593 Digital Publisher
CEIT
ISSN 2588-0705

Propuesta de Buenas Prácticas para Mitigar Ciberataques en Usuarios de Entidades Financieras

Proposal of Good Practices to Mitigate Cyberattacks in Users of Financial Institutions

Sandra Rocío Flores-Álava[1]
Pontificia Universidad Católica del Ecuador
Sede Ambato - Ecuador
srfloresa@pucesa.edu.ec

Liliana del Rocío Mena-Hernández[2]
Pontificia Universidad Católica del Ecuador
Sede Ambato - Ecuador
lmena@pucesa.edu.ec

doi.org/10.33386/593dp.2023.4.1652

V8-N4 (jul-ago) 2023, pp. 159-173 | Recibido: 26 de diciembre de 2023 - Aceptado: 14 de mayo de 2023 (2 ronda rev.)

1 Pontificia Universidad Católica del Ecuador Sede Ambato
Estudiante de la maestría en Ciberseguridad la Pontificia Universidad Católica del Ecuador Sede Ambato Tecnóloga programadora e Ingeniera en Sistemas Informáticos de la Universidad Técnica de Manabí, actualmente Analista de Infraestructura Y Sistemas Informáticos de la Policía Nacional del Ecuador provincia de Manabí.
ORCID: https://orcid.org/0009-0002-7747-8128

2 Docente Pontificia Universidad Católica del Ecuador Sede Ambato, Directora Revisora de trabajos de titulación (Grado y Posgrado), Autora de artículos y ponencias nacionales e internacionales.
ORCID: https://orcid.org/0000-0003-3531-7350

Cómo citar este artículo en norma APA:

Flores-Álava, S., & Mena-Hernández, L., (2023). Propuesta de Buenas Prácticas para Mitigar Ciberataques en Usuarios de Entidades Financieras. 593 Digital Publisher CEIT, 8(4), 159-173, https://doi.org/10.33386/593dp.2023.4.1652

Descargar para Mendeley y Zotero

RESUMEN

Los ciberataques son cada vez más frecuentes y cada año son causantes de las pérdidas de miles de millones de dólares a nivel mundial, en Ecuador los ciberataques se han centrado en tres ciudades: Quito, Guayaquil y Portoviejo, no se cuenta con estudios específicos en cada uno de estos sectores, por dificultad de acceso y los problemas de logística para levantar información. Por ello es relevante estudiar el comportamiento de los usuarios de entidades financieras para proponer buenas prácticas para evitar ciberataques. Centralizar el estudio en zonas geográficas pequeñas, permite individualizar y segmentar el problema de investigación facilitando tanto el acceso a la información cuanto la efectividad de la propuesta. En este sentido, el propósito de este trabajo de investigación es diseñar una propuesta de buenas prácticas para la prevención frente a los ciberataques a usuarios de entidades financieras. El enfoque de la investigación es mixto y los datos de estudio se centrarán en el Distrito Policial Portoviejo, la información cuantitativa y la selección de la muestra se estudiará en base a los datos obtenidos del CMI (Cuadro de Mando Integral Policial), para finalmente proponer una guía de buenas prácticas a los usuarios de entidades financieras del Distrito Policial Portoviejo, con los cuales se validará la propuesta cualitativamente.

Palabras clave: buenas prácticas, ciberataques, entidades financieras, distrito policial Portoviejo.

ABSTRACT

Cyberattacks are increasingly frequent and each year cause the losses of billions of dollars worldwide, in Ecuador cyberattacks have focused on three cities: Quito, Guayaquil and Portoviejo, there are no specific studies in each of these sectors, due to difficulty of access and logistical problems to collect information. It is therefore important to study the behavior of users of financial institutions to propose good practices to prevent cyberattacks. Centralizing the study in small geographical areas allows to individualize and segment the research problem facilitating both access to information and the effectiveness of the proposal. In this sense, the purpose of this research work is to design a proposal of good practices for the prevention of cyber attacks on users of financial institutions. The research approach is mixed and study data will focus on the Police District Portoviejo, quantitative information and sample selection will be studied based on data obtained from the CMI (Police Integral Command Board), to finally propose a guide of good practices to users of financial institutions of the Police District Portoviejo, with which the proposal will be validated qualitatively.

Key words: best practices, cyber attacks, financial institutions, Portoviejo police district.

593 Digital Publisher CEIT ISSN 2588-0705

Introducción

Los ciberataques son las actividades maliciosas que se llevan a cabo por un atacante que afecta a una o múltiples víctimas, su mecanismo de operación es mediante la red de internet o una red local. Según Gómez (2017), la intención es sacar provecho generalmente económico de esa información a la que se ha accedido sin autorización.

En este sentido, Atencia (2021), consideran que la era digital ha propiciado mayores oportunidades para este tipo de ataques debido a que la mayor parte de las empresas, incluidas las instituciones financieras, empezaron a tener más presencia por medios virtuales y apelando a los últimos recursos tecnológicos. No obstante, estas actividades ilícitas requieren estar actualizadas con los nuevos sistemas de seguridad. De allí la importancia de disponer de una propuesta de buenas prácticas para mitigar ciberataques en usuarios de entidades financieras.

Según Machín (2016), el impacto que sufre una entidad financiera al estar expuesta a los ciberataques es muy grande y esos daños se manifiestan en bloqueos de los sistemas informáticos, proceso de producción o en el desarrollo de las actividades de una organización, lo cual hace que el funcionamiento normal de la empresa sea imposible en estos casos cuando está bajo un ataque cibernético. Además, puede generar graves repercusiones a futuro como perder clientes y/o proveedores lo que afectaría la economía de la empresa.

Uno de los elementos de las organizaciones, incluidas las instituciones financieras, que más corre peligro de sufrir un ciberataque son los datos personales que tenga acerca de sus clientes, proveedores o empleados; por lo cual recae sobre la empresa una responsabilidad muy grande de tomar medidas que puedan proteger esos datos de posibles ciberataques. Con el creciente intento de ciberataques a las empresas en todo el mundo la mayoría está buscando mecanismos que les permita estar a la vanguardia en protección de ataques cibernéticos como la violación de datos personales, hurto al patrimonio y el acceso abusivo de datos informáticos y así evitar los posibles daños económicos o de reputación que conlleva a sufrir este tipo de ataque (Díaz y Mosquera, 2022, p. 11).

En este contexto, los ciberataques utilizan las brechas de seguridad presentes en las tecnologías de información para pasar a copiar, borrar o reescribir la información de la víctima y se aprovechan de las vulnerabilidades que presentan la mayor parte de las estructuras cibernéticas como, por ejemplo, las redes sociales. “En el siglo XXI los bits y los bytes pueden ser tan amenazantes como las balas y las bombas. El número y variedad de los ciberataques puede llegar a ser alto, debido a la evolución y metamorfosis de instrumentos informáticos” (Gómez, 2012, p. 156).

