Cultura de Seguridad Digital en Estudiantes Universitarios: Estudio Descriptivo en la Corporación Universitaria Reformada (CUR)

Autores:

Jesús Bolaño

Orlando Altamar

Tutores:

Jonathan Quant

Hernando Domínguez

Corporación Universitaria Reformada.

Ingeniería Informática.

Facultad de Ingeniería.

Barranquilla, Colombia.

Noviembre 2025.

Tabla de contenido

Tabla de ilustraciones

1. Planteamiento del problema

En la actualidad, los entornos educativos utilizan de forma constante plataformas virtuales y redes sociales para el desarrollo de actividades académicas. No obstante, esta dependencia tecnológica ha expuesto a los estudiantes universitarios a riesgos cibernéticos como el robo de información, el phishing, la suplantación de identidad y el mal uso de contraseñas. A pesar de ello, muchos jóvenes no reconocen la importancia de la seguridad digital, adoptando prácticas inseguras como reutilizar la misma contraseña en varias plataformas o divulgar información personal sin precaución.

En este contexto, surge la necesidad de estudiar el nivel de cultura de seguridad digital en los estudiantes de la Corporación Universitaria Reformada (CUR), identificando sus hábitos, percepciones y conocimientos para establecer estrategias de mejora que contribuyan a la formación de usuarios digitales más responsables y conscientes. Esta situación se ve reforzada por la limitada formación en temas de seguridad digital dentro del ámbito académico y la creencia de que la ciberseguridad es un asunto exclusivamente técnico, lo que genera desinformación y una baja percepción del riesgo. Como resultado, los estudiantes se enfrentan a consecuencias como la exposición a fraudes, la pérdida de información personal, el deterioro de su reputación digital y una mayor vulnerabilidad frente a amenazas cibernéticas.

En el documento CONPES 3995 de 2020, “Política Nacional de Confianza y Seguridad Digital”, se define que “la seguridad digital es la situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), derivada de la realización de los fines esenciales del Estado mediante: la gestión del riesgo de seguridad digital, la implementación efectiva de medidas de ciberseguridad, el uso efectivo de las capacidades de ciberdefensa.”

Según el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), “la población de jóvenes y adultos con habilidades TIC básicas es de 34,7 % en Colombia; con habilidades intermedias 26,4 % y con habilidades avanzadas apenas 4,6 %”. Además, el MinTIC

reporta que en 2024 Colombia enfrentó cerca de 36 000 millones de intentos de afectación cibernética, lo que evidencia la magnitud del reto en materia de seguridad digital para el país.

2. Formulación del Problema

¿Cuál es el nivel de cultura de seguridad digital en los estudiantes universitarios de la Corporación Universitaria Reformada (CUR)?

3. Justificación.

La presente investigación busca contribuir al fortalecimiento de una cultura de seguridad digital entre los estudiantes universitarios, fomentando el uso responsable, ético y seguro de las tecnologías de la información y la comunicación (TIC).

De acuerdo con el CONPES 3995 (2020) y la Ley 1581 de 2012, la protección de los datos personales y la formación de ciudadanos digitales conscientes constituyen objetivos prioritarios dentro de la Política Nacional de Seguridad Digital. En este sentido, el proyecto no solo aborda una necesidad educativa, sino también social e institucional, al promover competencias que permitan reducir los riesgos asociados al uso indebido de la información.

Los resultados obtenidos podrán servir como base para la implementación de campañas institucionales, talleres formativos y políticas de seguridad digital orientadas al fortalecimiento de la conciencia cibernética en la comunidad académica. De esta manera, se espera contribuir al desarrollo de entornos digitales más seguros y confiables dentro de la educación superior.

4. Objetivos

4.1 OBJETIVOS GENERAL

Determinar el nivel de cultura de seguridad digital en los estudiantes de la Corporación Universitaria Reformada (CUR)

4.2 Objetivos específicos

1. Diagnosticar los niveles de conocimiento.

2. Analizar las consecuencias derivadas del desconocimiento.

3. Diseñar una propuesta de sensibilización institucional que promueva hábitos seguros en el uso de internet y redes sociales.

5. Hipótesis y variables

Hipótesis general: A menor conocimiento sobre seguridad digital, mayor exposición a riesgos cibernéticos entre los estudiantes universitarios.

Variable independiente: Nivel de conocimiento en seguridad digital.

Variable dependiente: Grado de exposición a riesgos cibernéticos.

