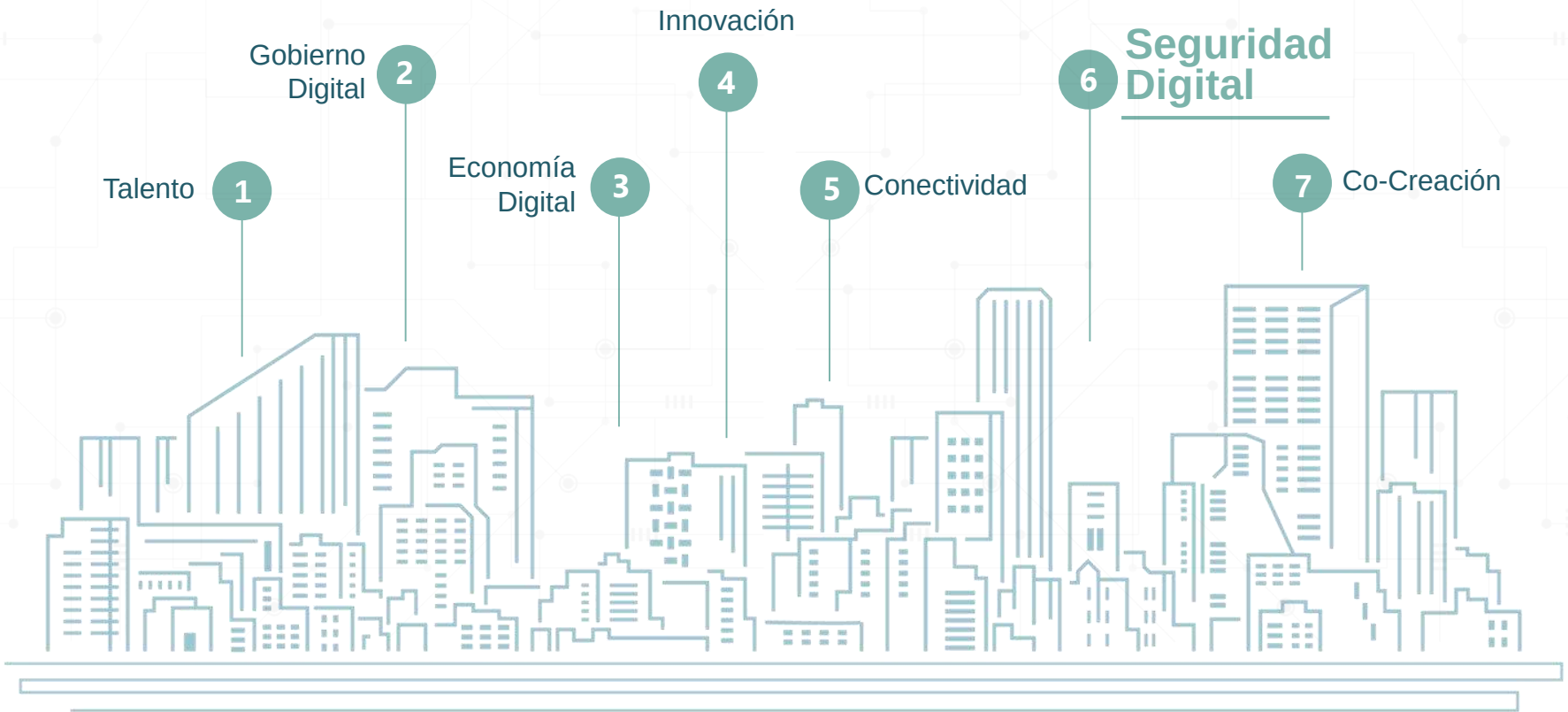
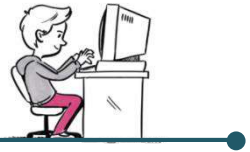
CIBERSEGURIDAD

Una **sociedad digital** construida de la mano con el sector privado



Historia de la Ciberseguridad

5 generaciones



Los ataques de virus en ordenadores independientes comenzaron como bromas o con afán destructivo.
Para detenerlos se desarrollaron productos antivirus.

VIRUS

Gen 1

Finales de **1980**

Los hackers pueden conectarse desde internet.
Nace la industria de la seguridad en red y se lanza el primer firewall.

REDES

Gen 2

Mediados de **1990**

Redes y software para explotar vulnerabilidades en toda la infraestructura de TI.
Se impulsan productos de sistemas para prevención de intrusiones (IPS).

APP´s

Gen 3

Principios del **2000**

Espionaje internacional, brechas masivas de información personal y la interrupción de Internet a gran escala.
Con esto se introdujo el 'sandboxing' y 'Anti-bot'

CARGA ÚTIL

Gen 4

Aprox. **2010**

Las herramientas de hacking avanzadas 'de grado militar' se filtran.
Se desarrolla una arquitectura unificada con soluciones avanzadas de prevención de amenazas en tiempo real.

MEGA

Gen 5

Aprox. **2017**

Fuente: Check Point Software Technologies LTD, 2019

Entendiendo los **Ciberataques**

¿En Dónde puede ser el ataque?

IoT

Networks

The Cloud

Attack Venue

¿A Qué?

- Hardware
- Firmware
- Operating System
- Application Software

¿A Quién?