Con el surgimiento de la era tecnológica a nivel mundial, los ciberataques han tomado otro enfoque, como ejemplo, se visualiza en las noticias en el mundo los ciberataques, donde millones de víctimas son extorsionadas y estafadas por medios tecnológicos, presentando un impacto económico grave a cualquier persona u organización. Dentro de la vulneración del derecho a la propiedad privada, se puede encontrar la presencia de delitos relacionados con la vulneración de los medios electrónicos, ciberdelitos relacionados a la apropiación fraudulenta por medios tecnológicos, así, se puede encontrar a la provincia de Manabí, ocupando el tercer espacio territorial con mayor problemática, considerando que esta provincia, concentra el 6% de la problemática.

Los ciberataques son cada vez más frecuentes y año a año son causantes de las pérdidas de miles de millones de dólares a nivel mundial, de acuerdo a los últimos reportes proporcionados en la base de datos de la Policía Nacional, en Ecuador en ciberataques a entidades financieras en el periodo de enero a agosto del 2022, se reportan 9474 incidentes por estafas en línea, a través de la apropiación fraudulenta por medios electrónicos, debido a los códigos maliciosos que se insertaron en los dispositivos de usuarios finales.

Los ciberataques, se registran en gran medida a nivel nacional, concentrándose un 27% de la problemática dentro del distrito Metropolitano de Quito, con 2592 eventos, así mismo en distrito Metropolitano de Guayaquil incide con 1587, dando un 17% de eventos, por otra parte también, considerar que la provincia de Manabí se ubica en el tercer lugar a nivel nacional, con 695 eventos que equivale al 6%, por lo que se presenta también como uno de los espacios territoriales de mayor incidencia, verificándose lo antes mencionado en el sistema CMI (Cuadro de Mando Integrar Policial) de la Dirección General de Seguridad Ciudadana y Orden Público. Para el planteamiento de la propuesta debe considerarse que, según datos de este organismo, de enero a noviembre de 2022 estos son los tipos de ataques más frecuentes y se encuentran distribuidos en el siguiente cuadro:

Tabla 1
Ataques a la ciberseguridad más frecuentes

Variables	Frecuencia	Porcentaje %
Caída del rango de IP en listas negras	112	22%
Saturación e	22	4%
intermitencias de	302	60%
señal	56	11%
Ingreso de correos sospechosos	12	3%
Intentos de acceso a los equipos de personal no autorizado		
Otros métodos		
Total	504	100%

Fuente: datos obtenidos del CMI (Cuadro de Mando Integrar Policial) y de la Dirección General de Seguridad Ciudadana y Orden Público.

En Manabí, y de acuerdo con las estadísticas, un 80% de la problemática se registra dentro de los cantones: Manta, Portoviejo, Pedernales, Chone y El Carmen; sin embargo, los delitos de apropiación fraudulenta por medios tecnológicos, se desarrollan en el Cantón de Portoviejo, registrándose entre 25 y 41 eventos mensuales, asimismo se debe considerar que Manta, es un cantón con una importante actividad comercial, económica y turística dentro de la provincia, a más de ser una de las mayores ciudades dentro de la provincia de Manabí con un variado sector Bancario. El eslabón más débil en ciberseguridad siempre han sido las personas, ya que por desconocimiento pueden proporcionar datos personales en internet. Dentro de los ciberataques más comunes y tipos de filtraciones de datos se tienen los indicados en la tabla 1.

Por esta razón, estudiar el comportamiento de los usuarios de entidades financieras resulta de vital importancia para proponer buenas prácticas para evitar ciberataques. De este modo, el objetivo general de este trabajo de investigación es diseñar una propuesta de buenas prácticas, para la prevención frente a los ciberataques de usuarios de entidades financieras. Así, se determina el problema de la siguiente forma: ¿Cuáles son las prácticas que se deben implementar para mitigar ciberataques en usuarios de entidades financieras?

Método

El enfoque de la investigación es cuantitativo. Los datos de los estudios se centraron en el distrito Policial Portoviejo, la información es cuantitativa y la selección de la muestra se basó en los datos obtenidos del Cuadro de Mando Integral Policial (CMI). Finalmente, se espera proponer una guía de buenas prácticas a los usuarios de entidades financieras del distrito Policial Portoviejo con los cuales se valida la propuesta cualitativamente. Para el desarrollo de esta investigación se utiliz**ó** la Metodología Kanban, la cual es una secuencia de pasos que ayudan a mejorar de manera efectiva su productividad y consiste en organizar y distribuir las tareas de manera flexible con el objetivo de que se cumplan en un plazo determinado.

Las tareas que se han considerado en el contexto de la Metodología Kanban son las

Digital Publisher CEIT ISSN 2588-0705

siguientes: elaboración de una encuesta a los técnicos en TIC de las entidades financieras para el análisis de vulnerabilidades y la realización de la guía para la prevención frente a los ciberataques en usuarios de entidades financieras.

Resultados

Como se indicó en el apartado anterior se realizó una encuesta a los técnicos en TIC de las entidades financieras de la ciudad de Portoviejo con el propósito de conocer información relacionada con los ciberataques. Las entidades bancarias consideradas para este trabajo fueron la siguientes: Pacífico, Internacional, Pichincha, Comercial, BanEcuador, BIESS, Bolivariano, Produbanco; y las Cooperativas: Comercio, 15 de Abril, Calceta y 29 de Octubre. Se trabajó con una muestra intencional de 12 técnicos cuyos criterios fueron pertinentes y funcionales a la presente investigación. Los resultados de la aplicación de este instrumento de investigación se detallan a continuación.

Sobre el conocimiento de medidas

Tabla 2

¿Qué nivel de conocimiento considera usted que posee sobre las medidas de ciberseguridad en los sistemas informáticos de su lugar de trabajo?

Variables	Frecuencia	Porcentaje %
Alto	6	50%
Medio	3	25%
Bajo	3	25%
Total	12	100%

Fuente:Basado en Romero (2022) Pin y Pinargote (2022)

Acerca del nivel de conocimiento que se posee sobre las medidas de ciberseguridad en los sistemas informáticos de su lugar de trabajo hay respuestas divididas que otorgan los encuestados. Un 50% considera que es alto, mientras que un 25% señaló que es medio. Finalmente, el 25% indicó que es bajo.