6. Marco de referencia

6.1 Marco conceptual

El marco conceptual reúne los principales términos, categorías y constructos que sustentan la comprensión del fenómeno estudiado: la cultura de seguridad digital en estudiantes universitarios. Cada concepto se articula con la problemática planteada, permitiendo definir los elementos necesarios para interpretar los resultados y orientar el análisis.

- **Cultura Digital**: Hábitos y valores asociados al uso responsable de la tecnología.
- **Contraseña segura**: combinación compleja que impide el acceso no autorizado.
- **Phishing**: Fraude digital que busca obtener datos personales mediante engaño.
- **Privacidad digital**: derecho de controlar el uso y divulgación de la información personal en línea.
- **Seguridad digital**: conjunto de medidas que protegen la información y los sistemas informáticos.

6.2 Marco teórico

La seguridad digital comprende el conjunto de estrategias, herramientas y hábitos que permiten proteger la información personal, académica y profesional frente a amenazas tecnológicas. Según González (2021), la falta de educación en ciberseguridad incrementa la vulnerabilidad de los usuarios, lo que demuestra la importancia de promover la formación continua en el uso responsable y seguro de las tecnologías de la información.

Según el CONPES 3995 (2020), la cultura de seguridad digital en Colombia tiene como propósito "garantizar un entorno digital confiable, promover el uso seguro de las tecnologías y fortalecer las capacidades de los ciudadanos frente a los riesgos del entorno digital". En este sentido, la seguridad digital no se limita a la implementación de medidas técnicas, sino que involucra un componente social y educativo orientado al desarrollo de competencias digitales seguras.

Asimismo, el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC, 2024) señala que el 34,7 % de la población colombiana posee habilidades TIC básicas, el 26,4 % habilidades intermedias y únicamente el 4,6 % habilidades avanzadas, lo cual evidencia una brecha significativa en la alfabetización digital y la formación en seguridad informática. Esta carencia de competencias digitales implica una mayor exposición a riesgos cibernéticos como el robo de información, el fraude electrónico y la vulneración de la privacidad.

A nivel internacional, el Cybersecurity Awareness Model propuesto por Jansen y Van Niekerk (2017) plantea que la conciencia en ciberseguridad se construye mediante la integración de tres componentes fundamentales: conocimiento, actitud y comportamiento. Dicho modelo sugiere que una persona digitalmente consciente no solo sabe cómo proteger su información, sino que adopta hábitos preventivos que disminuyen su exposición al riesgo.

De igual manera, el Digital Literacy Framework de la UNESCO (2018) enfatiza que la alfabetización digital no debe limitarse al uso técnico de las herramientas, sino incluir la comprensión crítica de los riesgos y responsabilidades del entorno digital. Esta perspectiva

promueve la idea de que la educación en seguridad digital debe ser parte integral de la formación ciudadana.

Por su parte, Safa, Maple y Watson (2016) afirman que la ausencia de conciencia sobre ciberseguridad dentro de las instituciones educativas está directamente asociada con un mayor número de incidentes informáticos, debido a la falta de políticas institucionales y programas de sensibilización. En consecuencia, el fortalecimiento de la cultura de seguridad digital desde la educación superior es esencial para reducir vulnerabilidades y promover comportamientos éticos y seguros en el ciberespacio.

En conjunto, estos aportes teóricos evidencian que el desarrollo de una cultura de seguridad digital debe abordarse como un proceso educativo, ético y social que permita a los estudiantes universitarios actuar de manera consciente, crítica y responsable dentro de los entornos tecnológicos actuales.

6.3 Marco legal

El proyecto se sustenta en las principales normas nacionales relacionadas con la protección de datos y la ciberseguridad en Colombia:

6.3.1 Ley 1273 de 2009: tipifica y sanciona delitos informáticos, creando un nuevo bien jurídico tutelado para preservar la confidencialidad, integridad y disponibilidad de los sistemas de información y las comunicaciones. Esta ley modifica el Código Penal e incluye artículos sobre delitos como el acceso abusivo a sistemas informáticos,

6.3.2 Ley 1341 de 2009: reorganiza las entidades del sector, promueve la competencia y la inversión, y establece principios para el acceso universal y la protección de los derechos de los usuarios. Esta ley fue creada para modernizar el sector, reducir la brecha digital y asegurar que las TIC sirvan al interés general.

