanos que deben gestionarse, los comportamientos para gestionar esos riesgos y la forma más eficaz de comunicar dichos comportamientos.

- En el 100% de las empresas consultadas, la frecuencia de ejecución de entrenamientos en ciberseguridad es 1 vez por año.

- En el 100% de las empresas consultadas, se encontró que hay mínimo involucramiento de la alta gerencia.

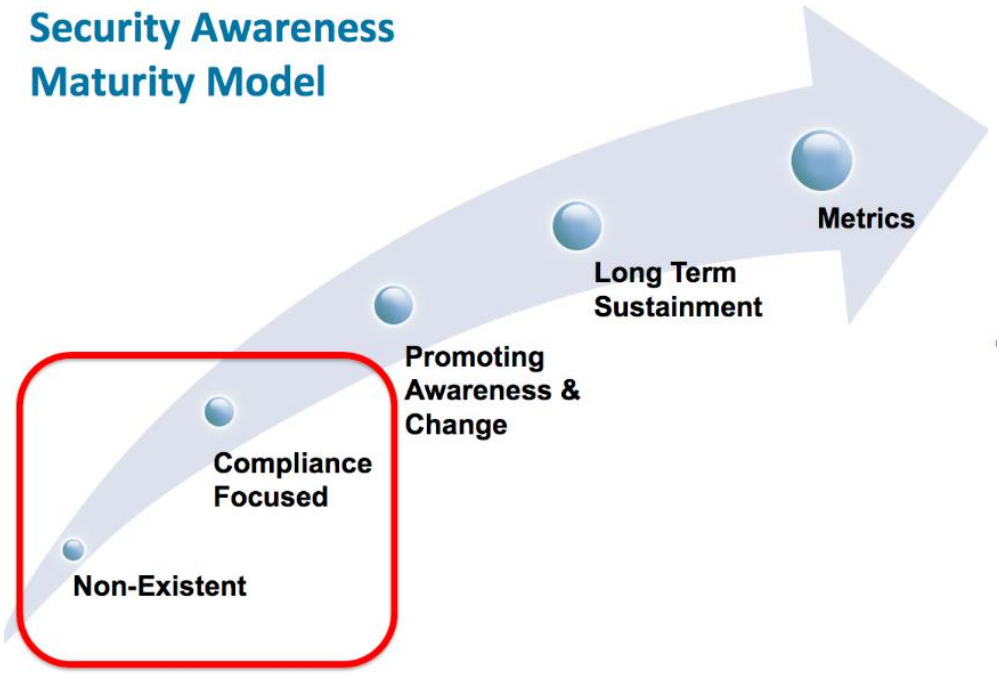
- Los programas de entrenamiento en ciberseguridad son realizados para cumplir con auditorías en algunos casos (66.66%), el resto (33.34%) no aplica al no estar regulado/sujeto a auditoria.

- En el 100% de las empresas consultadas, la alta gerencia cree que ciberseguridad es un problema técnico.

Por lo antes expuesto, preliminarmente podemos ubicar a las empresas objetos de estudio dentro del nivel de madurez "2 - Compliance Focused" acorde al "Security Awareness Maturity Model", el cual va del uno (1) al cinco (5). Un análisis especializado podría proporcionar el nivel de madurez real.

Es importante destacar que, en el estudio "2018 SANS Security Awareness Report" realizando por SANS Institute en base a respuestas de más de 1,700 profesionales especialistas en programas de concientización a nivel global (65 países) nos muestra que solo el 23% de los programas de concientización de los participantes se encuentran en el nivel de madurez "2 - Compliance Focused" y la gran mayoría, 53%, se encuentran en el nivel de madurez "3 - Promoting Awareness & Behavior Change", lo cual nos da un indicador que en nuestra realidad aún tenemos gran trabajo que realizar.

Figura 5.1. *Niveles de Madurez según el SANS Security Awareness Maturity Model*



Fuente: SANS Institute, 2018.

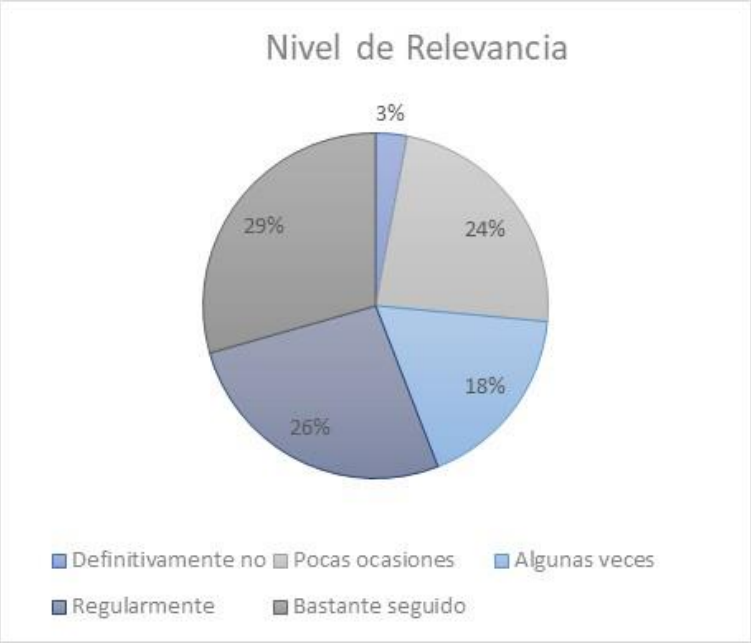
Elaboración: SANS Institute.

5.2. Resultados de Nivel 1

Para la obtención de los datos del Nivel 1, se utilizó un cuestionario de retrospección aplicado al final del entrenamiento (Anexo C). Los resultados son los siguientes:

Nivel de relevancia: A la pregunta ¿Con que frecuencia vas a aplicar lo aprendido en tu día a día?, la cual captura información si los participantes podrán utilizar lo aprendido en su trabajo diario, la Ilustración 10 muestra que el uso de lo aprendido se podría dar regularmente o bastante seguido por el (54%) de los participantes, por tanto, el nivel de relevancia es MEDIO.

