

Foro: Ciberseguridad para estudiantes Perspectiva institucional

Heysel Escamilla Alcántara
Profesora de asignatura en FCPyS, UNAM
Consultora en Comunicación y Nuevos medios en Sepuede.mx

Viernes 5 de noviembre, 2021
San Francisco de Campeche, Campeche

La nube, herramienta clave para la educación del futuro

El objetivo es transformar el salón de clase y garantizar que la experiencia virtual de un estudiante sea similar a la presencial; ese será el reto en los próximos años.









Pekín refuerza sus controles sanitarios ante el “grave” rebrote de Covid-19

La capital china refuerza sus restricciones sanitarias, mientras toda China se enfrenta a un rebrote epidémico del Covid-19 “grave y complejo”.



Reuters
30 de octubre de 2021, 12:24



Foto: Reuters.

Pekín cierra cines por rebrote de covid-19

Todos los cines del distrito de Xicheng, que agrupa a barrios al oeste de la plaza Tiananmen, están cerrados hasta el 14 de noviembre

SEBASTIÁN GARCÍA

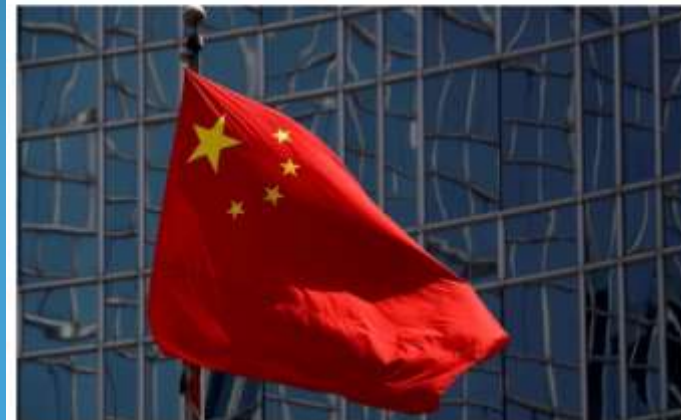


Cómo medida de precaución, unos seis millones de cines están confinados en ciudades en las que se han detectado casos. (Foto: APN)

China pide guardar provisiones ante posibles confinamientos por rebrotes de covid-19



El Ministerio de Comercio pidió en un comunicado a las familias a hacer acopio de artículos de necesidad básica.



Bandera de China (Reuters)



WU
Felix Dierckx | 11/2021 14:50

China ha pedido a las familias que hagan esfuerzos para asegurarse el abastecimiento de víveres en medio de los rebrotes ahora activos en distintos puntos del país, los cuales han provocado confinamientos parciales y totales en algunas ciudades.

Se investigan los casos de covid-19



Disfruta de los mejores programas en vivo en la app de **Imagen Radio**

DESCARGA LA APP

Disponible en la App Store

IMAGEN RADIO | Promovido por Imagen y patrocinado por la empresa patrocinadora.

E-learning.



Blended learning. Incorpora tecnología a la enseñanza tradicional.



Ciberseguridad

«La ciberseguridad es la capacidad de defender las computadoras y los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos, también se le conoce como seguridad de Tecnologías de la Información o seguridad de la Información Tecnológica, se aplica a numerosos elementos, desde la seguridad informática hasta recuperación ante desastres y educación del usuario final.»

Navarro Pulido, Miguel Ángel, Praxis.

<https://mexico.praxisglobe.com/recursos/diseminaciones/SEGURIDAD/SGD-WP-01-2020-PUBL.pdf>

La ciberseguridad es la práctica de proteger sistemas, redes y programas de ataques digitales. Por lo general, estos ciberataques apuntan a acceder, modificar o destruir la información confidencial; Extorsionar a los usuarios o los usuarios o interrumpir la continuidad del negocio.

Actualmente, la implementación de medidas de seguridad digital se debe a que hay más dispositivos conectados que personas, y los atacantes son cada vez más creativos.

Cisco

https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html

Transformación digital de las organizaciones.

- Inteligencia Artificial
- Ciencia de datos
- Internet de las cosas
- **Ciberseguridad**
- Robótica y automatización

«La falta de conciencia y cultura de prevención es la mayor vulnerabilidad en la seguridad informática.»

Navarro Pulido, Miguel Ángel, Praxis.

<https://mexico.praxisglobe.com/recursos/diseminaciones/SEGURIDAD/SGD-WP-01-2020-PUBL.pdf>

Zero Trust

Nada es confiable.

¿Seguridad dentro de la organización?

Ciberseguridad para **estudiantes**.

