REVISTA RIDING
Revista de Investigaciones, Desarrollo e Innovación en Ingenierías
Barrancabermeja - Colombia
Revista para la difusión y divulgación de avances de Investigación e Innovación
ISSN 2590-5929

vol. 08, No. 01, enero-junio de 2024 páginas 21-27.
ISSN 2590-5929

Fortaleciendo la Seguridad Informática: Un Enfoque Comparativo en Organizaciones Gubernamentales, Privadas y Públicas

Strengthening Cybersecurity: A Comparative Approach in Governmental, Private, and Public Organizations

Jan Franco Piocuda Cervantes [1]
jan.piocuda@unipaz.edu.co

Instituto Universitario de la Paz, Escuela de Ingeniería de Producción, Grupo de Investigación en Reingeniería, Innovación Y Productividad, GREIP (1)

Recibido: marzo17 de 2024 – Aceptado: junio 19 de 2024

Resumen

Este artículo ofrece una visión completa de la evolución de la seguridad de la información a lo largo de los años. Comienza con un vistazo a la antigüedad y los primeros métodos criptográficos, incluido el famoso "Código César" en la antigua Roma. Se destaca la importancia de la confidencialidad en la comunicación militar de la época.
Luego, se menciona el papel clave que desempeñó la máquina Enigma durante la Primera Guerra Mundial, marcando un hito en la historia de la criptografía y la seguridad de la información. La transición a la era digital y la transformación de la información se abordan, junto con los desafíos actuales que enfrentan las organizaciones debido a las amenazas cibernéticas.
El artículo también introduce los pilares fundamentales de la seguridad de la información: confidencialidad, integridad y disponibilidad, conocidos como el "triángulo de la seguridad de la información". Estos principios esenciales subrayan la importancia de proteger la información contra el acceso no autorizado, la manipulación y garantizar su disponibilidad cuando sea necesario.
Se exploran errores comunes en seguridad informática, como el uso de contraseñas débiles y la ingeniería social. Además, se destacan las amenazas, incluyendo el phishing, la vulnerabilidad de dispositivos móviles y las catástrofes naturales, que pueden poner en peligro la seguridad de la información.
El artículo enfatiza la importancia de las políticas de seguridad informática en organizaciones gubernamentales, privadas y públicas, y cómo estas políticas pueden adaptarse a diferentes contextos. Se detalla una serie de políticas clave, como la protección de datos, el uso de Internet y del correo electrónico, y la seguridad física y de red.
En conclusión, este artículo destaca la relevancia continua de la seguridad de la información en la sociedad actual y la necesidad de medidas proactivas para proteger los datos y sistemas. Se resalta que la seguridad de la información es un campo multidisciplinario que requiere la colaboración de diversos profesionales y que el factor humano sigue siendo un eslabón crucial en la cadena de seguridad informática

Palabras clave: seguridad informática, seguridad de la información, amenazas, vulnerabilidad, ingeniería social, políticas de seguridad.

Abstract

This article provides a comprehensive overview of the evolution of information security over the years. It begins with a glimpse into antiquity and the early cryptographic methods, including the famous "Caesar Cipher" in ancient Rome. The importance of confidentiality in military communication of that time is emphasized.
Next, it mentions the pivotal role played by the Enigma machine during World War I, marking a milestone in the history of cryptography and information security. The transition to the digital age and the transformation of information are addressed, along with the current challenges organizations face due to cyber threats.
The article also introduces the fundamental pillars of information security: confidentiality, integrity, and availability, known as the "information security triangle." These essential principles underscore the importance of protecting information from unauthorized access, manipulation, and ensuring its availability when needed.
Common errors in computer security are explored, such as weak passwords and social engineering. Additionally, threats are highlighted, including phishing, mobile device vulnerabilities, and natural disasters, which can jeopardize information security.

REVISTA RIDING
Revista de Investigaciones, Desarrollo e Innovación en Ingenierías
Barrancabermeja - Colombia
Revista para la difusión y divulgación de avances de Investigación e Innovación
ISSN 2590-5929

vol. 08, No. 01, enero-junio de 2024 páginas 21-27.
ISSN 2590-5929

The article emphasizes the importance of computer security policies in government, private, and public organizations and how these policies can be adapted to different contexts. A series of key policies are detailed, such as data protection, Internet and email use, and physical and network security.
In conclusion, this article highlights the continued relevance of information security in today's society and the need for proactive measures to protect data and systems. It underscores that information security is a multidisciplinary field that requires the collaboration of various professionals and that the human factor remains a crucial link in the computer security chain.