Figura 5.2. *Resultados de Evaluación del Nivel de Relevancia*

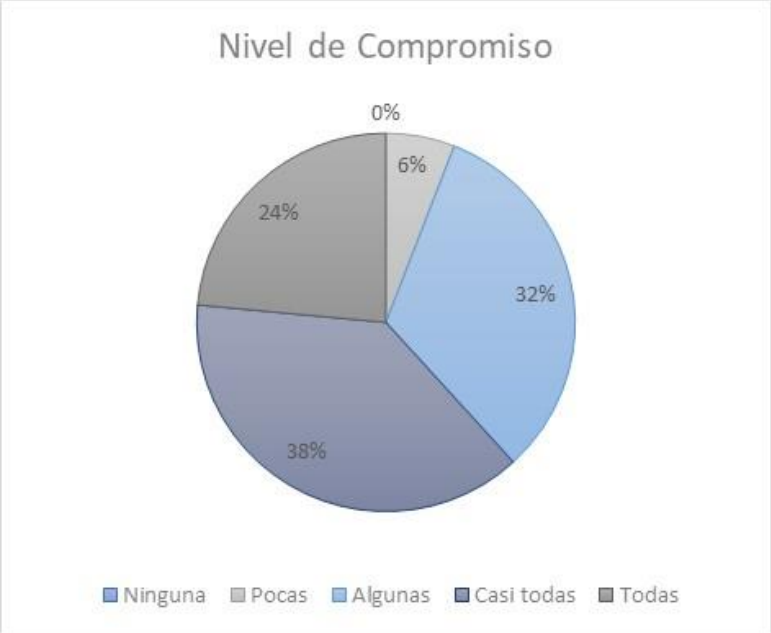


Fuente: Datos recolectados.

Elaboración: Autores de la tesis.

Nivel de Compromiso: A la pregunta ¿En cuántas actividades participaste activamente (colaboraste con ideas, conceptos, consultas, etc.)? la cual captura información si los participantes participaron activamente en las actividades durante el entrenamiento, la Ilustración 11 muestra que el (62%) de los participantes participó activamente en casi todas o todas las actividades, por tanto, el nivel de compromiso fue ALTO.

Figura 5.3. *Resultados de Evaluación del Nivel de Compromiso*



Fuente: Datos recolectados.

Elaboración: Autores de la tesis.

Nivel de Satisfacción: A la pregunta ¿Cuéntanos cuanto te gusto el entrenamiento? la cual captura información sobre la satisfacción de los participantes con el entrenamiento, la Ilustración 12 muestra que el (68%) de los participantes indicó que le pareció bien o le encantó el entrenamiento, por tanto, el nivel de satisfacción fue ALTO.

Figura 5.4. *Resultados de Evaluación del Nivel de Satisfacción*

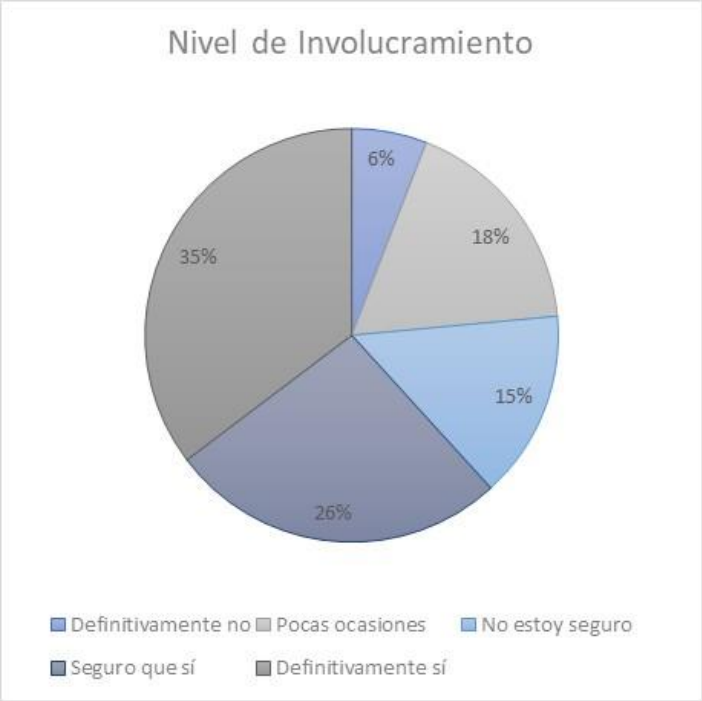
Fuente: Datos recolectados. Elaboración:
Elaboración: Autores de la tesis.

5.3. Resultados de Nivel 2

Para la obtención de los datos del Nivel 2, se utilizó el cuestionario antes aplicado y un cuestionario de conocimientos (Anexo E). Los resultados son los siguientes:

Nivel de Involucramiento: Está referida a la pregunta "¿Vas a aplicar lo aprendido?", la cual captura información sobre la intención de aplicar lo aprendido en el futuro. La Ilustración 13 muestra que el (62%) de los participantes considera que si o definitivamente si, por tanto, el nivel de involucramiento es ALTO.