6.3.3 Ley 1581 de 2012: establece los derechos y deberes para el tratamiento de información personal. Esta ley garantiza a los ciudadanos el derecho a conocer, actualizar y rectificar sus datos, y aplica a entidades públicas y

privadas que manejan bases de datos. La Superintendencia de Industria y Comercio (SIC) es la autoridad encargada de supervisar su cumplimiento y sancionar a quienes la infrinjan.

6.3.4 El Decreto 1377 de 2013 reglamenta parcialmente la Ley 1581 de 2012, precisando los procedimientos para la autorización, recolección y uso de los datos personales, su objetivo es desarrollar el derecho constitucional de las personas a conocer, actualizar y rectificar su información personal, y define aspectos clave como la autorización del titular, el tratamiento de datos, los derechos de los titulares, las transferencias internacionales de datos y la responsabilidad demostrada

6.3.5 Ley 1621 de 2013: Normas sobre inteligencia, contrainteligencia y protección de la información reservada, su objetivo es facilitar el cumplimiento de su misión constitucional y legal, garantizando que actúen con base en la proporcionalidad, la necesidad y con respeto por la Constitución. La ley también regula aspectos como la recolección, almacenamiento y depuración de datos, así como la protección de derechos humanos.

6.3.6 Decreto 1008 de 2018: establece los lineamientos generales de la Política de Gobierno Digital en Colombia, reemplazando la antigua estrategia de "Gobierno en Línea". Su objetivo es promover la transformación digital del Estado para mejorar la calidad de vida de los ciudadanos y la competitividad del país mediante el uso de tecnologías de la información y las comunicaciones (TIC) en un entorno de confianza digital.

6.3.7 CONPES 3995 de 2020: establece la Política Nacional de Confianza y Seguridad Digital en Colombia, con el objetivo de fortalecer la confianza y la seguridad en el entorno digital.

7. Metodología

El estudio se desarrollará bajo un enfoque mixto, de tipo descriptivo y exploratorio. La población estará conformada por estudiantes de la CUR de diferentes programas. Se aplicará una encuesta estructurada para recolectar datos cuantitativos y cualitativos sobre conocimientos, percepciones y hábitos de seguridad digital.

Los datos cuantitativos serán representados en gráficos estadísticos. Los resultados cualitativos se interpretarán mediante análisis de contenido, permitiendo identificar patrones y factores de riesgo.

8. Análisis y discusión de los resultados

El estudio realizado permite identificar el nivel de cultura digital y las prácticas de seguridad que tienen los participantes al interactuar en internet y redes sociales. Los resultados muestran una combinación de buenas intenciones, hábitos parcialmente adecuados y debilidades críticas, especialmente relacionadas con la formación y las prácticas preventivas.

Este análisis reúne todos los resultados de todas las imágenes.

1. Uso y gestión de contraseñas

✓ Resultados clave:

- **40%** casi nunca cambia sus contraseñas → *nivel malo*
- **49%** las cambia algunas veces al año → *regular*
- **12%** las cambia periódicamente → *bueno*

✓ Fortalezas:

- El **53%** utiliza contraseñas fuertes (pregunta 7).
- Algunos usuarios mencionan cambiar contraseñas, no dejarlas guardadas y hacerlas alfanuméricas.

❌ Debilidades:

- **No existe una cultura constante de cambio de contraseñas.**

- La mayoría depende de contraseñas fuertes, pero **no las actualiza**, lo cual reduce su efectividad.

2. Protección de información personal en internet

✓ Resultados:

- **74% considera muy importante proteger su información personal.**
- Solo **2%** afirma que no lo considera relevante.

✓ Fortalezas:

- Alta percepción de importancia.
- Muchos mencionan que no comparten datos personales o que verifican la autenticidad de las páginas.

❌ Debilidad crítica:

- Aunque reconocen su importancia, **no siempre actúan en consecuencia**, lo que refleja brecha entre *percepción* y *práctica*.

3. Identificación de mensajes sospechosos (phishing)

✓ Resultados:

- Malo: 12%
- Regular: 44%
- Bueno: 44%

✓ Interpretación:

- La mitad identifica correctamente intentos de phishing.
- La otra mitad presenta vulnerabilidad.

❌ Riesgo:

- Una parte importante podría caer en fraudes por no reconocer mensajes engañosos o enlaces maliciosos.

