Datos generales del curso, sección de Criptografía:

|  |  |
| --- | --- |
| Nombre del curso | Seguridad en Redes |
| Área | Ciencias Computacionales |
| A quién está dirigido | Estudiantes de Ciencias Computacionales y Redes y Seguridad de la Información |
| Duración | Semanas: 8  Horas de docente: 32  Horas individuales: 32 |

Competencia del curso

|  |
| --- |
| Que sea capaz de proteger la confidencialidad y la integridad de la información tanto en tránsito como en reposo, y que pueda autenticar de manera eficiente el acceso a los recursos. |

Módulo 0

Introducción al curso

|  |
| --- |
| Se sugiere sea concisa (uno o dos párrafos) amena y atractiva, que invite, motive al estudio. Conviene utilizar un lenguaje sencillo y cordial. Puede contener la bienvenida al participante y/o alguna idea general del contenido o propósito del curso. |
| Este es un primer curso sobre la Seguridad de la Información. Los servicios básicos de la seguridad de la información son: confidencialidad, integridad y disponibilidad. La criptografía nos puede servir para garantizar la confidencialidad y la integridad de la información, mientras que una infraestructura de red bien diseñada y la autenticación nos ayuda con la disponibilidad. El curso se divide en dos secciones: criptografía e infraestructura de red, esta sección se enfoca a la criptografía. |

Representación gráfica del curso (Opcional)

|  |
| --- |
| Sección de Criptografía |

Cronograma general:

|  |
| --- |
| Se estipulan periodos y fechas o plazos para que el participante realice las actividades de aprendizaje.  El participante puede identificar con facilidad las acciones y actividades a realizar, los periodos para trabajarlas, las fechas para entregar los productos y los medios a través de los cuales se trabajarán las distintas actividades y se compartirán los productos trabajados. |
| Sección de Criptografía |

Formas de comunicación

|  |
| --- |
| Se utiliza para informar a los participantes sobre algún evento, modificación de actividades, fechas de entrega, notificaciones en general. Puede ser un foro o a través del sistema de mensajes propio de cada LMS. Algunos profesores usan herramientas externas que acuerdan con sus estudiantes. Clave esté bien definida, todos la conozcan y sepan será el medio de estos comunicados. |
| El Sistema LMS de este curso será el Canvas, en donde se tendrá todo el material en línea para descargar, así como los enlaces a recursos multimedia, foros de discusión, enlaces externos y los exámenes en línea que así se requieran.   1. La parte en línea síncrona de la clase, así como el chat oficial para la parte de **Criptografía**, será vía MS Teams en el siguiente enlace: [ENLACE]. 2. La parte en línea síncrona de la clase, así como el chat oficial para la parte de **Infraestructura**, será vía [PENDIENTE] en el siguiente enlace: [ENLACE]   Cualquier otro asunto se podrá resolver vía correo electrónico, pero se preferirá vía [MS Teams]. En caso de que no esté disponible la plataforma por saturación, se podrá utilizar [Cisco Webex] en el siguiente enlace: [ENLACE], los detalles de conexión se mostrarán aquí en el Canvas en la sección de Anuncios.  Las tareas se subirán a la plataforma en formato PDF y en su caso, se deberá de proporcionar un enlace privado al video en YouTube en donde presenten la práctica en los casos en que se requiera un Screencast. |

Evaluación del curso

|  |
| --- |
| La evaluación del curso es 50% criptografía y 50% infraestructura, divididos a su vez de la siguiente manera:   * Tareas: 30% * Proyecto: 40% * Exámenes: 30%   Es necesario un promedio mínimo del 60% en cada punto a evaluar en ambas secciones, por lo que reprobar una sección de la materia implica no aprobar la totalidad del curso. |

Desarrollo de unidades

|  |  |
| --- | --- |
| Curso | Seguridad en Redes |
| Unidad | 1. Introducción a la Seguridad Informática / Introducción a la Criptografía |

|  |  |
| --- | --- |
| Objetivo de la unidad | Dar una introducción a los conceptos generales de seguridad informática y de criptografía |