Desde la perspectiva de Esteves et al. (2018), la ciberdelincuencia es algo que siempre estará presente, es un tema delicado debido que en ciertos casos se utilizan a hackers para brindar seguridad en alguna empresa financiera, con el propósito de conocer los mecanismos tecnológicos que se emplean y así encontrarse protegidos frente a estas amenazas.

En este mismo sentido, un estudio de Quispe (2021) evidencia que más del 90% de entidades bancarias en la región ha implementado procesos de detección y análisis de eventos de seguridad digital como cortafuegos y actualizaciones automatizadas de virus y sistemas. Esto con el fin de prevenir riesgos cibernéticos que podrían perjudicar, en gran medida, no solo la experiencia de usuario sino también la confianza hacia las entidades financieras. Es por ello que, con el incremento de usuarios digitales y las facilidades de acceso a la tecnología, la industria financiera tiene varios retos en términos de ciberseguridad en los que debe trabajar y son clave para su crecimiento.

Sobre información previa

Tabla 3

¿Ha escuchado de algún ataque informático realizado ya sea a una persona cercana o a una institución financiera?

Variables	Frecuencia	Porcentaje %
Sí	3	25%
No	9	75%
Total	12	100%

Fuente: Basado en Romero (2022) Pin y Pinargote (2022)

En esta pregunta de la encuesta, un 25% de los técnicos en TIC de las entidades financieras de la ciudad de Portoviejo consultados señalaron que sí han escuchado de algún ataque informático realizado ya sea a una persona cercana o a una entidad, mientras que la gran mayoría, el 75%, señaló lo contrario.

Los ataques de este tipo son cada vez más frecuentes. Para Ojeda et al. (2020), los cambios que adopta la banca en la era digital representan

hoy en día nuevos riesgos que amenazan su permanencia en el mercado, por lo que, "el departamento de gestión de riesgo de las entidades financieras, entre estas cooperativas de ahorro y crédito, deben transfigurarse y familiarizarse a la digitalización para prevenir y mitigar de manera oportuna los riesgos, mediante reglamentos internos de protección de los usuarios y de toda la entidad" (p. 194). Estas medidas deben responder a una oferta de servicios financieros de una manera responsable con los grupos de interés, por consiguiente, los riesgos a los que se enfrentan las entidades están relacionados con el resguardo de datos, identificaciones de los clientes, manejo correcto de la Big Data y lo que concierne con la ciberseguridad.

Al respecto, un estudio de Cuesta et al. (2015), señala que, las instituciones financieras afrontan su digitalización para responder a las exigencias de los cambios del nuevo entorno competitivo y de los hábitos de los consumidores, por tanto, el proceso de digitalización de la banca ha llevado tres fases: partiendo en la innovación de nuevos productos y canales de información, la segunda fase la adaptación a la transformación de la infraestructura tecnológica; y por último, la transición de toda la estructura organizacional para posicionarse en la era digital en un mercado exigente.

Sobre normas de prevención

Tabla 4
¿En la institución financiera donde trabaja existen normas o prácticas enfocadas a la ciberseguridad?

Variables	Frecuencia	Porcentaje %
Sí	11	91%
No	1	9%
Total	12	100%

Fuente:Basado en Romero (2022) Pin y Pinargote (2022)

En esta pregunta de la encuesta, el 91% de técnicos consultados sostuvo que en la institución financiera donde trabaja sí existen normas o prácticas enfocadas a la ciberseguridad, mientras que el 9% aseguró lo contrario.

El tema abordado en esta pregunta es complejo, puesto que estas prácticas requieren admitir que existe una posible amenaza e invertir para evitar riesgos mayores. Desde la perspectiva de Ordóñez et al. (2020), se debe "cumplir con las políticas del banco en todos los aspectos de confianza, seguridad y tranquilidad para el usuario" (p. 203). Uno de los inconvenientes es que, en el Ecuador hay mínimos estándares de calidad en el avance tecnológico. Sin embargo, el sector de la banca continúa avanzando, brindando servicios eficientes y atención de calidad al cliente que contribuyen al desarrollo de las familias con la colocación de préstamos pagaderos en un mediano plazo y la generación de rendimientos financieros mediante la captación de ahorros de los clientes.

Pese a las amenazas en el ámbito tecnológico que existen en la actualidad, Traisnel (2018) considera que la banca debe seguir innovando y brindando nuevos servicios a través de los corresponsales no bancarios, ya que estos aportan en gran medida a que los productos financieros tengan menor costo de inversión entre infraestructura y los equipos necesarios, lo que proporciona rentabilidad a la banca.

Sobre capacitaciones en el tema de ciberseguridad

Tabla 5
¿La institución financiera donde labora realiza capacitaciones sobre temas de ciberseguridad y prevención ante amenazas cibernéticas?

Variables	Frecuencia	Porcentaje %
Sí	9	75%
No	3	25%
Total	12	100%

Fuente:Basado en Romero (2022) Pin y Pinargote (2022)

En esta pregunta de la encuesta, un 75% de técnicos consultados que la institución

Digital Publisher CEIT ISSN 2588-0705

financiera donde labora sí realiza capacitaciones sobre temas de ciberseguridad y prevención ante amenazas cibernéticas, mientras que el 25% aseguró lo contrario.

Para investigadores como Trullols (2018), las capacitaciones en este sentido deben incrementarse, solo así se podrá hacer frente a las inminentes amenazas. Se debe recordar que los ataques cibernéticos aumentaron debido a la virtualidad, esto se debe a que empleados suelen utilizar programas piratas, licencias falsas y algunos no cuentan con antivirus. Actualmente, el Ecuador se encuentra en la posición número 40 de los países con más ataques cibernéticos en el mundo según estadísticas en tiempo real de Kaspersky.

En cambio, un estudio de De Tomas (2014), señala que la consecución de una cultura de ciberseguridad no es posible a través de acciones de divulgación, aun cuando son necesarias, sino que requiere de una ingente labor formativa especializada que tenga en cuenta en ese proceso de enseñanza/aprendizaje a todos los sectores de la sociedad. Se requiere instaurar una cultura de ciberseguridad inserta en una cultura de seguridad y defensa para implicar en ella a toda la sociedad.

Sobre reconocimiento de indicios

Tabla 6

¿Usted puede reconocer los indicios de un ciberataque?

Variables	Frecuencia	Porcentaje %
Sí	10	83%
No	2	17%
Total	12	100%

Fuente Basado en Romero (2022) Pin y Pinargote (2022)

En esta pregunta de la encuesta, un 83% de técnicos consultados señaló que sí pueden reconocer los indicios de un ciberataque, mientras que el 17% indicó lo contrario.