4. Formación o capacitación en seguridad digital

✓ Resultados:

- **47%** nunca ha recibido capacitación → *malo*
- **33%** ha recibido información básica → *regular*

- **21%** ha recibido capacitación formal → *bueno*

❌ **Conclusión:**

La falta de capacitación es un factor decisivo que explica:

- Contraseñas mal gestionadas
- Baja identificación de phishing
- Errores en manejo de enlaces
- Falta de protocolos de revisión de seguridad

5. Uso de contraseñas seguras

✓ **Resultados:**

- Malo: 0%
- Regular: 47%
- Bueno: 53%

Esto representa un punto fuerte: más de la mitad conoce y aplica criterios básicos de creación de contraseñas seguras, aunque no las cambie periódicamente.

6. Verificación de sitios web antes de ingresar datos (confiabilidad)

✓ **Resultados:**

- Malo: 12%
- Regular: 42%
- Bueno: 47%

✓ **Interpretación:**

La mayoría revisa mínimamente:

- El candado de seguridad
- La dirección correcta
- La fiabilidad del sitio

Pero un 54% aún lo hace de forma irregular o insuficiente.

7. Comportamientos reales (pregunta abierta)

Las 43 respuestas permiten identificar cinco patrones de comportamiento:

🔵 A. Prácticas básicas (más comunes)

Incluyen:

- Navegar en modo incógnito
- No brindar datos personales
- Revisar fuentes
- Evitar enlaces extraños

Estas prácticas son útiles, pero **no suficientes** para una protección sólida.

🔵 B. Prácticas intermedias

Algunos usuarios reportan:

- Uso de VPN
- Redes seguras
- Antivirus
- No conectar a Wi-Fi públicos

Indican intención de protección, aunque no sistemática.

🔵 C. Prácticas avanzadas (menos comunes)

Muy pocas respuestas incluyen:

- Contraseñas alfanuméricas complejas
- No dejar sesiones abiertas
- Actualización frecuente de software
- Revisión de opciones de rastreo

Son usuarios con mayor conocimiento digital.

🔵 D. Comportamientos de riesgo

Varios participantes expresaron:

- “Nada”
- “Casi nada la verdad”
- “No hago mucho”

- “Con la bendición de Dios”

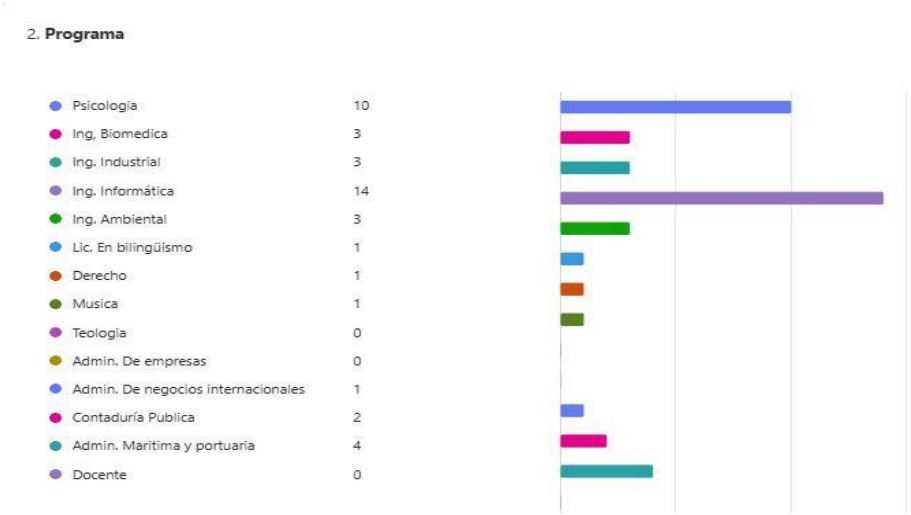
Este grupo es el más vulnerable a amenazas digitales.

🔵 E. Respuestas vagas o sin claridad

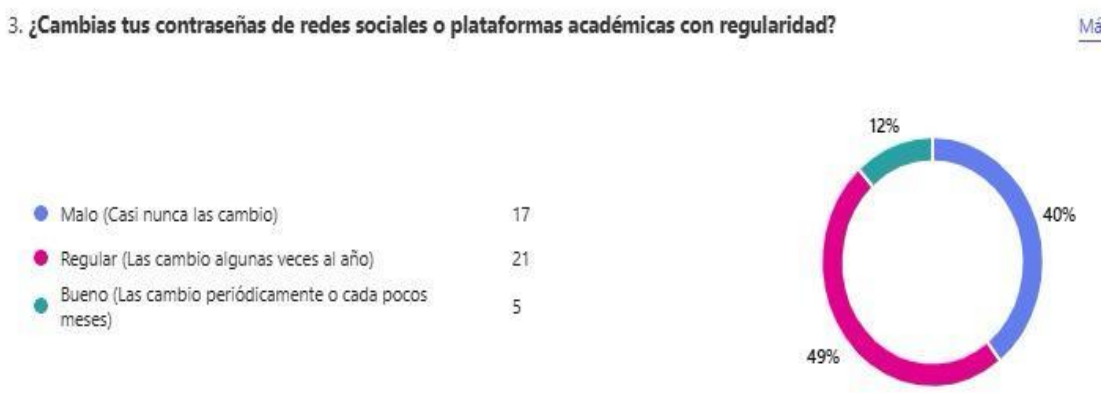
Ejemplos:

- “Muchas cosas”
- “Revisar ocasionalmente”
- “Leo bien”

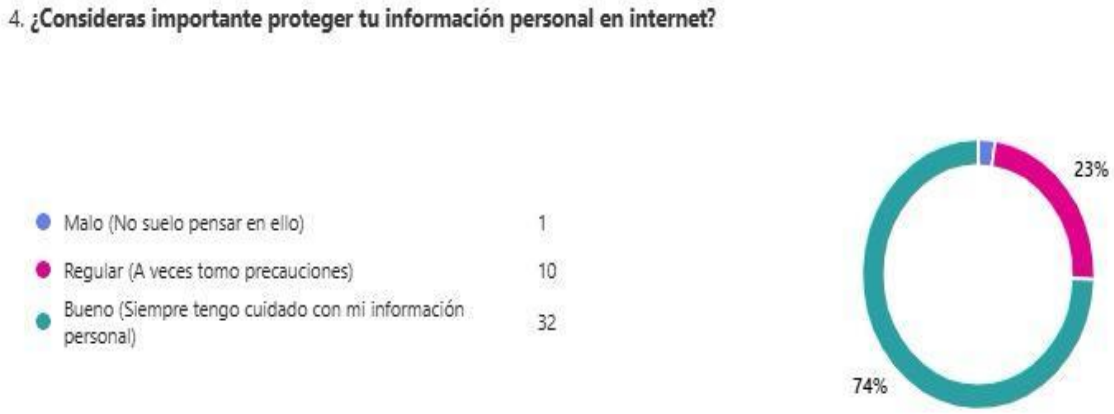
Evidencian falta de conocimiento o de hábitos consistentes.



1 Programa



2¿Cambias tus contraseñas de redes sociales o plataformas académicas con regularidad?

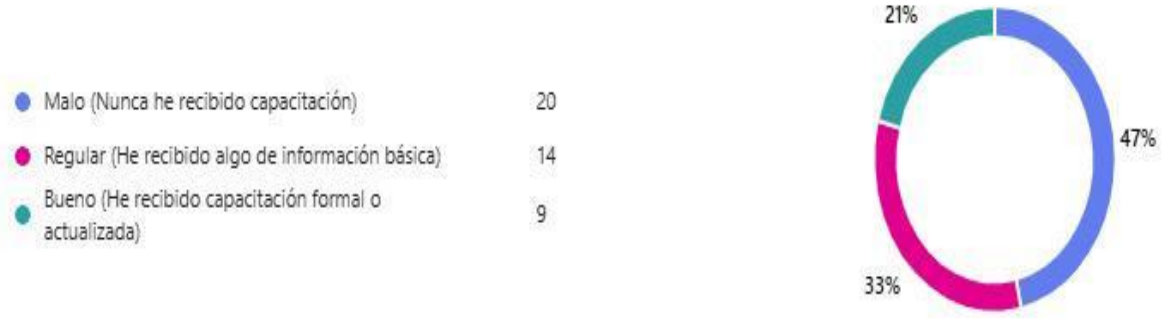


3 ¿Consideras importante proteger tu información personal en internet?