Introducción a la Unidad

|  |
| --- |
| * *En esta unidad veremos 2 temas principalmente:*   + *Introducción a la Seguridad de la Información*   + *Introducción a la Criptografía* * *En la introducción a la Seguridad de la Información veremos un panorama general del estado actual de la seguridad y su relación con el contexto histórico y de los años anteriores* * *Asimismo, veremos algunos tipos de vulnerabilidades que existen* * *En la introducción a la Criptografía veremos un contexto histórico de la criptología, así como las diversas áreas que conforman: criptografía y criptoanálisis.* * *Asimismo, veremos los tipos de criptografía, así como sus principales aplicaciones en la seguridad de la información* * Se espera que el estudiante se familiarice con los conceptos básicos de seguridad * El alumno encontrará que el panorama no es nada halagador, pero que con un esfuerzo de todos podemos salir adelante * El alumno levantará una página web segura para demostrar una de las aplicaciones de la criptografía |

|  |  |
| --- | --- |
| Actividad 1 | Estado actual de la Seguridad de la Información |
| Introducción a la actividad: | Se expondrá un panorama general de la seguridad de la información, cubriendo diversos temas:   * Reporte Symantec * Clasificación de Vulnerabilidades |
| Instrucciones: | 1. Investigar sobre alguna vulnerabilidad o malware de su elección de los que se mencionaron en la clase 2. Participación en el foro sobre la vulnerabilidad o malware investigado 3. Subir documento a la plataforma |
| Recursos:  *(Incluir enlaces, imágenes, bibliografía)* | * CWE * CVE |
| Criterios de evaluación: | Foro:   * Que abra hilo * Que participe con comentarios   Documento:   * Formato: PDF * Estilo: LNCS o IEEE * Citas: IEEE |
| Duración de la actividad: | 2 días |

|  |  |
| --- | --- |
| Actividad 2 | Sitio Web con TLS |
| Introducción a la actividad: | Se expondrá un panorama general de la criptografía, cubriendo los siguientes temas:   * Inicios de la criptografía * Criptografía Simétrica * Criptografía Asimétrica * Protocolos de aplicación * Estado actual |
| Instrucciones: | 1. Investigar cómo levantar un sitio web 2. Conseguir Certificado TLS 3. Armar esqueleto básico de sitio web 4. Presentar información del Certificado |
| Recursos:  *(Incluir enlaces, imágenes, bibliografía)* | * AWS * GoDaddy * Otro VPS * Understanding Cryptography. Christof Paar, Jan Pelzl. 2010. Springer-Verlag Berlin Heidelberg. 978-3-642-04100-6. |
| Criterios de evaluación: | * Sitio activado con certificado válido |
| Duración de la actividad: | 1 semana |

|  |  |
| --- | --- |
| Curso | Seguridad en Redes |
| Unidad | 2. Matemáticas para la Criptografía |

|  |  |
| --- | --- |
| Objetivo de la unidad | Que los alumnos se nivelen en los conceptos necesarios de matemáticas para la criptografía |

Introducción a la Unidad

|  |
| --- |
| * *En esta unidad vamos a ver conceptos básicos de las matemáticas para la criptografía, conceptos que son necesarios para la elaboración de bibliotecas criptográficas.* * *En esta unidad veremos los siguientes temas:*   + *Probabilidad*   + *Teoría de Números*   + *Aritmética Modular*   + *XGCD*   + *CRT* * *Se espera que el estudiante pueda elaborar un programa que calcule el inverso modular, elemento necesario para la criptografía tipo RSA, de curvas elípticas y poscuántica* * *El alumno descubrirá que las matemáticas son necesarias para la vida real, aunque no necesariamente es preciso conocer las entrañas de las matemáticas avanzadas para poder utilizarlas* |