Figura 5.5. *Resultados de Evaluación del Nivel de Involucramiento*

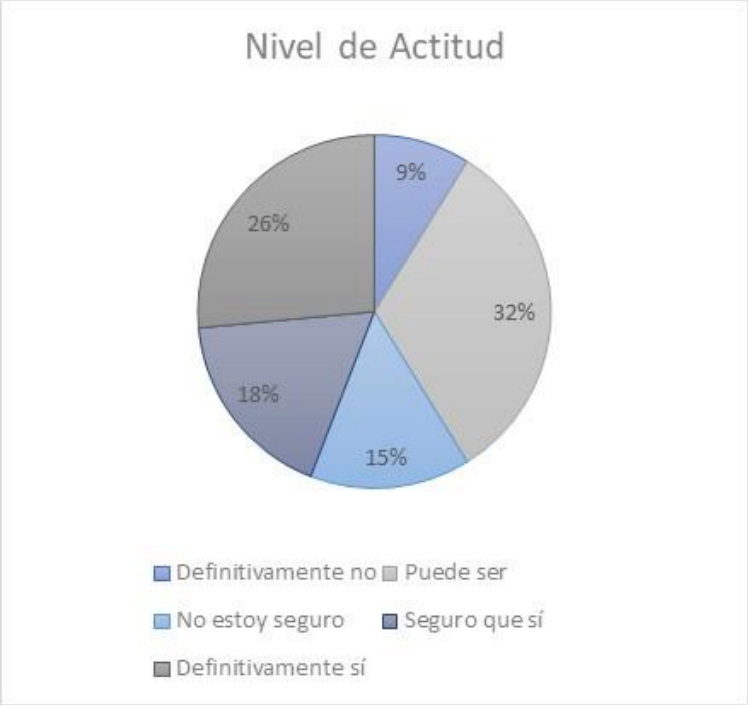


Fuente: Datos recolectados.

Elaboración: Autores de la tesis.

Nivel de actitud: Está referida a la pregunta "¿Consideras que lo aprendido será valioso en tu trabajo diario?", la cual captura información sobre si consideran lo aprendido valioso para su trabajo. La Ilustración 14 muestra que el (44%) de los participantes considera que si o definitivamente si, por tanto, el nivel de actitud es MEDIA.

Figura 5.6. *Resultados de Evaluación del Nivel de Actitud*



Fuente: Datos recolectados.

Elaboración: Autores de la tesis.

Nivel de confianza: Está referida a la pregunta "¿Crees que podrás realizar lo aprendido en caso te suceda?", la cual captura información sobre si llegado el momento serán capaces de ejecutar lo aprendido. La Ilustración 15 muestra que el (68%) de los participantes considera que si o definitivamente si, por tanto, el nivel de confianza es ALTO.

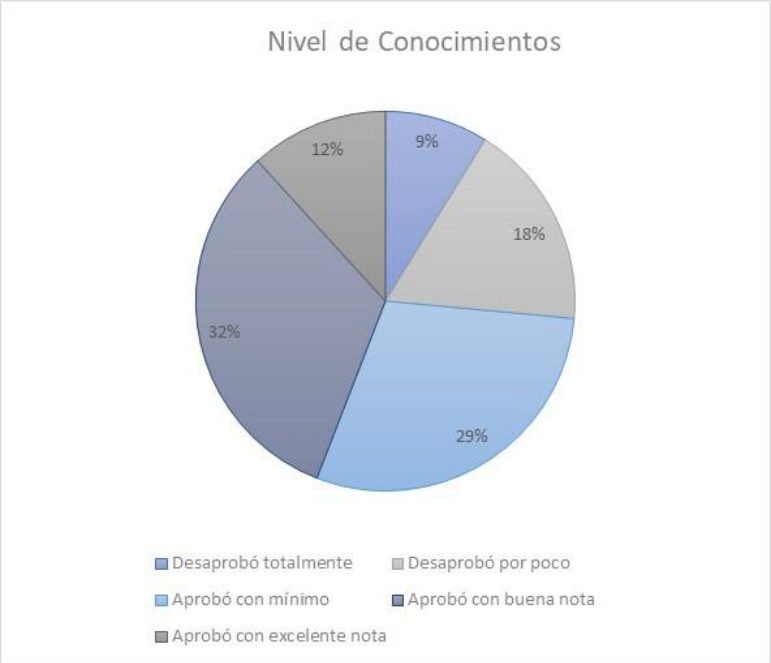
Figura 5.7. *Resultados de Evaluación del Nivel de Confianza*

Fuente: Datos recolectados.

Elaboración: Autores de la tesis.

Nivel de conocimientos: Está referida a las preguntas del 1 al 5 en el cuestionario de evaluación entregado a los participantes, donde se evalúa que los participantes conocen los términos explicados durante el entrenamiento. La Ilustración 16 muestra que el (74%) de los participantes APROBÓ, por tanto, el nivel de conocimientos es ALTO.

Figura 5.8. Resultados de Evaluación del Nivel de Conocimientos



Fuente: Datos recolectados.

Elaboración: Autores de la tesis.

Nivel de habilidades: Está referida a las preguntas del 6 al 10 en el cuestionario de evaluación entregado a los participantes, donde se evalúa que los participantes saben cómo ejecutar una tarea o acción. La Ilustración 17 muestra que el (65%) de los participantes APROBÓ, por tanto, el nivel de conocimientos es ALTO.

Figura 5.9. Resultados de Evaluación del Nivel de Aprendizaje

Fuente: Datos recolectados.

Elaboración: Autores de la tesis.

CAPITULO VI: DISCUSIÓN

Para verificar que la efectividad del entrenamiento propuesto, debemos primero mirar que eventos causan un impacto en la efectividad para determinar si fue alta o no. Basados en el modelo de Kirkpatrick, tenemos un conjunto de variables que pertenecen a los dos primeros niveles, los correspondientes a medir la efectividad. Estos niveles nos permitirán evaluar la efectividad mediante la medición de la reacción y el aprendizaje de los participantes.

