Ciberseguridad

implicaciones y retos en la sociedad del conocimiento.

Los temas asociados a la ciberseguridad vienen cobrando vital importancia en la sociedad del conocimiento en la que vivimos actualmente. Con los avances tecnológicos y la creciente dependencia al internet, es imprescindible entender las implicaciones y retos que surgen en este ámbito, así como adoptar medidas de prevención adecuadas.

La ciberseguridad se define de acuerdo con el Consejo Nacional de Política Económica y Social (CONPES) 3701 (2011) como la "capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos ante amenazas o incidentes en materia cibernética" (p. 2). En Colombia el tema ha cobrado gran relevancia debido a los ataques contra entidades del estado presentados en los últimos meses.

Estadísticas de Molano (2023) evidencian que alrededor del 91% de los ataques cibernéticos se dan por errores humanos a partir de técnicas como el *phishing*[1] . A continuación, en la Figura 1, se puede ampliar la información sobre la ciberseguridad en Colombia.

Figura 1. Estadísticas en Colombia sobre ciberseguridad.

Fuente: (Molano, 2023).

Las implicaciones de la ciberseguridad son numerosas y afectan diferentes aspectos de la vida cotidiana. De un lado, la protección de la información personal se vuelve fundamental en un mundo digitalizado donde los datos personales están expuestos a posibles ataques cibernéticos que pueden comprometer la privacidad y seguridad. Ante esto se hace necesario tomar medidas para proteger la identidad en línea y evitar ser víctimas de robo de información o suplantación.

Otro aspecto importante a tener en cuenta es la protección de la información sensible de las empresas e instituciones. La ciberdelincuencia se ha convertido en una amenaza constante para las organizaciones, ya que los ciberdelincuentes buscan acceder a datos confidenciales o sabotear sistemas informáticos con el fin de robarlos y posteriormente exigir altas sumas de dinero para su rescate, también es común, robar datos para suplantar la identidad para contratar servicios de pago o simplemente venderlos a terceros. Esto puede tener consecuencias graves, tanto económicas como reputacionales, por lo que empresas y personas pueden implementar medidas de seguridad tales como evitar conectarse a redes públicas o gratuitas de wifi, no descargar archivos de correos de los cuales se desconoce el remitente, no instalar aplicaciones de fuentes desconocidas y utilizar contraseñas seguras (mínimo 10 caracteres que incluyan letras, números y caracteres especiales) para prevenir posibles ataques.

Además, la ciberseguridad también tiene implicaciones en el ámbito político y de estabilidad nacional. Los ciberataques pueden ser utilizados como medio para desestabilizar países (ataques a entidades públicas) o interferir en procesos electorales. Por lo tanto, es fundamental que los gobiernos y las instituciones internacionales trabajen de manera conjunta para prevenir y combatir este tipo de amenazas.

Tipos de riesgos que se presentan con el uso de internet

Ciberacoso

También llamado *cyberbullying*, es una forma de ejercer acoso a otros por medio de redes sociales y/o medios digitales. Normalmente, quienes lo ejercen no muestran su identidad, pero pueden generar graves efectos psicológicos a sus víctimas.

De acuerdo con el informe de Bullying sin fronteras (2023) Colombia ocupa el puesto número 9 de 30 en el mundo con 41.500 casos graves de *bullying* y *ciberbullying* en el último año. Esta cifra aumentó en más de un 500 por ciento con relación al informe anterior (8.981 casos).

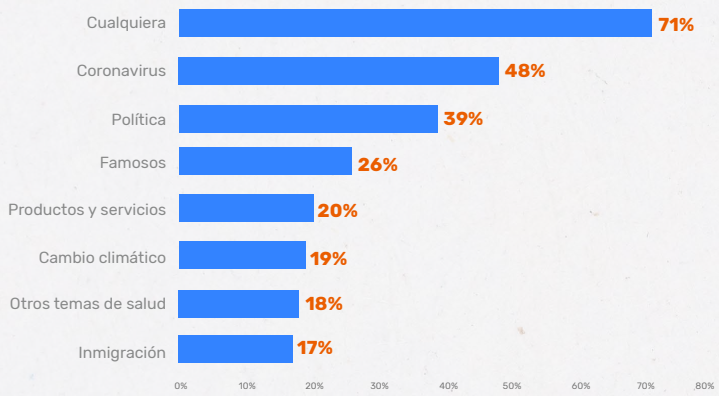
Noticias falsas:

Conocidas también como *fake news*, son contenidos engañosos que buscan distorsionar la realidad de algún tema, generando información falsa o distorsionada. En Colombia se ha vuelto frecuente usar este tipo de contenidos en las contiendas electorales.

