UNIVERSIDAD PERUANA
Simón Bolívar

FACULTAD DE INGENIERIA Y COMUNICACIONES

CARRERA PROFESIONAL DE INGENIERÍA DE SISTEMAS Y SEGURIDAD INFORMÁTICA

TRABAJO DE SUFICIENCIA PROFESIONAL

PHISHING EN LAS CUENTAS BANCARIAS Y SU ESTAFA EN LOS CLIENTES DEL BANCO DE LA NACIÓN DEL PERÚ, IQUITOS, 2022.

AUTOR: BACHILLER

Tenazoa Paredes, Jorge Maicol

Para obtener el Título Profesional en

Ingeniero de Sistemas y Seguridad Informática

Lima - Perú

2023

INFORME DE SIMILITUD

JORGE_TENAZOA PAREDES

INFORME DE ORIGINALIDAD

14%	13%	4%	4%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	repositorio.unp.edu.pe Fuente de Internet	2%
2	www.bn.com.pe Fuente de Internet	1%
3	repositorio.uncp.edu.pe Fuente de Internet	1%
4	hdl.handle.net Fuente de Internet	1%
5	repositorio.uap.edu.pe Fuente de Internet	1%
6	andrescusi.files.wordpress.com Fuente de Internet	1%
7	vsip.info Fuente de Internet	<1%

PHISHING EN LAS CUENTAS BANCARIAS Y SU ESTAFA EN LOS CLIENTES DEL BANCO DE LA NACIÓN DEL PERÚ, IQUITOS, 2022

ASESOR Y MIEMBROS DEL JURADO

Mg. Julio Becar Mendoza
ASESOR

Hugo Marcial GARCÍA RIVADENEIRA
PRESIDENTE

Catherine Lucia CALDERON GÁLVEZ
SECRETARIO

Bernardo Pedro HUAMAN CARBAJAL
ESPECIALISTA

DEDICO MI TRABAJO A:

Mis padres, saludo afectuoso y abrazo especial hasta el cielo para mi señor padre, mi mamá por estar conmigo siempre apoyándome y a mi mujer e hijos por ser el apoyo y motivación para superarme como persona y profesionalmente.

AGRADECIMIENTO

A la Universidad por brindarme las aulas y docentes que me abrigaron y brindaron todos los conocimientos que mi carrera profesional lo amerita durante todos estos años de estudios.

RESUMEN

El presente trabajo, de Phishing en las cuentas bancarias y su estafa en los clientes del banco de nación del Perú se realizó, ya que la problemática de perder el dinero de una cuenta bancaria viene de muchos años atrás, las técnicas que utilizan los hackers para obtener los datos con el tiempo han ido evolucionando, en un principio los hackers buscaban la forma de como ingresar físicamente a los establecimientos financieros u otros lugares de interés para ellos, con el fin de instalar softwares que capturaban las claves de las computadoras, para poder colarse dentro de los bancos, oficinas, etc, realizaban un estudio a detalle de los trabajadores, lo que ahora conocemos y llamamos ingeniería social.

Hoy en día el Phishing usa técnicas de envió de correos con temas de interés para la potencial víctima, en ese correo envían un link que lleva a sitios maliciosos, por ejemplo, en nuestro caso un sitio web de un banco donde una vez ingresado te piden tus datos personales y hasta contraseñas, sin saber que estas entregando tus datos a personas inescrupulosas, que con esos datos pueden vaciar tus cuentas. Por tal motivo, se hace un análisis y se brinda las recomendaciones necesarias para no ser víctimas de esta estafa informática.

Palabras Clave: Phishing, Hackers, Softwares,Informática, Cuenta bancaria, Ingeniería social, link y sitio web.

ABSTRACT

The present work, of Phishing in the bank accounts and its swindle in the clients of the bank of nation of Peru was carried out, since the problem of losing the money of a bank account comes from many years ago, the techniques that the hackers use to obtain the data with the time have been evolving, In the beginning hackers were looking for ways to physically enter financial establishments or other places of interest to them, in order to install software that captured the passwords of computers, in order to sneak into banks, offices, etc., they conducted a detailed study of the workers, what we now know and call social engineering.

Nowadays Phishing uses techniques of sending emails with topics of interest to the potential victim, in that email they send a link that leads to malicious sites, for example, in our case a website of a bank where once entered they ask you for your personal data and even passwords, without knowing that you are giving your data to unscrupulous people, who with that data can empty your accounts. For this reason, an analysis is made and the necessary recommendations are provided so as not to become victims of this computer scam.

Keywords: Phishing, Hackers, Software's, IT, Bank account, Social engineering, link and website.

INTRODUCCION

La pandemia del Covid-19 hizo que los delincuentes informáticos más conocidos como hackers, en estos dos últimos años incrementen sus campañas de ataques, gracias a que el modelo de trabajo cambio a modalidad online o trabajo desde casa, este tipo de trabajo obliga necesariamente a realizar todas las operaciones en línea a través de plataformas digitales, páginas web, correos masivos, llamadas y mensajes de texto. El Phishing de una cuenta bancaria está reconocido como delito en el código penal porque si se llega a ser víctima de este tipo de estafa las perdidas pueden ser millonarias. Esta técnica estafa es parte de la ingeniería social.

El Phishing como ingeniería social es el estudio que el cibercriminal hace de su potencial victima fijándose a detalle en cada ámbito de su vida personal, dentro de redes sociales, recopilando información sobre los gustos, preferencias hobbies para poder armar algún contenido que sea de total interés para la persona, de esta manera el cibercriminal busca engañar a las personas.

En vista que existe este tipo de peligros para las personas que confían en abrir sus cuentas bancarias, se realiza un análisis de cómo realizar las operaciones bancarias en las múltiples plataformas digitales que brindan las instituciones financieras, para nuestro caso el banco de la nación en Iquitos – Perú y brindar las recomendaciones pertinentes con el propósito de evitar ser víctimas de las estafas informáticas.

Capítulo I: Se examina la realidad del problema, los límites de la investigación, el problema en sí, los objetivos de la investigación, su importancia y justificación, los límites de la investigación y otras cuestiones relacionadas.

Capítulo II: Se realiza lo siguiente: Antecedentes relacionados con la Investigación, Marco Histórico, Marco Legal, Marco Teórico y Marco Conceptual.

Capítulo III: Descripción y evaluación de las actividades realizadas

Capítulo IV: Los objetivos planteados en las conclusiones y recomendaciones señalan que el phishing afecta directamente a los clientes del banco de la nación en Iquitos porque permite obtener información sensible sin el consentimiento del usuario o cliente.

Fuente Bibliográfica

Anexos (fotos, Resolución, etc.)

INDICE

CAPÍTULO I LA EMPRESA

1.1. Explicación real del problema

Perú lleva la delantera en ataques de Phishing de toda Latinoamérica en el año 2022 con un 33%, dejando por mucho a México, Ecuador y Argentina que promedian entre el 8% y 14%. En la ciudad de Iquitos vivía uno de los cinco principales cibercriminales del Perú, desde donde operaba creando paginas falsas de reconocidas entidades financieras. Esta modalidad de estafa es conocida como Phishing, la pandemia Covid-19 la hizo más notoria, pues el cambio en el modelo laboral obligaba a trabajar desde casa online, aumentando el uso de plataformas digitales, correros electrónicos, mensajes de texto, llamadas y WhatsApp.

Datos de la empresa de ciberseguridad, ESET menciona que los ataques referentes al Phishing en el Perú se cuadruplico a comparación de las cifras del año 2021, lo que refleja que cada peruano está cada vez más propenso a caer en este tipo de estafa. La ciberseguridad se ve afectada a una gran escala a raíz del uso de tácticas de ingeniería social, los criminales informáticos lo emplean para apropiarse de datos e información secreta de los usuarios. Está claro que dicha información lo obtienen de forma fraudulenta y así suplantar la identidad de dichas personas.

Las entidades financieras hacen un llamado a sus clientes para que hagan uso de sus plataformas digitales, páginas web y consultas telefónicas como canales de atención para que la salud de sus colaboradores y clientes no peligre, en ese entonces por la pandemia del Covid-19 no estaba permitido salir de casa, esta coyuntura llevo a que personas hagan uso de estos canales de atención sin tener mucha experiencia de cómo usar correctamente estas herramientas, siendo un blanco fácil para caer en la estafa de los cibercriminales.

El Phishing como método común más usado es él envió de correo electrónico, donde el cibercriminal se disfraza como organización de confianza donde la potencial victima ya es cliente, socio, o tiene algún interés, de esta manera se gana la confianza para poder pedirle información muy personal, como el número de su tarjeta, su clave, su cvv. Dentro de estos correos también suelen adjuntar archivos que son programados para recopilar la información de tu computadora una vez lo hayas descargado y más aún si lo llegas a instalar, estos archivos son conocidos como malware.

El problema con el Phishing es la magnitud del daño que puede ocasionar en las personas y empresas que caen víctimas de esta estafa, un ataque exitoso significa grandes pérdidas económicas, literalmente puede llevar a la bancarrota a una empresa o persona natural, el cibercriminal una vez que se apodera de los datos de las tarjetas bancarias ya tiene acceso total a ellas y puede usarlo para retirar dinero hacer comprar, etc, este problema es una dura realidad que azota nuestro país, ocupamos el primer puesto en ataques de todo Latinoamérica, las empresas de seguridad de la información tienen mucho por combatir, la tecnología sufre constantes cambios, evoluciona.

1.2. Límites de la investigación

1.2.1. Limitación del Área

El estudio se realizará en el Departamento de Loreto, Provincia de Maynas, Ciudad de Iquitos.

1.2.2. Limitación del Tiempo.

2022 será el año de la investigación porque es cuando se produjeron la mayoría de los ataques de phishing.

1.2.3. Limitación Social.

Se encuentran involucrados los cibercriminales, las empresas, entidades financieras, personas naturales, agentes de inteligencia, fiscales especializados en ciberdelincuencia.

1.3. Planteamiento del Problema

1.3.1. Problema Principal

¿De qué forma se puede evitar el Phishing en las cuentas bancarias y su estafa en los clientes del banco de la nación en Iquitos - Perú?

1.3.2. Problemas Secundarios

PS1. ¿Cuánto el Phishing puede afectar a los clientes del banco de la nación en la ciudad de Iquitos?

PS2. ¿Cómo se da la estafa en los clientes del banco de la nación en la ciudad de Iquitos?

1.4. Propósito de la investigación

1.4.1. Propósito general

Examinar los intentos de phishing en las cuentas bancarias y su estafa en los clientes del banco de la nación. Iquitos, 2022, para evitar ser víctima y afianzar al cliente.

1.4.2. Propósitos específicos

OE1. Estudiar cuanto el Phishing afecta a los clientes del banco de la nación. Iquitos, 2022, para evitar ser víctima y afianzar al cliente.

OE2. Evaluar cómo se da la estafa en los clientes del banco de la nación. Iquitos, 2022, para evitar ser víctima y afianzar al cliente.

1.5. Justificación e importancia

1.5.1. Justificación

Justifico mi trabajo por el interés y preocupación de saber cómo podemos estar protegidos ante un ataque de Phishing y evitar ser víctima de esta estafa, si es posible modificar y hacer más riguroso la condena en el código penal. Debemos estar conscientes del daño que nos puede causar este tipo de estafa, sobre todo cuando las personas y empresas afectadas cuentan con una fuerte cantidad de dinero en sus cuentas bancarias, así mismo el Phishing también sirve como medio para espiar y sacar información de las empresas y venderlo a la competencia.

1.5.2. Importancia

Ante la creciente ola de ataques de Phishing en nuestro país, es sumamente importante saber cuáles son las condenas que se aplican a los cibercriminales y de ser posible hacerlo más riguroso con el fin de proteger los bienes económicos, materiales e intelectuales de las personas y empresas. Todos pueden ser víctimas de este tipo de estafa informática el desconocimiento de herramientas de ciberseguridad y no estar consciente de ello juega en su contra, la necesidad de hacer operaciones en línea en entidades financieras o de otra índole es aprovechada por los cibercriminales, este peligro está a la orden del día, por ello se considera una realidad.

1.6. Restricción de la Investigación

Las restricciones que encontré para desarrollar esta labor investigativa son varias una de ellas es la dificultad de encontrar material bibliográfico, los libros tienen un costo elevado y están en otro idioma, mucha información se obtuvo de artículos, entrevistas de informática y algunos libros donde los autores cuentan sus experiencias.