En base a Kirkpatrick, el nivel de reacción es directamente proporcional a su nivel de compromiso, nivel de relevancia y nivel de satisfacción en base al curso dictado. En base al análisis obtenido hemos identificado que los elementos de nuestra muestra presentan un MEDIO nivel de relevancia (54%), un ALTO nivel de compromiso (62%) y un ALTO nivel de satisfacción (68%). Con lo que podemos identificar que el nivel de reacción (61%) obtenido es ALTO.

De igual manera, el nivel de aprendizaje descrito por el modelo de Kirkpatrick es directamente proporcional a los niveles de conocimiento, habilidades, actitudes, confianza e involucramiento que presente el participante de la muestra. En los resultados obtenidos hemos observado un nivel de conocimiento (74%) ALTO, un nivel de habilidades (65%) ALTO, un nivel de actitudes (44%) MEDIO, un nivel de confianza (68%) ALTO, y un nivel de involucramiento (62%) ALTO. Con lo que podemos identificar que el nivel de aprendizaje (63%) obtenido es ALTO.

Como consecuencia de lo expuesto tenemos como resultado que la efectividad obtenida es relacional al nivel de reacción (61%) y al nivel de aprendizaje (63%). Esto nos da un resultado de nivel ALTO (62%).

Si bien podemos concluir que la muestra comprueba la hipótesis de la presente, también tenemos que aclarar que la muestra fue limitada a las empresas de tres rubros diferentes, con tres poblaciones diferentes. Y si bien la edad y el género no son factores determinantes para la distinción de la población, la educación y experiencia en el tema si son factores que influyen con relación a conocimiento. Además, la pre-disponibilidad de los participantes influye indirectamente en la relación de los valores. El modelo de

Kirkpatrick es un modelo que nos orienta a identificar los elementos que evaluar. Pero la final depende de las muestras realizadas y el universo escalable que deseamos verificar.

Sin embargo, lo que hemos comprobado aquí es que, si bien los resultados tienen una relevancia alta, los elementos lúdicos aplicados a cursos de ciberseguridad suelen ser favorables para el entendimiento de los conceptos y el ejercicio de las actividades refuerza las habilidades de los participantes para que realmente impacte en sus futuros favorablemente.

CAPITULO VII: CONCLUSIONES Y RECOMENDACIONES

A continuación, se muestran las conclusiones y recomendaciones obtenidas a lo largo de la presente investigación.

7.1. Conclusiones

- Se estableció el estado de los programas de entrenamiento en ciberseguridad usados por las empresas objeto de estudio, utilizando el modelo "Security Awareness Maturity Model" del SANS Institute. Los resultados obtenidos muestran a las empresas estudiadas dentro del nivel 2, el cual por definición está enfocado en cumplir con las regulaciones.

- Se identificaron 5 tópicos en ciberseguridad relevantes para los entrenamientos basados en estudios de reputadas instituciones a nivel mundial, los cuales fueron: cómo evitar archivos maliciosos, cómo evitar enlaces maliciosos, como proteger contraseñas, seguridad en el uso de dispositivos USB y precauciones contra el phishing dirigido.

- Se identificaron los componentes de ludificación más idóneos para la creación de los escenarios de entrenamiento en ciberseguridad basado en lo expuesto por Kapp (2012), los cuales fueron la base de juego, mecánica, estética, idea de juego, conexión juego-jugador, jugadores, motivación y la promoción del aprendizaje.

- Se evaluó la efectividad del programa de capacitación propuesto, basándose en los 2 primeros niveles modelo propuesto por Kirkpatrick (2016). Los resultados obtenidos muestran que el entrenamiento propuesto tiene una efectividad ALTA en una escala de 5 niveles.

- Reafirmamos lo expresando preliminarmente en la sección de "1.4 Justificación" del presente documento, en donde indicamos la importancia de incluir entrenamientos en tópicos de ciberseguridad como parte de un plan de mitigación de ciber riesgos, independientemente al sector al que pertenezcan y los controles de seguridad que pudiesen tener.

7.2. Recomendaciones

- Dadas las restricciones sobre las cuales se elaboró esta investigación, se recomienda a otros investigadores aplicar el entrenamiento con una muestra probabilística, de manera que el número de participantes sea estadísticamente representativo.

- Para futuros estudios, se recomienda incluir otros tópicos como por ejemplo uso inadecuado de privilegios o seguridad física debido a que tienen relación con las técnicas de ataque más utilizadas después de las seleccionadas para este estudio.

- Asimismo, debido a que en la presente tesis solo se han desarrollado cinco tópicos de ciberseguridad, a continuación se recomiendan los siguientes tópicos que toda organización debe considerar como mínimo al entrenar a sus colaboradores:
    1. ¿Cómo evitar archivos adjuntos maliciosos?
    2. ¿Cómo evitar enlaces maliciosos?
    3. ¿Cómo proteger tus contraseñas?
    4. Dispositivos USB seguros
    5. Precauciones contra el Phishing dirigido
    6. ¿Cómo proteger tu información personal?
    7. ¿Cómo destruir tu información de forma segura?
    8. ¿Qué es la ingeniería social y como evitar ser víctima de ella?
    9. Consejos para mantener tu ambiente de trabajo seguro
    10. ¿Por qué es importante mantener escritorios limpios?
    11. ¿Cómo mantener tu dispositivo móvil seguro?
    12. ¿Por qué no debo compartir mis contraseñas?
    13. Consejos para hacer uso de internet y redes sociales de forma segura
    14. ¿Qué debo hacer si identifico un incidente de seguridad?
    15. Consejos básicos para no ser víctima del Ransomware

Para la enseñanza de estos tópicos de Ciberseguridad se pueden emplear las siguientes tecnologías.

