



PROCESO DE GESTIÓN DE FORMACIÓN PROFESIONAL INTEGRAL

FORMATO GUÍA DE APRENDIZAJE

1. IDENTIFICACIÓN DE LA GUIA DE APRENDIZAJE

- Denominación del Programa de Formación: **DESARROLLO DE HABILIDADES DIGITALES PARA EXPERIENCIAS SEGURAS EN LINEA**
- Código del Programa de Formación: **23310013**
- Nombre del Proyecto Formativo (si aplica): **No aplica**
- Fase del Proyecto (si aplica): **No aplica**
- Actividad de Proyecto Formativo (si aplica): **No aplica**
- Competencia: **220501110 Implementar el sistema de seguridad de la información según modelo y estándares técnicos.**
- Resultados de Aprendizaje:
 - 220501110 - 01 Preparar las estrategias de ciberseguridad de acuerdo a los recursos Informáticos utilizados.
 - 220501110 - 02 Aplicar las estrategias de ciberseguridad conforme a los recursos y servicios digitales utilizados.
 - 220501110 - 03 Realizar un uso adecuado y responsable de los recursos tecnológicos para garantizar la integridad de la persona.
- Duración de la Guía de Aprendizaje (horas): **48**



2. PRESENTACIÓN

Bienvenido al curso Desarrollo de Habilidades Digitales para Experiencias Seguras en Línea, diseñado para fortalecer tus habilidades en la gestión segura de material y experiencias en contextos digitales. Aprenderás a aplicar medidas preventivas y mejores prácticas que te permitirán identificar y mitigar riesgos, proteger información sensible, y gestionar de manera segura las interacciones en línea, especialmente en videojuegos y entornos interactivos.

Este curso te anima a adoptar una actitud proactiva y organizada, aprovechando tus conocimientos previos para construir un aprendizaje significativo. Promoveremos el trabajo colaborativo para que, junto a tus compañeros, puedas compartir y ampliar tus conocimientos, creando un entorno de aprendizaje enriquecedor y seguro.

Tu participación activa te permitirá desarrollar políticas y procedimientos que garanticen la seguridad de la información compartida. ¡Prepárate para una aventura educativa que no solo fortalecerá tu conocimiento, sino que también te empoderará para ser un defensor activo de la seguridad en línea!

3. FORMULACIÓN DE LAS ACTIVIDADES DE APRENDIZAJE

- **Descripción de la(s) Actividad(es)**

En este curso, los aprendices realizarán tres actividades clave: crear un mapa mental sobre amenazas digitales en videojuegos y entornos interactivos, diseñar una infografía sobre herramientas y estrategias de protección digital, y desarrollar una presentación interactiva sobre riesgos y amenazas en nuevas tecnologías.

Utilizando herramientas digitales como MindMeister, Canva, Prezi, y otras, los aprendices visualizarán y explicarán diversas amenazas como el robo de identidad, phishing, delitos contra la propiedad intelectual, y ciberacoso, así como las medidas preventivas y estrategias de mitigación. Estas actividades promoverán el aprendizaje autónomo y colaborativo, fomentando la comprensión integral y práctica de la seguridad digital en entornos interactivos.



3.1 Actividades de reflexión inicial:

Descripción de la actividad:

Esta actividad inicial está diseñada para motivar y orientar a los aprendices en la importancia de implementar sistemas de seguridad de la información en los videojuegos y el metaverso, conforme a modelos y estándares técnicos reconocidos. La reflexión se centrará en cómo estas prácticas pueden mejorar la protección de datos y la seguridad de los usuarios en estos entornos digitales.

Pregunta de Reflexión

¿De qué manera crees que la implementación de un sistema de seguridad de la información, basado en modelos y estándares técnicos, puede mejorar la experiencia de los usuarios y la protección de datos en videojuegos y el metaverso?

Ambiente requerido: Plataformas Zajuna y Videoconferencia en (Google Meet).

Estrategias o técnicas didácticas activas:

- Discusión guiada en línea: Utilizar salas de reunión virtual para compartir ideas y experiencias sobre seguridad de la información.
- Trabajo en grupos virtuales: Dividir a los participantes en salas de reunión para analizar estándares de seguridad.
- Mapeo mental colaborativo en línea: Usar herramientas digitales como MindMeister o Coggle para crear un mapa mental sobre desafíos y soluciones.

Material de apoyo:

- 01 Ciberseguridad y seguridad de la información
- 02 Herramientas y estrategias de protección Digital
- 03 Riesgos o amenazas asociados al uso de las nuevas tecnologías

Duración de la actividad: 1 hora.



