

Arquitectura y Sistemas Operativos

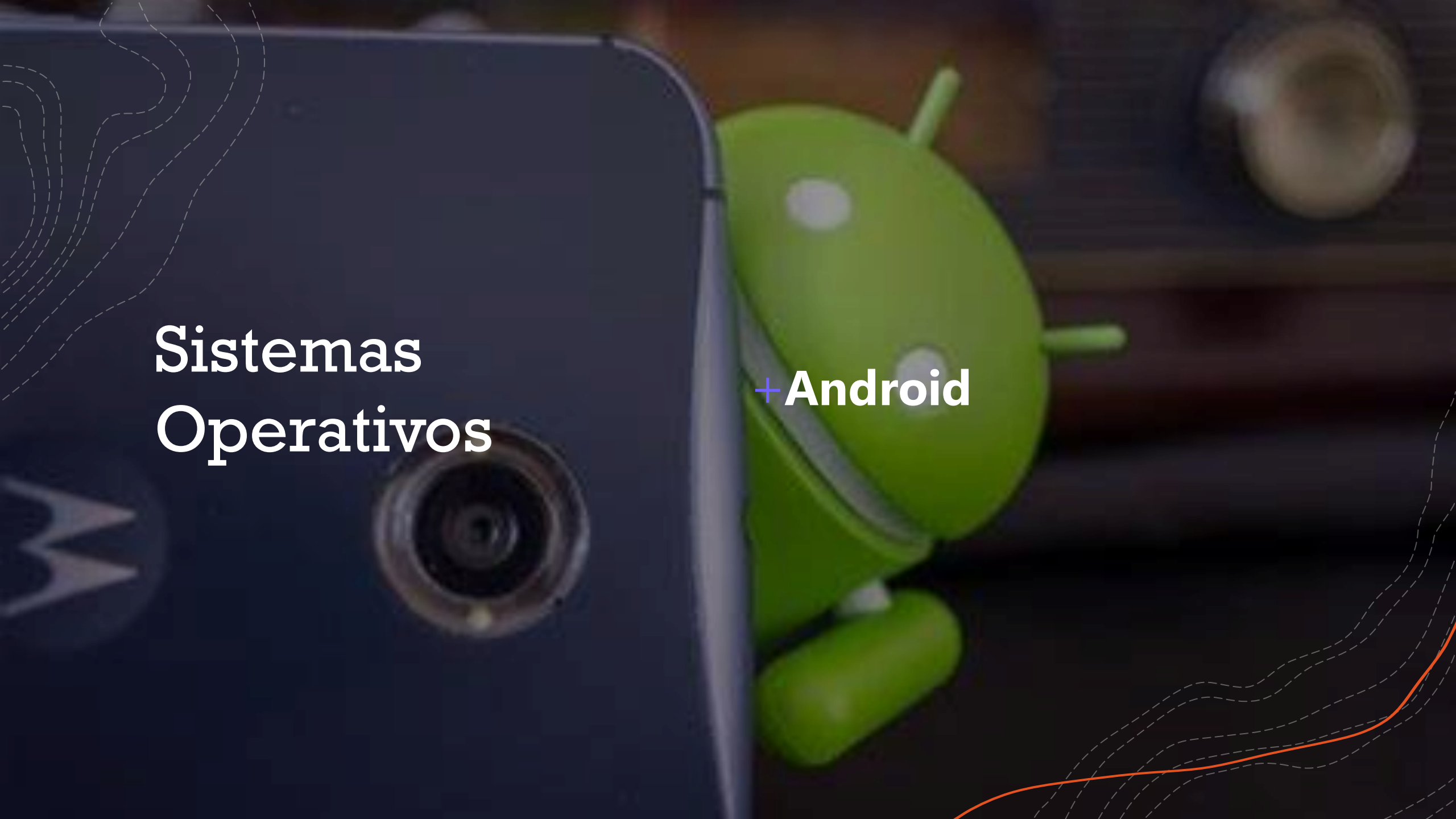
+


Clase 7

Prof: Natalia Lucero

Sistemas Operativos

+Android



- 
- + Este sistema operativo heredó el núcleo de Linux, así como otros programas provenientes de la comunidad de código abierto. Ha sido **diseñado para funcionar en dispositivos móviles que tienen pantalla táctil.**