|  |  |
| --- | --- |
| Actividad 3 | GCD |
| Introducción a la actividad: | Calcular el Máximo Común Divisor de una pareja de números para determinar si son coprimos o si uno es número primo |
| Instrucciones: | 1. Seguir el algoritmo genérico presentado en clase 2. Programarlo en Python de manera inicial 3. Probar con varias parejas de números |
| Recursos:  *(Incluir enlaces, imágenes, bibliografía)* | * Python * Material de clase * An Introduction to Mathematical Cryptography. Jeffrey Hoffsteinn, Jill Pipher, Joseph H. Silverman. 2014. Springer-Verlag New York. 978-1-4939-1711-2. |
| Criterios de evaluación: | * Código funcional |
| Duración de la actividad: | 1 día o durante la clase |

|  |  |
| --- | --- |
| Actividad 4 | XGCD |
| Introducción a la actividad: | Calcular el inverso modular utilizando como referencia el código de la a |
| Instrucciones: | 1. Seguir el algoritmo genérico presentado en clase 2. Programarlo en Python de manera inicial 3. Probar con varias parejas de números |
| Recursos:  *(Incluir enlaces, imágenes, bibliografía)* | * Python * Material de clase * An Introduction to Mathematical Cryptography. Jeffrey Hoffsteinn, Jill Pipher, Joseph H. Silverman. 2014. Springer-Verlag New York. 978-1-4939-1711-2. |
| Criterios de evaluación: | * Código funcional * Documentación en formato PDF, LNCS, IEEE. |
| Duración de la actividad: | 2 días o durante la clase |

|  |  |
| --- | --- |
| Curso | Seguridad en Redes |
| Unidad | 3. Ciencias Computacionales para la Criptografía |

|  |  |
| --- | --- |
| Objetivo de la unidad | Que los alumnos se nivelen en los conceptos computacionales necesarios para la criptografía |

Introducción a la Unidad

|  |
| --- |
| * *Introducir al tema* * *Qué se espera del estudiante en esta unidad* * *Qué es lo que va a encontrar* * *Qué es lo que va a hacer*   *CS-PRNG, RTSC, AVX, TCP/UDP* |

|  |  |
| --- | --- |
| Actividad 5 | Números pseudoaleatorios |
| Introducción a la actividad: | En esta actividad aprenderemos a utilizar de manera adecuada los generadores de números pseudoaleatorios criptográficamente seguros del sistema operativo. |
| Instrucciones: | Generar un programa que utilice el /dev/random y el /dev/urandom sobre números enteros de 32 y 64 bits  Verificar la entropía de los números generados |
| Recursos:  *(Incluir enlaces, imágenes, bibliografía)* | C/C++  Serious Cryptography: A Practical Introduction to Modern Encryption. Jean-Philippe Aumasson. 2017. No Starch Press, USA. ISBN:978-1-59327-826-7 |
| Criterios de evaluación: | * Código funcional * Documentación en formato PDF, LNCS, IEEE. |
| Duración de la actividad: | 1 día o durante la clase |

|  |  |
| --- | --- |
| Actividad 6 | Aritmética con números multiprecisión |
| Introducción a la actividad: | En la criptografía contemporánea son requeridos valores más allá del tamaño de palabra de los procesadores comerciales, dependiendo del tipo de criptografía y del nivel de seguridad deseado, es la cantidad de bits necesarios. En esta actividad el estudiante simulará operaciones aritméticas básicas con números formados por más de una palabra utilizando instrucciones especializadas del procesador.  El estudiante descubrirá que ciertas actividades que normalmente hace el procesador automáticamente no son posibles o no son realizadas cuando manejamos números criptográficamente grandes. |
| Instrucciones: | * Programar números de 256 bits en estructuras en C/C++, hacer la operación de suma, resta y multiplicación * Utilizar los intrinsics para las operaciones de suma, resta y multiplicación de 256 de bits. * Programar números de 1024 bits y programar las operaciones de suma, resta y multiplicación con intrinsics de 256 bits. |
| Recursos:  *(Incluir enlaces, imágenes, bibliografía)* | * C/C++ * Guide to Elliptic Curve Cryptography. Darrel Hankerson, Alfred J. Menezes, Scott Vanstone. 2004. Springer-Verlag New York. 978-0-387-95273-4. * Intel® 64 and IA-32 Architectures Software Developer’s Manual Combined Volumes: 1, 2A, 2B, 2C, 2D, 3A, 3B, 3C, 3D, and 4. 2020. |
| Criterios de evaluación: | * Código funcional * Documentación en formato PDF, LNCS, IEEE. |
| Duración de la actividad: | 1 semana |