- Java, lenguaje de programación multipropósito y robusto que permitirá el desarrollo de apps que funcionen en Android. Teniendo en cuenta que el sistema operativo que más se utiliza en celulares es Android conviene desarrollar aplicaciones en este entorno. De esta manera las personas podrán acceder al entrenamiento desde cualquier parte y podrán consultar los temas del entrenamiento de acuerdo a su ritmo. Pudiendo complementar su formación con varios niveles de acuerdo al nivel del participante. La inclusión de videos, cuestionarios interactivos, textos relevantes y elementos de gamificación significarían una propuesta interesante y prometedora.

- Haciendo uso de la realidad aumentada se podrán desarrollar módulos de entrenamiento que capturen completamente la atención del participante. De esta manera se puede llevar el entrenamiento a un nivel de interacción complemente distinto al tradicional. Se incentivaría la motivación y el nivel de atención del participante al poder llevar a cabo un impacto fuerte y positivo en las personas. Además, permitiría que las personas asocien y asimilen mejor los conceptos al llevar la teoría en un contexto que le sea más familiar.

- Haciendo uso de HTML5, Boostrap y hojas de estilo, se podrían desarrollar interesantes sitios Web que permitan a las empresas brindar capacitaciones en Ciberseguridad a sus empleados. Estas tecnologías, permitirán que estos sitios Web se logren visualizar de manera apropiada en una gran diversidad de dispositivos. De igual manera permiten que se desarrollen sitios web con un alto contenido visual que permitirá enriquecer el entrenamiento que reciban los colaboradores de la empresa.

ANEXOS

I. Cuestionario de evaluación psicológica y predisposición a curso lúdico

1.	**Nombre**					
2.	**Edad**	18 - 40			41 - 60+	
3.	**Genero**	Mujer			Hombre	
4.	**¿A qué te dedicas?**					
5.	**¿Has llevado algún curso en Ciberseguridad?**					
		Sí				
		No				
6.	**¿Has participado de actividades no deportivas en grupo?**					
		Sí				
		No				
7.	**¿Hace cuánto has participado de una capacitación?**					
		Menos de 1 mes				
		Menos de 6 meses				
		Menos de 1 año				
		Más de 1 año				
8.	**¿Has conocido sobre ciberataques o vulnerabilidades en la oficina?**					
		Sí				
		No				
9.	**¿Te mantienes informado sobre temas de Seguridad en la Oficina?**					
		Sí				
		No				

II. Entrenamiento básico de ciberseguridad aplicado a empresas

DATOS DE LOS DOCENTES

Profesor: Diego Alfredo Yañez Herrera
Correo electrónico: 1705344@esan.edu.pe

Profesor: Jorge Luis Mendoza Pasco
Correo electrónico: 1702262@esan.edu.pe

Profesor: Juan Carlos Mendoza Blanco
Correo electrónico: 1704679@esan.edu.pe

Profesor: Daniel Fernando Doig Diaz
Correo electrónico: 150615@esan.edu.pe

I. SUMILLA

La asignatura tiene el propósito de desarrollar habilidades de reconocimiento y prevención contra ciberamenazas como archivos adjuntos maliciosos, enlaces peligrosos, contraseñas inseguras, dispositivos de almacenamiento removibles infectados y phishing dirigido.

Durante el curso los participantes aprenderán sobre los ciber riesgos que estas ciberamenazas representan para su compañía, además de participar en ejercicios didácticos que refuercen estos conocimientos para contribuir a prevenir estas amenazas.
Este curso abarca cinco (05) temas: 1. ¿Cómo evitar archivos adjuntos maliciosos?, 2. ¿Cómo evitar enlaces maliciosos?, 3. ¿Cómo proteger tus contraseñas?, 4. Dispositivos USB seguros, y 5. Precauciones contra el Phishing dirigido.

II. OBJETIVO DE LA ASIGNATURA

Al final del curso, los participantes podrán reconocer las ciberamenazas básicos para la ciberseguridad de la compañía donde laboran y permitiéndoles reaccionar adecuadamente ante una ciberamenaza.

III. PROGRAMACIÓN DE CONTENIDOS

Tema 1: ¿Cómo evitar archivos adjuntos maliciosos? (15 Minutos)

Resultados esperados:
Al finalizar este tema, el participante podrá analizar los correos electrónicos y sus adjuntos de manera crítica para reconocer efectivamente el origen de estos y reaccionar de forma adecuada ante una ciberamenaza.

Tema 2: ¿Cómo evitar los enlaces maliciosos? (15 Minutos)

Resultados esperados:

Al finalizar la unidad de aprendizaje, el participante podrá analizar los enlaces a direcciones web de manera crítica para reconocer efectivamente si se trata de una ciberamenaza en los enlaces y tomar acciones preventivas.

Tema 3: ¿Cómo proteger tus contraseñas? (15 Minutos)

Resultados esperados:
Al finalizar la unidad de aprendizaje, el participante será capaz de hacer uso de técnicas y herramientas para la creación y respaldo de contraseñas de forma segura.

Tema 4: Dispositivos USB seguros (15 Minutos)

Resultados esperados:
Al finalizar la unidad de aprendizaje, el participante será capaz de utilizar los dispositivos de almacenamiento USB con los que trabaja con seguridad, y también a mitigar los ciber riesgos propios de su uso.

Tema 5: Precauciones contra el Phishing dirigido (15 Minutos)

Resultados esperados:
Al finalizar la unidad de aprendizaje, el participante será capaz de analizar críticamente el contenido de correos electrónicos sospechosos y tomar las acciones pertinentes ante la presencia de uno de estos casos.

IV. METODOLOGÍA

El curso tendrá como insumos la exposición del profesor del curso, la participación en las actividades y discusiones sobre los tópicos.

Los elementos de aprendizaje a emplearse son:

- Exposiciones del profesor del curso.
- Las actividades en clase.
- Las discusiones en grupo.

Al finalizar el curso, los participantes deberán tomar una evaluación de conocimientos sobre los temas expuestos en clase.
Para el buen desarrollo y aprovechamiento de las clases, se requiere la presencia puntual de los participantes y no se permite el uso de teléfonos celulares durante las sesiones.