Keywords: computer security, information security, threats, vulnerability, social engineering, security policies.

INTRODUCCIÓN

Antigüedad y los Primeros Métodos Criptográficos

Los primeros indicios de seguridad de la información se pueden rastrear hasta el siglo I a.C. con la aparición del llamado "Código César". Este método criptográfico consistía en desplazar las letras del alfabeto en un número fijo en el alfabeto para proteger mensajes militares en la antigua Roma. La confidencialidad era esencial para asegurar la comunicación segura en un contexto militar.

La Máquina Enigma y la Criptografía Avanzada

Durante la Primera Guerra Mundial, el ejército alemán introdujo la máquina Enigma, que empleaba cifrado de sustitución monoalfabética, una forma más avanzada de criptografía. Esta máquina desempeñó un papel crucial en la protección de las comunicaciones militares alemanas. Su ruptura por parte de los aliados marcó un hito en la historia de la criptografía y la seguridad de la información.

La Era Digital y la Transformación de la Información

Estos datos representados en grandes cantidades de papel lo cual podemos digitalizar, almacenar en dispositivos electrónicos (USB, Discos duros, Ordenadores) utilizando sistemas informáticos reduciendo espacios ocupados y facilitando el análisis y procesamiento de la información. Pero aparecen otros problemas en las empresas ya que están expuesta a gran cantidad de amenazas como un ataque informático que pueden vulnerar su sistema informático y poner en riesgo la integridad de la información. No es de carácter técnico el principal problema de la pérdida o manipulación de información sino la toma de consciencia de los peligros potenciales en la transmisión de información confidencial y desconocimiento de técnicas de hacking.
La seguridad de la información la podemos definir como un conjunto de medidas y técnicas utilizadas para la protección de información contra el acceso no autorizados, perdida, robo, manipulación o daño.

Estándares y Normativas en Seguridad de la Información

En respuesta a las crecientes amenazas, se han desarrollado estándares y normativas internacionales, como la ISO 27001:2013, que define los requisitos para establecer, implementar, mantener y mejorar un sistema de gestión de seguridad de la información. Estos estándares brindan un marco sólido para la protección de la información y la garantía de la confidencialidad, integridad y disponibilidad de los datos.
En la era digital actual, la seguridad informática se ha convertido en un pilar fundamental para proteger la información crítica en un mundo cada vez más interconectado. Desde datos gubernamentales confidenciales hasta la información personal de los ciudadanos y los secretos comerciales de las empresas, la seguridad informática desempeña un papel crucial en la preservación de la integridad, confidencialidad y disponibilidad de los datos.

DESARROLLO DEL ARTÍCULO

Ajustes según la Aplicación en los Tipos de Organización

La seguridad informática es un campo dinámico que requiere enfoques y ajustes específicos según el tipo de organización. La aplicación de políticas y prácticas de seguridad informática varía significativamente entre organizaciones gubernamentales, empresas privadas y entidades públicas. A continuación, se detallan algunos ejemplos de cómo se ajusta la seguridad informática en función de la aplicación en estos contextos

1. **Organizaciones Gubernamentales**

En las instituciones gubernamentales, la seguridad de la información desempeña un papel fundamental en la protección de datos sensibles y la toma de decisiones

vol. 08, No. 01, enero-junio de 2024 páginas 21-27.
ISSN 2590-5929

basadas en información confiable. Algunos ejemplos de aplicabilidad incluyen:

- Protección de Datos Sensibles: Las agencias gubernamentales manejan información confidencial, como datos de ciudadanos, registros financieros y documentos legales. Las políticas de seguridad informática son cruciales para proteger esta información contra el acceso no autorizado.

- Ciberseguridad Nacional: La seguridad de la información a nivel nacional es una prioridad en muchos países. Las políticas y estrategias de seguridad informática gubernamentales tienen como objetivo proteger las infraestructuras críticas y prevenir ciberataques.

- Intercambio Seguro de Información: Las instituciones gubernamentales a menudo necesitan compartir información de manera segura con otras agencias o países. Las políticas de seguridad facilitan el intercambio seguro y protegido de datos.

En organizaciones gubernamentales, la seguridad de la información va más allá de la protección de datos; también implica la seguridad nacional. Por ejemplo, el Departamento de Defensa de un país puede implementar políticas de seguridad informática para proteger las comunicaciones militares y prevenir ciberataques de actores extranjeros. Estas políticas incluyen la encriptación de datos confidenciales, la autenticación de usuarios y la monitorización constante de amenazas cibernéticas.