1.7. Datos Generales

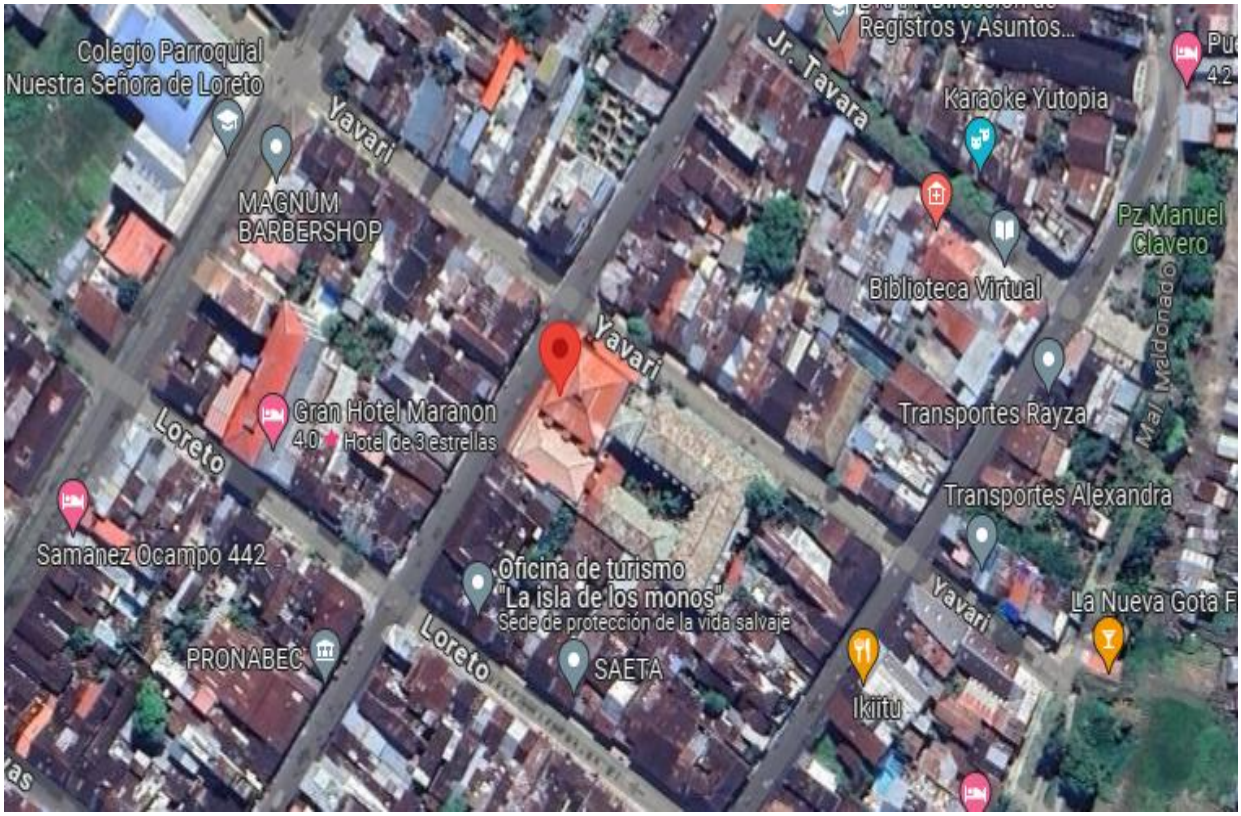
El Banco da Nación es una sociedad jurídica, perteneciente al Sector Económico y Financiero, trabaja con independencia económica, financiera y administrativa. Esta entidad financiera tiene activos propios y tiene tiempo ilimitado.

1.8. Nombre o razón social

Banco de la Nación con RUC N° 20100030595.

1.9. Ubicación del Banco

El presente trabajo centra su investigación en la sede del Banco de la Nación, tiene como dirección calle La Condamine 488 con Yavari, Distrito de Iquitos, Provincia de Maynas.



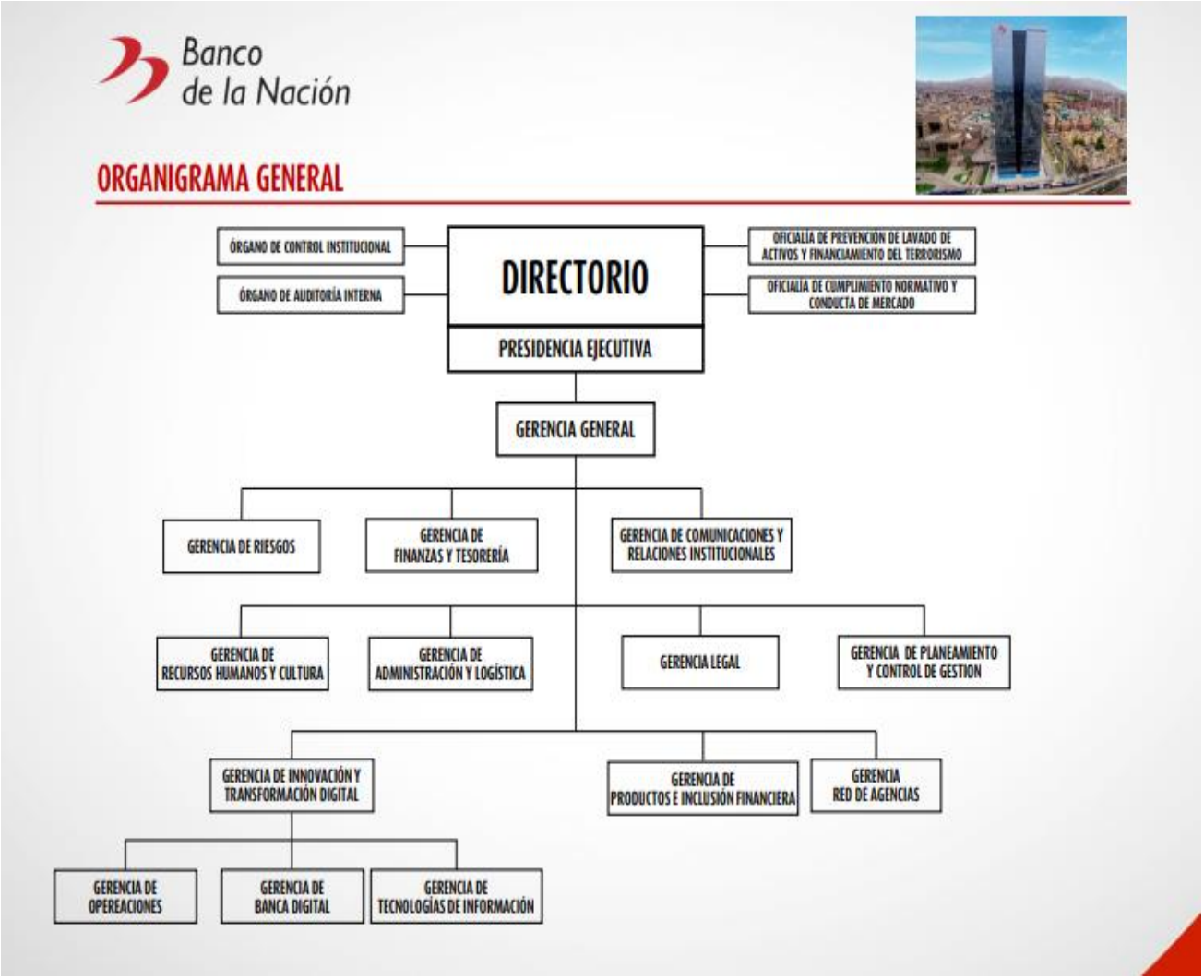
1.10. Giro de la empresa

Banco de la Nación como empresa pública que pertenece al estado cumple la función de administrar las cuentas de las arcas Nacionales y de dar servicios financieros al estado con el fin de gestionar la economía pública.

1.11. Tamaño del Banco

El Banco de la Nación es una organización pública y pertenece al Gobierno en el sector de economía y finanzas.

1.12. Organigrama de la empresa



1.13. Misión, Visión, Valores

1.13.1. Misión

Ofrecer al pueblo productos y servicios financieros mediante múltiples canales de atención, siempre evolucionando de la mano del desarrollo tecnológico para agilizar el proceso de inclusión financiera en nuestro país, a raíz del esfuerzo de los colaboradores para conseguir este objetivo.

1.13.2. Visión

Evolucionar en el mundo digital con continuidad y con acceso para todos los ciudadanos del país, brindando una experiencia de servicio cercana y de clase a sus clientes y usuarios.

1.13.3. Valores

Los valores del banco son:

- Responsabilidad
- Atención de calidad
- Evolución
- Colaboración
- Integridad

1.14. Servicios al cliente

Giros bancarios

- Tele giros a nivel nacional y extranjero
- Varios

Créditos Hipotecarios

- Compra de inmuebles
- Full mejoras

Préstamos

- Con tarjeta clásica conocida como multired y también convenios
- Para estudiantes
- Se financia deudas de tarjetas de crédito
- Se hacen descuentos por planilla

Seguros

- Ofrecen seguros para tu tarjeta de débito
- Seguros con cuotas protegidas
- Seguros oncológicos
- Seguros post mortem

Pagos

- SUNAT
- Pagos interbancarios
- Pagos MasterCard
- Transferencias por Internet (SATM)
- líneas de teléfonos móviles y recargas
- Pagos a los proveedores de BN en cuenta corriente
- Pagos a pensionistas
- Pago salarial y pensiones (UOB)

Cuentas Bancarias

- En las zonas con una única agencia bancaria, cualquier persona natural o jurídica puede abrir una cuenta de ahorro.
- El sector público puede abrir sus cuentas de ahorro en moneda extranjera o local.
- El sector privado puede abrir sus cuentas de ahorros en

moneda local.

- Cuenta de Detracciones.
- Los proveedores estatales pueden abrir su cuenta corriente.
- Las asociaciones de pescadores pueden abrir su cuenta corriente.
- Cuenta de Depósitos a plazo en localidades que tienen una única agencia bancaria.
- Cuenta DNI.

Transferencias

- Envíos o depósitos
- Transferir del mismo banco a cuenta de ahorros
- Entre distintos bancos con cargo a cuenta de ahorros
- Transferir del mismo banco a cuenta corriente
- Entre distintos bancos con cargo a cuenta corriente
- Envíos del extranjero para pago de Pensionistas
- Envíos del extranjero en efectivo - Persona natural
- Liquidación Bruta transferida en Tiempo Real

Cheques

- Emitidos por una entidad financiera (de gerencia)
- Cambio de cheques electrónicos para clientes
- Verificación y revocación de cheques certificados
- Cheques pagados en diferentes lugares
- Pagos con cheque certificado realizados en otro lugar
- Retención del pago de cheques
- Dejar de emitir cheques
- otros

Microfinanzas

- Oficina Compartida - Ventanilla MYPE
- Línea de Crédito – PROMYPE

Más servicios

- Cambio de divisas
- Certificados de pago
- Certificados bancarios
- Emisión de copias microfilm / emisión de estado de cuenta corriente
- Cobros simples en el extranjero
- servicio de correo
- Depósitos Judiciales y Administrativos
- Billetera digital
- Comercio electrónico
- Reconocimiento de derechos de pensión
- Servicio Yape con el BN

1.15. Logros, Premios y Reconocimiento

1.15.1. Logros

- subió 97 puestos en el top 1000 de los bancos del mundo - agosto 2009.
- Galardón a la sostenibilidad económica y cuidado del medio ambiente Empresarial 2011 - junio 2011.
- Según FITCH RATINGS el banco de la nación subió de nivel en el rating de Viabilidad obteniendo “bbb- “- octubre 2014.
- Banco de la Nación es certificado con la ISO/IEC 20000-I: 2011 - diciembre 2014.
- Banco de la Nación recibe nuevamente el certificado ISO

9001:2008 del Meta proceso “Solución de pago electrónico para los proveedores del Estado a través del SIAF” - octubre 2016.

- Banco de la Nación es calificada como A3 por primera vez - febrero 2019.
- El BN califico de nuevo con A3 según la Seleccionadora extranjera de Riesgos Moody's- febrero 2020.

1.15.2. Premios

- Buen manejo empresarial - octubre 2010, agosto 2008, agosto 2007.
- BN tiene Proyectos Inclusivos Exitosos estos son elogiados por la OEA Y CONADIS - diciembre 2010.
- Premios ALIDE - mayo 2010.
- BN afianzo como Buena Práctica de Gestión Pública el Sistema de Gestión de Calidad 2012 - julio 2012.
- Premio a la innovación Empresarial 2014 por nuestra ayuda progresista MultiExpress - noviembre 2014.
- BN tiene la agencia bancaria con mayor altitud del mundo, obteniendo un Récord Guinness - noviembre 2015.
- BN fue galardonado por su excelente Atención Al Ciudadano - Setiembre 2015.
- BN recibe el rotulo de Empresa Socialmente Responsable - junio 2017.
- BN recibe la distinción como Empresa Socialmente Responsable por segunda vez, otorgado por Perú 2021 y CENEFI - abril 2018.
- BN pasa a la final del Premio Ingenio Empresarial 2018 - octubre 2018.
- BN obtiene reconocimiento por Buena Práctica en Gestión Pública otorgada por CAD 2018 - octubre 2018.

