Riesgos de **Robos de Credenciales Bancarias** en el Sistema Financiero Nacional de la República Dominicana

Por:

1073505

Ing. Miguel Alfonso Peña Gago

Trabajo final de Graduación Presentado al Área de Ingeniería del Instituto Tecnológico de Santo Domingo, INTEC, de la República Dominicana en Cumplimiento de parte de los Requisitos para la Obtención del Título de Master en Ciberseguridad.

Instituto Tecnológico de Santo Domingo

2019

Agradecimientos

A Dios todopoderoso por permitirme experimentar en carne propia el camino de la vida, por darme sus fuerzas a través de personas sencillas, desposeídas, débiles pero llenas de lo más importante y lo que hace falta en la humanidad “el Amor de Dios”.

A mi madre Dra. María Del Carmen Gago Lebrón por ser la persona que primero me entreno y preparo para vivir en estos tiempos, siempre haciendo un equilibro entre Dios y la Tecnología, y por enseñarme a creer en un Dios de lo imposible a través de sus enseñanzas y gran compañía.

A mi padre Lic. Ildefonso Garibaldi Peña Núñez, gracias padre por tu esfuerzo en un tiempo donde las personas como tú ya la valoran muy poco, aun con tus defectos y virtudes hiciste hasta lo imposible por mantenerte en familia a pesar de los cambios y de las crisis familiares y financieras.

A mi hermana Lic. María Mercedes Peña Gago por siempre estar ahí presente para discutir conmigo temas difíciles, gracias por tus conocimientos de la historia de la República Dominicana, sobre todo estar en familia junto a todos nosotros en estos tiempos de tantos cambios.

A mi fuerza especial Aux. Helen Reynoso Rodríguez por acompañarme en tiempos tan duros, por darme el calor de sus manos, su cariño, amor, amistad, aprecio y sobretodo seguir junto a mí y tratar de entender mis ideas, gracias Dios te bendiga y te lleve a ti y tus hijos al lugar que elijas y mereces de acuerdo a lo que has hecho conmigo, le pido a Dios un matrimonio feliz contigo y tus hijos.

A todas las iglesias del mundo, sobre todo las que siguen a Jesús, a los que creen en la naturaleza, a los que todavía no creen en nada y a aquellos que siguen confundidos por lo que está sucediendo con la humanidad, les aseguro que todos nos sorprenderemos.

A la Biblioteca Nacional Pedro Henríquez Ureña y La Biblioteca Pública Municipal Prof. Juan Bosch, por permitirme tener mi único empleo durante 6 años y mantenerme mi salario y esforzarse por tratar de entender lo que es ser una persona altamente sensible en esta dimensión física, escuchar esta propuesta que hoy se hace realidad, gracias al Dr. Diomedes Núñez Polanco y al Lic. Héctor Nina por escuchar mis ideas, y Por último a UCATECI e INTEC por darme una brecha abierta hacia un mundo misterioso y fascinante, y sobre todo por formar jóvenes capaces de avanzar a un nuevo mundo tecnológico más competitivo de acuerdo a nuestros tiempos, gracias Ing. Miguel María Árias Romero por la oportunidad brindada espero no defraudarlo; gracias profesor, gracias.

Resumen

El Riesgo de robo de credenciales bancarias en el sistema financiero nacional de la República Dominicana está aumentando cada día y es urgente poner en ejecución el reglamento de seguridad cibernética aprobado por el Banco Central y la Superintendencia de Bancos (nov. 2018) lo más rápido posible. Pero es más urgente dar a conocer en que consiste este reglamento e informar a la población general en que consiste el riesgo de robo de credenciales bancarias como prevenirlo, que hacer y donde dirigirse para solucionar esta problemática.

Mi trabajo es un comienzo para la ejecución de nuevas ideas en esta área. Implemente encuestas anónimas en el área financiera (Ya que está prohibido dar información), encuestas en la población general donde se señala las interrogantes y las posibles soluciones para hacer una buena política en esta problemática. A partir de esto realizar un periódico digital de ciberseguridad e informativo donde se presente las principales interrogantes de la población, como solucionarlas, prevenir el robo de credenciales bancarias donde dirigirse si está envuelto en esta situación y cuales instituciones tanto financieras como tecnológicas están respaldadas por el Reglamento de Seguridad Cibernética dictado por el Banco Central de la República Dominicana. Así tendremos una población más educada, más alerta y más prevenida en esta problemática.

Sabemos que nos falta mucho camino por recorrer, pero hay personas e instituciones que están dando los primeros pasos para que a partir de los próximos dos años tengamos más información poblacional, más personal capacitado en esta área y mejor desempeño nacional e internacional en esta problemática que le origina al sistema financiero y tecnológico muchas pérdidas económicas a la República Dominicana.