Sobre el reconocimiento se encuentran diversos estudios que se actualizan de forma permanente, debido a las novedosas herramientas que existen en los dispositivos tecnológicos. Al respecto, Véliz (2022), señala que "los ciberataques son cada vez más comunes y este término es más utilizado para definir cualquier tipo de evento en internet desde robos o protestas" (p. 12). Para ser víctima de un ciberataque solo basta con ingresar a páginas equivocadas en línea o la descarga de algún archivo peligroso. Estos ataques se caracterizan por ser silenciosos, esto quiere decir que un ataque puede ser efectivo y el usuario no lo notará, son muy comunes en dispositivos que no cuentan con protección ya sea con antivirus o con conocimientos informáticos básicos para evitar ser víctima de estos.

Esta situación ha ido incrementando la preocupación desde diversos sectores, incluido el académico. Para López (2020), la sociedad actual se enfrenta a una nueva realidad y a un clima geopolítico en el que las personas o entidades malintencionadas disponen de tiempo, recursos y financiación ilimitados para llevar a cabo ciberataques. Por ello se requiere la adopción de medidas contra nuevas amenazas, cada vez más innovadoras y peligrosas. Para prevenir ciberataques se necesita estar protegido a toda costa, por lo que se emplea el uso de antivirus, estos se deben configurar bien y debe cumplir con las necesidades de la empresa, persona o industria

Sobre medidas a adoptar

Tabla 7

¿Sabe qué hacer o qué medidas adoptar en caso de sufrir un ataque ciberataque?

Variables	Frecuencia	Porcentaje %
Sí	9	75%
No	3	25%
Total	12	100%

Fuente:Basado en Romero (2022) Pin y Pinargote (2022)

En esta pregunta de la encuesta, un 75% de técnicos señaló que sí sabe qué hacer o qué medidas adoptar en caso de sufrir un ciberataque, mientras que el 25% aseguró lo contrario.

Entre las medidas que se deben adoptar, un estudio de Ojeda et al. (2020), establece que se deben contratar empresas dedicadas a brindar servicios de seguridad de datos. "No se habla de una asistencia puntual, sino que se espera que exista un sistema de control que se adapte cada vez a las exigencias de seguridad del sistema implementado" (p. 212). Esta misma investigación señala que se debe disponer de un sistema riguroso para el manejo de datos que vaya desde el ingreso de estos con sistemas de protección de datos a través de encriptación. Además, se sugiere implementar modelaciones de impacto financiero en función de los riesgos cibernéticos que asume la entidad financiera, con el fin de determinar la relación costo/beneficio, precisando así la proyección de continuidad de estos sistemas.

Según Cerasela (2021), se debe analizar con frecuencia los informes emitidos por el *software* de ciberseguridad, de manera que, en caso de detectar fraude, se disponga de un tiempo pertinente para investigar el delito, reparar daños y encontrar responsables. Otro aspecto que también se recomienda es establecer la relación entre diferentes indicadores cuantitativos de datos, usuarios, ingresos, trámites, y otros indicadores de acuerdo con la necesidad específica de la cooperativa y el manejo del entorno cibernético, para valorar las diferentes dimensiones de riesgo.

Sobre implementación de propuesta

Tabla 8

¿Considera que es importante implementar una propuesta de buenas prácticas para mitigar ciberataques en usuarios de entidades financieras?

Variables	Frecuencia	Porcentaje %
De acuerdo	10	83%
Poco de acuerdo	2	17%
Poco conforme	0	0%
No es necesario	0	0%
Total	12	100%

Fuente: elaboración propia. Basado en Romero (2022) Pin y Pinargote (2022)

En esta pregunta de la encuesta, un 83% de técnicos señaló que se encuentra de acuerdo con el hecho de implementar una propuesta de buenas prácticas para mitigar ciberataques en usuarios de entidades financieras, mientras que apenas el 17% se encuentra poco de acuerdo con este aspecto.

La implementación de una propuesta de buenas prácticas para mitigar ciberataques en usuarios de entidades financieras tiene acogida. Desde el enfoque particular de Allauca (2022), este tipo de instituciones deben incrementar sus medidas de ciberseguridad y gestionar posibles riesgos, tanto en la infraestructura tecnológica como en los procesos financieros. Esto significa que las empresas se pueden enfrentar a una gran cantidad de amenazas que, si un ciberdelincuente aprovecha las vulnerabilidades, comprometerán seriamente sus activos de información.

Discusión

De acuerdo con Chávez et al. (2021), debido al desarrollo tecnológico, las formas de fraudes cibernéticos se han sofisticado, vulnerando cualquier tipo de sistema de control interno y generando pérdidas económicas a las compañías. Actualmente los crímenes financieros representan una amenaza latente que debería tener muy alertas a todas las organizaciones empresariales para prevenir y detectar posibles violaciones a su sistema de seguridad de la información. Es así como, "en las instituciones financieras se hace indispensable prestar atención a los ataques cibernéticos causados a los sistemas, ya que pueden generar problemas potenciales de alto riesgo donde podrían ser víctimas de crímenes financieros" (p. 26).

A criterio de Hayes (2020), el crecimiento vertiginoso de estos ataques cibernéticos

593 Digital Publisher CEIT ISSN 2588-0705

asociados al crimen financiero ha propiciado el desarrollo de algún componente de programas antifraude. "El uso de modelos de aprendizaje de computadoras y los procedimientos analíticos predictivos desarrollados para la detección oportuna de patrones de transacciones y comportamientos atípicos han resultado de gran utilidad (p.8).

Para Guerrero y Castillo (2017), el auge de la globalización y la tecnología ha creado un ciberespacio en el cual encontramos un sin número de recursos y plataformas que han ayudado al desarrollo de la actividad humana, no obstante, también está el aspecto negativo como la ciberdelincuencia que están generando en las organizaciones y los gobiernos el replanteamiento de las estrategias para combatir estos delitos prospectivamente.

Los bancos o entidades financieras son más susceptibles a estos tipos de ataques cibernéticos, debido a que "la materia prima con la que se prestan los servicios bancarios es el dinero. Estas circunstancias propician la aparición de casos de fraude y exponen a los bancos a la realización de estafas" (Arcenegui, et al. 2016, p. 627). Es decir, los delincuentes cibernéticos viajan por el mundo virtual y realizan incursiones fraudulentas cada vez más y con mayor frecuencia y mayor impacto, los dispositivos de almacenamiento y procesamiento de información llámense servidores, estaciones de trabajo o simplemente PC son vulnerados en sus elementos más sensibles, dejando expuestos no sólo múltiples y significativos datos de distinto valor (financiero, crediticio, estratégico, productivo), sino los mismos patrimonios reales de personas y organizaciones y, aún más, su dignidad, su honra y su vida (Ojeda y Arias, 2010, p. 45).