V. EVALUACIÓN

La nota final del curso se obtendrá del siguiente aspecto:

- Examen final (100%)
  Esta calificación corresponde a la resolución de un cuestionario de preguntas utilizando los conocimientos adquiridos durante el curso.

VI. FUENTES DE INFORMACIÓN

- 2018 SANS Security Awareness Report. Building Successful Security Awareness Programs. Recuperado de https://www.sans.org/security-awareness-training/reports/2018-security-awareness-report

- Best Practices for Dealing With Phishing and Ransomware (2016). An Osterman Research White Paper. Recuperado de https://www.domaintools.com/resources/white-papers/best-practices-for-dealing-with-phishing-and-ransomware

- Building an Information Technology Security Awareness and Training Program (2003). National Institute of Standards and Technology (NIST) Special Publication 800-50. Recuperado de https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-50.pdf

- Social Engineering (Phishing) Assessment Report (2016). Rhino Security Labs. Recuperado de https://rhinosecuritylabs.com/landing/social-engineering-assessment-report/

- 2017 Security Awareness Report. SANS Security Awareness. Recuperado de https://www.sans.org/security-awareness-training/blog/2017-security-awareness-report

- Spitzner L. Top Human Risks. Securing The Human. Recuperado de https://www.sans.org/sites/default/files/2018-01/STH-TopSevenHumanRisks.pdf

- Spitzner L. Human Metrics: Measuring Behavior. Securing The Human. Recuperado de http://www.itpss.com/pdf/STH-Presentation-HumanMetrics.pdf

- Secrets to an Effective Phishing Program. Securing The Human. Recuperado de https://www.sans.org/sites/default/files/2017-12/STH-Presentation-PhishingYourEmployees.pdf

III. Cuestionario de retrospección

Con el objetivo de obtener información de mejora continua para el curso y los temarios presentados, la opinión de los alumnos es necesaria. Para dicho objetivo se presentará a los tres días de haber culminado el curso el siguiente cuestionario de opinión sobre lo dictado.

1	¿Puedes aplicar lo aprendido en tu día a día?				
	0-No creo	1-Pocas ocasiones	2-Algunas veces	3-Regularmente	4-Bastante seguido
2	¿En cuántas actividades participaste activamente (colaboraste con ideas, conceptos, consultas, etc.)?				
	0-Ninguna	1-Pocas	2-Algunas	3-Casi todas	4-Todas
3	¿Cuéntanos cuanto te gusto el entrenamiento?				
	0-Definitivamente no	1-No me gusto	2-No opino	3-Me parecieron bien	4-Me encantaron
4	¿Con qué frecuencia vas a aplicar lo aprendido en tu día a día?				
	0-No creo	1-Pocas ocasiones	2-Algunas veces	3-Regularmente	4-Bastante seguido
5	¿Consideras que lo aprendido será valioso en tu trabajo diario?				
	0-No creo	1-Puede ser	2-No opino	3-Ocasionalmente	4-De seguro
6	¿Crees que podrás realizar lo aprendido en caso te suceda?				
	0-No creo	1- Pocas ocasiones	2- Algunas veces	3-Regularmente	4- Bastante seguido

IV. Cuestionario para encargados de Ciberseguridad

Con el objetivo de realizar un diagnóstico a alto nivel de los métodos o programas de entrenamiento en ciberseguridad utilizados actualmente por las empresas que forman parte del estudio. Asimismo, lograr clasificar preliminarmente su programa o método de entrenamiento según el modelo de madurez de concientización de seguridad ("Security Awareness Maturity Model") de SANS Institute, la opinión de los responsables del equipo de Ciberseguridad es necesaria. Para dicho objetivo se le realizará el presente cuestionario al responsable del equipo de Ciberseguridad.

1	¿Cuentan con un Plan Estratégico de Seguridad de la información donde se incluye la definición de los tópicos a trabajar y la frecuencia de despliegue?				
	1-Sí	2-No			
2	¿Con qué frecuencia ejecutan el entrenamiento en tópicos de ciberseguridad?				
	1- Mensualmente	2- Trimestralmente	3- Semestralmente	4- Anualmente	5- Bianual
3	¿Cuál es el nivel de involucramiento de la alta gerencia en el programa de concientización?				
	1-No hay involucramiento	2-Mínimo	3-Regular	4- Involucrado	5-Muy involucrado
4	¿El programa es realizado únicamente para cumplir con regulaciones/auditorias?				
	1-Sí	2-No	3- No Aplica		
5	¿La ejecución del programa es tarea de tiempo parcial de una única persona?				
	1-Sí	2-No			
6	¿Existe participación de otras unidades?				
	1-No hay participación	2-Poca participación	3-Participación Regular	4-Existe participación	5-Alta participación
7	¿La alta gerencia cree que la seguridad es un problema meramente técnico?				
	1-Sí	2-No			

V. Evaluación de conocimiento y habilidades

Con el objetivo de calificar el conocimiento obtenido por los participantes se presenta el siguiente cuestionario de preguntas, el cual cubre las bases explicadas en el material del curso dictado.