3.2 Actividades de contextualización e identificación de conocimientos necesarios para el aprendizaje:

Actividad 1 Presentación interactiva Riesgos y Amenazas en Nuevas Tecnologías para Videojuegos y Entornos Interactivos

Descripción de la actividad:

Los aprendices del curso de Tecnólogo en Desarrollo de Videojuegos y Entornos Interactivos deberán desarrollar y compartir una presentación interactiva con el título: “Riesgos y Amenazas en Nuevas Tecnologías para Videojuegos y Entornos Interactivos”. La presentación debe abordar cinco puntos clave:

- Riesgos o Amenazas Asociados a los Videojuegos
- Posibles Fraudes en el Metaverso o en Videojuegos
- Delitos contra la Propiedad Intelectual en Videojuegos
- Amenazas a la Privacidad
- Cyberbullying o Ciberacoso en Videojuegos en Línea
- Adicionalmente, los aprendices deben enfocarse en los delitos contra la propiedad intelectual y el cyberbullying/ciberacoso en las áreas de realidad virtual, aumentada y el metaverso.

Herramientas Sugeridas

- Genially: Para crear presentaciones interactivas y dinámicas.
- Prezi: Para presentaciones visualmente atractivas con efectos de zoom.
- Google Slides: Para presentaciones colaborativas con funciones de integración multimedia.
- Microsoft PowerPoint: Para presentaciones tradicionales con opciones interactivas avanzadas.

Ambiente requerido: Plataformas Zajuna y Videoconferencia en (Google Meet).

Estrategias o técnicas didácticas activas:

- Discusión Guiada en Línea
- Utilizar herramientas colaborativas (Google Slides, Microsoft Teams) para que los aprendices trabajen simultáneamente en la presentación, compartiendo ideas y recursos en tiempo real.
- Fomentar la discusión y retroalimentación continua dentro de los grupos y en sesiones plenarias.



- Utilizar funciones de las plataformas (por ejemplo, encuestas en Zoom o Genially) para obtener feedback inmediato de los compañeros.

Material de apoyo:

- 01 Ciberseguridad y seguridad de la información
- 02 Herramientas y estrategias de protección Digital
- 03 Riesgos o amenazas asociados al uso de las nuevas tecnologías

Duración de la actividad: 16 horas.

3.3 Actividades de apropiación:

Actividad 2 Mapa Mental sobre Amenazas Digitales en Videojuegos y Entornos Interactivos

Descripción de la actividad:

Los aprendices del curso de Tecnólogo en Desarrollo de Videojuegos y Entornos Interactivos deberán crear un mapa mental que visualice y explique las diferentes amenazas digitales que pueden afectar a los desarrolladores y usuarios de videojuegos y entornos interactivos. El mapa mental debe incluir las siguientes amenazas y características de seguridad en los videojuegos en línea:

- Spam
- Pharming
- Phishing
- Ransomware
- Spyware
- Malware
- Virus
- Características de Seguridad en los Videojuegos en Línea

Herramientas Sugeridas

- MindMeister: Para crear mapas mentales colaborativos y visualmente atractivos.
- Coggle: Para elaborar mapas mentales de manera simple y efectiva.
- XMind: Para mapas mentales con muchas opciones de personalización.
- Microsoft OneNote: Para integrar mapas mentales con otras notas y recursos.
- Lucidchart: Para mapas mentales y diagramas detallados y compartibles.

Ambiente requerido: Plataformas Zajuna y Videoconferencia en (Google Meet).



Material de apoyo:

- 01 Ciberseguridad y seguridad de la información
- 02 Herramientas y estrategias de protección Digital
- 03 Riesgos o amenazas asociados al uso de las nuevas tecnologías

Estrategias o técnicas didácticas activas:

- Discusión Guiada en Línea
- Utilizar herramientas colaborativas (Google Slides, Microsoft Teams) para que los aprendices trabajen simultáneamente en la presentación, compartiendo ideas y recursos en tiempo real.
- Fomentar la discusión y retroalimentación continua dentro de los grupos y en sesiones plenarias.
- Utilizar funciones de las plataformas (por ejemplo, encuestas en Zoom o Genially) para obtener feedback inmediato de los compañeros.