- + Fue originalmente creado por **la compañía Android Inc.** Posteriormente, fue adquirida por la multinacional **Google**, que le ha dado continuidad a su desarrollo desde entonces. En 2007, fue presentado como una solución de estándar abierto para dispositivos móviles, y el 23 de septiembre de 2008 fue lanzada la primera versión al público en general.



INNOVACIÓN



- + Se trataba de una apuesta innovadora, ya que, hasta ese momento, cada fabricante de teléfonos inteligentes y tabletas desarrollaba software exclusivo para sus propios equipos. Este concepto no tardó en hacer mella en la industria, y en unos cuantos años ya se había convertido en el mejor sistema operativo en cuanto a cuota de participación en el mercado.

CARACTERÍSTICAS

- + Entre las características de Android, destaca su **capacidad para adaptarse a todo tipo de pantallas**, independientemente de su tecnología y su resolución; su **alta compatibilidad** con una gran cantidad de tecnologías de conexión inalámbricas, y la gran **variedad de ofertas** en lo que se refiere a sus servicios de mensajería.



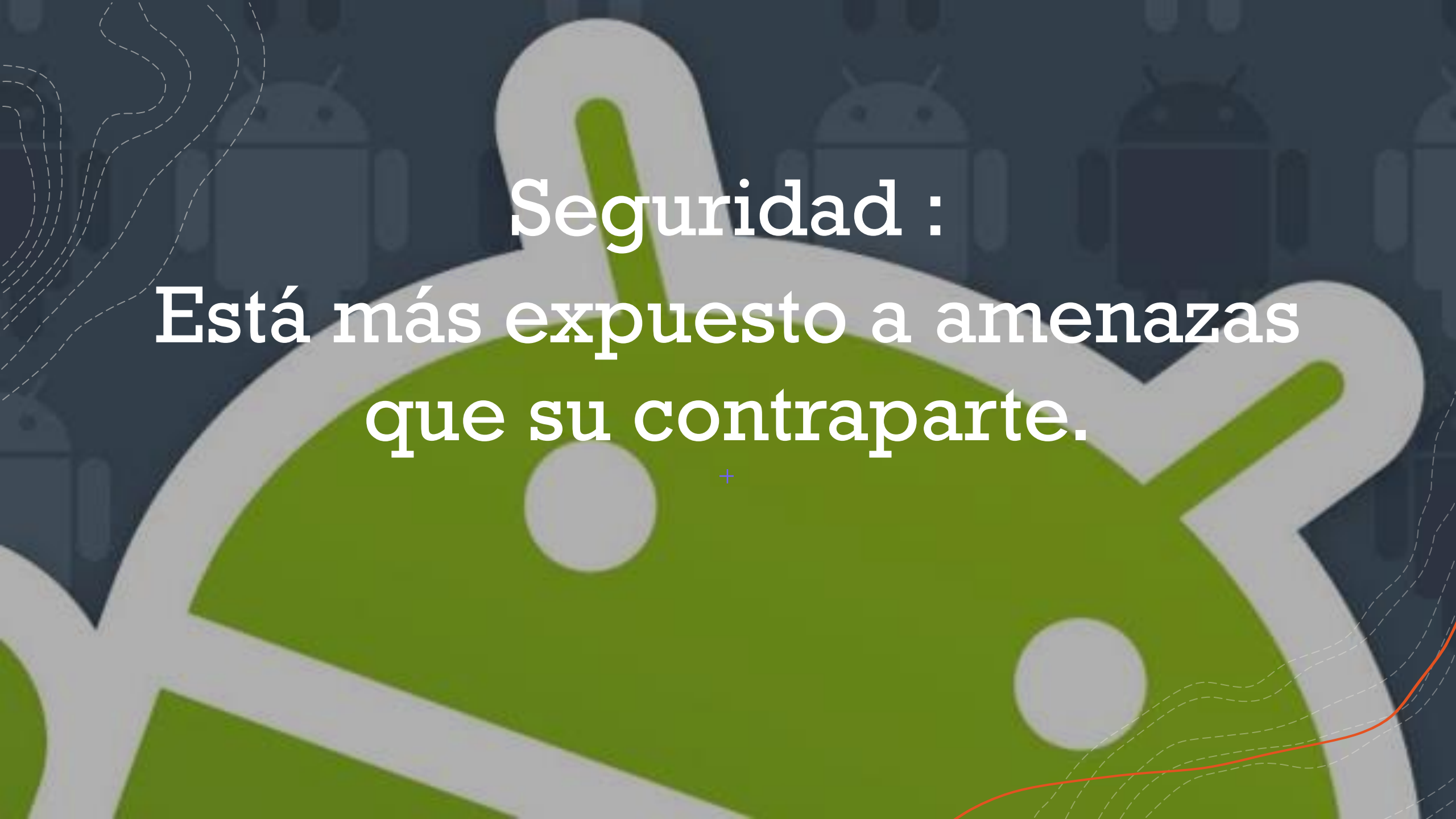
- + Otras prestaciones de este SO son su navegador de internet Google Chrome y su catálogo de aplicaciones **Google Play**, presente en todas sus versiones; su capacidad para mostrar imágenes y reproducir video y sonidos en una inmensa cantidad de formatos, y su soporte para distintas tecnologías nuevas.