- BN recibe la distinción como Empresa Socialmente Responsable por tercera vez - mayo 2019.
- BN recibe la distinción como Empresa Socialmente Responsable por quinta vez - junio 2021.

1.15.3. Reconocimiento

- Ranking Final Instituciones Públicas Ecoeficientes Modelo (EcoIP) 2022.
- Diploma Huella de Carbono Perú- Segundo Nivel.
- Diploma Huella de Carbono Perú- Primer Nivel.
- El staff legal del Banco de la Nación es incluido en la calificación de los mejores del Perú 2019-marzo 2019 de una prestigiosa publicación jurídica internacional.
- BN recibe dos premios por mejorar y verificar el nivel de sus operaciones - octubre 2018.
- Reconocimiento de la Liga Oncológica - noviembre 2016.
- BN recibe Certificación Leed Silver - Setiembre 2016.
- La Asociación de Buenos Empleadores certifica al BN como "Socio Emprendedor" - agosto 2016.
- Indecopi considera al BN en el concurso Primero los Clientes - marzo 2015.

1.16. Responsabilidad con la sociedad

El banco tiene tareas relacionadas al cumplimiento de los estándares y mediciones de los entes reguladores, así como de estándares organizacionales:

▪ Sostener el grado de madurez de la RSE (líder) reportado al FONAFE.

▪ Obtener el Distintivo Empresa Socialmente Responsable impulsado por Perú Sostenible (ex Perú 21).

CAPÍTULO II MARCO TEÓRICO

2.1. Precedentes del trabajo a estudiar

2.1.1. Precedentes Internacionales

El Phishing como riesgo informático, técnicas y prevención en los canales electrónicos: un mapeo sistemático.

Luis Fernando Rosero Tejada (2021), Universidad Politécnica Salesiana sede Guayaquil – Ecuador.

Las vías digitales o electrónicas envían y reciben información constante, pues mayor son las operaciones y peticiones de información realizadas en plataformas digitales o sitios web, la seguridad informática esta vulnerable ante este peligro y cada vez aumenta más. Lo grave del asunto es que ya no es un simple problema, a raíz de ello las instituciones que velan por nuestra seguridad lo pueden tipificar como delito informático, los afectados por esta amenaza son los usuarios que usan internet en su vida cotidiana, también son afectados empresas de todo tipo de rubro en especial las financieras dedicadas a actividades económicas.

La prioridad es que el phishing sea reconocido y por ende saber a lo que no enfrentamos para así evitarlo adecuadamente. Este trabajo analizara de forma descriptiva y cuantitativa, usara una técnica de rastreo automático en portales o sitios web que contengan materiales académicos relacionados con el phishing y sus características.

Al concluir el trabajo podremos ver estadísticamente la evolución en los últimos seis años, campañas de phishing, así como provincias con mayor tasa de incidencia; Se elabora una matriz de efectividad en base a la mayor proporción de denuncias y se presentan estrategias preventivas. En conclusión, el phishing evoluciona, se hace más prolijo convirtiéndose en un peligro informatico, por lo que hay que prevenirlo: educar y formar para reducirlo.

Desarrollo de sistema de análisis automático de Phishing.

Sergio Frontera Díaz de Quintana (2020), Universidad Autónoma de Madrid – España.

La tecnología se está desarrollando rápidamente y el boom de Internet todavía se sigue explotando. Internet ofrece cientos de oportunidades para que los ciberdelincuentes utilicen diversas tecnologías para llevar a cabo actividades ilegales con el fin de robar nuestra información más sensible, como información bancaria, información personal u otra información personal. La ciberseguridad es parte de las tecnologías de la información que cada vez cobra más importancia y hay que estar siempre alerta para luchar contra innumerables estafas que se difunden cada día en Internet.

El tipo más común de fraude digital es el phishing, donde el criminal suplanta a otra persona o empresa atrayendo a las personas para robar su información. En la actualidad existen muchas herramientas para prevenir el phishing. Los correos electrónicos son los más usados en las campañas de phishing, estos correos usan el protocolo SMTP deficiente en seguridad, DMARC se usa como complemento pues fusiona los protocolos SPF y DKIM haciendo la comunicación más segura mitigando el ataque del phishing.

Además, el uso del encabezado "Refer" en el protocolo HTTP ayuda a detectar muchos casos de phishing, Refer ayuda a detectar sitio web falsos que re direccionan a dominios verdaderos. Esta investigación da como solución desarrollar un software que se pueda instalar en cualquier computadora su arquitectura está basada en dos módulos (frontend del sitio web y API) para comunicarse. El trabajo de este software consiste en filtrar los sitios web en función de sus recursos y, a continuación, utilizar algún tipo de función hash para obtener un identificador único para cada sitio web, de modo que los datos puedan cotejarse con los ya

conservados en la base de datos.

La base de datos se actualiza, porque el software agrega información sobre los recursos del sitio, tanto legales como ilegales, lo que ayudará más adelante en el análisis de URL sospechosas, y también podrás ver información sobre la empresa que incluyas en la base de datos. También tiene un algoritmo que coteja o compara la relevancia o lo importante de un recurso web en relación con otros.

2.1.2. Precedentes Nacionales

Fraude informático en la modalidad de phishing y la necesaria actualización de la legislación para una eficiente persecución y sanción penal.

Nazario y Villanueva (2022), Universidad Señor de Sipán, Pimentel – Perú.

Este estudio examina el problema central de delito informático generada por campañas de phishing, esta problemática insta al estado peruano a modificar la legislación, se tiene como meta modificar la legislación con el fin de los castigos y sanciones penales sean ejemplares hacia los delitos informáticos ocasionados por campañas de phishing, considerando que fue desarrollado con un método mixto de enfoque cuantitativo y cualitativo, donde participan jueces, fiscales y abogados penalistas de la localidad de Chiclayo.

Se concluye que, Las nuevas leyes vigentes definen la ciberdelincuencia como un delito y están mejor regulados, es posible perseguir eficazmente el engaño informático conocido como phishing y ser penalizado, anteriormente este fraude quedaba impune ya que no se conocía al atacante y no dañaba directamente a la sociedad. un vacío legal para que otros en posesión de información electrónica puedan llevar a cabo estas actividades ilegales con impunidad.

El Phishing y su vulneración a la protección de datos personales en los delitos informáticos.

Aredo Luján, Luciano Antonio (2021), Universidad Cesar Vallejo, Trujillo – Perú.

El propósito general del estudio realizado es: Conocer que tan expuesto están la información personal tras ser atacados por técnicas de fraude informático o phishing y sus metas primarias: a) Conocer el alcance y efecto del phishing como apropiación de datos personales; b) Conocer la importancia del phishing y cómo proteger nuestros datos personales como medida de seguridad de nuestra privacidad c) analizar los presupuestos de delitos informáticos en el derecho penal peruano. El tipo de estudio es la investigación fundamental, porque sólo se analizan documentos, pero no se realiza ningún software.

En los resultados vemos un cambio necesario en la regulación, la forma de influir en una persona conduce a la comisión de otros delitos, y también se deben implementar campañas mediáticas que creen una cultura de prevención para evitar a la ingeniería social En cuanto a las conclusiones, se aprovechan de la falta de pedagogía informática haciendo trampas o artimañas. Se deben utilizar mecanismos de autenticación como huella digital y reconocimiento facial, señal digital con mensaje de texto, protección de datos personales. Las estimaciones de delitos informáticos utilizan definiciones muy generales que no permiten una demarcación adecuada del phishing.

El phishing como conducta delictiva no regulada en el ordenamiento jurídico peruano. Propuesta de incorporación del artículo 7-A en la ley de delitos informáticos 30096.

Hidalgo y Solano (2021), Universidad Nacional del Santa Chimbote – Perú.

El propósito de este estudio es concientizar sobre el problema existente al no contar con una ley clara en los procesos judiciales contra delitos informáticos, especialmente en los casos de phishing, donde existen ciertos métodos que no pueden clasificarse bajo ningún tipo de delito fijo en la Ley de Delitos Informáticos; Esto crea impunidad para tales comportamientos porque es difícil para un ministerio público actuar como motor del crimen.

El presente trabajo de investigación describe y aplica métodos científicos y legales de tal manera que preparamos un proyecto de ley específicamente para regular el phishing en su forma penal, que incluya todas las formas de perpetrar esta actividad ilegal.

2.2. Marco histórico

2.2.1. Marco histórico, Nacimiento del Phishing

Desde que apareció el internet el día 7 de abril de 1969, conocido como ARPANET, el Phishing tuvo su nacimiento 26 años después alrededor de 1995, pero para la gente común este tipo de estafas se hizo conocido recién después de 10 años, sin embargo, no le quitemos relevancia ya que desde el inicio fue una amenaza en potencia para las víctimas de tales estafas.

Esta técnica usa correos electrónicos y sitios web falsos como señuelos que invitan a las personas a digitar sus datos confidenciales, por este motivo el término Phishing se usa para describir estas técnicas. Otra buena razón para usar el “ph” reemplazando la “f” en la ortografía del término es que los primeros hackers que exploraban, experimentaban y estudiaban los sistemas de comunicación eran conocidos como phreaks, entonces la ortografía “ph” sirve para vincular las estafas de Phishing con las comunidades de hackers.

El primer ataque registrado fue en la década de los 90, el 2 de enero de 1996. Un noticiero de Usenet llamado AOHell, menciono

que en la empresa proveedora de internet América Online (AOL) se producía los primeros ataques el cual sería inicio de un gran problema criminal. La primera forma de ataque consistía en robar las contraseñas de los usuarios y con un algoritmo crear números de tarjetas de crédito aleatorios, las mismas que servían para abrir cuentas en AOL, cuentas que se usaban para enviar spam a otros usuarios.

AOL logro frenar el ataque con el generador de números de tarjeta de créditos aleatorios, no obstante, los phishers crearían una nueva técnica que hasta el día de hoy perdura, se trata del uso de los sistemas de mensajería instantánea y correo electrónico de AOL, se remitían mensajes a los usuarios haciéndose pasar por trabajadores de AOL. Estos mensajes solicitaban a los usuarios verificar sus cuentas o que validen la información de su facturación.

Victor Poitevin(stormshield) El Phishing un mecanismo malicioso para timar a una persona, llevándole a realizar acciones peligrosas con el fin de robarle sus datos personales, como fechas especiales, contraseñas, números de tarjeta de crédito, esta técnica emplea diferentes formas para hacerse de la información, las más usadas son clonacion de sitio web, de nombres de dominio, de identidades, etc. Y usa canales como correos electrónicos, llamadas de voz, sms, etc.

Teniendo como base estas afirmaciones nace el concepto de Spray and Pray en el año 2000 que consiste en hacerse pasar por una empresa reconocida mundialmente y va dirigido a direcciones de correos electrónicos de forma masiva, se hace más atractivo cuando a los correros llegan asuntos como premios de loterías, campañas benéficas, cierre de su cuenta bancaria, sin embargo las primeras campañas de phishing eran reconocibles ya que tenían muchas faltas ortográficas, de tipografía e imágenes de pésima calidad.

En consecuencia y siguiendo las nuevas prácticas los ciberdelincuentes ahora son unas organizaciones estructuradas que en su conjunto buscan vulnerar los correos de empresas B2B como por ejemplo Microsoft, en el 2022 un proveedor de ciberseguridad Vade encontró casi 23 millones de email de phishing que se hicieron pasar por Microsoft, los proveedores de ciberseguridad le hacen frente a este ataque usando filtros antiphishing basados en sobres de correos, contenidos, direcciones IP y tecnologías de doble autenticación.

La publicidad para concientizar al público ante este peligro ha hecho que las campañas de phishing sean más complejas y sofisticadas llegando hacer uso de psicología para llevar siempre a la víctima hacer algo, los correos simples ya no sirven estos deben crear una necesidad de urgencia, miedo hasta codicia para motivarlos hacer clic.