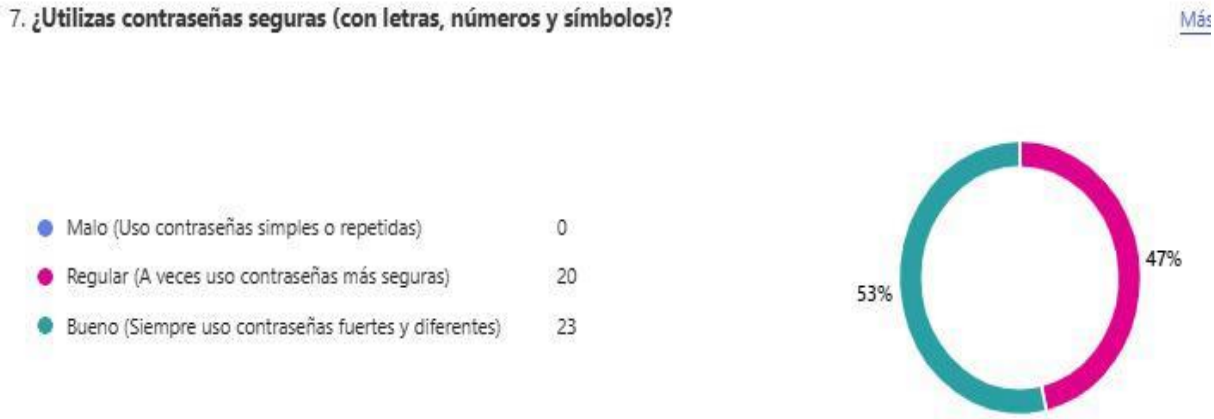
5. **¿Sabes identificar un enlace o mensaje sospechoso (phishing)?**

4 ¿Sabes identificar un enlace o mensaje sospechoso(phishing)?

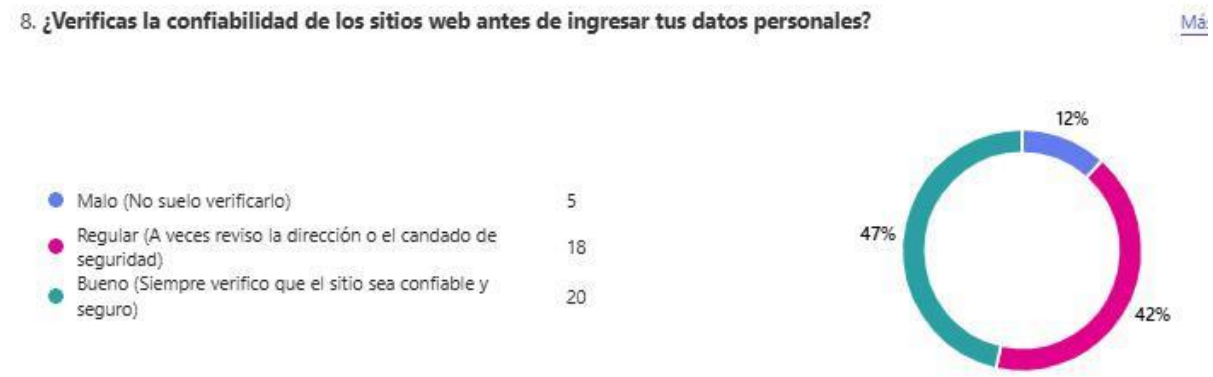
6. **¿Has recibido alguna capacitación o información sobre seguridad digital?**



5 ¿Has recibido alguna capacitación o información sobre seguridad digital?



6 ¿Utilizas contraseñas seguras (con letras, números y símbolos)?



7¿Verificas la confiabilidad de los sitios web antes de ingresar tus datos personales?

9. ¿Qué haces normalmente para cuidar tu información cuando usas internet o redes sociales? (Pregunta abierta)

43 Respuestas

ID ↑	Nombre	Respuestas
1	anonymous	Intento resguardar todo
2	anonymous	Uso algun vpn
3	anonymous	La mayoría de veces las hago en incógnito
4	anonymous	No subo datos personales y evito la ubicación en tiempo real. Evito promociones en páginas y evito los mensajes raros de bancos
5	anonymous	No coloco datos que ayuden a perjudicarme
6	anonymous	Estar en una red segura y proteger mis datos personales
7	anonymous	Cambiar las contraseñas y hacerlas de manera alfanuméricas.
8	anonymous	normal mente intento no dar mucha informacion personal y siempre rectifico si la pagina web en segura y es oficial
9	anonymous	No dejar mi inicio de sesión de mis cuentas de Google o cualquier cuenta guardada en PC
10	anonymous	Nada

8¿Qué haces normalmente para cuidar tu información cuando usas internet o redes sociales?