2. **Empresas Privadas**

En el sector empresarial, la seguridad informática es esencial para proteger la propiedad intelectual, la reputación de la empresa y la confidencialidad de los datos. Ejemplos de aplicabilidad incluyen:

- Protección de Datos del Cliente: Las empresas privadas almacenan información confidencial de clientes, como datos de tarjetas de crédito y registros de transacciones. Las políticas de seguridad garantizan la privacidad de estos datos.

- Prevención de Fugas de Datos: Las políticas de seguridad ayudan a prevenir la fuga de datos y la filtración de información confidencial, lo que podría tener graves consecuencias legales y financieras.

- Seguridad en la Cadena de Suministro: Las organizaciones privadas dependen de la colaboración con proveedores y socios comerciales. Las políticas de seguridad se extienden a la cadena de suministro para garantizar la integridad de los sistemas y datos compartidos.

En el sector empresarial, las políticas de seguridad informática son esenciales para proteger la propiedad intelectual. Por ejemplo, una empresa de tecnología puede implementar políticas que prohíban el uso de dispositivos de almacenamiento USB no autorizados para evitar fugas de datos. Además, pueden requerir contraseñas fuertes y autenticación de dos factores para acceder a sistemas críticos y datos confidenciales de clientes

3. **Organizaciones Públicas**

Las organizaciones públicas, como hospitales, escuelas y bibliotecas, también requieren políticas de seguridad informática para proteger datos sensibles y brindar servicios de manera eficiente y segura. Ejemplos de aplicabilidad incluyen:

- Protección de Datos de Pacientes y Estudiantes: Los hospitales y las escuelas almacenan información personal de pacientes y estudiantes. Las políticas de seguridad garantizan la confidencialidad y la integridad de estos datos.

- Seguridad en Bibliotecas Digitales: Las bibliotecas digitales almacenan una gran cantidad de recursos digitales. Las políticas de seguridad aseguran que estos recursos estén disponibles y protegidos contra la alteración no autorizada.

- Acceso Seguro a Servicios Públicos en Línea: Muchos servicios gubernamentales se brindan en línea. Las políticas de seguridad garantizan que los ciudadanos puedan acceder de manera segura a estos servicios y protegen la información personal.

Las organizaciones públicas, como las bibliotecas digitales, enfrentan desafíos de seguridad. Por ejemplo, una biblioteca digital puede establecer políticas que garanticen la integridad de los archivos almacenados,

REVISTA RIDING
Revista de Investigaciones, Desarrollo e Innovación en Ingenierías
Barrancabermeja - Colombia
Revista para la difusión y divulgación de avances de Investigación e Innovación
ISSN 2590-5929

evitando la modificación no autorizada de documentos históricos. Además, pueden implementar medidas de seguridad en línea para proteger la privacidad de los usuarios que acceden a recursos digitales.

Bases de la seguridad informática

Las empresas han tomado conciencia de la importancia de administrar los riesgos de seguridad informático utilizando estrategias para demostrar a sus clientes la seguridad y protección de su información. Existen tres elementos o principios básicos de la seguridad informática que se pueden resumir en: la confidencialidad, la integridad y la disponibilidad (conocidos como el triángulo de la seguridad de la información).

Fig. 1. Seguridad de la información. Tomado de: http://recursostic.educacion.es/observatorio/web/gl/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=1

Confidencialidad: Tiene como propósito la protección de la información para evitar que personas no autorizadas puedan acceder a ella. Es importante que la información confidencial, como datos personales o secretos comerciales, estén protegidos de accesos no autorizados.

Esto significa que solo una persona o un grupo de individuos definidos por el responsable de la información, deben de conocer estos datos. Supongamos que una organización de atención médica maneja registros de pacientes. Para garantizar la confidencialidad, solo el personal médico autorizado debe acceder a estos registros. Se utilizan sistemas de autenticación y cifrado para proteger esta información contra el acceso no autorizado.

Integridad: En términos de seguridad de la información, la integridad evita que sea manipulada o alterada sin autorización. La integridad garantiza que la información es exacta y no ha sido modificada por terceros. La integridad de los datos es fundamental para cualquier organización ya que tiene que garantizar la confiabilidad (la integridad del origen) y exactitud (la integridad de los datos) de la información. Si los datos no son precisos o fiables para la toma decisión pueden provocar pérdidas financieras y darle una mala reputación a la organización.