Algunas Citas:

Adrien Gendre (Vade):
Cuando aparecio el phishing, los objetivos eran principalmente personas a través de marcas de consumo. El episodio de AOHell es un gran ejemplo de esto, ya que American Online era una marca sólida y un actor importante en el mercado de ISP en ese momento. Entonces el mismo escenario puede afectar a millones de usuarios.

Adrien Gendre (Vade):

En el pasado, algunos actores individuales atacaban con la tecnica de phishing a una que otra víctima. Ahora hablamos de organizaciones cibercriminales estructuradas que utilizan el phishing para obtener ingresos, espionaje industrial o guerra económica. Esto nos lleva a actividades de phishing que imitan a las marcas B2B.

Sébastien Viou(stormshield):

Los ciberdelincuentes explotan las emociones primarias de sus víctimas para asegurarse el máximo de clics, principalmente por miedo. Miedo a perder dinero, miedo a cancelar un pedido, miedo a ser despedido; A menudo estos miedos son incontrolables y provocan una rápida reacción instintiva. Por eso este tipo de ataque tiene tanto éxito.

Así llegamos a la modernización de las campañas de phishing, los ciberdelicuentes usan herramientas automatizadas como Gophish, sniperphish. Estos utilizan moldes de páginas de captura, patrones de correo electrónico ya listas, donde para poder engañar a sus víctimas los ciberdelincuentes se adaptan a las tendencias de la sociedad y redes sociales, los mismos que pasaron a ser las marcas más usadas en este tipo de campañas y tras la aparición de la pandemia covid-19 las empresas de reparto como DHL, FedEX, Amazon y AliExpress son las marcas más suplantadas.

2.2.2. Marco histórico del Banco de la Nación

Tener un banco es una necesidad tan antigua, desde que aparecieron las sociedades las personas operaban con cambios y créditos a nivel personal, de inmediato todo se puso más complejo, las funciones crecieron abarcando más personas de esta manera se forman las organizaciones, claro ejemplo es Grecia en el siglo IV A.C. se crearon bancos públicos administrados por personas entrenadas para esta labor.

El banco de la nación se creó cuando el congreso acepto la ley 16000 el 27 de enero de 1966. Días más tarde el ejecutivo presidido por Fernando Belaunde Terry le da el alta. La espera había terminado pues muchos años atrás en el año 1914 nace la necesidad de formar un banco que consolidara las tareas, económicas y financieras.

El predecesor del Banco Nacional fue el establecimiento de los Fondos de Depósito y Transferencia en 1905, encabezados por el Sr. José Pardo con la ley de 2 de noviembre de 2005 núm. 53. La Agencia amplió sus actividades en 1927 y, según la Ley núm. 5746 se le encomendó la responsabilidad de gestionar los estancos de tabaco y opio, así como recaudar los ingresos públicos, derechos e impuestos de licores, defensa, etc. Por último, en diciembre del mismo año, fue designado encargado de toda la recaudación de ingresos de todo el país.

Se nacionaliza las agencias de envíos y recepción de dinero mediante el Decreto Supremo N° 47 el 9 de agosto de 1963 proclamándola de necesario para el uso público, el Estado empezó a recaudar nuevamente los impuestos, a custodiar los depósitos administrativos y judiciales, gracias al decreto antes mencionado, esta privatización se produjo cuando las agencias bancarias contaban con diez bancos entre sus socios: Crédito, Popular, Internacional, Wiese, Comercial, Continental, Gibson, De Lima, Unión y Progreso.

El Banco de la Nación tuvo las siguientes funciones:

- Reunir el dinero del estado, las sociedades y municipios del sector público independiente según el acuerdo.
- Aceptaba o no depósitos de inversiones únicamente del sector público y del estado peruano, excluidos las cajas estatales y el Banco Central de Crédito.
- Se realizaba el abono de las órdenes de pago emitida por el sector publico usando sus propios fondos.
- Se le consignaba la custodia de todos los laudos judiciales y administrativos.
- Llevar a cabo la función de recaudación tributaria.

  El 12 de junio de 1981, durante el segundo mandato de Fernando Belaúnde Terry, se promulgó el Decreto Legislativo Ley Orgánica No. 199, que otorgó funciones adicionales al

Banco de la Nación.

- consolidar los tributos del Sector Público Nacional.
- Realizar transacciones de crédito activas y pasivas con bancos del extranjero y nacionales netamente a nombre y cuenta del Estado.
- Recauda depósitos de fondos exclusivamente del sector público y de empresas estatales en todo el país, excluyendo los bancos y cajas financieras nacionales.

Alberto Fujimori Fujimori, actualizo las labores del banco mediante el Decreto Supremo N° 07- 94-EF en 1994, estas funciones se ejecutarán sin exclusividad alguna en las empresas que trabajan en el rubro financiero:

- Pagos de acuerdo con las directrices proporcionadas por la Dirección General del BCR.
- Trabajar como recaudador de deudas en nombre de los contribuyentes.
- Ofrece y gestiona, transacciones de las subcuentas bancarias del BCR.
- Actúa como caja bancaria del gobierno.
- Interactúa con otros bancos para realizar operaciones financieras como transferencias.
- Realiza operaciones de comercio exterior a favor del estado.
- Ofrece oportunidades de financiación a municipios, gobiernos regionales, al estado cuando no cuentan con el apoyo del Sistema Financiero Nacional.
- El banco no se limita para brindar facilidades de pagos u otra operación financiera ya que no están sujetas a la Ley General de Bancos, Instituciones Financieras y Aseguradoras.
- Ofrece servicios de correo.
- Ofrecer a los proveedores del Estado y a las entidades del sector público nacional servicios de cuenta corriente.
- Obtenga créditos incluso en lugares sin sucursales bancarias.

2.3. Marco Legal

LEY NO. 30096

JEFE DE ESTADO

CONSIDERANDO:

Que el Congreso de la República

ha expedido la siguiente ley:

CAPÍTULO I:

LEY, SU OBJETO Y FINALIDAD

Artículo 1: Objeto de la Ley

Para combatir mejor la delincuencia en Internet, la ley pretende prevenir y sancionar las actividades delictivas que utilizan tecnologías de la información, incluidas las relacionadas con softwares, base de datos y demás activos ilícitos asociados a la delincuencia.

CAPÍTULO II

DELITO DE SISTEMAS DE DATOS E INFORMACIÓN

Artículo 2: Accesos ilegales.

El individuo que desobedeciere los protocolos de seguridad establecidos para impedir el uso no autorizado de todo el sistema informático o de una parte del mismo, se enfrentará a una pena mínima de un año, máxima de cuatro y de treinta a noventa días de prisión. Cualquiera que utilice el sistema informático más de lo permitido se enfrentará a las mismas consecuencias.

El texto del primer artículo de la Ley nº 30171, que se publicó el 10 de marzo de 2014, modifica este artículo:

Artículo 2: Acceso ilícito

Quien intencional e ilícitamente utilice cualquier parte o la totalidad de un

sistema informático será sancionado con restricción de libertad mínima de un año y máxima de cuatro años, así como con multa de treinta a noventa días, si viola las reglas de seguridad establecidas para impedirlo. Cualquiera que utilice el sistema informático por encima de lo permitido se enfrentará a las mismas consecuencias.

Artículo 3: Atentados en contra de la integridad de los datos informáticos.

Los usuarios de tecnologías de la información y la comunicación que introduzcan, supriman, dañen, alteren, borren o hagan inaccesibles datos informáticos se exponen a una pena de prisión de tres a seis años y a una multa de ochenta a ciento veinte días.

El artículo 1 de la Ley N° 30171, promulgada el 10 de marzo de 2014, modificó este artículo, su contenido es la siguiente:

Artículo 3: Violación la veracidad de los datos informáticos.

Quien haya destruido, alterado, degradado, alterado, suprimido o impedido el acceso a la información de manera deliberada e ilícita, se expone a una condena mínima de tres años de cárcel y máxima de seis años de confinamiento, junto con una multa de 80 a 120 días.

Artículo 4: Intento de comprometer la integridad de un sistema informático

Una persona conlleva un castigo mínimo de tres años de cárcel, con una pena máxima de seis años de prisión por utilizar información tecnológica y comunicación para destruir cualquier parte o todo un sistema informático, restringir el logueo al mismo, interferir en él o imposibilitar el control de cualquier sistema informático o el servicio.

Este artículo fue revisado por la Ley N° 30171, que entró en vigencia el 10 de marzo de 2014. Su nuevo texto es el siguiente:

Artículo 4: Ciberataques contra la veracidad de los sistemas informáticos.

El operador de un sistema informático serán penalizados con la privación de libertad. mínima de tres años, máxima de seis años y multa de ochenta

a ciento veinte días por inutilizar, bloquear el acceso o impedir el funcionamiento del sistema de manera intencional e ilegítima.

CAPÍTULO III

DELITOS VINCULADOS CON LA INFORMÁTICA, RELACIONADOS CON AGRESIONES Y ABUSOS SEXUALES

Artículo 5: Las agresiones sexuales contra jóvenes y menores a través de las tecnologías

Según los apartados 1, 2 y 4 del artículo 36 de la norma Penal, una persona que utilice las tecnologías de la información y la comunicación para ponerse en contacto con menores de 14 años y le pida o reciba fotos inapropiadas o participe en actividades sexuales con él puede ser detenida y enfrentarse a un mínimo de cuatro años de prisión y un máximo de ocho. Tampoco se les podrá permitir competir. El artículo 36 (1), (2) y (4) del Código Penal prohíbe la competencia y estipula que engañar a una víctima de entre 14 y 18 años conlleva una pena mínima de tres años y una máxima de seis.

Este artículo fue revisado por la Ley N° 30171, que entró en funcionamiento el 10 de marzo de 2014. Su nuevo texto se presenta a continuación:

Artículo 5: Protecciones contra la actividad sexual infantil mediada por tecnología.

Quien contacte personas menores de catorce años a través de Internet u otro medio similar, con la intención de solicitar o recibir material pornográfico o de mantener relaciones sexuales con ella, debe ser sancionado con cuatro años de prisión como mínimo y ocho años como máximo. Además, la participación está prohibida en virtud de los apartados 1, 2 y 4 del artículo 36 del Código Penal. Si hay fraude y la víctima tiene entre 14 y 18 años, El castigo es de tres a seis años de cárcel.

CAPÍTULO IV

DELITOS INFORMÁTICOS RELACIONADOS CON LA CONFIDENCIALIDAD Y LA PRIVACIDAD EN LAS COMUNICACIONES

Artículo 6: Tráfico de datos ilícitos

Se castigará, mínimo tres años y máximo cinco años de prisión a quien cree, utilice o haga un uso indebido de una base de datos de una persona física o entidad jurídica reconocida o diferenciable con el fin de comercializar, transmitir, vender, publicitar, promocionar u ofrecer información relativa a cualquier asunto personal, familiar, patrimonial, profesional, financiero o de otro tipo, haya causado o no perjuicios.

La Disposición Derogatoria Complementaria Única de la Ley N° 30171, promulgada el 10 de marzo de 2014, derogó este artículo.

Artículo 7: Interceptación de datos con ordenadores

Una persona será encarcelada si utiliza tecnología de la información o las comunicaciones para interceptar transmisiones privadas dentro, fuera o en el interior de un sistema informático. Esto incluye las señales electromagnéticas del sistema informático que incluyan datos informáticos. una multa de tres años o más, pero no inferior a seis.

Si las leyes pertinentes consideran que el material implicado en el delito es secreto, restringido o confidencial, la pena tiene duración mínima de cinco años y ocho la máxima.

Si el delito pone en peligro la protección, seguridad o integridad territorial, la condena deberá cumplirse durante 8 años mínimo y 10 máximo.

El artículo 1 de la Ley N° 30171, promulgada el 10 de marzo de 2014, modificó este artículo. Su contenido es el siguiente:

Artículo 7: Intromisión de datos con ordenadores

Cumplirá una pena de tres años de prisión como castigo como mínimo y seis años como máximo, el que intencional e ilegalmente intercepte comunicaciones privadas destinadas a un sistema informático que se originen u ocurran dentro de un sistema informático, incluyendo la señal electromagnética de un sistema informático que se utiliza para transferir

este tipo de datos.

Si la falta involucra material clasificado como secreto, reservado o confidencial según la Ley 27806, la Ley de Transparencia y la Ley de Acceso a la Información Pública, la pena mínima es de cinco años de cárcel y la máxima de ocho años.

Si el delito expone al peligro la defensa, seguridad o soberanía de la nación, la pena mínima es de ocho años de prisión y la máxima de diez años.

Si el agente decide cometerlo.