CARACTERÍSTICAS

- **Disponible en la mayoría de los dispositivos móviles.**
- **Se puede descargar sin coste, y ya viene instalado en muchos equipos.**



Seguridad :
Está más expuesto a amenazas
que su contraparte.

+



SU USO

Es fácil de dominar para el público en general y cuenta con una gran cantidad de aplicaciones gratuitas y de paga.

ANDROID




VERSIONES

- + En su corta, pero exitosa trayectoria, ha desarrollado muchas versiones distintas. En orden cronológico, son: Banana Bread, Cupcake, Donut, Eclair, Froyo, Gingerbread, Honeycom, Ice Cream Sandwich, Jelly Bean, KitKat, Lollipop, Marshmallow, Nougat, Oreo, Pie, 10 y 11.

VENTAJAS

Es de código libre, así que cualquier persona con los conocimientos suficientes puede crear una aplicación.



Ofrece libertad al propietario del dispositivo para instalar la aplicación que desee, ya sea desde Play Store o a través de un archivo ejecutable.



La interfaz es altamente personalizable, lo que significa que puede adaptarse a las preferencias de cada usuario.

DESVENTAJAS

Acceder a las actualizaciones del sistema operativo depende del fabricante, lo que impide a muchos usuarios disfrutar del software más reciente.

La gran apertura de lo expone más que otros SO a los ciberataques.

Al no verificar cuidadosamente la calidad del software de terceros, algunas de las aplicaciones de la tienda en línea dejan mucho que desear.

ÚLTIMA VERSIÓN

VERSIÓN 11

Dato: Hasta la fecha la versión más utilizada sigue siendo Android 10



CIBERSEGURIDAD



¿QUÉ ES LA CIBERSEGURIDAD?

La ciberseguridad es la práctica de proteger los sistemas importantes y la información confidencial de los ataques digitales. También conocida como seguridad de la tecnología de la información (TI)



MEDIDAS DE SEGURIDAD

Las medidas de Ciberseguridad o seguridad cibernética están diseñadas para combatir las amenazas contra sistemas en red y aplicaciones, ya sea que esas amenazas se originen dentro o fuera de una organización.

¿CÓMO TRABAJA?