Disponibilidad: En términos de seguridad de la información, se refiere a la protección de la información para garantizar que esté disponible y accesible cuando sea necesario. Es importante asegurar que los sistemas y la información estén disponibles y accesibles para los usuarios autorizados.

El propósito de la disponibilidad es prevenir interrupciones no autorizadas o incontroladas en los recursos informáticos. En términos de seguridad informática, "un sistema está disponible cuando su diseño e implementación permiten negar deliberadamente el acceso a ciertos datos o servicios". Es decir, un sistema es considerado disponible si puede controlar su indisponibilidad.

Un sistema "no disponible" es tan inútil como no tener sistema alguno. No cumple su propósito.

ERRORES COMUNES DE SEGURIDAD INFORMÁTICA

Los peligros en la red son cada vez mayores y el internet es una entrada a posibles filtraciones y ataques empleando métodos que están en continua evolución para burlar el software de seguridad de las computadoras. Pero el internet no es solo la limitación para que nuestra información sea robada o modificada.

Un error común en la seguridad informática es el uso de contraseñas débiles. Por ejemplo, usar una contraseña como '123456' o el nombre de una mascota es un grave riesgo de seguridad. Estas contraseñas simples son fáciles de adivinar para los atacantes, lo que puede llevar a la violación de cuentas en línea y la exposición de datos personales.

La Ingeniería Social es una técnica que utiliza el engaño y la persuasión para obtener información valiosa o inducir a la víctima a realizar una acción específica, como abrir un archivo adjunto en un correo electrónico.

REVISTA RIDING
Revista de Investigaciones, Desarrollo e Innovación en Ingenierías
Barrancabermeja - Colombia
Revista para la difusión y divulgación de avances de Investigación e Innovación
ISSN 2590-5929

Este método es comúnmente usado para descubrir nombres de usuario y contraseñas. Puede llevarse a cabo a través de medios tecnológicos, como Internet o teléfono, de manera impersonal, o bien en persona, cara a cara.[1].

Algunas medidas a tener en cuenta son:

- Nunca divulgar información sensible con desconocidos o en lugares públicos.
- Si se sospecha que alguien intenta realizar un engaño, hay que exigir que se identifique y tratar de revertir la situación intentando obtener la mayor cantidad de información del sospechoso.
- Llevar a cabo programas de concientización sobre la seguridad de la información.[3]

A continuación, se mencionarán algunos errores comunes en la seguridad Informática:

1. **No actualizar los softwares del ordenador:** Un equipo actualizado es muy importante ya que los virus van apareciendo día a día y de una manera más agresiva, por lo que se debe actualizar constantemente todas las aplicaciones que se encuentren instaladas en el PC.

2. **Contraseñas débiles:** Este es unos de los errores más comunes de la seguridad informática. Ya que algunas personas utilizan algunos detalles personales como la escuela donde estudio, fechas de aniversario, fecha de cumpleaños, son demasiado simples ante un ataque cibernético.

3. **No realizar copias de seguridad:** No realizar copias de seguridad periódicas puede provocar la pérdida de datos críticos. Las copias de seguridad pueden ayudar a recuperar los datos en caso de errores del sistema, fallos en el hardware o ataques cibernéticos.

4. **No educar a los usuarios:** Si no capacitamos o educamos a nuestro personal es un error común de la seguridad informática. Es importante tener capacitaciones de mejores prácticas y evidenciar los riesgos potenciales asociados con el mal uso de las tecnologías.

5. **No implementar medidas de protección contra Malware:** Puede afectar a nuestro equipo informático, servicio o red programable. El Malware puede afectar seriamente la seguridad informática. No implementar medidas de protección contra Malware, como software antivirus y firewalls, puede dejar al sistema vulnerable a ataques.

6. **No monitorear el sistema:** No monitorear el sistema es otro error común en la seguridad informática. Es importante supervisar el sistema de forma constante para detectar posibles amenazas o vulnerabilidades.

7. **Wifis públicas:** este tipo de conexión se desconoce el nivel de seguridad y pueden ser presas fáciles por un tercero. Si vas a utilizar este tipo de conexión en tu dispositivo móvil o en tu PC, solo debes usarlo para temas puntuales que no implique información personal o de la empresa. Es recomendable conectarse desde los datos móviles en casa o en la empresa donde trabajas para tratar asuntos privados.

Evitar estos y otros errores de seguridad informática es esencial para garantizar la protección de nuestros equipos y lo mas importante la información de nuestra compañía contra posibles amenazas y ataques.