|  |  |
| --- | --- |
| Actividad 7 | Biblioteca multiprecisión |
| Introducción a la actividad: | Ya que tenemos la aritmética con números de multiprecisión, es necesario armar la aritmética modular utilizando los resultados de la Actividad 6 |
| Instrucciones: | * Programar la suma y resta modular * Programar la multiplicación con reducción modular de Barret * Programar la multiplicación de Montgomery * Programar la exponenciación de Montgomery |
| Recursos:  *(Incluir enlaces, imágenes, bibliografía)* | * C/C++ * Guide to Elliptic Curve Cryptography. Darrel Hankerson, Alfred J. Menezes, Scott Vanstone. 2004. Springer-Verlag New York. 978-0-387-95273-4. * [MONTGOMERY] |
| Criterios de evaluación: | * Código funcional * Documentación en formato PDF, LNCS, IEEE. |
| Duración de la actividad: | 1 semana |

Desarrollo de unidades

|  |  |
| --- | --- |
| Curso | Seguridad en Redes |
| Unidad | 4. Firmas Digitales y Autenticación |

|  |  |
| --- | --- |
| Objetivo de la unidad | Que el alumno pueda firmar un documento digitalmente |

Introducción a la Unidad

|  |
| --- |
| * *La Integridad es uno de los principales servicios de la Seguridad de la Información.* * *Las firmas digitales proveen de un mecanismo de validación y verificación de la integridad de un documento almacenado o incluso de mensajes en tránsito.* * *Para que se logre verificar la integridad de un documento mediante las firmas digitales, es necesario establecer una infraestructura de clave pública que gestione las credenciales* * *Se espera que el estudiante logre generar la firma electrónica de un documento almacenado en su computadora y logre replicar este mismo ejercicio en una página web.* * *Para poder utilizar la firma electrónica, primero son necesarios los conceptos de funciones hash, que pueden ser para documentos, claves o para esquemas de autenticación multifactor, así como de los esquemas de codificado.* * *Una vez con los conceptos de las funciones ancilares, veremos los tipos básicos de firmas digitales.* * *Opcionalmente, el alumno utilizará sus propias credenciales del SAT para la firma de documentos a manera de ejercicio.* |

|  |  |
| --- | --- |
| Actividad 8 | Firma de documentos en PC |
| Introducción a la actividad: | En la primera actividad se realizará la firma electrónica de un documento utilizando un protocolo de firma electrónica. Un documento firmado y verificado adecuadamente, da garantía de que el documento no se ha alterado, dando el servicio de integridad de la información. |
| Instrucciones: | Implementar la firma y la verificación RSA en C/C++ y posteriormente con OpenSSL para utilizar la firma del SAT |
| Recursos:  *(Incluir enlaces, imágenes, bibliografía)* | * Actividad 7 * The exact security of digital signatures: How to sign with RSA and Rabin. Mihir Bellare and Phillip Rogaway.. 1996. Eurocrypt 96, Lecture Notes in Computer Science Vol. 1070, U. Maurer ed, Springer-Verlag, 1996. * Internet Engineering Task Force (IETF). Request for Comments: 8017. PKCS #1: RSA Cryptography Specifications Version 2.2. Noviembre 2016. * Introduction to Modern Cryptography. Jonathan Katz, Yehuda Lindell. 2014. Chapman and Hall/CRC. 2nd Ed. 9781466570269. * Opcional: Credenciales del SAT |
| Criterios de evaluación: | * Código funcional * Firma Verificada * Documentación en formato PDF, LNCS, IEEE. |
| Duración de la actividad: | 3 días |