Instrumentos de evaluación: Observación Directa: Evaluar la participación activa y el uso de herramientas colaborativas durante la actividad

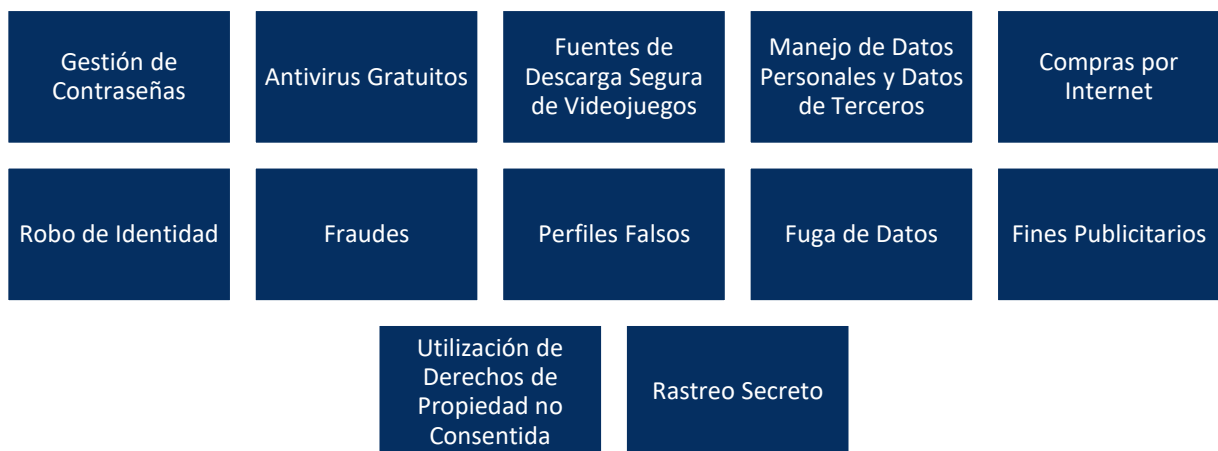
Duración de la actividad: 16 horas.

3.4 Actividades de Transferencia el Conocimiento:

Actividad 3 Juego Interactivo sobre Herramientas y Estrategias de Protección Digital en Videojuego

Descripción de la actividad:

Los aprendices del curso de Tecnólogo en Desarrollo de Videojuegos y Entornos Interactivos desarrollarán un juego interactivo que ayude a identificar y comprender diversas herramientas y estrategias de protección digital aplicables en los videojuegos. El juego deberá abordar los siguientes temas:





Herramientas Sugeridas

- WordWall: Una plataforma que permite crear juegos interactivos como cuestionarios, emparejamientos, y juegos de memoria de manera fácil y rápida.
- Educaplay: Una herramienta para diseñar actividades interactivas como crucigramas, sopas de letras, y cuestionarios que facilitan el aprendizaje.
- Educima: Una plataforma que ofrece diversas opciones para crear materiales educativos interactivos, como juegos de preguntas y respuestas, y actividades de arrastrar y soltar.

Ambiente requerido: Plataformas Zajuna y Videoconferencia en (Google Meet).

Material de apoyo:

- 01 Ciberseguridad y seguridad de la información
- 02 Herramientas y estrategias de protección Digital
- 03 Riesgos o amenazas asociados al uso de las nuevas tecnologías

Estrategias o técnicas didácticas activas:

- Discusión Guiada en Línea
- Utilizar herramientas colaborativas (Google Slides, Microsoft Teams) para que los aprendices trabajen simultáneamente en la presentación, compartiendo ideas y recursos en tiempo real.
- Fomentar la discusión y retroalimentación continua dentro de los grupos y en sesiones plenarias.
- Utilizar funciones de las plataformas (por ejemplo, encuestas en Zoom o Genially) para obtener feedback inmediato de los compañeros.

Instrumentos de evaluación: Observación Directa: Evaluar la participación activa y el uso de herramientas colaborativas durante la actividad

Duración de la actividad: 16 horas.



4. PLANTEAMIENTO DE EVIDENCIAS DE APRENDIZAJE PARA LA EVALUACIÓN EN EL PROCESO FORMATIVO.

Fase del proyecto formativo	Actividad del proyecto formativo	Actividad de Aprendizaje	Evidencias de Aprendizaje	Criterios de Evaluación	Técnicas e Instrumentos de Evaluación
N/A	N/A	N/A	<p>Actividad 1 Presentación interactiva Riesgos y Amenazas en Nuevas Tecnologías para Videojuegos y Entornos Interactivos</p> <p>Actividad 2 Mapa Mental sobre Amenazas Digitales en Videojuegos y Entornos Interactivos</p> <p>Actividad 3 Juego Interactivo sobre Herramientas y Estrategias de Protección Digital en Videojuego</p>	<p>220501110 - 01</p> <p>describe los conceptos y aplicación de la confidencialidad, integridad y disponibilidad en la protección y uso adecuado de la tecnología de acuerdo a la aplicación de la triada de la seguridad de la información.</p> <p>reconoce los riesgos informáticos y su impacto de acuerdo a los recursos tecnológicos utilizados.</p> <p>establece las estrategias de protección disponibles según el tipo de riesgo y recurso tecnológico utilizado.</p>	Observación Directa