CAPÍTULO V

CRIMENES INFORMÁTICOS HACIA LA PROPIEDAD

Artículo 8: Timo informático

El que utilice las tecnologías de la información y la comunicación para formar, integrar, cambiar, borrar, clonar o interferir en el funcionamiento de datos informáticos con el fin de obtener beneficios ilícitos para sí o para otros, o que cause daño a un tercero, se enfrenta a penas de cárcel. de sesenta a ciento veinte días de multa, así como un mínimo de tres y un máximo de ocho años.

Si se trata de bienes del Estado dirigidos a ser benéficos o a un programa de asistencia social, la pena es de ochenta a cuarenta días de prisión y un mínimo de cinco años de cárcel.

El artículo 1 de la Ley N° 30171, promulgada el 10 de marzo de 2014, modificó este artículo. Su contenido es el siguiente:

Artículo 8: Delito cibernético

Por diseñar, implementar, cambiar, borrar, eliminar, clonar o interferir o manipular de cualquier manera el uso de un sistema informático, una persona puede ser sancionada con pena privativa de libertad mínima de tres años y máxima de ocho años, así como con multa de hasta sesenta a ciento veinte días, por buscar voluntaria e ilícitamente beneficios ilícitos para sí o para otro a costa de un tercero.

Si afecta a bienes del Estado direccionados con fines benéficos o a un

programa de asistencia social, la pena es de ochenta a cuarenta días de prisión y un mínimo de cinco años de cárcel.

CAPÍTULO VI

CIBERDELITOS QUE MINAN LA CONFIANZA DE LOS CIUDADANOS

Artículo 9: usurpación de identidad

Cualquier persona declarada culpable de fraude patrimonial o intelectual, que implica proporcionar información falsa de datos secretos de una persona normal o judicial mediante el uso de tecnologías de la información y la comunicación, se enfrenta a un castigo mínimo de tres años de prisión y cinco máximos.

CAPÍTULO VII

DIRECTRICES COMUNES

Artículo 10: Uso indebido de equipos y programas de computadoras.

Quien diseñe, desarrolle, fabrique, comercialice, distribuya, importe u obtenga uno o más programas, dispositivos, contraseñas, identificadores u otros datos informáticos con la intención de utilizarlos para perpetrar cualquiera de los delitos enumerados en esta ley. Quien preste o realice un servicio que persiga este objetivo se enfrenta a una pena mínima de uno a cuatro años de prisión, con una penalidad de treinta a noventa días.

El artículo 1 de la Ley N° 30171, promulgada el 10 de marzo de 2014, modificó este artículo. Su contenido es el siguiente:

Artículo 10: Uso incorrecto de computadoras y programas informáticos.

Será reprimido con prisión mínima de uno a cuatro años y sanción de treinta a noventa días, quien a sabiendas e ilícitamente crea, elabore, diseñe, desarrolle, vende, publicite, distribuye, importe u obtuviese para su uso cualquier mecanismo, programa informático, dispositivo, contraseña, clave de acceso u otra información informática que sea creada específicamente para cometer delitos contra la persona protegida por esta ley.

Artículo 11.- Agravantes

Para un delito menor enumerado en esta Ley, un magistrado puede ampliar la sentencia hasta un tercio del máximo legal si:

1. si el agresor es miembro de un grupo delictivo en el momento de cometer el delito.

2. Cuando el atacante comete un delito accediendo a datos o información confidencial en el ejercicio de su cargo o funciones, o abusando de su posición privilegiada para conocer esas historias.

3. El agente comete un delito con ánimo de lucro, pero sólo por delitos relacionados con estas circunstancias.

4. La seguridad, la defensa, el bienestar y la soberanía de la nación corren peligro a causa de estos delitos.

Artículo 12: Inmunidad de jurisdicción penal

No incurre en responsabilidad penal quien realice las pruebas aprobadas u otras acciones autorizadas enumeradas en los artículos 2, 3, 4 y 10 para salvaguardar los sistemas informáticos. Artículo aprobado por la Ley N° 30171, difundida el 10 de marzo de 2014, según consta el artículo 3.

RESUMEN DE LAS CONDICIONES SUPLEMENTARIAS

PRIMERA: codificar toda pornografía juvenil.

Para que lo guardias nacionales puedan desempeñar las funciones, sólo puede conservar fotos de niños en plataformas informáticas de almacenamiento que cuenten con la aprobación y supervisión del Ministerio. Para ello, existe una base de datos codificada.

En un plazo de 30 días, el departamento de justicia y la Policía Nacional del Perú crearán un protocolo de coordinación que garantice el cumplimiento de los lineamientos señalados en la página anterior.

SEGUNDA: Agente encubierto de ciberdelincuencia

Los fiscales pueden investigar los delitos que están cubiertos por este estatuto, así como los delitos que se cometen utilizando la tecnología. La Ley 957 autorizó el artículo 341 del Código de Procedimiento Penal, que

permite la comunicación incluso en relación con una asociación delictiva.

TERCERA: Alianzas del Ministerio Público y la Policía Nacional del Perú a través de las fronteras institucionales.

Las tareas de investigación del Ministerio Público están siendo coordinadas por una agencia separada que la Policía Nacional del Perú está fortaleciendo. La Policía Nacional del Perú recopila datos, intercambia experiencias en la creación de actividades y programas para perseguir adecuadamente la ciberdelincuencia, y elaborar planes de seguridad y defensa con el objeto de crear canales de dialogo con las áreas administrativas del Ministerio Público.

El artículo 2 de la Ley N° 30171, promulgada el 10 de marzo de 2014, modificó esta disposición. Contiene lo siguiente:

TERCERA: Alianzas entre el Ministerio Público, la Policía Nacional y otras organizaciones especializadas más allá de los límites institucionales

La Policía Nacional del Perú está reforzando una unidad especializada encargada de coordinar los hallazgos con el Ministerio Público. Proporcionar canales de comunicación con las oficinas administrativas del Ministerio de Estado, la Policía Nacional, la Agencia de Gobierno Electrónico y Tecnologías de la Información (ONGEI), el Centro Gubernamental de Respuesta Temprana a Ciberataques (Pe-CERT) y unidades especiales de las Fuerzas de Defensa. recopila datos, difunde su experiencia a la hora de formular directrices y protocolos para el procesamiento eficaz del crimen cibernético y crea planes de seguridad y defensa.

CUARTA: colaboración efectiva

Para aplicar esta ley en la lucha contra el fraude en Internet deberán establecerse procedimientos para mejorar la colaboración operativa en los treinta días siguientes a su entrada en vigor. Estos protocolos deben garantizar que la Policía Nacional del Perú, el Departamento de Estado, el poder judicial y los actores del sector privado puedan compartir

información, colaborar en equipos de investigación, entregar documentos, realizar escuchas telefónicas y realizar actividades similares.

Sección reformada por el artículo 2 de la Ley N° 30171, que fue publicada el 10 de marzo de 2014, y que tiene el siguiente texto:

CUARTA: Cooperación operativa

El Ministerio, el Poder Judicial, la Policía Nacional del Perú, el Pe-CERT (Centro Gubernamental de Respuesta Temprana a la Ciberseguridad) y otras partes relevantes se asegurarán de que se comparta la información, se formen equipos de investigación conjunta, se entreguen los documentos y se realicen las comunicaciones, interceptados y se toman medidas similares para garantizar la implementación de la ley, en el plazo de treinta días desde la aprobación de esta ley, los organismos de defensa, la ONGEI (Agencia Nacional de Gobierno Electrónico y Tecnologías de la Información), los actores del sector privado que participan para erradicar el ciberdelito y las agencias especiales relacionadas con la defensa crearán protocolos actualizados de cooperación operativa.

QUINTA: Capacitación

La Policía Nacional del Perú, el Ministerio de Estado y el ordenamiento jurídico dispondrán capacitaciones para mejorar el talento profesional del personal, particularmente en lo que respecta a la tramitación de infracciones enumerados en esta ley. Esta es una responsabilidad de los organismos estatales comprometidos con la prevención y erradicación de los delitos informáticos.

SEXTA: Medidas de seguridad

Para proteger la autenticidad de los datos y sistemas informáticos sensibles, la Oficina Nacional de Gobierno Electrónico y Tecnología de Información (ONGEI) colabora con empresas del sector público para avanzar en medidas de seguridad aún más estrictas.

SÉTIMA: Buenas prácticas

El Estado del Perú colabora con otros países para implementar medidas y

métodos específicos para combatir ataques a gran escala contra infraestructuras de TI y preparar las medidas preventivas necesarias, incluyendo respuesta e intercambio de conocimientos y excelentes prácticas.

OCTAVA: Acuerdos bilaterales

El Gobierno del Perú Apoya la ratificación y firma de varios acuerdos de cooperación con otros países para perseguir los delitos informáticos.

NOVENA: Terminología

En este estatuto se cita el artículo 1 del Convenio de Budapest de 23.XI.2001 sobre ciberdelincuencia:

a. Un programa de computo es cualquier equipo, único, grupo de dispositivos relacionados o red de dispositivos relacionados cuya función principal es procesar datos automáticamente cuando se ejecuta un programa.

b. Los datos informáticos incluyen programas creados para llevar a cabo las funciones de los sistemas informáticos y representar eventos, información o conceptos de una manera apropiada para el procesamiento de computo.

DÉCIMA: Control y sanciones monetarias por parte de la AFP, Superintendencia de Banca y Seguros

Dependiendo de las particularidades, complejidad y circunstancias de cada caso, la Inspección Bancaria, Seguros y AFP establece el monto de la multa a las empresas de su competencia que violen las cláusulas del artículo 235 inciso 5 del reglamento penitenciario autorizado mediante el Decreto 957.

Para calcular la multa, el tribunal notifica al órgano de control la negligencia de la empresa, así como las precauciones tomadas en relación con los detalles, la complejidad y las circunstancias del caso en un plazo de setenta y dos horas.

UNDÉCIMA: El Organismo Supervisor de la Inversión Privada en Telecomunicaciones regula y establece las multas

La autoridad supervisora establece una escala de multas para las inversiones en telecomunicaciones privadas. Esta escala se fundamenta en las peculiaridades, la complejidad y las circunstancias del caso que se aplican a empresas que están bajo su supervisión e incumplen las obligaciones previstas en el artículo 230 inciso 4 del Código Penal. Decreto 957 que confirma la orden.

Para imponer la multa, el juez deberá notificar al consejo de control la negligencia del negocio y medidas de seguridad adecuadas a las particularidades, complejidades y circunstancias del caso en un plazo de setenta y dos horas. Sección reformada por el artículo 2 de la Ley N° 30171, que fue difundida el 10 de marzo de 2014, contiene lo siguiente:

UNDÉCIMA: La Agencia Supervisora de Inversión Privada en Telecomunicaciones regula e impone penalidades

Las empresas bajo la tutela del organismo de supervisión de inversiones en telecomunicaciones están sujetas a multas si no cumplen las condiciones establecidas en el artículo 230, párrafo 4 de la Ley de Procedimiento Penal, aprobada por el Reglamento 957. Empresarios de telecomunicaciones organizan su personal y suministros de manera que les permita cumplir con prontitud y diligencia las responsabilidades estipuladas en el artículo 230, párrafo 4, de la Ley de Procedimiento Penal. El juez notifica a la autoridad de control la negligencia de la empresa en un plazo de 72 horas, permitiendo a la autoridad de control imponer la sanción correspondiente.

MODIFICACIÓN DE CLÁUSULAS COMPLEMENTARIAS

PRIMERA: Modificación a la Ley 27697, quien faculta a la fiscalía intervenir y monitorear comunicaciones y registros privados en circunstancias extraordinarias.

Se modifica el Decreto Legislativo 991 y la Ley 30077, al artículo 1 de la Ley 27697, que faculta a la fiscalía intervenir y regular las transmisiones y

registros secretos en casos extraordinarios. Corregido por errores

Artículo 1: Estructura e intención

El objetivo de esta ley es mejorar la autoridad constitucional brindada a los tribunales para supervisar y escuchar a la persona sometida a investigación preliminar o detención judicial.

Son únicos los delitos para los cuales se podrá utilizar la autoridad de esta ley:

1. Rapto.
2. Esclavitud moderna (Trata de personas).
3. Pornografía protagonizada por niños.
4. Robo grave.
5. Coerción.
6. Narcotráfico.
7. Trata de personas migrantes.
8. Crímenes de lesa humanidad.
9. Traición y atentados a la seguridad nacional.
10. Malversación de fondos.
11. Corrupción oficial.
12. Actos de terror.
13. Infracciones aduaneras y fiscales.
14. El blanqueo de dinero.
15. Crimenes cibernéticos.