La ciberseguridad trata de trabajar en robustos sistemas que sean capaces de actuar antes, durante y después, no sirve solo para prevenir, sino también dar confianza a los clientes y al mercado, pudiendo así reducir el riesgo de exposición del usuario y de los sistemas.

LOS CIBERDELINCUENTES

Los ciberdelincentes se enfocan en obtener la información de identificación personal (PII) de los clientes: nombres, direcciones, números de identificación nacional (por ejemplo, números de seguridad social en los EE. UU., códigos fiscales en Italia) e información de tarjetas de crédito para posteriormente vender estos registros en mercados digitales clandestinos.



Los expertos en la ciberseguridad se encuentran muy demandados en el mercado laboral, y cada día este número aumenta.

Las empresas necesitan de estos profesionales ya que saben que la prevención es la clave para proteger la información y no verse inmiscuido en situaciones de debilidades con secuelas inmensas para dichas empresas. Por tanto, estar formado en ciberseguridad es una muy buena opción para encontrar empleo a día de hoy.



EL PERFIL DE CIBERSEGURIDAD: LO MÁS DESEADO

HERRAMIENTAS PARA AUMENTAR LA SEGURIDAD

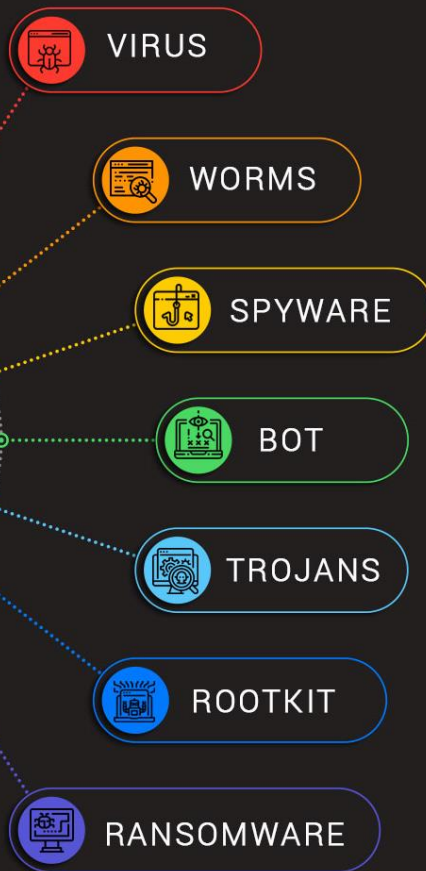


LA PROTECCIÓN CONTRA EL CÓDIGO MALICIOSO MALWARE:

Comúnmente se conoce como antivirus, este tipo de seguridad **es imprescindible para cualquier organización**, sin importar su actividad o tamaño, además es importante ir mas allá de sistemas informáticos, puesto de trabajos o servidores, y reunir todos los aspectos que se relacionan con la movilidad. La gran cantidad de distintos tipos de malware y su evolución, se transforman en una de las amenazas más difíciles de lidiar.



TYPES OF MALWARE



TIPOS DE MALWARE

LA PROTECCIÓN ANTIFRAUDE O PISHING :



Esta es una de las más importantes, el sentido común. El engaño, se ha convertido en una de las prácticas más usadas en internet, tanto para infectar miles de dispositivos, como para conseguir datos de los usuarios. Aquí no existen herramientas para combatir estas amenazas, se tiene que contar con el sentido común y desconfiar de lugares sospechosos.

PHISHING

Frases comunes



Acceda al siguiente **enlace** para conocer sus adeudos.



Presione **clic aquí** para **descargar** su estado de cuenta.



Multa por incumplimiento de obligaciones fiscales.



Evite sanciones, revise por favor el **documento anexo**.