TEMA 1	**¿CÓMO EVITAR ARCHIVOS ADJUNTOS MALICIOSOS?**	**TIPO**
P.1.	**Recibes un correo electrónico inesperado de un compañero de trabajo con el cual no has tenido contacto en buen tiempo. En este correo te solicita ingreses a un enlace para que lo ayudes con una encuesta. ¿Qué acción realizarías?**	**Habilidad**
R.1.	Verificar con tu administrador de correo electrónico que se trate de un mensaje seguro.	
R.2.	Ingresar al enlace. Como se trata de un correo interno enviado por un compañero de trabajo, no necesitas preocuparte.	
R.3.	Llamar a tu compañero para confirmar si él envío dicho correo electrónico.	
R.4.	Responderle a tu compañero a través del correo electrónico consultándole sobre dicho mensaje enviado.	
P.2.	**¿Qué es lo primero que revisarías al recibir un correo electrónico?**	**Conocimiento**
R.1.	Destinatario y remitente.	
R.2.	Asunto y remitente.	
R.3.	Remitente, asunto, contenido y adjunto(s).	
R.4.	Remitente, adjunto(s) y destinatario.	
TEMA 2	**¿CÓMO EVITAR ENLACES MALICIOSOS?**	**TIPO**
P.1.	**¿Cuál es una buena práctica al abrir un enlace?**	**Conocimiento**
R.1.	Solo abrir los enlaces que envíen personas conocidas o de confianza.	
R.2.	Pasar el cursor por encima del enlace y leer la URL que aparece, pero sin hacer clic en él.	
R.3.	Abrir el enlace en un navegador en modo incognito.	
R.4.	Abrir el enlace en modo administrador.	
P.2.	**¿Cuál de las siguientes URLs se puede considerar segura?**	**Habilidad**
R.1.	http://photoscape.ch/Setup.exe	
R.2.	http://fourthgate.org/Yryzvt	
R.3.	www.studiolegaleabbruzzese.com/flight_4832.pdf	
R.4.	https://b2b.intercorpretail.pe	

TEMA 3	¿CÓMO PROTEGER TUS CONTRASEÑAS?	TIPO
P.1.	**¿Qué características debe tener una contraseña segura?**	**Conocimiento**
R.1.	Compuesta por caracteres numéricos y letras.	
R.2.	Compuesta por frases contraseña sencillas de recordar.	
R.3.	Compuesta por caracteres especiales.	
R.4.	Todas las respuestas anteriores son correctas.	
P.2.	**El área de Gestión Humana de tu empresa te solicita crear un usuario y contraseña para el portal de Evaluación de Desempeño. ¿Cuál sería el criterio principal para escoger la nueva contraseña?**	**Habilidad**
R.1.	Facilidad para recordar la contraseña.	
R.2.	Colocar la contraseña que permita la creación más rápida del nuevo usuario.	
R.3.	No hay ningún criterio que sea relevante para realizar esta actividad.	
R.4.	Colocar una contraseña que sea difícil de vulnerar por algún ciberataque.	
TEMA 4	**DISPOSITIVOS USB SEGUROS**	**TIPO**
P.1.	**¿Qué debes hacer si encuentras un USB en el suelo de tu trabajo?**	**Habilidad**
R.1.	Conectarlo para ver si con la información contenida en él puedo identificar al dueño para devolvérselo.	
R.2.	Utilizar el dispositivo USB para mi uso diario.	
R.3.	Darle el dispositivo USB a un compañero para que lo utilice.	
R.4.	Entregarlo inmediatamente al departamento de seguridad física de tu empresa.	
P.2.	**¿Cuál de estos no es un dispositivo USB?**	**Conocimiento**
R.1.	Mouse.	
R.2.	Teclado.	
R.3.	Dispositivos de almacenamiento.	
R.4.	Ninguna de las respuestas anteriores es correcta.	
TEMA 5	**PRECAUCIONES CONTRA EL PHISHING DIRIGIDO**	**TIPO**
P.1.	**¿Cómo identificarías un correo electrónico de Phishing dirigido?**	**Conocimiento**
R.1.	No conozco al remitente del correo electrónico.	
R.2.	La forma de dirigirse a ti es sospechosa.	
R.3.	Te envía adjuntos que no esperas.	
R.4.	Todas las respuestas anteriores son correctas.	
P.2.	**Te llega un mensaje de texto indicándote que el banco donde tienes tu cuenta sueldo necesita que**	**Habilidad**

	actualices unos datos de manera urgente. ¿Cuál debería ser la manera más sensata de reaccionar a esto?	
R.1.	Proporcionar los datos que se están solicitando cuanto antes.	
R.2.	Proporcionar solo los datos que consideras debería conocer el banco y no todos lo que se piden.	
R.3.	Tratar de comunicarte con el número que ha mandado el mensaje para obtener más información de porque se está solicitando estos datos.	
R.4.	Ignorar el mensaje.	

BIBLIOGRAFÍA

Gil, F. (2018). Ciberseguridad: El 70% del valor de una empresa puede ser afectado tras un ataque informático. Recuperado de https://gestion.pe/tecnologia/ciberseguridad-70-empresa-afectado-ataque-informatico-245430

SANS Institute (2018). 2018 SANS Security Awareness Report. Building Successful Security Awareness Programs. Recuperado de https://www.sans.org/security-awareness-training/reports/2018-security-awareness-report

Verizon (2018). 2018 Data Breach Investigations Report. 11th Edition. Verizon. Recuperado de https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf

Ernst & Young (2018-19). EY Global Information Security Survey 2018-19. Recuperado de https://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2018-19/$FILE/ey-global-information-security-survey-2018-19.pdf

Ponemon Institute (2018-19). 2018 Cost of a Data Breach Study: Global Overview. Recuperado de https://www.ibm.com/security/data-breach

IBM (2014). IBM Security Services 2014 Cyber Security Intelligence Index. Recuperado de https://media.scmagazine.com/documents/82/ibm_cyber_security_intelligenc_20450.pdf

Accenture (2017). Cost of Ciber Crime Study. Recuperado de https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf

Poblete, P., Marusic, M. (2018). Gerente general de Banco de Chile, Eduardo Ebensperger por ciberataque: "El evento fue destinado a dañar al banco, no a los clientes". Recuperado de https://www.latercera.com/pulso/noticia/gerente-general-banco-chile-eduardo-ebensperger-ciberataque-evento-fue-destinado-danar-al-banco-no-los-clientes/198912/