|  |  |
| --- | --- |
| Actividad 9 | Firma de documentos en Web |
| Introducción a la actividad: | En la segunda actividad se realizará la firma electrónica de un documento utilizando la firma electrónica del SAT o su equivalente en el repositorio generado en la Actividad 2. Un documento firmado y verificado adecuadamente, da garantía de que el documento no se ha alterado, dando el servicio de integridad de la información. |
| Instrucciones: | Implementar la firma y la verificación RSA con Libsodium o OpenSSL en su página web generada |
| Recursos:  *(Incluir enlaces, imágenes, bibliografía)* | * Actividad 2 * The exact security of digital signatures: How to sign with RSA and Rabin. Mihir Bellare and Phillip Rogaway.. 1996. Eurocrypt 96, Lecture Notes in Computer Science Vol. 1070, U. Maurer ed, Springer-Verlag, 1996. * Internet Engineering Task Force (IETF). Request for Comments: 8017. PKCS #1: RSA Cryptography Specifications Version 2.2. Noviembre 2016. * Introduction to Modern Cryptography. Jonathan Katz, Yehuda Lindell. 2014. Chapman and Hall/CRC. 2nd Ed. 9781466570269. * Libsodium/OpenSSL * Opcional: Credenciales del SAT |
| Criterios de evaluación: | * Código funcional * Firma Verificada * Documentación en formato PDF, LNCS, IEEE. |
| Duración de la actividad: | 1 semana |

|  |  |
| --- | --- |
| Actividad 10 | Autenticación Multifactor |
| Introducción a la actividad: | Un esquema de autenticación a 2 factores da garantía de que tanto la información, así como el resto de los recursos de la organización están protegidos y vigilados por su equipo de TI. Se desea que el estudiante implemente un esquema de autenticación en su página web, así como que genere bitácoras adecuadas y esté utilizando una función hash adecuada para el almacenamiento de las credenciales de acceso. |
| Instrucciones: | * Implementar el soporte de autenticación a 2 factores HOTP o TOTP y enlace su página web a la aplicación del Google Autenticator o similar * Implementar una base de datos de bitácora con los accesos al sitio web conteniendo información de: nombre de usuario, dirección de IP, hora de entrada, hora de salida. * Utilizar la función Argon2i para el almacenamiento de los hash de las credenciales de usuario. |
| Recursos:  *(Incluir enlaces, imágenes, bibliografía)* | * Actividad 9 * Introduction to Modern Cryptography. Jonathan Katz, Yehuda Lindell. 2014. Chapman and Hall/CRC. 2nd Ed. 9781466570269. * Libsodium/OpenSSL * Opcional: Credenciales del SAT |
| Criterios de evaluación: | * Código funcional * Bitácora de accesos * 2FA activado * Documentación en formato PDF, LNCS, IEEE. |
| Duración de la actividad: | 1 semana |

Desarrollo de unidades

|  |  |
| --- | --- |
| Curso | Seguridad en Redes |
| Unidad | 5. Cifradores Simétricos |

|  |  |
| --- | --- |
| Objetivo de la unidad | Que el alumno pueda cifrar un documento |