Es importante ser conscientes de la información que se recibe a través de las redes sociales y verificar mediante diferentes fuentes la veracidad de esta. De hecho, información relacionada con el coronavirus y política fueron las más consumidas por la población en general. En la Figura 2, se muestran las temáticas de las cuales se generaron más noticias falsas en 2022.

1. Práctica fraudulenta que suplanta la identidad de una organización o persona con el fin de acceder a datos privados, personales y/o bancarios.

Figura 2. Porcentaje de población que consumió información falsa o engañosa en el mundo en 2022, por temática informativa.



Fuente: (Statista, 2023).

Sexting

El acto de enviar fotos de carácter sexual a otras personas mediante dispositivos electrónicos. Aunque esta práctica es una decisión personal, es riesgosa ya que las fotos pueden ser compartidas sin el consentimiento de quien las envía.

De acuerdo con un estudio realizado por la Universidad de Medellín (2022), los y las adolescentes entre 14 y 15 años participan más del sexting. En Colombia, "el 15% de estos han enviado o reenviado fotos o vídeos con contenido sexual; el 24,8% ha recibido este tipo de contenidos y el 29,4% exhibió conductas de sexting" (Morillo Puente et al., 2022, p. 1). Además, que las mujeres tienen una tendencia mayor a este tipo de conductas con una participación del 56% según las cifras de estudio siendo a su vez, las más vulnerables.

Algunas recomendaciones para proteger la información propia y ajena

A medida que la tecnología avanza, también lo hacen las amenazas cibernéticas, lo que implica que se deben tomar las medidas necesarias para proteger la información personal, organizacional y estatal y garantizar la seguridad en línea.

Es fundamental comprender los riesgos que existen en torno a la ciberdelincuencia en la era digital. La amenaza de ataques cibernéticos está presente constantemente, lo que significa que se debe estar conscientes de los peligros a los que se expone al utilizar internet y las diversas plataformas digitales. El conocimiento sobre los riesgos es un primer paso crucial para la protección.

Además, es importante familiarizarse con la normativa vigente en materia de ciberseguridad. Existen leyes y regulaciones que buscan proteger a las y los usuarios y garantizar la seguridad de la información en el ámbito digital. Comprender y cumplir con estas normativas brinda una base sólida para proteger nuestra información de manera efectiva. En Colombia, la Ley 1273 de 2009 establece normas sobre delitos informáticos y define los tipos penales relacionados con el acceso no autorizado a sistemas informáticos, daño y sabotaje informático, uso de software malicioso, entre otros.

Otro aspecto importante es la protección de los dispositivos electrónicos. Es recomendable contar con sistemas de seguridad confiables, como antivirus y *firewall* [2], que ayuden a prevenir la entrada de *malware* [3] y otros programas maliciosos en los dispositivos. Además, es importante mantener estos sistemas actualizados, ya que los ciberdelincuentes están constantemente buscando vulnerabilidades en el software.

La educación también juega un papel fundamental en la protección de nuestra información en línea. Es importante ser conscientes de las prácticas recomendadas para navegar por internet y evitar caer en las trampas de los estafadores. Suele ser común que en países hispanoparlantes el uso de las contraseñas para acceder a cuentas, portales o plataformas, no sea un tema cuidado por los usuarios, valiéndose de información genérica o que se utiliza de forma indiscriminada.

Figura 3. Contraseñas más usadas en países hispanohablantes.