11	anonymous	No poner el wifi en todas partes
12	anonymous	No
13	anonymous	Pongo contraseñas seguras y entro en incógnito
14	anonymous	Cambio contraseñas, y no entro a links inseguros
15	anonymous	Cambio contraseña, e ingresar a sitios en modo incógnito
16	anonymous	Contraseñas
17	anonymous	Leo bien
18	anonymous	Verifico que todo está en orden
19	anonymous	Mirar que sea una página segura y confiable
20	anonymous	Tener cuidado donde ingreso
21	anonymous	Cambiar de contraseña y no dejar las claves guardadas
22	anonymous	Cambiarla

9 Ilustración.

23	anonymous	.
24	anonymous	Cambio contraseña
25	anonymous	No usar información personal
26	anonymous	Nada
27	anonymous	Nada, con la bendición de Dios
28	anonymous	No abrir enlaces jejej
29	anonymous	Reviso Fuentes
30	anonymous	Llaves y opciones de rastreos
31	anonymous	Nada
32	anonymous	No interactuo con desconocidos
33	anonymous	Casi nada la verdad
34	anonymous	Ver si es una red segura y confiable

10 Ilustra. Final

9. Análisis general de las consecuencias según los niveles de respuesta

1. ¿Cambias tus contraseñas de redes sociales o plataformas académicas con regularidad?

Malo (Casi nunca las cambia)

Consecuencias:

* Mayor probabilidad de robo de cuentas.

* Alto riesgo de secuestro de perfiles académicos.

* Vulnerabilidad ante ataques de fuerza bruta o filtraciones previas.

Regular (A veces las cambia)

Consecuencias:

* Seguridad moderada pero insuficiente a largo plazo.

* Riesgo de que una contraseña expuesta siga activa durante meses.

Bueno (Las cambia periódicamente)

Consecuencias:

* Menor riesgo de accesos no autorizados.

* Adecuada protección contra filtraciones antiguas.

* Mejora la higiene digital general.

2. ¿Consideras importante proteger tu información personal en internet?

Malo (No piensa en ello)

Consecuencias:

* Acciones impulsivas que comprometen su información.

* Mayor exposición a estafas, phishing y robo de identidad.

Regular (A veces toma precauciones)

Consecuencias:

* Protección inconsistente.

* Riesgo de caer en fraudes cuando baja la atención.

Bueno (Siempre tiene cuidado)

Consecuencias:

* Menor probabilidad de fuga de datos.

* Conductas preventivas más sólidas y constantes.

3. ¿Sabes identificar un enlace o un mensaje sospechoso (phishing)?

Malo (No los reconoce)

Consecuencias:

* Alta probabilidad de caer en phishing.

* Pérdida de contraseñas, información personal o cuentas.

Regular (A veces los identifica)

Consecuencias:

* Riesgo moderado.

* Puede evitar ataques simples, pero no los más elaborados.

Bueno (Los reconoce fácilmente y los evita)

Consecuencias:

* Menor riesgo de estafas y robo de credenciales.

* Contribuye a una red académica más segura.

4. ¿Has recibido capacitación o información sobre seguridad digital?

Malo (Nunca ha recibido capacitación)

Consecuencias:

* Vulnerabilidad elevada.

* Falta de criterio para actuar ante amenazas digitales.

* Dependencia de recomendaciones informales.

Regular (Información básica)

Consecuencias:

* Conocimientos mínimos pero incompletos.

* Puede cometer errores en situaciones avanzadas.

Bueno (Capacitación formal o actualizada)

Consecuencias:

* Mejora su comportamiento digital.

* Reduce riesgos a nivel individual e institucional.

5. ¿Utilizas contraseñas seguras?

Malo (Contraseñas simples o repetidas)

Consecuencias:

* Muy fácil de vulnerar por ataques automatizados.

* Riesgo de accesos indebidos a cuentas sensibles.

Regular (A veces usa contraseñas fuertes)

Consecuencias:

* Seguridad parcial.

* Puede comprometerse si usa patrones previsibles.

Bueno (Contraseñas robustas y variadas)

Consecuencias:

* Alta protección contra ataques.

* Buen hábito de seguridad.

6. ¿Verificas la confiabilidad de los sitios web antes de ingresar datos personales?

Malo (No verifica)

Consecuencias:

* Riesgo de entregar información a sitios falsos.

* Posible robo de identidad o datos financieros.

Regular (A veces verifica)

Consecuencias:

* Protección irregular.

* Puede caer en sitios fraudulentos en momentos de descuido.

Bueno (Siempre verifica)

Consecuencias:

* Menor probabilidad de comprometer información.

* Comportamiento seguro y crítico frente a páginas web.

10. Diseño de propuesta.

1. Nombre de la propuesta

“Conectados con Seguridad”: Estrategia Institucional de Sensibilización Digital

2. Objetivo de la propuesta

Promover hábitos seguros en el uso de internet y redes sociales dentro de la comunidad académica mediante acciones educativas, comunicativas y preventivas que fortalezcan la conciencia y la responsabilidad digital.