SEGUNDA: Modificación a la Ley 30077: Ley que Prohíbe el Crimen Organizado. Modificar la Ley contra el crimen organizado de la Ley 30077, Artículo 3, Numeral 9, para quedar así:

Artículo 3: Entre los crímenes están

Estos delitos están cubiertos por esta ley:

TERCERA: Reformas del Código Procesal Penal

Modificado por el Decreto Legislativo 957 y reformado por la Ley 30077, actualícese el numeral 4 del artículo 230, el numeral 5 del artículo 235 y el

literal a) del numeral 1 del artículo 473 del Código Procesal Penal en las siguientes formas:

CORREGIDO POR ERRORES

Artículo 230: Infiltración, grabación de llamadas telefónicas u otro tipo de comunicación.

Los operadores de los servicios telefónicos públicos tienen que proporcionar información sobre la ubicación de los teléfonos móviles, las perturbaciones en las comunicaciones, grabación, registro y la identificación del prestador del servicio telefónico en un plazo máximo de 30 días hábiles.

Brindar acceso irrestricto a clientes, teléfonos y dispositivos celulares y números de protocolo de internet en cumplimiento de órdenes judiciales en tiempo real, las 24 horas del día, los 365 días del año. Tenga en cuenta que no hacerlo puede resultar en responsabilidad legal. Los empleados de la empresa deben mantener la confidencialidad a menos que sean firmados como testigos en cualquier actividad. El plazo lo establece el tribunal en función de la naturaleza, circunstancias y complejidad del caso.

Dichos licenciatarios brindan su logueo tecnológico, compatibilidad y vinculación al Sistema de Comunicación y Vigilancia de la Policía Nacional del Perú. Cuando los licenciatarios actualicen su hardware o software debido a actualizaciones técnicas, Tienen que seguir trabajando con el Sistema de Comunicación y Vigilancia de la Policía Nacional del Perú.

Artículo 235: Se levanta la confidencialidad bancaria.

Las empresas u otras entidades que estén sujetas a una orden judicial están obligadas a proporcionar datos, registros y documentos pertinentes (incluidos sus originales si es necesario), así como enlaces adicionales al Procedimiento decisorio, todo dentro de un máximo de 30 días hábiles después de siendo informados de sus obligaciones legales. El plazo lo fija el juez de acuerdo con los detalles, complejidad y circunstancias de cada caso.

Artículo 473: Alcance y competencia del proceso

Podrán ser objeto de convenio, además de los previstos por la ordenanza, los siguientes delitos:

- ✓ Afiliación ilegal
- ✓ terrorismo,
- ✓ blanqueo de dinero
- ✓ cibercriminal
- ✓ contra la humanidad.

CUARTA: Reformas al Código Penal Artículos 162, 183-A y 323

Modificar las siguientes disposiciones de los artículos 162, 183-A y 323 del Código Penal, aprobado por Decreto Legislativo 635:

Artículo 162: Interferencia de teléfonos

Las penas impuestas a quien interrumpa o escuche injustificadamente una llamada telefónica u otra conversación son un mínimo de tres años y un máximo de seis años de prisión.

El artículo 36, numerales 1, 2 y 4, establece que, si el agente es funcionario público, la pena será mínima de cuatro años y máxima de ocho años de prisión e inhabilitación. Si el delito involucra información que la normativa aplicable clasifica como secreta, reservada o confidencial, la pena mínima es de cinco años de cárcel y la máxima de ocho años. Si el delito pone en peligro la defensa, la seguridad o la soberanía del Estado, la pena mínima es de ocho años de cárcel y la pena máxima de diez años.

Comparar con el Artículo 4 de la Ley N° 30171, publicada el 10 marzo 2014.

Artículo 183-A: pornografía juvenil

Cualquier persona que tenga, promocione, cree, distribuya, muestre o difunda, traiga o exporte cualquier obra escrita, imagen, grabación de sonido, video o artículo, donde se muestre espectáculos pornográficos en vivo presentando a seres humanos menores de edad entre las edades de 14 y 18 años serán sancionadas con multa de 125 a 315 días de cárcel, así como pena de prisión no menor de 6 ni mayor de 10 años.

Se impondrá una pena de prisión mínima de diez años y máxima de doce años, así como de cincuenta a trescientos sesenta y cinco días de multa, cuando:

1. El menor tiene menos de catorce años.
2. Mediante el uso de las tecnologías de la información y las comunicaciones se difunden contenidos pornográficos.

La pena consiste en un mínimo de doce años y un máximo de quince años de cárcel si la víctima cumple alguno de los criterios enumerados en el último párrafo del artículo 173, o si el agente participa en una organización que promueva la pornografía infantil. En este caso, el representante será inhabilitado conforme a los apartados 1, 2 y 4 del artículo 36.

Artículo 323: Prejuicio

Se impondrá pena mínima de dos a tres años de prisión o de sesenta a ciento veinte días de servicios comunitarios al que, directamente o por medio de terceros, discrimine a una o más personas o grupos, o que abiertamente aliente o promueva discriminación por motivos de raza, religión, orientación sexual, factor genético, afiliación, edad, discapacidad, idioma, identidad étnica o cultural, vestimenta, política u otras opiniones del Estado, o por posiciones financieras encaminadas a cancelar o debilitar el reconocimiento y ejercicio de los derechos humanos.

Según el artículo 36, párrafo 2, la pena será mínima de dos años y máxima de cuatro años, así como la inhabilitación, si el agente es funcionario o trabajador administrativo. Si la discriminación se realizó utilizando tecnologías de la información o las comunicaciones, o si se realizó con el uso de violencia corporal o psicológica, se considera la denegación de libertad mencionada en el párrafo anterior.

Comparar con el Artículo 4 de la Ley N° 30171, publicada el 10 marzo 2014.

QUITAR LA SECCIÓN COMPLEMENTARIA

ÚNICA: Se Deroga
Se derogan el artículo 186, segundo párrafo, número 4, y los artículos 207-A, 207-B, 207-C y 207-D del Código Penal. RECTIFICADO POR ERROR

2.4. Marco Teórico

2.4.1. Marco teórico de Phishing

Una de las teorías relacionadas a como no ser víctimas del phishing es la teoría de crear una cultura de concientización sobre la ciberseguridad.

Christopher Hadnagy (2018) indica que el comportamiento habitual del trabajador incide mucho para la evaluación y tomas de decisiones dentro de la organización, el simple hecho de abstenerse a comer por estar dentro de un programa de dieta ya demuestra el grado de conciencia que tiene para lograr bajar de peso, verse bien y mejorar su salud, estos resultados serían su recompensa, entonces para los trabajadores que detectan el phishing también deben tener su recompensa que los motive a realizar el trabajo.

Christopher Hadnagy (2018) hace énfasis en como motivar a los trabajadores ya que no todos toman a bien recibir capacitaciones y lo ven como pérdida de tiempo, pero con ideas simples como darles recompensas, reconocimientos hace que se genere una cultura de concientización sobre la ciberseguridad, de esta manera los trabajadores comenzaran a tomar mejores decisiones (p. 271).

Yolanda corral (2021) sobre la ciberseguridad, manifiesta que el brote de COVID-19 ha maximizado el uso de internet y concientizar en seguridad digital es la clave, la ciberseguridad va ganando fuerza ya sea porque las personas, empresas y organizaciones se

han dado cuenta de lo importante y necesario que es para salvaguardar la información, mejor ser preventivos que reaccionar después de un ataque.

La evolución digital pandémica llego para quedarse, esto debe ser clave para entender que, si no se trabaja en infraestructuras de ciberseguridad, auditorias constantes para saber cómo están las empresas y sobre todo formar a los trabajadores en ciberseguridad poco o nada se podrá hacer ante campañas de phishing modernas y automatizadas.

Kevin Mitnik (2018) en su libro “Ghost in the Wires” comparte todas sus hazañas sobre como introducirse dentro de las instituciones particulares y estatales como el FBI, haciendo uso de ingeniería social y conocimientos de programación, a raíz de esto Mitnik fue encarcelado en varias oportunidades para luego por cosas del destino lo contratan para ser consultor de seguridad, brinda consejos como nunca dar tu contraseña a nadie, capacitación constante para los trabajadores a cerca de ciberseguridad, renovar cada cierto tiempo las contraseñas, concientizar sobre lo importante que es cada puesto e información que maneja el trabajador.

Entonces para hacer frente a estos ataques los autores mencionados anteriormente coinciden en algunas estrategias y técnicas de prevención, ya sabemos que actualmente una campaña de phishing envía un correo electrónico malicioso para obtener su usuario y contraseña, para no caer en el engaño se utilizan técnicas de detección como son software de clasificación de correo, programas de concientización y no esta demás contratar proveedores de servicios de seguridad, es importante también aprender de experiencias anteriores ello se puede hacer usando un software con algoritmo de aprendizaje automático.

Profundicemos un poco más en las técnicas de detección pues lo podemos clasificar como:

- Plan de detección: Puedo abordarlo de dos maneras: primero, enseñando al usuario a diferenciar entre correos electrónicos que son peligrosos y los que no lo son. Utilizar la automatización que categorice los correos electrónicos de phishing sería el segundo paso para reducir el error humano.
- Plan defensa ofensiva: se logra brindándole al atacante credenciales falsas, pero en masa de esta manera el intruso perderá mucho tiempo para encontrar el original.
- Plan de corrección: una vez detectado el phishing se lo reporta a los proveedores de servicios para que lo den de baja.
- Plan de prevención: trata sobre prevenir que los usuarios sean víctimas y para ello primero de detecta al atacante para poder demandarlo y se le sancione legalmente.

2.4.2. Marco Teórico de estafas en cuentas bancarias

Los estafadores tienen un talento increíble para ser muy convincentes, usan herramientas como llamadas, mensajes de texto, envían correos electrónicos, siempre con la intención de conseguir nuestro dinero o información delicada.

El ensayo de un foro jurídico analiza la estructura ideal para administrar de forma segura la información del sistema de protección de datos personales del Perú. Según Alvarado (2016), un programa informático está desarrollado para recopilar, almacenar, procesar y distribuir información para tomar el control, el análisis, la comprensión y ejecutar decisiones apropiadas para la empresa o negocio; su seguridad debe evitar el acceso no autorizado, manipulación, robo o daño físico. a través de políticas, procedimientos y técnicas encaminadas a proteger hardware,

software, redes de telecomunicaciones y datos.

Nos referimos a ella como seguridad de datos porque cubre tanto material digital como impreso. Los bancos y otras instituciones que manejan datos están obligados a inventar normas seguras para blindar sus datos y prevenir el fraude. El blindaje de la información o datos, según la norma ISO 27001, es la implementación de una serie de estrategias destinadas a preservar el secreto, disponibilidad y veracidad de la información.

La gestión de la información en todas las empresas debe cumplir con los tres principios de seguridad de la información para satisfacer suficientemente los requisitos de eficacia y eficiencia. Es ampliamente reconocido que mantener la confidencialidad, la integridad y la disponibilidad son los tres pilares de un sistema seguro y confiable.

LA CONFIDENCIALIDAD

La información sólo es accesible a quienes están autorizados. El acceso a la información se facilita mediante supervisión y autorización. El requisito de ocultar o mantener la privacidad de datos o recursos específicos se conoce como confidencialidad. Prevenir la difusión no autorizada de información sobre nuestra firma es el objetivo de la confidencialidad.

LA INTEGRIDAD

Esto implica que los datos no se alterarán en caso de accidente o intención malévola. Los cambios en la información solo se pueden realizar con logueo autorizado. La integridad se enfoca en detener cambios de datos no deseados.

LA DISPONIBILIDAD

Quiere decir que, si el sistema informático está en uso, no habrá

ninguna disminución en el rendimiento. Cuando sea necesario, las consultas que requieren los usuarios registrados deben ser accesibles. Las personas autorizadas deben tener acceso a la información. El objetivo es evitar interrupciones ilegales de los recursos informáticos.

¿Qué papel juega la seguridad de la información en una organización?

Los sistemas de seguridad de la información deben poder manejar y superar los riesgos actuales de tal forma que afecten lo menos posible al negocio. Esto significa que los sistemas de seguridad de su empresa pueden prevenir, evitar o eliminar riesgos o ataques a los datos y al procesamiento de datos.

Como resultado, las empresas necesitan contar con suficientes soluciones tecnológicas que no sólo garanticen la protección, sino que también les permitan monitorear el nivel de protección en todo momento y proporcionar los recursos necesarios para mantener las actividades de la empresa en caso de un desastre. (ataque).