Desde la perspectiva de Cerasela (2021), el derecho internacional no ofrece una definición aceptada por unanimidad del término "ataque cibernético", mientras que las estrategias nacionales de seguridad cibernética adoptadas por varios Estados, proponen definiciones muy diferentes de este término. Pese a esta diversidad, se puede observar que las definiciones existentes parecen converger hacia un enfoque amplio del término "ataque cibernético", como por ejemplo aquellos ataques que incluyen el acceso, uso, manipulación, interrupción o destrucción no intencionados o no autorizados (a través de medios electrónicos) de información electrónica y/o la infraestructura electrónica y física utilizada para procesar, comunicar y/o almacenar esa información. La gravedad del ciberataque determina el nivel apropiado de respuesta y/o medidas de mitigación: es decir, seguridad cibernética.

Al respecto, un estudio de Quispe (2021) clasifica los tipos de ataques de la siguiente forma:

Tabla 9

Tipología de ataques

Tipos de ataques	Caracterización
Ransomware	Software malicioso que compromete el sistema, al secuestrar la información y exigir el pago como rescate o liberación del equipo para evitar daños colaterales
Escaneo de puertos abiertos.	Proceso que analiza los puertos de un ordenador conectado a la red con el propósito de verificar cuales están abiertos, cerrados o disponen de un protocolo de seguridad y en base aquello conocer la composición de la arquitectura, agujeros de seguridad y sistema operativo de la computadora para luego ser explotado por el atacante.
Pishing	Envío de correos falsos que solicitan información respecto a trámites bancarios supliendo la identidad de la institución.
Robo de cookies	Proceso donde el usuario o cliente accede a un enlace y este automáticamente busca las diversas cookies almacenadas en la memoria del ordenador para posteriormente enviar al atacante.
DoS	Denial of Service traducido como la denegación del servicio, es decir, proceso que inhabilita el uso de una aplicación, sistema u ordenador al alterar o bloquear el funcionamiento.
Inyección SQL	Ciberataque oculto donde un hacker inserta código propio en un sitio o página web con el propósito de transgredir las medidas de seguridad y acceder a la información protegida del sitio y los usuarios.
Man-In-The-Middle	Ciberataque que intercepta la comunicación entre dos partes por medio del uso de una entidad externa o software.
Cross-site request	Falsificación de solicitudes en sitios cruzados que llevan al usuario a realizar un exploit malicioso, mediante comandos no autorizados que son transmitidos por el propio usuario que el sitio confía.
Redes Wireless	Acceso a datos sensibles transmitidos mediante la conexión WiFi, los cuales pueden ser manipulados por el atacante.

Fuente: Quispe (2021)

En este contexto, para Wilches (2015), la importancia de la ciberseguridad radica en la preservación de los medios humanos, tecnológicos, financieros e informativos adquiridos por las entidades para lograr los objetivos; y en la reducción de las amenazas, limitando las averías resultantes o daños, lográndose reanudar las operaciones tras un incidente informático, en un plazo de tiempo razonable y a un coste admisible. Por ello, se recalca como un factor de inversión y una necesidad de fomento de capacitación y formación de los responsables de la seguridad informática.

Sobre este importante aspecto, un informe de la OEA (2018) señala que en América Latina los riesgos de seguridad digital que merecen la mayor atención por parte de las entidades bancarias son: el robo de base de datos crítica, el compromiso de credenciales de usuarios privilegiados, y la pérdida de datos. Además, señala que resulta significativo que en la región el 49% de las entidades bancarias aún no están implementando herramientas, controles o procesos usando Tecnologías Digitales Emergentes, tales como *Big Data, Machine Learning* o Inteligencia Artificial, las cuales resultan muy importantes a la hora de prevenir ciberataques o determinar patrones sospechosos asociados a fraude, entre otras capacidades de detección. La perspectiva de la OEA frente a este tema no es para nada optimista, pues indica que "los ataques tendrán un amplio alcance y el cibercrimen continuará profesionalizándose, pues cada vez está más organizado" (p. 36).

Propuesta de buenas prácticas para mitigar ciberataques

En el proceso de planteamiento de la siguiente propuesta se han considerado aportes teóricos como los de Mariño (2020), una guía de ciberataques propuesta por el Gobierno de España, un estudio de Allauca (2022), entre otros referentes.

Tabla 9

Etapas que considerar para la gestión de la seguridad de la información y la ciberseguridad, instituciones como las entidades financieras deberán considerar

CONTROL	DESCRIPCIÓN GENERAL
Prevención	Prevención Establecer, mantener y documentar los controles de acceso (lógicos, físicos y procedimentales) y gestión de identidades bajo la premisa que las personas solo pueden disponer de los recursos que demande su trabajo, durante el tiempo que ello sea necesario. - Integrando al monitoreo los servidores de acceso, sistemas operativos, aplicaciones como bases de datos, servidores de archivos los cuales generaran logs de autenticaciones generadas, sesiones establecidas por usuarios y de esta manera registrar los accesos lógicos o físicos.

593 Digital Publisher CEIT ISSN 2588-0705

Adopción de políticas	Asumir procedimientos y mecanismos para evitar la fuga de datos e información. - Mediante la identificación de los usuarios que deben tener acceso a los recursos, servicios o repositorios de información dispuestos por la entidad y configurando grupos que funcionen como listas blancas o negras en el sistema de seguridad conocido como Security Information and Event Management (SIEM) para garantizar el adecuado acceso y evitando la fuga de datos.
Estructura	De acuerdo con la estructura, canales de atención, volumen transaccional y número de clientes, monitorear diferentes fuentes de información tales como sitios web, blogs y redes sociales, con el propósito de identificar posibles ataques cibernéticos contra la entidad. - Con la integración de los diferentes sistemas o fuentes de información al SIEM donde se configurarán reglas de correlación y se identificarán las técnicas más utilizadas por los ciberdelincuentes al sector financiero.
Protección y detección.	Las entidades deben desarrollar e implementar actividades apropiadas para identificar la ocurrencia de un evento de ciberseguridad. La función de protección y detección permite el descubrimiento oportuno de eventos e incidentes de ciberseguridad y cómo protegerse ante los mismos.
Procedimientos	Adoptar procedimientos y mecanismos para identificar y analizar los incidentes de ciberseguridad que se presenten- Se podrá realizar un estudio forense de los incidentes presentados haciendo un análisis de los sistemas involucrados y así detectar la mejor forma de implementar los respectivos controles y evitar que se repitan.
Monitoreo	Realizar un monitoreo continuo a su plataforma tecnológica con el propósito de identificar comportamientos inusuales que puedan evidenciar ciberataques contra la entidad. - Con la configuración de dashboards donde el personal pueda estar en el constante monitoreo de los comportamientos anómalos que se puedan presentar e identificar si pueden ser incidentes de seguridad.