3. Acciones estratégicas

3.1. Micro campañas Educativas Trimestrales

Cada trimestre, la institución implementará una micro campaña enfocada en un tema clave:

- Protección de datos personales
- Phishing y enlaces sospechosos
- Contraseñas seguras
- Privacidad en redes sociales

3.2. Talleres

Breves talleres incluidos antes de iniciar clases o reuniones institucionales.

Ejemplos:

- “3 señales de un enlace fraudulento”

- “Cómo saber si una cuenta es falsa”
- “Errores comunes que ponen en riesgo tu información”

3.3 Historias Reales de Estudiantes (Anonimizadas)

Publicación mensual de un caso real (sin nombres) ocurrido dentro de la institución:

- Robo de cuenta
- Suplantación
- Enlace malicioso
- Exposición de datos
- Cada historia incluirá:
- Qué pasó
- Qué error se cometió
- Cómo evitarlo

4. Recursos necesarios

- Un diseñador o monitor encargado de las piezas gráficas.
- Un profesional de sistemas o TIC para validar la información.
- Redes sociales institucionales y carteleras físicas.
- Espacios breves dentro de clases o reuniones.

5. Resultados esperados

- Mayor capacidad de los estudiantes para identificar riesgos en internet.
- Aumento del uso de contraseñas seguras y verificación de enlaces.
- Disminución de incidentes como suplantación o clics en enlaces maliciosos.
- Comunidad académica más consciente, informada y protegida.
- Fortalecimiento de la cultura institucional en seguridad digital, conforme al CONPES 3995.

11.Conclusión.

Los estudiantes de la CUR tienen una cultura de seguridad digital en desarrollo, con conocimientos básicos pero hábitos preventivos débiles, Persisten prácticas de riesgo: poco cambio de contraseñas, dificultad para identificar phishing y falta de capacitación formal. existe una brecha entre percepción del riesgo y comportamiento real. la ausencia de programas institucionales de sensibilización limita el fortalecimiento de la cultura de seguridad.

El nivel general es moderado, por lo que se requiere implementar acciones formativas y preventivas para reducir vulnerabilidades y mejorar la resiliencia ante amenazas.

12. Recomendaciones

- Implementar programas institucionales de sensibilización en seguridad digital.
- Ofrecer capacitaciones y contenidos formativos sobre buenas prácticas.
- Promover hábitos preventivos: contraseñas seguras, verificación de enlaces y uso responsable de redes sociales.
- Realizar simulaciones de phishing para fortalecer la detección de amenazas.
- Actualizar políticas internas y mejorar los canales de reporte y soporte.
- Evaluar periódicamente el nivel de cultura de seguridad digital en la comunidad estudiantil.

Referencias

1. Congreso de la República de Colombia. (2009). Ley 1273 de 2009. Protección de datos y delitos informáticos.

2. Congreso de la República de Colombia. (2012). Ley 1581 de 2012. Protección de datos personales.

3. Departamento Nacional de Planeación. (2020). CONPES 3995: Política Nacional de Seguridad Digital.

4. Departamento Nacional de Planeación. (2020). *CONPES 3995: Política Nacional de Confianza y Seguridad Digital*. https://colombiaaprende.edu.co/recurso-coleccion/seguridad-digital

5. González, M. A. (2021). *Educación en ciberseguridad y cultura digital en contextos universitarios*. *Revista Latinoamericana de Tecnología Educativa*, 20(3), 45–58. https://doi.org/10.7203/relatec.20.3.23401

6. Jansen, J., & Van Niekerk, B. (2017). *A Cybersecurity Awareness Model for Educational Environments*. *Journal of Information Security Education Research*, 8(2), 1–12.

7. Ministerio TIC. (s.f.). Programas de formación en seguridad digital. https://www.mintic.gov.co/

8. Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (2024). *Habilidades digitales de la población colombiana*. https://www.mintic.gov.co/portal/715/articles-334120_recurso_1.pdf

9. Safa, N. S., Maple, C., & Watson, T. (2016). *Information Security Awareness in Higher Education: An Empirical Study*. *Computers & Security*, 56, 75–85. https://doi.org/10.1016/j.cose.2015.10.006

10. UNESCO. (2018). *Digital Literacy Global Framework*. United Nations Educational, Scientific and Cultural Organization. https://unesdoc.unesco.org/ark:/48223/pf0000265403