Distinciones entre seguridad de la información y ciberseguridad

Aunque son ideas distintas, la ciberseguridad y la seguridad de la información están relacionadas. En primer lugar, examinemos la ciberseguridad y la seguridad de la información en su conjunto. Dicho de otra manera, la seguridad de la información engloba todos los procedimientos y métodos destinados a salvaguardar los datos y la información corporativa, ya sea en forma física o digital (archivos cargados en una red o base de datos). La ciberseguridad se limita a proteger los datos dentro del entorno digital del negocio.

La seguridad de la información evalúa los peligros y los detiene basándose en la protección del sistema en función de los aspectos

de defensa. La ciberseguridad, por otro lado, implica defensas basadas en ataques contra estas amenazas. La seguridad de los datos utiliza técnicas, herramientas, estructuras organizativas internas y métodos para salvaguardar los datos en cualquier lugar, incluidos los sistemas informáticos, bases de datos, etc., independientemente de si están interconectados. Aunque la ciberseguridad concierne a los sistemas en red, la información digital que se debe proteger se mueve y reside a través de ellos.

Si la información confidencial de alguna compañía, cliente, decisión, posición financiera Un oponente obtiene el control de una nueva línea de productos, podría provocar un descenso de la confianza de los clientes, insolvencia, juicios o pérdidas comerciales. Como resultado, salvaguardar la información privada no sólo es necesaria para fines comerciales sino también, frecuentemente, como lo exige la ley y la ética. La seguridad de la información tiene un gran impacto en los datos secretos de las personas y este impacto difiere según su cultura.

El Banco de la Nación está pendiente, vigilante para reguardar la informacion de sus clientes y, a medida que las amenazas a la seguridad en Internet continúan creciendo, trabajamos con nuestros clientes para informar, asesorar y crear estrategias que les ayuden a enfrentarlas. Para ello el banco a través de su área de tecnología de la información a desarrollado estas herramientas:

Clave Dinámica (Token)

El token consiste en crear un código con cifras numéricas de forma aleatoria que permite aumentar la seguridad de las operaciones en línea. Los datos de su tarjeta, su clave secreta de Internet o el token nunca son solicitados por el banco a través de ningún canal de atención al cliente. No dupliques tus Tarjetas, resguarda siempre tu tarjeta y token, sin especificar tu clave de internet. Nunca le dé su token a nadie, ni siquiera a los empleados del banco, en respuesta

a SMS, correos electrónicos o comunicación telefónica solicitándole que ingrese su código secreto o los datos de cualquier tipo de tarjeta que tenga.

Multired Virtual (Banca por Internet)

Las operaciones o transacciones por internet son fáciles e intuitivos, pero antes deberá asegurarse de haber accedido a la página oficial del banco nación.

2.5. Marco Conceptual

Phishing

Los ciberdelincuentes utilizan este método de ingeniería social para obtener datos confidenciales de usuarios, el canal más utilizado para el ataque son correos electrónicos con contenidos de gran interés que muchas veces el usuario necesita, para instarlo a interactuar con el mensaje llevándolo hacer clic en enlaces fraudulentos con sitios web falsos y hasta hacer descargas de contenidos sin saber q están instalando softwares maliciosos que se apoderan del ordenador del usuario.

En la actualidad hay varios tipos de phishing estos son:

- Phishing tradicional: consiste en recibir un correo malicioso, es el más usado.
- Phishing basado en malware: consiste en recibir correos con archivos de descarga, estos archivos son softwares maliciosos.
- Spear phishing: Dado que la información de la víctima puede usarse para engañar y obtener información privada, se usa con mayor frecuencia para una empresa o individuo en particular.
- Vishing: consiste en realizar llamadas telefónicas, voz IP, con el pretexto de que la víctima devuelva la llamada a un numero de una supuesta empresa, donde le solicitaran que brinde sus datos sensibles.
- Smishing: se trata de envíos de mensajes de textos a los celulares de las victimas ofreciendo premios, oportunidad laboral y beneficios, este tipo de phishing también se aplica en

los mensajes del Facebook, WhatsApp, Telegram, Instagram.

- Pharming: Al alterar la configuración DNS del servidor o redirigir el tráfico a una dirección IP ficticia, puede manipular el acceso de un sitio web legítimo a otro fraudulento, exigiendo a la víctima que introduzca su contraseña y nombre de usuario.
- Ceo suplantador: consiste en sustituir el correo electrónico para fines de transferencia de dinero, solicitándolas a trabajadores específicos de una empresa.

Hackers

Son personas con grandes conocimientos de informática, dominan todo tipo de lenguaje de programación e ingeniería social, su objetivo es buscar fallos de seguridad en sistemas informáticos con el fin de secuestrar información para pedir recompensas, los más sofisticados pueden entrar a sistemas complejos como de bancos o del mismo FBI, y los hackers de sombrero blanco hacen lo mismo, pero con la finalidad de arreglarlos o como se dice en términos informáticos parcharlos.

Softwares

son el conjunto de algoritmos programados con códigos para realizar diversas tareas dentro de un sistema informático.

Ingeniería social

Es el estudio previo que se realiza a las víctimas, para ello se hace uso de técnicas de manipulación para que la víctima no se dé cuenta que está brindando información sensible, actualmente este estudio lo hacen de forma remota y eso como sería posible pues los ciberdelicuentes tienen acceso a las publicaciones que realizan las personas en redes sociales, tan solo con revisar la información del perfil, fotos, etc., ya tienen lo suficiente como para arman algún tema que atraiga a la víctima.

Cuentas bancarias

La cuenta bancaria es el registro que mantiene un banco con tu nombre donde se guarda tu dinero contabilizando las salidas e ingresos del efectivo, en ella también puedes ver el saldo actual de efectivo que tienes a disposición, las cuentas más conocidas son la de ahorros y cuenta corriente.

Estafa

Se dice de aquella acción que permite timar, engañar a alguien con el propósito de quedarse con algo de otra persona ya sea una propiedad o patrimonio, a esto lo podemos llamar robo siendo este un delito que está considerado generalmente como de menor gravedad ante delitos como homicidio o abuso sexual, pero hay ocasiones donde el tipo de estafa hace demasiado daño que su castigo puede ser ejemplar para el criminal.

Clientes

Los clientes son las personas o instituciones que adquieren un producto o servicio de manera habitual en un negocio, esto los convierte en consumidores desde la perspectiva del negocio.

CAPÍTULO III DESCRIPCIÓN Y FUNCIONES DEL PUESTO

3.1. Descripción del puesto

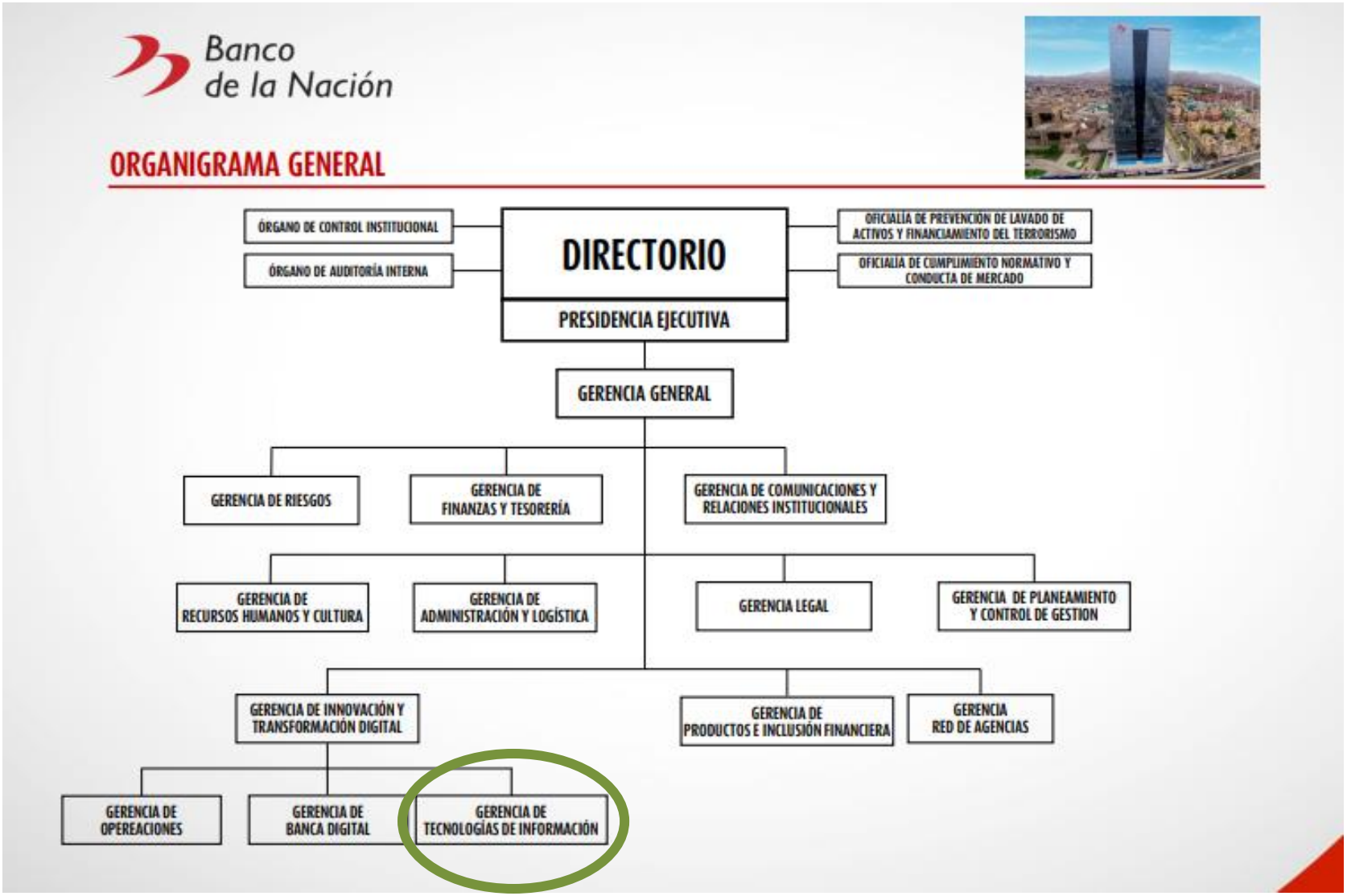
El área u oficina de seguridad informática siempre busca y contrata personal profesional calificado que disfrute de trabajar en seguridad informática, el puesto requiere mucha destreza y experiencia para contrarrestar cualquier tipo de ataque por parte de hackers. Lo principal es asegurar todos los sistemas que se esté manejando en el banco, los dispositivos en red y la base de datos donde se almacena información sensible.

El puesto requiere de profesionales capaces de solucionar rápidamente cualquier tipo de problema originado por los ataques que se pueda dar, la responsabilidad del trabajador está por encima de cualquier otro valor que