Introducción a la Unidad

|  |
| --- |
| * *Otra de los servicios de seguridad de la información más importantes es la confidencialidad.* * *Garantizar la confidencialidad de la información a los propietarios de la misma y garantizar que solamente pueda ser legible a las partes interesadas autorizadas es pieza crucial en la gestión de la información* * *En esta unidad cubriremos algunos de los esquemas de cifrado más utilizados y estandarizados actualmente.* * *Asimismo, daremos un repaso a los esquemas de cifrado amigables a los sistemas embebidos, que pueden utilizarse en los llamados dispositivos de IoT.* * *También veremos una alternativa a las firmas digitales.* * *Se espera que el estudiante comprenda los componentes internos de estas primitivas y pueda implementarlas para la protección de la información.* |

|  |  |
| --- | --- |
| Actividad 11 | Cifrado de documento en PC |
| Introducción a la actividad: | Un primer paso para la confidencialidad de la información es en nuestros dispositivos y en particular, en los documentos en reposo. Se desea cifrar y descifrar documentos almacenados |
| Instrucciones: | Implemente una solución de cifrado de documentos con AES-128. |
| Recursos:  *(Incluir enlaces, imágenes, bibliografía)* | * Actividad 10 * Introduction to Modern Cryptography. Jonathan Katz, Yehuda Lindell. 2014. Chapman and Hall/CRC. 2nd Ed. 9781466570269. * Libsodium/OpenSSL |
| Criterios de evaluación: | * Código funcional * Documento descifrado * Documentación en formato PDF, LNCS, IEEE. |
| Duración de la actividad: | 3 días |

|  |  |
| --- | --- |
| Actividad 12 | Cifrado de documento en Web |
| Introducción a la actividad: | Una vez que sabemos cifrar documentos almacenados, tenemos que llevar esto a nuestro repositorio que está en la web.  Muchas de las veces, nuestra información la tenemos que subir a la nube, quedando bajo custodia de un tercero que no necesariamente es un tercero de confianza o que está bajo la jurisdicción de las leyes de un país tercero, asimismo, este puede ser susceptible de ataques informáticos, por lo que es preciso proteger la información aún de a quienes le confiamos su respaldo y disponibilidad. |
| Instrucciones: | Implemente una solución de cifrado de documentos con AES-128 para el sitio web de la Actividad 10. |
| Recursos:  *(Incluir enlaces, imágenes, bibliografía)* | * Actividad 10 * Libsodium/OpenSSL |
| Criterios de evaluación: | * Código funcional * Documento descifrado * Documentación en formato PDF, LNCS, IEEE. |
| Duración de la actividad: | 3 días |

Desarrollo de unidades

|  |  |
| --- | --- |
| Curso | Seguridad en Redes |
| Unidad | Criptografía Poscuántica |

|  |  |
| --- | --- |
| Objetivo de la unidad | Compresión de la criptografía cuántica |

Introducción a la Unidad

|  |
| --- |
| * *La inminente creación de una máquina cuántica que pueda superar en varios órdenes de magnitud las capacidades de cómputo de las computadoras clásicas, ha traído desde hace tiempo la pregunta de cómo aplicar estos equipos en el rompimiento de las primitivas criptográficas y si algún gobierno, agencia de espionaje u otra persona mal intencionada, podría hacer un uso malicioso de esta tecnología.* * *En años recientes, el NIST ha establecido un concurso para proponer nuevos estándares de cifrado, firmas digitales e identificación que sean seguros ante ataque de máquinas cuánticas.* * *Actualmente los avances en computación cuántica están orientados hacia los problemas más fuertes de la humanidad, tales como la predicción del clima o de la traducción del lenguaje.* * *Se espera que el estudiante analice y comprenda este paradigma computaciones en relación a la criptografía.* |

|  |  |
| --- | --- |
| Actividad 13 | Discusión |
| Introducción a la actividad: | Se espera que el estudiante analice y comprenda este paradigma computaciones en relación a la criptografía. |
| Instrucciones: | Discuta su punto de vista sobre el avance actual en este tipo de computadoras y los ataques a las primitivas actuales, así como que cuestione si las nuevas tendencias van encaminadas hacia el camino correcto. |
| Recursos:  *(Incluir enlaces, imágenes, bibliografía)* | * Sitio web del Concurso NIST sobre Primitivas Criptográficas Poscuánticas * Post-Quantum Cryptography. Bernstein, Daniel J., Buchmann, Johannes, Dahmen, Erik. 2009. Springer-Verlag Berlin Heidelberg. 978-3-540-88701-0. |
| Criterios de evaluación: | Foro:   * Que abra hilo * Que participe con comentarios   Documento:   * Formato: PDF * Estilo: LNCS o IEEE * Citas: IEEE |
| Duración de la actividad: | 1 día |