				<p>determina la importancia de las redes sociales de acuerdo a su clasificación y uso.</p> <p>220501110 - 02</p> <p>describe las herramientas y técnicas de protección según los recursos y herramientas digitales utilizadas.</p> <p>elige las herramientas y estrategias de protección según los recursos tecnológicos usados.</p> <p>identifica los diferentes tipos de delitos informáticos de acuerdo a la legislación vigente.</p> <p>220501110 - 03</p> <p>identifica la exposición e</p>	
--	--	--	--	--	--



				<p>impacto ocasionados por el uso prolongado de tecnología de acuerdo a la clasificación de riesgos informáticos.</p> <p>establece los riesgos y sus consecuencias de acuerdo a la clasificación de enfermedades.</p>	
--	--	--	--	---	--

5. GLOSARIO DE TÉRMINOS

- Autenticación: Proceso de verificar la identidad de un usuario o sistema. Esto puede involucrar contraseñas, autenticación de dos factores (2FA), biometría, etc.
- Autorización: Proceso de otorgar a un usuario permiso para acceder a recursos o realizar acciones específicas en un sistema.
- Backdoor (Puerta Trasera): Método secreto para eludir las medidas normales de autenticación y obtener acceso no autorizado a un sistema.
- Botnet: Red de dispositivos infectados con malware, controlados de manera remota por un atacante para realizar actividades maliciosas como ataques DDoS.
- Cifrado: Proceso de convertir información legible en una forma codificada para protegerla de accesos no autorizados.
- CVE (Common Vulnerabilities and Exposures): Lista de vulnerabilidades de seguridad conocidas, mantenida por el MITRE Corporation.
- DDoS (Distributed Denial of Service): Ataque que intenta hacer que un servicio en línea no esté disponible, inundándolo con tráfico desde múltiples fuentes.



- Firewall (Cortafuegos): Dispositivo o software que controla el tráfico de red entrante y saliente basado en reglas de seguridad predeterminadas.
- Malware (Software Malicioso): Software diseñado para dañar, interrumpir o obtener acceso no autorizado a sistemas informáticos. Incluye virus, gusanos, troyanos, spyware, ransomware, etc.
- Phishing: Técnica de ingeniería social donde un atacante se hace pasar por una entidad confiable para engañar a las personas y hacer que revelen información sensible.
- Ransomware: Tipo de malware que cifra los archivos de la víctima y exige un rescate para proporcionar la clave de descifrado.
- Smishing: Variante del phishing que utiliza mensajes SMS para engañar a los usuarios y hacer que revelen información personal o descarguen malware.
- Spyware: Software que recopila información sobre una persona o entidad sin su conocimiento y la transmite a una entidad externa.
- SSL/TLS (Secure Sockets Layer/Transport Layer Security): Protocolos criptográficos diseñados para proporcionar comunicaciones seguras a través de una red, como Internet.
- Token: Dispositivo o pieza de software que proporciona una autenticación adicional más allá de la contraseña tradicional, utilizado comúnmente en sistemas de autenticación multifactor.
- Trojan (Troyano): Tipo de malware que se disfraza de software legítimo pero realiza actividades maliciosas una vez instalado.
- VPN (Virtual Private Network): Tecnología que crea una conexión segura y cifrada sobre una red menos segura, como Internet, para proteger la privacidad y la integridad de los datos transmitidos.
- Vishing: Variante del phishing que utiliza llamadas telefónicas para engañar a las personas y hacer que revelen información confidencial.
- Vulnerabilidad: Debilidad en un sistema o software que puede ser explotada por un atacante para obtener acceso no autorizado o causar daño.
- Worm (Gusano): Tipo de malware que se replica a sí mismo para propagarse a otros sistemas, a menudo a través de una red.
- Zero-Day: Vulnerabilidad en software desconocida para el fabricante o desarrollador, que puede ser explotada por atacantes antes de que se publique un parche.
- IDS (Intrusion Detection System): Sistema que monitorea el tráfico de red o las actividades del sistema en busca de actividades sospechosas o violaciones de políticas de seguridad.