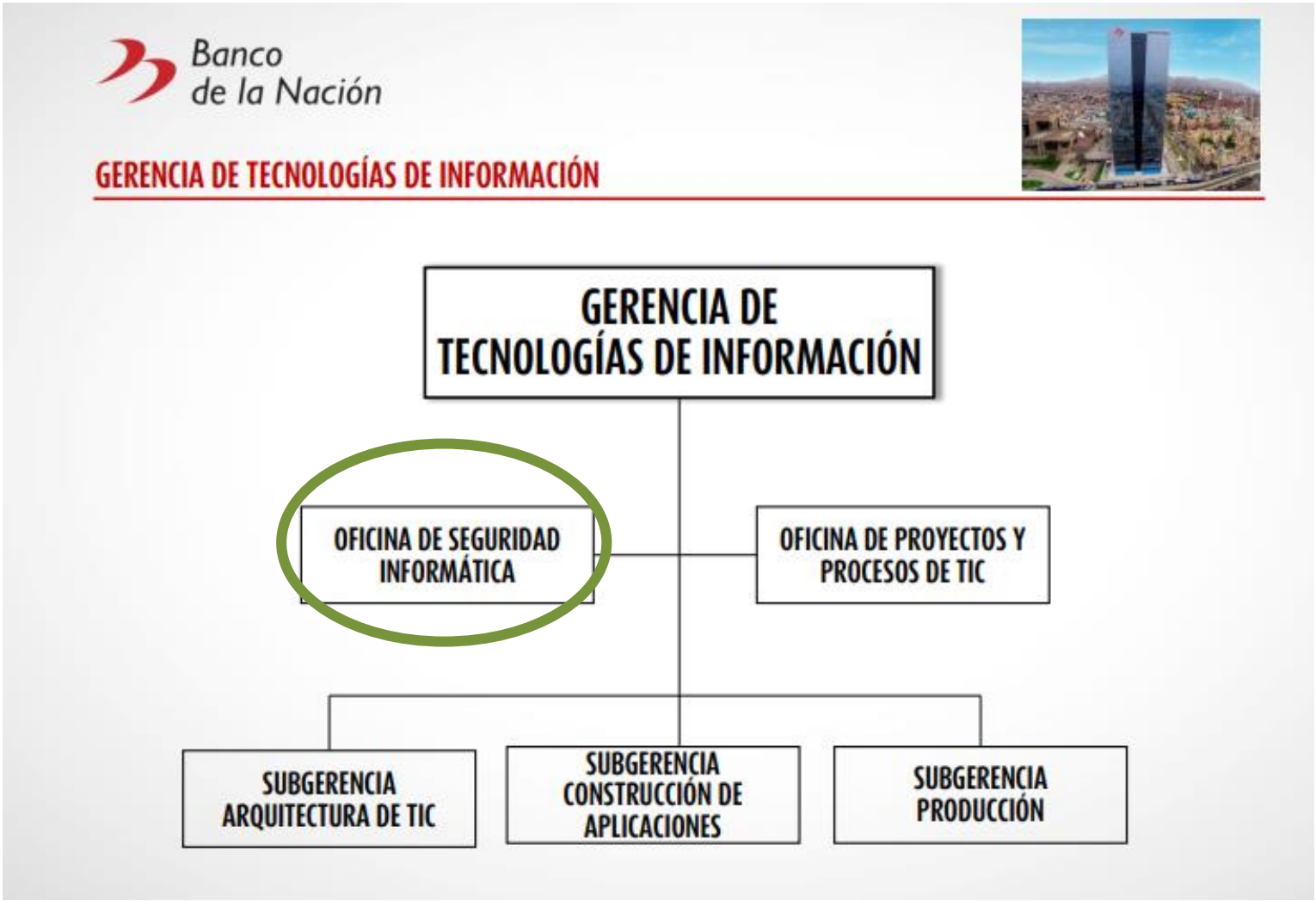
se necesite del mismo, un trabajador responsable siempre está atento a cualquier amenaza y previene, lo cual está mejor que buscar solucionar el problema.

En términos generales el puesto está dirigido para personas expertas en seguridad informática, el termino de no vale pestañear queda como anillo al dedo, de esta oficina va depender la continuidad de los trabajos durante el día, solucionando también las consultas internas de otras áreas por parte de los trabajadores, el jefe directo del área es un ingeniero de sistemas con especialidad en seguridad informática.

3.2. Ubicación del puesto en el organigrama general



3.3. Ubicación del puesto en el organigrama especifico.



3.4. Funciones del puesto

crea, pone en práctica y vigila procedimientos de seguridad de la información para salvaguardar datos, redes y sistemas informáticos.

Determinar y especificar las necesidades de seguridad del sistema.

Crear una base para la seguridad de la información y crear una estrategia exhaustiva para la ciberseguridad.

Crear y registrar protocolos y procedimientos operativos.

Configurar y diagnosticar el hardware de la infraestructura de seguridad.

Creamos soluciones tecnológicas e instrumentos de seguridad de vanguardia para ayudar a cerrar vulnerabilidades de seguridad y agilizar operaciones tediosas.

Se informa a la empresa de forma rápida y precisa sobre posibles incidentes de seguridad.

Se elabora un informe completo que recoge las conclusiones basadas en las valoraciones y resultados, recomendando así nuevas mejoras de seguridad.

CAPÍTULO IV S E CONCLUYE Y RECOMIENDA

4.1. Conclusiones

Conclusión el Phishing en cuentas bancarias y su fraude en los clientes bancarios del país son técnicas de ingeniería social muy usadas en la actualidad, crea muchos dolores de cabeza a las clientes víctimas de esta estafa, pierden bienes materiales como dinero y también propiedad intelectual.

Se concluye que, de acuerdo con los objetivos planteados, el phishing en las cuentas bancarias y los otros tipos de phishing, a medida que estos ataques vulneran tu sistema informático pueden apoderarse de ella y controlar todo de la manera que mejor le plazca, puede eliminar información sensible, copiar y compartirlo.

Se concluye que las estafas se originan con campañas de phishing, estos ataques pueden utilizar múltiples canales, aparte del correo electrónico, la más usada actualmente es la mensajería de las redes sociales.

Se concluye que las campañas de phishing que tienen como objetivo recabar información de cuentas bancarias se acrecentó en el 2012 Tras la pandemia de COVID-19, ocupamos el primer lugar en ataques de toda Latinoamérica.

Se concluye que las cuentas bancarias siempre van a ser acechadas por ciberdelincuentes buscando siempre un punto débil en la seguridad informática para apropiarse de las mismas.

Se concluye que para contrarrestar este ataque las personas deben estar conscientes de este peligro, por eso el banco por sus canales de comunicación siempre brinda información importante a cerca de cambios o modificaciones que puedan tener las operaciones financieras que realicen.

Se concluye que el área de seguridad informática es muy importante para dar soporte y resguardar los sistemas informáticos y dispositivos en red de todos los departamentos del banco, es la garantía para que el trabajo diario del banco se realice con total normalidad para la disponibilidad del cliente.

Se concluye que las buenas practicas e innovación en arquitecturas tecnológicas como parte de la gestión de la información cumple un rol relevante para asegurar el buen desempeño frente a los posibles ataques,

prevenir y no lamentar.

4.2. Recomendaciones

Recomendación para proteger su información

También es responsable de la seguridad de sus transacciones financieras. Lo exhortamos a realizar las siguientes recomendaciones de seguridad para evitar que otras personas abusen de estos servicios:

- ✓ Si recibe una llamada o un correo electrónico que dice ser de BN, no divulgue sus contraseñas por teléfono o en línea.
- ✓ BN nunca le enviará un correo electrónico solicitando sus contraseñas o información personal.
- ✓ Es fundamental que se comunique con nuestro help desk al 0800-10700 en todo el Perú. o envíe un correo electrónico a mconsultas@bn.com.pe si recibe estos mensajes por teléfono o correo electrónico.
- ✓ Si no está seguro del origen de un correo electrónico, no lo abra.
- ✓ Es fundamental que sus contraseñas permanezcan confidenciales; No los compartas con nadie más y no lo escribas en un lugar que sea fácil de encontrar.
- ✓ Modifique sus contraseñas periódicamente.
- ✓ Contraseñas que coinciden con el nombre de pila de la persona. Las contraseñas menos seguras incluyen aquellas que contienen letras o dígitos repetidos, números consecutivos e información específica del cliente (fecha de nacimiento, número de teléfono, etc.).
- ✓ Instale las versiones más actuales de su motor de búsqueda y actualícelas periódicamente.
- ✓ Desactive la función de guardar contraseña de la computadora.
- ✓ Absténgase de ingresar su contraseña en computadoras que no sean de confianza o en terminales públicas como cibercafés y aeropuertos.
- ✓ Nunca utilice motores de búsqueda o enlaces de correo electrónico

con direccionamiento al sitio web de BN. Asegúrate que el sitio web del BN es el correcto digitando cada vez la dirección en tu navegador: (https://www.bn.com.pe;https://zonasegura1.bn.com.pe/BNWeb/Inicio;https: //zonasegura1.bn.com.pe/BN_PTIV/).

- ✓ La imagen de un candado cerrado que los motores de busqueda muestran en la barra de estado o junto a la dirección es otra característica de seguridad.
- ✓ Asegúrese de tomar las precauciones adecuadas para evitar que lo observen o lo escuchen al escribir contraseñas o conversar por teléfono.
- ✓ La mejor defensa contra el fraude es NUNCA responder mensajerías de dudosa procedencia, SMS o llamadas telefónicas solicitando datos sensibles de carácter secreto de la persona. Este tipo de discusiones o demandas no son realizadas por BN con sus clientes.
- ✓ Ninguna comunidad u organización se comunicará con usted por teléfono, mensaje de texto o correo electrónico para solicitar contraseñas, números de tarjetas de crédito u otra información personal.
- ✓ Ingrese la dirección en la barra de direcciones de su navegador para acceder al Portal BN. NUNCA DEBEN UTILIZARSE ENLACES DE SITIOS DISTINTOS A “https://www.bn.com.pe”.
- ✓ Asegúrese de que el sitio web de Multired al que está ingresando sea seguro. Para lograr esto, abra la barra de direcciones o la barra de estado del navegador y busque un pequeño candado cerrado.
- ✓ Revisa tu cuenta bancaria periódicamente y con atención para detectar movimientos irregulares.

Recomendaciones de Seguridad en Internet para su computadora o dispositivo móvil

- ✓ Asegúrese de escanear periódicamente su computadora en busca de troyanos y malware.
- ✓ Asegúrese de que su navegador y sistema operativo estén siempre

actualizados.

- ✓ Utilice aplicaciones de seguridad como antivirus, antispyware, firewall y todas las herramientas disponibles para evitar intrusiones en sus sistemas. Verifique que estén actualizados y activos en todo momento.

¿Cómo podemos mantener nuestra PC segura?

- ✓ Tome estas sencillas precauciones para proteger su PC. Le recomendamos utilizar medidas de seguridad para salvaguardar su información personal cuando utilice Internet para reducir el riesgo de ser víctima de peligros en línea.
- ✓ Puede navegar por Internet de forma más segura si su PC está adecuadamente protegida.
- ✓ Defensa contra el software espía.
- ✓ Asegúrese de que el programa anti-spyware de su computadora esté actualizado y sea capaz de identificar y eliminar cualquier software espía que pueda alterar o robar datos confidenciales.
- ✓ Es fundamental dejar claro que el software espía es un software dañino que recoge datos de su PC y los envía a un tercero sin conocimiento o consentimiento del dueño de la máquina.
- ✓ Escanee periódicamente su PC con esta aplicación. Esta solución, que le protege de numerosos riesgos y ofrece ayuda al cliente en caso de que tenga algún problema, la ofrecen numerosas empresas de software antispyware.

  Asegúrese de que su programa antispyware esté actualizado para anticiparse a nuevos peligros.

Firewall

- ✓ Activar el firewall de su computadora, a veces llamado Firewall de acceso online, nos brinda acceso a numerosas funciones de seguridad de datos bloqueando intrusiones ilegales.

- ✓ Instale todos los parches de software; Si un parche corrige una falla de seguridad, también es posible encontrar "paquetes de servicio" o "parches" para los programas que están instalados en su computadora. Todos los programas, incluidos los sistemas operativos para Mac, Linux y Windows, deben actualizarse periódicamente.

REFERENCIA BIBLIOGRÁFICA

Mitnik, K. (2011). *Ghost in the Wires*. EE.UU. BlackstoneAudio Inc

Sartori, G. (1998). *HOMO VIDENS La sociedad teledirigida*. Buenos Aires. Taurus

Hadnagy C. (2018). *Social Engineering: The Science of Human Hacking*. Indianapolis. John Wiley & Sons, Inc

Nazario Delgado & Villanueva Sánchez, 2022, Perú, Universidad Señor de Sipán
Fraude informático en la modalidad de phishing y la necesaria actualización de la legislación para una eficiente persecución y sanción penal

Hidalgo Coronel & Solano Vidal, 2021, Perú, Universidad Nacional del Santa
El phishing como conducta delictiva no regulada en el ordenamiento jurídico peruano. propuesta de incorporación del artículo 7-a en la ley de delitos informáticos 30096

Sergio Frontera Díaz de Quintana, 2020, España, Universidad Autónoma de Madrid
Desarrollo de sistema de análisis automático de phishing

Luis Fernando Rosero Tejada, 2021, Ecuador, Universidad Politécnica Salesiana
El phishing como riesgo informático, técnicas y prevención en los canales electrónicos: un mapeo sistemático

https://andina.pe/agencia/noticia-el-phishing-es-ciberataque-mas-aumento-peru-a-raiz-de-pandemia-831392.aspx

https://larepublica.pe/tecnologia/2022/10/30/peru-es-el-pais-con-mas-ataques-de-phishing-en-latinoamerica-como-evitar-caer-en-esta-ciberestafa-evat

https://www.stormshield.com/es/noticias/breve-historia-del-phishing/

https://www.hackbysecurity.com/entrevista/yolanda-corral

https://www.bn.com.pe/seguridad/internet.asp

ANEXOS

Conocedores expertos en la concientización del Phishing

Recomendaciones del BN para evitar el Phishing

TOKEN

Asegurarse de teclear bien el acceso al sitio web del portal y zona segura.

Reconocer correos fraudulentos

Reporte donde el Perú ocupa el primer puesto en ataques de Phishing en Latinoamérica.