Iturrieta, F., Sherwood, D., Osterman, C. (2018). Bank of Chile trading down after hackers rob millions in cyberattack. Recuperado de https://www.reuters.com/article/us-chile-banks-cyberattack/bank-of-chile-trading-down-after-hackers-rob-millions-in-cyberattack-idUSKBN1J72FC

SANS Institute (2016). Security Spending Trends. Recuperado de https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697

Morgan, F. (2017). 2017 Cybercrime Report. https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf

Superintendencia Financiera de Colombia (2018). Instrucciones Generales Aplicables A Las Entidades Vigiladas. Recuperado de: https://www.supemaximrfinanciera.gov.co/descargas/institucional/pubFile1031729/ance007_18.docx

ESET (2016). 5 cosas que debes saber sobre la Ingeniería Social. Recuperado de https://www.welivesecurity.com/la-es/2016/01/06/5-cosas-sobre-ingenieria-social

Gallego, F.; Molina, F.; Llorens, F. (2014) Gamificar una propuesta docente. Diseñando experiencias positivas de aprendizaje. Recuperado de https://rua.ua.es/dspace/bitstream/10045/39195/1/Gamificacio%CC%81n%20(definicio%CC%81n).pdf

Kapp, K. (2012). The Gamification of Learning and Instruction: Game-Based Methods and Strategies for Training and Education. San Francisco: John Wiley & Sons.

Zichermann, G. y Cunningham, C. (2011). Gamification by Design: Implementing Game Mechanics in Web and Mobile Apps. Cambridge, MA: O'Reilly Media.

Hamari, J. y Koivisto, J. (2013). Social motivations to use gamification: an empirical study of gamifying exercise. En Proceedings of the 21st European Conference on Information Systems. Utrecht, Netherlands, June 5-8.

Green, J. (2015). Cyber Security: An Introduction for Non-Technical Managers. UK: Routledge.

Refsdal, A., Solhaug, B., Stølen, K. (2015). Cyber-risk Management. USA: Springer.

Kostopoulos, G. (2017). Cyberspace and Cybersecurity. USA: Auerbach Publications.

De la Corte, I., Blanco, J. (2014). Seguridad nacional, amenazas y respuestas. España: LID Editorial.

Fernández, J., Arias, D. (2017). Implementation of a gamification platform in a master degree (master in economics). WPOM-Working Papers on Operations Management, 8, 181-190.

Thornton, D., Trifas, M., Francia, I., Guillermo, Bowden, T. (2014). Gamification of information security awareness training. Emerging Trends in ICT Security, Page: 85-97.

Adams, M., Makramalla, M. (2015). Cybersecurity skills training: An attacker-centric gamified approach. Technology Innovation Management Review, 5(1), 5-14.

Kendrick, R. (2010). Cyber Risks for Business Professionals: A Management Guide. Reino Unido: IT Governance Publishing.

Skoudis, E., Zeltser, L. (2004). Malware: Fighting Malicious Code. New Jersey: Prentice Hall.

Ackerman, P. (2017). Industrial Cybersecurity: Efficiently secure critical infrastructure systems. Reino Unido: Packt Publishing Ltd.

Ozkaya, E., Aslaner, M. (2019). Hands-On Cybersecurity for Finance: Identify vulnerabilities and secure your financial services from security breaches. Reino Unido: Packt Publishing Ltd.

Niemelä, M. (2016). Anatomy of a cyberattack. New Jersey: BookBaby.

McGonigal, J. (2011). Reality Is Broken: Why Games Make Us Better and How They Can Change the World. New York: Penguin.

Gazabon, O., Alfredo, D., Villalobos Toro, B. I., De La Hoz Escorcia, S. M., Perez, M., Jovana, D. (2016). Gamificación para la gestión de la innovación a nivel organizacional. Una revisión del estado del arte. Espacios 37(8):2

Dicheva, D., Dichev, C., Agre, G., Angelova, G. (2015). Gamification in education: A systematic mapping study. Educational Technology & Society, 18(3), 75-88.

Boopathi, K., Sreejith, S., Bithin, A. (2015). Learning cyber security through gamification. Indian Journal of Science and Technology, 8(7), 642-649.

De Sousa Borges, S., Durelli, V.., Reis, H., Isotani, S. (2014). A systematic mapping on gamification applied to education. In Proceedings of the 29th annual ACM symposium on applied computing (pp. 216-222). ACM.

Fink, G., Best, D., Manz, D., Popovsky, V., Endicott-Popovsky, B. (2013). Gamification for measuring cyber security situational awareness. In International Conference on Augmented Cognition. Berlin: Springer.

Valda, F., Arteaga, C. (2015). Diseño e implementación de una estrategia de gamificacion en una plataforma virtual de educación. Fides et Ratio-Revista de Difusión cultural y científica de la Universidad La Salle en Bolivia, 9(9), 65-80.

Rivas, A., Delgado, L. (2016). Graduate XXI: Un mapa del futuro: Cincuenta innovaciones educativas en América Latina. Recuperado de https://publications.iadb.org/publications/spanish/document/Graduate-XXI-Un-mapa-del-futuro-Cincuenta-innovaciones-educativas-en-Am%C3%A9rica-Latina.pdf

Chicano, E. (2015). Gestión de incidentes de seguridad informática. IFCT0109. Málaga: IC Editorial.

Hernandez, R., Fernandez, C., Baptista, M. (2010). Metodología de la investigación Quinta Edición. Mexico: McGrawHill.

Kirkpatrick, J., Kirkpatrick, W. (2016). Kirkpatrick's Four Levels of Training Evaluation. Estados Unidos: Association for Talent Development.

SANS Institute (2018). Security Awareness Maturity Model / Kit. Recuperado de https://www.sans.org/security-awareness-training/blog/security-awareness-maturity-model-kit