UnAm
La Universidad
de la Nación

SER PREVISIVOS

Estas herramientas constan en conseguir por varios medios la supervivencia de la organización o empresa, después de un inconveniente de seguridad, dentro de esta solución se encuentran, copias de seguridad en la nube o en otros dispositivos, que mantienen a salvo la información de la empresa, la cual es indispensable para poder desempeñar sus funciones. También existen otras soluciones como las herramientas de recuperación de sistemas, la cual permiten restaurar un sistema desde un punto antes del ataque para perder el menor número posible de datos.



PROTECCIÓN DE COMUNICACIONES:

Estas soluciones se encargan de proteger a la organización de un grupo de amenazas, como los ataques de denegación de servicios, accesos no autorizados o la interceptación de las comunicaciones. También debemos de tener en cuenta que las amenazas no solo pueden partir desde Internet, sino también del interior de las empresas, es por ello que la protección de las comunicaciones es imprescindible cuando existen varias oficinas o sedes en varias partes del mundo, cuando se realizan diariamente a través de internet.

DOMINIOS DE CIBERSEGURIDAD



Una estrategia de ciberseguridad sólida tiene capas de protección para defenderse de los delitos cibernéticos, incluyendo aquellos que intentan acceder, cambiar o destruir datos, extorsionar a los usuarios o la organización, o interrumpir las operaciones empresariales normales. Las contramedidas deben abordar:



SEGURIDAD DE INFRAESTRUCTURA FUNDAMENTAL

Prácticas para proteger los sistemas informáticos, las redes y otros activos de los que depende la sociedad para la seguridad nacional, la economía y/o la seguridad ciudadana.



SEGURIDAD DE LA RED



Medidas de seguridad para proteger una red informática de intrusos, incluidas tanto las conexiones por cable como inalámbricas (Wi-Fi).

The background of the slide features a glowing pink padlock in the upper left quadrant. The entire background is a dark blue field filled with binary code (0s and 1s) and a glowing cyan fingerprint pattern in the lower right. A black rectangular box on the right side contains the title and a paragraph of text.

SEGURIDAD DE LA APLICACIÓN

Procesos que ayudan a proteger las aplicaciones que operan en entornos locales y en la nube. La seguridad debe integrarse en las aplicaciones en la etapa de diseño, teniendo en cuenta cómo se gestionan los datos, la autenticación del usuario, etc.

SEGURIDAD EN LA NUBE

Información verdaderamente confidencial que cifra los datos en la nube en reposo (almacenados), en movimiento (mientras migran hacia, desde y dentro de la nube) y en uso (durante el procesamiento) para garantizar la privacidad del cliente y cumplir con los requisitos comerciales y los estándares de conformidad regulatoria.



Medidas de protección de datos, como el Reglamento General de Protección de Datos o RGPD, que protegen sus datos más confidenciales contra el acceso no autorizado, la exposición o el robo.



SEGURIDAD DE INFORMACIÓN

EDUCACIÓN DEL USUARIO FINAL

Crear conciencia sobre la seguridad en toda la organización para fortalecer la seguridad de los puntos finales. Por ejemplo, se puede capacitar a los usuarios para eliminar archivos adjuntos de correo electrónico sospechosos, evitar el uso de dispositivos USB desconocidos, etc.



RECUPERACIÓN DE DESASTRES/ PLANIFICACIÓN DE LA CONTINUIDAD DEL NEGOCIO

Herramientas y procedimientos para responder a eventos no planificados, como desastres naturales, cortes de energía o incidentes de ciberseguridad, con una interrupción mínima de las operaciones principales.



ACTIVIDAD:

1- Responder cuestionario en el Aula del Campus para la asistencia:

2- En grupo realizar la siguiente actividad: enviar al correo de la profesora en formato pdf o doc. Word. Fecha de entrega 10/10. Nombre del grupo y alumnos que participaron

A -Realizar un cuadro comparativo entre las características y requerimientos del Sistema Andoide 10 y 11.

B - Realizar un cuadro comparativo con los Malware que pueden dañar nuestra seguridad. Puedes usar un mapa mental para realizar este punto.

C- Desarrollar 2 o 3 Malware (exponemos la próxima clase por grupo)