AMENAZAS

En términos generales, las amenazas se pueden clasificar en dos tipos: físicas y lógicas. Estas amenazas, ya sean físicas o lógicas, pueden ser causadas principalmente por personas, programas específicos o desastres naturales.

A. Phishing

Este tipo de ataque de suplantación de identidad es un tipo de fraude cibernético en el que un atacante intenta engañar a una persona para que revele información confidencial como contraseñas, información de cuentas bancarias, tarjetas de crédito u otra información personal. Estos atacantes envían correos electrónicos falsificados que parecen ser de bancos legítimos, solicitando a los destinatarios que revelen sus contraseñas y detalles de la cuenta. Un ejemplo sería un empleado de una empresa que recibe un correo electrónico falso de recursos humanos solicitando información confidencial.

REVISTA RIDING
Revista de Investigaciones, Desarrollo e Innovación en Ingenierías
Barrancabermeja - Colombia
Revista para la difusión y divulgación de avances de Investigación e Innovación
ISSN 2590-5929

B. Dispositivos Móviles

Hoy en día el uso de estos dispositivos son la herramienta personal y laboral de cada persona, ya que podemos realizar operaciones transaccionales, estar en redes sociales, entre otros. Pero lo que no sabemos que existen personas inescrupulosas que buscan aprovechar las vulnerabilidades para encontrar información personal como laboral.

Todo esto sucede cuando los equipos móviles son conectados a redes publicas que no son seguras y cuando ingresan a las redes de la organización traen algún tipo de virus malicioso. Esto a conllevado a que las organizaciones implementen una serie de medidas con los dispositivos móviles en cuando a la información de la empresa. De tal manera las organizaciones instalan certificados de seguridad y establecen una conexión segura a servidores que tienen la propiedad para monitorear el comportamiento de los cambios que puede tener el dispositivo móvil, al igual que eliminar los datos del dispositivo, ya sea de trabajo o en su totalidad.

C. Ingeniería Social

Este tipo de ataque relacionado con los ya mencionados no se necesita de un dispositivo si no una serie de preguntas a personas, para conocer información valiosa que puede pertenecer a una organización o personal. Las organizaciones no le prestan mucha importancia a esta técnica de manipulación y no concientizan a sus empleados de la información sensible que almacenan en la mente humana.

La Ingeniería Social se basa en un principio simple: "el usuario es el eslabón más débil". Dado que todos los sistemas dependen de seres humanos, la Ingeniería Social es una vulnerabilidad universal, independiente de la tecnología usada. Los expertos en seguridad suelen decir que la única computadora segura es la que está desconectada, pero los entusiastas de la Ingeniería Social responden que siempre se puede convencer a alguien para que la conecte [4]

D. Catástrofes Naturales

Este tipo de amenazas generalmente provocan la interrupción de los servicios, afectando principalmente a la disponibilidad de la información, ejemplos de este tipo de amenazas son los provocados por la naturaleza: las inundaciones, terremotos, tornados, etc.

BUENAS PRÁCTICAS POLÍTICAS DE SEGURIDAD INFORMÁTICA

Las políticas de seguridad informática de una empresa son un conjunto de reglas y directrices que establecen las practicas recomendadas y procedimientos para proteger la información y los sistemas de una organización.

Lo primero que se debe hacer en una organización es un análisis y estudio de las probabilidades de que ocurran posibles amenazas que puede sufrir el sistema informático. A partir del análisis se diseña ciertas políticas claras, concisas, aplicables y búsqueda de responsables dentro de la organización, para evitar amenazas o minimizar los efectos si se llegan a producir.

Las políticas de seguridad deben ser conocidos por todo el personal de una organización. En el contenido de los documentos deben estar claramente establecidos: El objetivo, los responsables del cumplimiento, las medidas que se aplicarán en caso de incumplimiento. Estas políticas deben ser revisadas, y si es necesario actualizadas periódicamente [5]:

Políticas de Objetivos y alcance: Las políticas de seguridad informática deben definir claramente los objetivos y el alcance de las políticas, es decir, qué se pretende proteger y quiénes están sujetos a las políticas.

Políticas de Tratamiento de la información: Definirá claramente los tipos de información que es manejada por las personas autorizadas dentro de la organización.

Políticas de Accesos y autorizaciones: Las políticas deben definir los requisitos de acceso y autorización para los sistemas y los datos. Esto incluye la autenticación de los usuarios y la gestión de los permisos de acceso.