Fuente: Allauca (2022).

Respuesta y comunicación

Aún con las medidas de seguridad adoptadas, las entidades deben desarrollar e implementar actividades para mitigar los incidentes relacionados con ciberseguridad. Según un reporte realizado por el Gobierno de España (2020), para hacerle frente a esta situación las entidades deben realizar lo siguiente:

Establecer procedimientos de respuesta a incidentes cibernéticos tales como: desconexión automática de equipos, cambios de contraseñas, actualizar la base de firmas del antivirus, bloqueo de direcciones IP o cualquier otro que determine la entidad.

Dentro de las funciones que tienen algunos equipos, cuentan con la capacidad de responder automáticamente a los comportamientos inusuales y que se puedan categorizar como incidentes de seguridad y generar respuestas activas como la desconexión de tarjetas de red, apagado o desconexión de los equipos, bloqueo de direcciones IP, reinicio de servicios, desconexión de usuarios.

En la medida de lo posible, preservar las evidencias digitales para que las áreas de seguridad o las autoridades puedan realizar las investigaciones correspondientes.

Los SIEM[1] funciona como un servidor *Syslog* en donde puede consultar las evidencias a través del tiempo como históricos y si bien no cuenta con esta opción se configuran reportes automáticos en donde se pueda tener las evidencias para las investigaciones o auditorias pertinentes.

Utilizar un antivirus para analizar todas las descargas y archivos sospechosos. Se debe mantenerlo siempre actualizado y activo.

Mantener el sistema operativo, navegador y aplicaciones siempre actualizadas a su última versión para evitar vulnerabilidades. Utilizar contraseñas robustas y diferentes para proteger todas tus cuentas.

Si es posible, utilizar la verificación en dos pasos u otro factor de autenticación.

Desconfiar de los adjuntos sospechosos, enlaces o promociones demasiado atractivas.

La mayoría de los fraudes se basan en ataques de ingeniería social que pueden ser detectados aplicando el sentido común.

1 SIEM (información de seguridad y gestión de eventos), es una tecnología capaz de detectar rápidamente, responder y neutralizar las amenazas informáticas.

Tener cuidado por donde se navegas. Utilizar solo *web* segura con https y certificado digital y utilizar el modo incógnito cuando no se quiera dejar rastro.

Descargar solo de sitios oficiales aplicaciones o software legítimo para evitar acabar infectado por *malware.*

En el caso de las aplicaciones, recordar dar solo los permisos imprescindibles para su funcionamiento.

Evitar conectarte a redes wifi-públicas o a conexiones inalámbricas desconocidas. Especialmente cuando se vaya a intercambiar información sensible, como los datos bancarios.

Y, en caso de tener que conectarse por una emergencia, trata de utilizar una VPN.

No compartir la información personal con cualquier desconocido ni publicar o guardar en páginas o servicios *web* no fiables.

Hacer copias de seguridad para minimizar el impacto de un posible ciberataque

Adicional a lo anterior, en el siguiente cuadro, tomado de Allauca (2022), se identifican los riesgos a la Ciberseguridad y se muestran las directrices apropiadas, para garantizar los requisitos de seguridad. En el cuadro en mención se indica el control y las descripciones generales de cada una de ellas y está basado en los controles de la norma ISO 27000.

Tabla 10

Controles norma ISO 27000

CONTROL	DESCRIPCIÓN GENERAL
Controles a nivel de aplicación	Exponer notificaciones cortas con resúmenes claros, concisos sobre el tema de políticas de seguridad. Asegurar el manejo de sesiones para las aplicaciones Web. Esto incluye mecanismos online como cookies. Asegurar la validación y manejo de las entradas para prevenir ataques comunes, tales como la Inyección SQL. Asegurar el scripting de la página Web para prevenir ataques comunes como las Secuencias de órdenes en Sitios Cruzadoso Cross-site Scripting. Revisar y testear la seguridad de los códigos por medios de entidades cualificadas apropiadamente. Que el proveedor use un subdominio desde un nombre de dominio con marca registrada de la organización y posiblemente el uso de credenciales HTTPS registrado a nombre de la organización.
Protección del servidor	Configurar los servidores, incluye los sistemas operativos subyacentes, de acuerdo con una guía de configuración de seguridad base. Reforzar los controles de acceso en los directorios y archivos de programa y sistema y habilitar el registro de auditoria de, particularmente, la seguridad y otros eventos de fallas en el sistema. Es más, se recomienda instalar un sistema mínimo en un servidor para reducir el vector de ataque. Implementar un sistema para probar e implementaractualizaciones de seguridad y asegurarse de que el sistema operativo y aplicaciones del servidor se mantenganactualizados. Revisar la configuración de seguridad y seguimiento del desempeño de seguridad del servidor. Hacer escaneos constantes en busca de posibles vulnerabilidades y ejecutar controles *anti-software* malicioso (como *spyware* o *malware*) en el servidor. Escanear todo el contenido alojado y subido, de manera regular, usar controles actualizados *anti-software* malicioso y realizar evaluaciones de vulnerabilidades y pruebas deseguridad de manera constante.
Controles para los usuarios finales	El sistema operativo y el software de aplicación se actualizaríancon respecto a los parches de seguridad. Usar herramientas anti-virus y *anti-spywares*, el *software* de seguridad se actualizaría con respecto a los parches de seguridad y a las bases de datos de firmas. Los navegadores Web y barras de herramientas de navegador comunes que incorporen capacidades como bloqueadores de pop-ups que evitan que sitios Web maliciosos muestren ventanas que contienen *spyware* o software engañoso. Los navegadores proveerán alertas, normalmente en forma deresaltos codificados con color, para advertir a los usuarios del potencial riesgo. Las organizaciones establecerán una política para habilitar el uso de dicha herramienta. Los proveedores de servicios fomentarán el uso de funciones de firewall y HIDS personales y/o sugerir otros productos de firewall y HIDS personales de terceros que han sido evaluados y considerados como confiables, además, de educar y ayudar a los usuarios a habilitar una seguridad de red básica a nivel desistema de usuario final. Las aplicaciones en las que confían los usuarios (por ejemplo, productos antispyware y antivirus) se habilitaran para que realicen actualizaciones automáticas. Esto asegura que los sistemas se actualicen con los últimos parches de seguridad.
Controles contra los ataques de ingenieríasocial	Desarrollar y documentar controles de seguridad específicos para la protección contra la exposición accidental y el acceso no autorizado intencional. Publicar procedimiento de cómo manejar las propiedades intelectuales de una compañía, los datos personales y otra información confidencial Acuerdo de política de seguridad con el proveedor de servicios. Que los usuarios cursen un número mínimo de horas de formación para asegur que estén conscientes de sus roles y responsabilidades en el Ciberespacio, además, de los controlestécnicos que estos implementarían como individuos al usar el Ciberespacio. Las personas necesitan estar conscientes de los riesgos relacionados en el Ciberespacio, y las organizaciones establecerán políticas pertinentes y dar pas proactivos para patrocinar programas relacionados para asegurar la conciencia competencia de las personas. Se considera la provisión de soluciones de autenticación sólidas, ya sea como parte de la autenticación de acceso y/o cuando se ejecuten transacciones crítica Usar un "Certificado de Alta Seguridad" para proporcionar una seguridad adicional a los usuarios online
Disposición de la Ciber protección	Controles técnicos adicionales que se aplicaran para mejorar ladisposición en el área de detección de eventos, a través de una *Darknet* para seguimiento; la investigación, a través de *Tracebacks*; y la respuesta, a través de una Operación *Sinkhole*, como parte de la Ciber protección de una organización. Otros controles incluirán algunos relacionados con la alerta y cuarentena de dispositivos que están comprometidos en actividades sospechosas u observadas, a través de la correlación de eventos desde los elementos del ISP o empresacomo los servidores DNS, el flujo de red de router, la filtración de mensajes salientes y las comunicaciones *peer-to-peer*.
Otros Controles	