Colombia

1	123456	<1
2	password	<1
3	123456789	<1
4	12345678	<1
5	12345	<1

Chile

1	123456	<1
2	123456789	<1
3	12345678	<1
4	12345	<1
5	1234	<1

México

1	123456	<1
2	110110jp	3
3	123456789	<1
4	america1	<1
5	12345	<1

España

1	123456	<1
2	123456789	<1
3	swing	6
4	1234	<1
5	12345678	<1

*Basado en la evaluación de una base de datos de 3TB procedentes de 30 países.
Fuente: NordPass

Tiempo para descifrarla (en segundos)

Fuente: (Statista, 2023).

2. Programa informático que controla el acceso de una computadora a la red y de elementos de la red a la computadora, por motivos de seguridad

3. Software malicioso.

Aprendiendo definiciones y algunas diferencias:

Ciberseguridad: práctica de defender todo tipo de dispositivo (servidores, computadoras), sistemas electrónicos, redes y datos a través del uso de tecnologías y/o prácticas ofensivas de ataques maliciosos que llevan a cabo los cibercriminales.

Seguridad informática: disciplina que se encarga de proteger la integridad y privacidad de la información que se almacena en los sistemas informáticos.

Seguridad en la información: elementos para la prevención y reacción en pro de salvaguardar la información, además de generar lineamientos para su almacenamiento, procesamiento o transmisión.

Hacker: persona con conocimientos en modificar sistemas pero que los usa para detectar brechas de seguridad en los mismos.

Cracker: persona que se aprovecha de sus conocimientos para romper o vulnerar la seguridad de un sistema, generalmente para obtener un beneficio económico.

En conclusión, la ciberseguridad es una preocupación creciente en todos los países, especialmente, en Colombia donde aún existe mucha vulnerabilidad y desconocimiento al respecto. Sigue siendo importante que las organizaciones y las personas tomen medidas para protegerse contra las amenazas cibernéticas. Los elementos clave para hacer frente a estos retos son la educación, la inversión en tecnologías para la seguridad y la colaboración.

Desde Sapiencia

Se propende por la ciberseguridad y las buenas prácticas en la web. A través del programa Talento Especializado se promueve la formación en cursos cortos como Seguridad para bases de datos, Redes y ciberseguridad y otros relacionados con redes e internet, en los cuales 295 personas de estratos 1, 2 y 3, principalmente, se han matriculado en estas competencias, promoviendo así las buenas prácticas en el Distrito de Ciencia, Tecnología e Innovación.

Referencias:

Bullying sin fronteras. (2023). Estadísticas mundiales de bullying 2022/2023. https://bullyingsinfronteras.blogspot.com/2018/11/estadisticas-de-bullying-en-colombia.html#:~:text=COLOMBIA%3A,informe%20anterior%20(8.981casos)

CONPES 3701. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

Lisa Institute. (s.f.). Diferencia entre Ciberseguridad, Seguridad Informática y Seguridad de la Información. https://www.lisainstitute.com/blogs/blog/diferencia-ciberseguridad-seguridad-informatica-seguridad-informacion?_pos=1&_sid=00aec10f5&_ss=r

López Orozco, R. (s.f.). Ciberseguridad: cómo protegerte en internet. Unicef. https://www.unicef.org/mexico/ciberseguridad

Molano, D. (2023, 28 de junio). Ciberseguridad en Colombia [sesión de conferencia – foro virtual]. La seguridad de la información en la era de la inteligencia artificial.

Morillo Puente, S., Ríos Hernández, I. N., Henao López, G. C. (2022). Evaluación empírica del sexting y las actividades rutinarias de los adolescentes en Colombia. OBETS. Revista De Ciencias Sociales, 17(2), 285-304. https://doi.org/10.14198/OBETS2022.17.2.07

Statista. (2023). Las contraseñas más usadas en países hispanohablantes. https://es.statista.com/grafico/29993/contrasenas-mas-usadas-en-2022-en-en-algunos-paises-hispanohablantes/

Statista. (2023). Porcentaje de población que consumió información falsa o engañosa en el mundo en 2022, por temática informativa. https://es.statista.com/estadisticas/1347026/consumo-mundial-de-noticias-falsas-o-enganosas-por-tematica-informativa/