Institucional

Profesorado

Personal administrativo

Estudiantado

Gobierno federal

Gobiernos locales

Secretaría de Educación

Secretaría de Seguridad

Sociedad

Familias

Medios de comunicación

Facultad de Ciencias Políticas y Sociales (FCPyS), UNAM



IntegraTic

Fortaleciendo la
transmisión
del conocimiento

Introducción ▾ Planeación ▾ Herramientas ▾ Cursos Moodle ▾ Interactividad ▾ Recomendaciones ▾ Ayuda



**DESCUBRE QUE TAN PREPARADO
ESTÁS PARA EL MODELO HÍBRIDO**



DESCÚBRELO AQUÍ

Modalidad de
enseñanza presencial



Modalidad de
enseñanza en línea

Sincrónica: Aprendizaje con el Docente

Asincrónica: Aprendizaje Autogestivo

AULA HÍBRIDA

Prevención de la Violencia Mediática y el Acoso Sexual en las Redes Sociales

El propósito de esta actividad es que los estudiantes identifiquen y describan los tipos de violencia mediática y acoso sexual en las redes sociales, así como también que identifiquen y describan los tipos de violencia mediática y acoso sexual en las redes sociales.



Expresiones de la Ciberviolencia

La violencia mediática es cualquier tipo de violencia que se realiza a través de los medios de comunicación (radio, televisión, prensa, internet, etc.), ya sea en forma de acoso sexual, acoso psicológico, acoso físico, acoso verbal, acoso por correo electrónico, acoso por mensajes de texto, acoso por redes sociales, acoso por videoconferencias, acoso por videojuegos, acoso por aplicaciones de mensajería instantánea, acoso por aplicaciones de redes sociales, acoso por aplicaciones de mensajería instantánea, acoso por aplicaciones de mensajería instantánea, acoso por aplicaciones de mensajería instantánea.

Consejos para Igualdad en el Aula Virtual

- ▶ Promover y ejercer los derechos de la información responsablemente y con respeto.
- ▶ Generar relaciones respetuosas con los estudiantes, no solo en el aula virtual, sino en el aula presencial, desde los aulas virtuales.
- ▶ Utilizar la lengua inclusiva y no sexista.
- ▶ Promover la equidad de género y el respeto y el diálogo, así como el "género inclusivo" en el lenguaje y en la comunicación.
- ▶ Respetar los derechos de los estudiantes, así como la igualdad y equidad.
- ▶ No utilizar "bullying" que pueda tener consecuencias físicas, psicológicas, emocionales o académicas.
- ▶ No discriminar, así como respetar los derechos de todos y todas en el aula virtual.
- ▶ Respetar los derechos de los estudiantes y promover la equidad y el respeto en el aula virtual.
- ▶ Tener cuidado con el uso de la cámara y el micrófono en el aula virtual.
- ▶ Promover la equidad y el respeto, así como la igualdad y equidad en el aula virtual.
- ▶ Promover la equidad y el respeto, así como la igualdad y equidad en el aula virtual.
- ▶ Promover la equidad y el respeto, así como la igualdad y equidad en el aula virtual.
- ▶ Promover la equidad y el respeto, así como la igualdad y equidad en el aula virtual.



¡Tú también puedes promover una cultura de la igualdad y prevenir la violencia de género en las Aulas Virtuales!

Ciberdelincuencia



Las acciones en la web pueden volverse no sólo un delito, sino un fraude y la de otros. ¡Cuida la información que compartes!



Muévete con seguridad en el mundo digital

“E” los ciberdelincuentes” abarcan todo lo que ha que en internet se que control de información, como: identidad, salud, finanzas, seguridad, empleo, educación, comercio, pagos de servicios y datos personales confiables.

Los ciberdelincuentes usan los datos y aplicaciones para intervenir en el mundo virtual, generar nuevos información y actividades que de ellos se genera, a la vez, la cual está controlada por algoritmos o dispositivos interconectados entre sí.



Algunos programas que desde un sistema de cómputo pueden acceder a personal de datos, y hacer mal uso de ellos.



Ciberdelincuencia

Los delitos ciberdelincuenciales son aquellos que se cometen a través de internet.

Principalmente se refieren a los delitos de fraude y robo de información por medio electrónico.

Además, algunos delitos electrónicos son: robo de identidad, fraude electrónico, robo de información personal.

Actualmente, los delitos ciberdelincuenciales se refieren a la vulneración de derechos.



A los delitos en los delitos son los delitos electrónicos, que se cometen a través de internet.

Los delitos en los delitos son los delitos electrónicos, que se cometen a través de internet.