- IPS (Intrusion Prevention System): Sistema similar al IDS, pero que además de detectar, puede tomar medidas automáticas para prevenir actividades maliciosas.
- Exploit: Software, fragmento de datos o secuencia de comandos que se aprovecha de una vulnerabilidad para causar un comportamiento no intencionado o no deseado en software o hardware.
- APT (Advanced Persistent Threat): Tipo de ataque sofisticado y prolongado en el tiempo, llevado a cabo por grupos organizados para infiltrarse en una red y robar información de manera continua.

6. REFERENTES BIBLIOGRÁFICOS

Avance Jurídico Casa Editorial Ltda. (2021). Leyes desde 1992 - Vigencia expresa y control de constitucionalidad [Ley 1273 de 2009]. Senado de la República de Colombia.

http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Bastidas, H. (2021). Gestión de contraseñas. <https://www.youtube.com/watch?v=WuO1Fu38yPk>

Bastidas, H. (2021). Huella digital. <https://www.youtube.com/watch?v=-p5HezBeYQE>

Cano, J. (2011). Ciberseguridad y ciberdefensa: dos tendencias emergentes en un contexto global. *Sistemas (Asociación Colombiana de Ingenieros de Sistemas)*, 119, 4-7.

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. (2017) Cartillas de seguridad para internet. <https://cartilla.cert.br>

Cynthus (2020). ¿Qué hay de nuevo en COBIT® 2019? <https://www.cynthus.com.mx/que-hay-de-nuevo-en-cobit-2019/>

Díaz y García Conlledo, M. (s.f.). Delitos contra la propiedad intelectual e industrial especial atención a la aplicación práctica en España. *Derecho Penal y Criminología*, 30(88), 93-134. <https://revistas.uexternado.edu.co/index.php/derpen/article/view/612>

Edusalta. (2015). Cyberbullying - Guía práctica para adultos.

<http://www.edusalta.gov.ar/index.php/docman/secretaria-de-planeamiento-educativo/buenas-practicas-de-convivencia-institucional/2728-cyberbullying-guia-practica-para-adultos>



Eset. (2014). Top 5 de riesgos para la privacidad que debes conocer.

<https://www.welivesecurity.com/la-es/2014/08/29/top-5-riesgos-privacidad-debes-conocer/>

Fernández, J. (2018). Ciberbullying. Guía rápida para la prevención del

acoso https://www.ararteko.eus/RecursosWeb/DOCUMENTOS/1/1_1218_3.pdf

Iniseg. (2018). Ciberseguridad al día, qué es oversharing, la sobreexposición en redes que nos

persigue. <https://www.iniseg.es/blog/ciberseguridad/oversharing-conocelo-y-frenalo/>

Interpol. (s.f). Huellas dactilares. <https://www.interpol.int/es/Como-trabajamos/Policia-cientifica/Huellas-dactilares>

Molina, M., Furnari, A., y Hagelstrom, I. (2017). Guía de sensibilización sobre convivencia digital.

https://www.unicef.org/argentina/sites/unicef.org.argentina/files/2018-04/COM-Guia_ConvivenciaDigital_ABRIL2017.pdf

NIST (s.f). Framework for Improving Critical Infrastructure Cybersecurity

<https://www.businesswire.com/news/home/20180522005533/en/HITRUST%C2%AE-Provides-NIST-Cybersecurity-Framework-Certification>

OMPI, Organización Mundial de la Propiedad Intelectual. (2021). ¿Qué es la propiedad intelectual?

<https://www.wipo.int/about-ip/es/>

Portafolio. (28 de octubre de 2015). Amenazas que afectan la privacidad en Internet.

<https://www.portafolio.co/negocios/empresas/amenazas-afectan-privacidad-internet-36348>

Sánchez, G. (2012). Delitos en internet: clases de fraudes y estafas y las medidas para prevenirlos.

Boletín de Información, 324, 67-88.

<https://dialnet.unirioja.es/descarga/articulo/4198948.pdf>

Soriano, M. (2014). Seguridad en redes y seguridad de la información. Obtenido de

<http://improvet.cvut>.

https://www.academia.edu/40156122/Seguridad_en_redes_y_seguridad_de_la_informaci%C3%B3n



7. CONTROL DEL DOCUMENTO

	Nombre	Cargo	Dependencia	Fecha
Autor (es)	PAULA ALEJANDRA CANIZALES YEISON CASTELLANOS GORDILLO	INSTRUCTORES	CENTRO DE COMERCIO Y SERVICIOS	JUNIO 2024

8. CONTROL DE CAMBIOS

(diligenciar únicamente si realiza ajustes a la guía)

	Nombre	Cargo	Dependencia	Fecha	Razón del Cambio
Autor (es)					