Consideraciones:

## **Webcam**

* Es necesario **habilitar la cámara web para resolver todo examen**.
  + En caso de no hacerlo no tendrá derecho a calificación en este rubro.
* Es necesario **habilitar la cámara web en todas las sesiones de videoconferencia**.
  + En caso de no hacerlo no tendrá derecho a hacer preguntas en las sesiones de videoconferencia.

## Exámenes durante etapas 100% en línea

* Los exámenes serán aquí, a través de la herramienta CANVAS, y**deberán entregarse las evidencias por el mismo medio.**
* **Se deberá asistir a la sesión de videoconferencia durante el examen.**
* Los exámenes que sean utilizando las **herramientas integradas** de CANVAS, se deberán de enviar antes de que termine el tiempo.
* Los exámenes que sean utilizando **herramientas externas** deberán de **adjuntar el enlace correspondiente** dentro del tiempo señalado.
* **Considere el tiempo de carga de archivos de evidencia**, incluyendo fotografías de trabajos a mano que se tengan que adjuntar en la plataforma.
* **No se recibirán exámenes fuera de la fecha y hora de entrega** descrita en el mismo.
* En caso de no tener conexión a Internet, suministro de energía eléctrica u otro imprevisto deberá **comunicarse por correo electrónico con el profesor lo antes posible** para atender su caso.

## **Sesiones en línea**

* Todas las videoconferencias por MS Teams se grabarán y estarán disponibles en el canal de MS TEAMS del curso, en [https://web.microsoftstream.com/ (Links to an external site.)](https://web.microsoftstream.com/) y aquí como un enlace en el CANVAS
* Las videoconferencias por Cisco Webex estarán accesibles por CANVAS
* No se garantiza que las videoconferencias grabadas estén disponibles después de que termine el curso. En la medida de la capacidad de espacio de almacenamiento, estarán disponibles el resto del curso.

## Asistencia a Videoconferencias

* Es responsabilidad de cada alumno concertase a las videoconferencias. **Se nombrará lista al inicio de la misma**.  Se tienen 10 minutos de tolerancia para los alumnos en modalidad mixta y para cambio de sesión.
* La SEP nos exige al menos un **80% de asistencia a las clases**, además se pedirá al menos asistencia al 60% de las clases en línea para la modalidad semipresencial, respetando el requisito 80% de la asistencia.

## **Reglas de Convivencia en Línea**

* Incluir **fotografía reciente** en su perfil de la herramienta de videoconferencia. Se prefiere fotografía tipo credencial para la clase.
* Cada participante deberá de asegurarse de que **al incio de la sesión** su **cámara** esté **encendida** y que su **audio** esté **silenciado** (en mute).
* Se podrá estar apagando y encendiendo la **webcam** una vez iniciada la clase, pero recordando que es**necesaria para hacer preguntas o participar.**
* **Se sugiere tener encendida la webcam** como medida de salud mental, pero considere el uso de su ancho de banda.
* Se sugiere utilizar la opción de "levantar la mano" sobre la opción de chat hacia el profesor.
* Si se pierde o debilita la señal, prefiera el uso de chat para preguntar el estado actual de la clase.

## **Reglas de Convivencia Presenciales**

* El uso de **cubrebocas es obligatorio**, se sugiere el uso de careta. Lleve su gel antibacterial y si lo considera, el uso de guantes es bienvenido.
* **Se sugiere el uso de un gafete** y una fotografía a color grande.
* Respetar la **sana distancia**
* Saludar de lejos
* **Limpiar su área antes y después** de utilizarla, incluyendo teclado y ratón
* **No estará permitido ingerir alimentos** debido a que implica quitarse el cubrebocas