Fuente: Basado en la norma ISO 27000, disponible en un estudio de Allauca (2022).

593 Digital Publisher CEIT ISSN 2588-0705

Tabla 11.
Eventos por monitorear como buenas prácticas

Eventos	Buenas prácticas
Eventos que monitorear de un firewall.	Monitoreo de accesos o cambios de los usuarios fuera de los horarios laborales que estipule la entidad financiera. Es claro que las entidades financieras podrían contar con personal que cumple con horarios de disponibilidad y 24/7 como lo podría ser el área de tecnología, por lo que hay que definir grupos que tengan permitido este acceso en estos horarios, pero aun así continuar con el monitoreo constante de ellos. En el caso del personal que no deba conectarse en horarios diferentes a los permitidos por la entidad establecer una serie de alarmas que estén informando al personal encargado del monitoreo cuando pasen estos eventos e identificar si se puede tratar de un incidente de seguridad.
Reglas de acceso	Creación o cambios de las políticas configuradas (reglas de acceso). Tener un registro de todos los cambios a nivel de reglas de acceso aprobados por los oficiales de seguridad o del área encargada donde se debe tener un seguimiento y evidencia de las actividades realizadas durante los cambios.
Cambios en el estado de servicios	Monitorear el performance del dispositivo garantizando la disponibilidad de los servicios, establecer listas de procesos a monitorear; como una lista blanca de procesos aprobados para el funcionamiento en los servidores o en los hosts finales de los usuarios, así mismo como una lista negra de procesos que no deberían ejecutarse por que puedan afectar la seguridad de la información en la entidad y catalogarse como un posible incidente.
Detección de actividad sospechosa	Ya sea URLs con amenazas, escaneo de redes y puertos, tomando los datos de navegación como las URLs y comparándola con los sitios conocidos con amenazas determinar si se llega a establecer una conexión con estos sitios, evidenciar los escaneos de la red y de puertos buscando una correlación para determinar si ocurre un incidente.
Registrar intentos fallidos	Registrar intentos fallidos y exitosos de inicio de sesión por VPN. Hay que realizar una segregación de usuarios buscando evidenciar a que sitios o recursos de red tienen permitido ingresar teniendo en cuenta sus roles y funciones por tal motivo es necesario registrar todas autenticaciones por VPN evidenciando a que recursos de red están ingresando. Así como las autenticaciones fallidas de usuarios que no pertenezcan a la entidad y si son muy concurrentes establecer bloqueos de IPs evitando posibles incidentes.
Puertos utilizados	Puertos utilizados para conexiones de aplicaciones o servicios. Cada aplicación o servicio utilizan puertos específicos para sus conexiones de red, estas conexiones deben estar permitidas desde ciertos segmentos de red o desde determinados host, por tal motivo es necesario evidenciar cuando se presentan eventos de descubrimiento de puertos abiertos a los servidores o servicios y así lograr detectar posibles conexiones fallidas o exitosas a estos puertos.

Fuente: Traisnel (2018).

Conclusiones

Cada vez más las instituciones financieras están expuestas a los riesgos cibernéticos debido a la creciente dependencia en la tecnología que podrían tener graves consecuencias de no tomar medidas seguras ante las amenazas eminentes; por ello, la implementación de la transformación digital de cualquier entidad financiera debe estar de la mano de una fuerte inversión en ciberseguridad y de gestión de riesgos para afrontar los nuevos desafíos de hoy en día.

El monitoreo de actividades es el control recurrente de cada una de las actividades propuestas, tanto en la valoración de su eficacia técnica, como logros en relación temporal. Por tanto, se debe realizar un monitoreo constante de las actividades sugeridas en esta propuesta con la finalidad de que el Comité de ciberseguridad pueda verificar los resultados de manera efectiva, caso contrario, de no haber conseguido los resultados esperados, se tendrá la posibilidad, de cambiar dichas etapas del modelo, para así mejorar la seguridad de los datos.

Referencias Bibliográficas

Allauca, E. (2022). Propuesta de mejores prácticas de ciberseguridad para la comunicación en redes de clientes corporativos (Tesis de maestría). Pontificia Universidad Católica del Ecuador, Quito, Ecuador. https://repositorio.pucesa.edu.ec/bitstream/123456789/3779/1/78213.pdf

Arcenegui, J., Obrero, V., & Martín, J. (2016). Propuesta de un modelo para la prevención y gestión del riesgo de fraude interno por banca paralela en los bancos españoles. *Cuadernos De Contabilidad, 16*(42), 625-660. doi:https://doi.org/10.11144/Javeriana.cc16- 42.pmpg

Atencia, V. (2021). *Metodología para cuantificar las pérdidas económicas y financieras de una empresa, tanto a nivel nacional o internacional, cuando es afectada por ciberataques o ataques informáticos.* (Tesis de maestría). Universidad EAFIT, Medellín, Colombia. https://repository.eafit.edu.co/bitstream/handle/10784/30140/V%C3%ADctorRafael_AtenciaUrueta_2021.pdf?sequence=2&isAllowed=y

Cerasela, A. (2021). *La seguridad cibernética y los derechos humanos – los límites de la restricción de derechos humanos para la protección del espacio cibernético.* (Tesis doctoral). Universidad Carlos III de Madrid, Madrid, España. https://e-archivo.uc3m.es/bitstream/handle/10016/33038/tesis_alexandra_cerasela_pana_2021.pdf?sequence=1&isAllowed=y