Destino de ataques

Impacto

Seguridad Informática

Cibercrimen roba **3 mil mdd** y ya supera en ganancias al narcotráfico

70% de las organizaciones cree que su riesgo de seguridad creció considerablemente en el 2020.

Costo global del cibercrimen **$445 Billones de dolares**

43% de los ciberataques afectan a pequeños negocios.

Las empresas gastan un estimado de **$2.4 millones en defensa.**

Ataques más frecuentes son de malware y aquellos basados en la web. Las empresas gastan **$2.4 millones en defensa.**

Se proyecta que el daño relacionado a ciberataques llegará a los **$6 trillones de dólares anuales para el 2021**.

A una compañía le toma entre **6 meses**, o 197 días, detectar una **brecha de seguridad**.

Fuente: Interpol, Ponemon Institute,2017/ Small Business Trends, 2019/ Accenture, 2019/ CyberSecurity Ventures/ Time, 2019

Cibercrimen

Durante COVID-19

Los correos electrónicos de phishing han aumentado un 700%

El spam y las detecciones oportunistas aumentaron en un 26,3%,

El malware aumentó 35,16%

Aplicaciones de videoconferencia experimentan una violación de seguridad a medida que el número de usuarios aumentó un 300%

La suplantación aumentó 30,3%,

El bloqueo de los clics de URL en un 55,8%.

Fuente: Forbes

Colombia

Hoy

Comparativo denuncias enero a mayo
-2019: **7.197**
-2020: **10.503**
Implica un incremento del 46%

Principales delitos:
-Hurto por medios informáticos: **3803**
-Intrusiones: **1893**
-Violación de datos personales: **1764**
-Fraude: **1430**

Delitos que más se incrementaron:
-Suplantación de sitios web para capturar datos personales: **339%**
-Acceso abusivo a un sistema informático: **52%**
-Violación de datos personales: **51%**
-Hurto por medios informáticos y semejantes: **9%**

Comparativo de incidentes enero a mayo:
-2019: **7.393**
-2020: **3.751**
Implica una disminución del 49%

Sectores más afectados:
-Ciudadano: **2.397**
-Financiero: **384**
-Gobierno: **184**
-Educativo: **107**
-Salud: **28**

POLÍTICA PÚBLICA
de Transformación Digital para la 4IR

ODS impactados con la política de Transformación Digital

Plan Nacional de Desarrollo

147: Artículo de Transformación Digital
12 Principios que orientan los proyectos de Transformación Digital

Directivas y Decretos

Directiva Presidencial Gov.Co
Decreto para Servicios Ciudadanos Digitales

Nuevas Políticas

- Marco Ético
- Inversión
- Regulación Inteligente
- Talento

CONPES Transformación Digital + IA
CONPES de Confianza y Seguridad Digital
Convenio de Budapest
CONPES de Big Data (Actualización)
Lineamientos Base Políticas Blockchain
Plan 5G (IoT)
CONPES de Tecnologías para Educar

Fuente: Proyecto de Ley N° 311 de 2019 Cámara - 227 de 2019 Senado

Siguiente nivel de la CIBERSEGURIDAD

Seguro

Integrar la ciberseguridad en todo desde el principio

Desarrollar mejores formas de administrar los datos

Vigilante

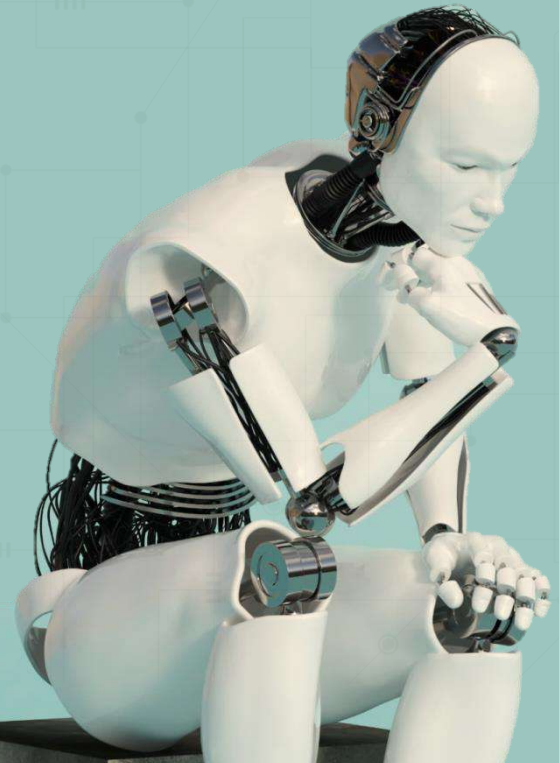
Utilizar tecnologías avanzadas para identificar y cazar amenazas de manera proactiva

Comprender y abordar las amenazas exponenciales

Resiliente

Desarrollar playbooks de amenaza y situaciones especificas

Desarrollar un enfoque de respuesta



El futuro digital debe ser *inclusivo*; segundo, la ***confianza*** es la base de todas y cada una de las interacciones; y tercero, se necesita un mundo digital *sostenible*, en términos sociales, económicos y medioambientales

"Foro Económico Mundial - *Our Shared Digital Future Building an Inclusive, Trustworthy and Sustainable Digital Society*"