Políticas de Software legal: Definirá claramente el uso de software en la Empresa con licencias de uso legal.

Políticas de Protección de datos: Las políticas deben definir las medidas de protección de datos para garantizar la integridad, confidencialidad y disponibilidad de la información.

Políticas de Uso del servicio de Internet y del correo electrónico: Describirá la protección de la información mediante el uso de correo electrónico y del servicio de Internet.

vol. 08, No. 01, enero-junio de 2024 páginas 21-27.
ISSN 2590-5929

Políticas de respaldo: Las políticas deben incluir las políticas de respaldo y recuperación de datos para garantizar la disponibilidad de la información en caso de desastres o fallas en el sistema.

Políticas de Seguridad en las comunicaciones: Describirá la protección de la información durante los procesos de transmisión y recepción de datos en las redes internas y externas.
Políticas de Auditorías de los sistemas: Que permitirá hacer un control de los eventos de seguridad de los sistemas.

Políticas de seguridad física: Las políticas deben incluir las políticas de seguridad física para garantizar la protección de los activos físicos de la organización, como los servidores y el equipo de red.

Políticas de seguridad de red: Las políticas deben incluir las políticas de seguridad de red para proteger los sistemas y la información de los ataques cibernéticos.

Políticas de sanciones por incumplimientos: Este documento contemplará las medidas que se aplicarán por incumplimiento de las reglas definidas.

Las políticas de respaldo son fundamentales para garantizar la disponibilidad de datos en caso de desastres. Una empresa puede establecer una política que exija copias de seguridad diarias de todos los datos críticos en servidores redundantes fuera del sitio. Esto garantiza que, incluso en caso de fallos del sistema, los datos puedan recuperarse sin pérdida significativa

CONCLUSIONES

Entre las conclusiones que se pueden obtener del presente artículo, se debe tener en cuenta las políticas de seguridad para disminuir las malas practicas en las organizaciones. Con respecto a la seguridad de la información se necesita ser persistente en las buenas prácticas para proteger la información, y así evitar ser parte del grupo de víctimas.

Se observa que el factor humano es la parte más débil del eslabón de la seguridad informática, debido a que no se ha formado la concientización de la importancia de la información que manipulan de una organización ya que son información confidencial y no se puede divulgar de manera fácil. Los delitos informáticos no esperan a las víctimas, solo con enviar un correo electrónico u otro medio que le solicite puede estar en riego sus datos personales o de su organización.

Considere la instalación de software de seguridad en sus equipos como firewalls, antivirus con antispyware y tenerlos actualizados periódicamente.

En la actualidad existen muchas empresas que carecen de orientación sobre la protección adecuada de su sistema de información o que desconocen la existencia de estos, por esto las empresas no deben de evadir esta realidad que cada día aumenta la probabilidad de que su información esté en manos equivocadas. En este sentido, debemos insistir en el conocimiento, difusión e implantación de cuantos medios sean necesarios para garantizar la seguridad informática y seguridad de la información.

REFERENCIAS

[1] Wordpress.com. [Online]. Available: https://nebul4ck.wordpress.com/wp-content/uploads/2015/08/hacking-etico-carlos-tori.pdf.

[2] "Ingeniería Social: Corrompiendo la mente humana," *Unam.mx*. [Online]. Available: https://revista.seguridad.unam.mx/numero-10/ingenier%C3%AD-social-corrompiendo-la-mente-humana.

[3] "Social Engineering 1," *Grn.es*. [Online]. Available: http://ww2.grn.es/merce/2002/is.html.

[4] W. Vega Velasco, "POLITICAS Y SEGURIDAD DE LA INFORMACION," *Fides Et Ratio*, vol. 2, no. 2, pp. 63–69, 2008.

[5] P. A. López, Seguridad informática. Editorial Editex, 2010.

[6] "Projects," Nist.gov. [Online]. Available: https://csrc.nist.gov/projects.

[7] Oas.org. [Online]. Available: https://www.oas.org/es/sms/cicte/awswhitepaper.pdf.

Jan Franco Piocuda Cervantes. Ingeniero de sistemas de la Universidad Cooperativa de Colombia en el año 2008 en el municipio de Barrancabermeja Santander. Especialista en Gerencia integral de Proyecto de la Universitaria de Investigación y Desarrollo UDI en el año 2016 en el municipio de Barrancabermeja Santander. Actualmente, se desempeña como Docente ocasional tiempo completo en la escuela de Ingeniería de Producción del Instituto Universitario de la Paz.