Cerasela, A. (2021). La seguridad cibernética y los derechos humanos – los límites de la restricción de derechos humanos para la protección del

espacio cibernético. (Tesis doctoral). Universidad Carlos III de Madrid, Madrid, España. https://e-archivo.uc3m.es/bitstream/handle/10016/33038/tesis_alexandra_cerasela_pana_2021.pdf?sequence=1&isAllowed=y

Cuesta, C., Ruesta, M., Tuesta, D., & Urbiola, P. (16 de Julio de 2015). La transformación digital de la banca. Observatorio Económico Digital, 7(2), 1-11. https://www.bbvaresearch.com/wp-content/uploads/2015/08/Observatorio_Banca_Digital_vf.pdf

Chávez, J., Malpartida, D., Villacorta, A., y Orellano, J. (2021). La influencia de la automatización inteligente en la detección del cibercrimen. *Boletín de Coyuntura, 31*(12), 26-33. https://revistas.uta.edu.ec/erevista/index.php/bcoyu/article/view/1462

De Tomas, S. (2014). Hacia una cultura de ciberseguridad: capacitación especializada para un "proyecto compartido". Especial referencia al ámbito universitario. icade. Revista cuatrimestral de las Facultades de Derecho y Ciencias Económicas y Empresariales, 2(1), 13-47. https://revistas.comillas.edu/index.php/revistaicade/article/view/4093/3914

Díaz, Y., y Mosquera, E. (2022). *Influencia del blockchain en procesos contables y Financieros.* (Tesis de pregrado). Universidad Cooperativa de Colombia, Medellín, Colombia. https://repository.ucc.edu.co/bitstream/20.500.12494/46111/8/2022_influencia_blockchain_procesos.pdf

Esteves, J., Ramalho, E., y De Haro, G. (2018). El problema de la ciberseguridad. Si no puedes vencerles, únete a ellos. Harvard Deusto business review, 282(12), 22-28. https://dialnet.unirioja.es/servlet/articulo?codigo=6558396

Gobierno de España (2020). *Guía de ciberataques.* https://www.osi.es/sites/default/files/docs/guia-ciberataques/osi-guia-ciberataques.pdf

Gómez, Á. (2012), *El ciberespacio. Nuevo escenario de confrontación.* Madrid: Ministerio de Defensa.

Gómez, M. (2017). Ciberataques: ¿Está seguro nuestro dinero? Inversión: el líder semanal de la bolsa, economía y gestión de activos, 3(2), 30-32. https://dialnet.unirioja.es/servlet/articulo?codigo=6016838

Guerrero, B., y Castillo, D. (2017). *Desafíos técnicos y jurídicos frente al ciberdelito en el sector bancario colombiano.* (Tesis de grado) Universidad Nacional Abierta y a DIstancia, Escuela de ciencias básicas tecnología e ingeniería, Bogotá. https://repository.unad.edu.co/bitstream/handle/10 596/13387/52498805.pdf?sequence=5&isAllowed =y

Hayes, S. M. (2020). *El impacto de los delitos financieros*. México: KPMG. https://assets.kpmg/content/dam/kpmg/mx/pdf/2020/06/El-impacto-de-los-delitos-financieros.pdf

López, D. (2020). Tiempo de poder. Automática e instrumentación. 56(23). 24-28. https://www.politecnicojic.edu.co/images/downloads/biblioteca/ediciones-digitales/automatica-instrumentacion/automatica-instrumentacion-518.pdf

Machín, M. (2016). La ciberseguridad como factor crítico en la seguridad de la Unión Europea. *Revista UNISCI, 42*(3). 47-68. https://www.redalyc.org/pdf/767/76747805002.pdf

Mariño, J. (2020). *Propuesta de buenas prácticas de eventos a monitorear en un Siem para cooperativas financieras en Colombia dando cumplimiento a la circular 007.* (Tesis de pregrado). Universidad Católica de Colombia, Bogotá, Colombia. https://repository.ucatolica.edu.co/server/api/core/bitstreams/1184e90b-c4d0-44f1-9854-8331aee754d8/content

Digital Publisher CEIT ISSN 2588-0705

OEA (2018). *Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe.* https://www.oas.org/es/sms/cicte/sectorbancariospa.pdf

Ojeda, F., Moreno, V, Torres, M. (2020). Gestión del riesgo y la ciberseguridad en el sector financiero popular y solidario del Ecuador. Cienciometría, 6(2), 192-219. https://dialnet.unirioja.es/buscar/documentos?querysDismax.DOCUMENTAL_TODO=Fredy+Israel+Ojeda

Ojeda, J., y Arias, M. (2010). Delitos informáticos y entorno jurídico vigente en Colombia. *Cuadernos Contables, 11*(28), 41-66. http://www.scielo.org.co/pdf/cuco/v11n28/v11n28a 03.pdf

Ordóñez, E. Narváez, C. y Erazo, J. (2020). El sistema financiero en Ecuador: Herramientas innovadoras y nuevos modelos. Revista Arbitrada Interdisciplinaria Koinonía, 5(10), 195-216. https://www.redalyc.org/journal/5768/576869215008/576869215008.pdf

Quispe, C. (2021). *Procedimiento de gestión para ciberseguridad en la infraestructura tecnológica del sector financiero segmento 1 regulado por la superintendencia de economía popular y solidaria (seps) en el cantón Ambato, Ecuador.* (Tesis de pregrado). Universidad Técnica de Ambato, Ambato, Ecuador. https://repositorio.uta.edu.ec/bitstream/123456789/33703/1/t1877si.pdf

Traisnel, J. (2018). Desafíos para las empresas de dinero electrónico. Byte España, 260(16), 56-58. https://dialnet.unirioja.es/servlet/articulo?codigo=7939870

Véliz, D. (2022). Estudio de ciberseguridad en sistemas SCADA y sistemas informáticos como respuesta a la industria 4.0 en el Ecuador (Tesis de pregrado). Universidad Católica de Santiago de Guayaquil, Guayaquil, Ecuador. http://201.159.223.180/bitstream/3317/19158/1/T-UCSG-PRE-TEC-IECA-155.pdf

Wilches, Y. (2015). *Importancia de la implementación del concepto de ciberseguridad organizacional en las organizaciones tipo PYMES.* (Tesis de pregrado). Universidad Militar Granada, Bogotá, Colombia. https://repository.unimilitar.edu.co/bitstream/handle/10654/7325/Importancia%20de;jsessionid=A1EEA7B9703993215A297C5401EB3CAB?sequence=1