Maximiza las medidas de seguridad

Configura bien tus dispositivos para que sean seguros en el mundo virtual de la computación de redes.

No accedas a redes sociales sin verificar la identidad de los usuarios que se conectan con ellos, para evitar ser víctima de fraudes.

Evita de la información que se genera en internet, que puede ser utilizada para fines ilícitos, como: robo de identidad, fraude electrónico, robo de información personal.



Evita de la información que se genera en internet, que puede ser utilizada para fines ilícitos, como: robo de identidad, fraude electrónico, robo de información personal.

Evita de la información que se genera en internet, que puede ser utilizada para fines ilícitos, como: robo de identidad, fraude electrónico, robo de información personal.



Evita de la información que se genera en internet, que puede ser utilizada para fines ilícitos, como: robo de identidad, fraude electrónico, robo de información personal.

Busca más información en

Ciencia UNAM



Evita de la información que se genera en internet, que puede ser utilizada para fines ilícitos, como: robo de identidad, fraude electrónico, robo de información personal.

¿GOBIERNO DE LA CIBERSEGURIDAD?

Rosa Kochi Sarabia Barajas

Seguridad | IT/OT | Seguridad | Gobierno de la ciberseguridad | Datos | Normas | Contratos | Estructura organizacional

Resumen



Hoy en día, las amenazas cibernéticas se introducen en las organizaciones de diversas formas, ya sea por medio de los empleados, aplicaciones o sistemas dirigidos a las empresas con la intención de ocasionar daño.

La seguridad requiere la participación activa de los altos directivos de las empresas. El término que describe el compromiso de la alta dirección es el gobierno de la ciberseguridad, asegurar que los objetivos sean alcanzados, garantizar que los riesgos sean gestionados adecuadamente, y verificar que los recursos

Por lo tanto, la ciberseguridad debe ser parte integral del gobierno corporativo para lograr sus objetivos, no sólo para cubrir las necesidades actuales sino también

El objetivo de la seguridad de la información es desarrollar, implementar y administrar un programa de seguridad que alcance los siguientes cinco resultados

1. Alineación estratégica: Alinear la seguridad de la información con la estrategia de negocio.
2. Administración de riesgos: Ejecutar medidas apropiadas para mitigar los riesgos y reducir el posible impacto que tendrían en los activos de información.
3. Entrega de valor: Optimizar las inversiones en la seguridad.
4. Administración de recursos: Utilizar el conocimiento y la infraestructura de la seguridad de la información con eficiencia y eficacia.
5. Medición del desempeño: Monitorear y reportar métricas de seguridad de la información para garantizar que se alcanzan los objetivos.

Webinar “Ciberseguridad en las instituciones educativas”



El pasado 27 de mayo, Lizbeth Barreto y Roberto Sánchez de la Dirección de Sistemas y Servicios Institucionales participaron como panelistas en la sesión semanal de la Asociación Nacional de Universidades e Instituciones de Educación Superior (ANUIES.)

Ciberseguridad en las instituciones educativas, fue el tema central del Webinar, al que se conectaron 80 participantes de diversas universidades e instituciones educativas del país, que son miembros de la ANUIES.

Lizbeth Barreto abordó el tema de Continuidad de la Operación con Firma Electrónica Avanzada y Roberto Sánchez Continuidad de operaciones utilizando las mejores prácticas internacionales.

La referencia al sitio web es: <https://recursosdigitales.anui.es.mx/>

Riesgos generales de la comunidad estudiantil de educación superior

- Sexting



- Grooming



- Cyberbullying



Prácticas escolares en el nivel superior

Dentro y fuera de las aulas

Sesiones en vivo.

Protección de datos personales.

Malas prácticas. Contraseñas.

Contraseñas complejas no garantizan seguridad. La podemos anotar en un papel (jejejeje).

Gestión de las contraseñas.

Creer que la tecnología nos solucionará todo.

Conclusiones

- El modelo educativo *Blended learning*, en este momento, responde a las necesidades del entorno.
- La ciberseguridad es parte fundamental de la transformación digital de las organizaciones, incluyendo a las educativas.
- El liderazgo institucional educativo deberá promover una cultura de ciberseguridad con lo cual se proyectará una imagen corporativa congruente con el entorno y de responsabilidad social.
- Generar una cultura de ciberseguridad compete a las instituciones educativas, gobiernos, familias y medios de comunicación.

¡Gracias por su atención!

Heysel Escamilla Alcántara

Profesora de asignatura en FCPyS, UNAM

Consultora en Comunicación y Nuevos medios
en Sepuede.mx