Abstracts

The risk of theft of banking credentials in the national financial system of the Dominican Republic is increasing every day and it is urgent to implement the cybersecurity regulation approved by the Central Bank and the Superintendency of Banks (Nov.2018) as quickly as possible. But it is more urgent to make known what this regulation consists of and inform the general population about the risk of stealing bank credentials, how to prevent it, what to do and where to go to solve this problem.

My work is a beginning for the execution of new ideas in this area. Implement anonymous surveys in the financial area (Since it is forbidden to give information), surveys in the general population where the questions and possible solutions to make a good policy on this problem are pointed out. From this, create a digital cybersecurity and information newspaper where the main questions of the population are presented, such as how to solve them, prevent the theft of bank credentials to address if you are involved in this situation and which financial and technological institutions are supported by the Cybersecurity Regulation issued by the Central Bank of the Dominican Republic. Thus we will have a more educated population, more alert and more prevented in this problem. We know that we still have a long way to go, but there are people and institutions that are taking the first steps so that from the next two years we have more population information, more personnel trained in this area and better national and international performance in this problem. It originates from the financial and technological system many economic losses to the Dominican Republic.

Índice

Contenido

Palabras claves

Robo de Identidad: Consiste en robos de documentos de identificación personal existentes en el mundo real físico palpable como son números de cédula, de seguridad social, toda aquella documentación que acredite a la persona de quien es, a que familia pertenece y que función desempeña en la sociedad a la que pertenece.

Web-Crawler: Su traducción al español es tractor de la web, también se le llama araña web o robot araña, su objetivo principal es que al usuario escribir lo que busca este con su gran capacidad realiza una búsqueda por todo internet visible y arroja el resultado que el cliente solicitó.

Robo de Identidad Digital: Aquí tenemos que solo sucede en tierras digitales, es decir, en Internet, por ejemplo, el Aparente Ciberdelincuente puede robar lanzando un Web-Crawler para recolectar toda información en internet relacionado con una persona en particular, obtener cuentas de redes sociales, entre otros que den un perfil digital claro de quien es la persona detrás de la imagen.

Robo de Credenciales Bancarias: Esta estafa se refiere a nombres de usuario, contraseñas, números de identificación de préstamos, cantidad monetaria en la cuenta, números de cuentas bancarias, fechas de depósito y retiros digitales, historial de acceso a la banca personal por internet, entre otros.

Troyanos Bancarios: Es una infección maliciosa digital cuyo objetivo principal es que pasen desapercibidos por los controles internos de la organización sobre todo de los equipos críticos de la empresa como pueden ser servidores de bases de datos, proveedores de servicios, aplicaciones de análisis, entre otros.

Phishing: Su vía de ataque es a través del correo electrónico sin importar que sea gratuito o de pago, su propósito es engañar al usuario para empujarlo a que de Click en un enlace desconocido y así insertar su virus malicioso con la intención de robar credenciales, entre otras.

Spear-Phishing: Este ubica una organización específica o grupo de personas y envía un ataque masivo hacia su objetivo inundando así todo el correo electrónico de su objetivo grupal.

Hacker: Aparente ciberatacante de sistemas computacionales, el cual utiliza gran cantidad de habilidades informáticas para analizar, mejorar, prevenir, causar daños en infraestructuras críticas como bancos, electricidad, estaciones de metro, ciudades inteligentes, conexiones inalámbricas de gran escala, entre otras.

TED Comunidad Online de Conferencias: Es un lugar en internet donde expertos e investigadores presentan de forma gratuita y democrática su imaginación, conocimientos y habilidades sobre temas sociales, científicos, nuevos descubrimientos, entre otros.

Malware: Es un programa maligno cuyo fin es infectar dispositivos digitales con la finalidad de extraer información personal, contraseñas, robar dinero para uso propio, transferir dinero entre cuentas de forma invisible y transparente para el usuario y el personal a cargo de las cuentas bancarias de los clientes.

Crimeware: Único software específico para **robo de credenciales bancarias** dedicado a sobrepasar los controles informáticos de cualquier empresa.

Crimeware Kits: Conjunto de programas de computadora para extraer credenciales bancarias filtrándose sin ser detectados por las empresas y los bancos.

CISO: Certified Information Security Officer, cuya traducción es certificado como oficial de seguridad de la información, es quien desarrolla, despliega y mantiene un programa de seguridad de la información, el cual sirve para proteger a todos los datos de los negocios que son almacenados y procesados, este es un rol más integral en una organización, identificando los riesgos a través de todo el negocio asegurando que todos los empleados estén de acuerdo y con conocimiento del daño que pueden hacer las fugas de datos, muchas organizaciones solo están iniciando a ver los grandes beneficios de emplear a estas personas especialmente porque saben manejarse con los ciberataques de hoy en día.

TI: Siglas del inglés Technology Information, tecnología de la información, la cual utiliza computadoras centralizadas o grupos de computadoras para soportar las demandas de datos de los ciudadanos digitales de hoy en Día, sin embargo, sus propósitos son almacenar, retirar y recuperar datos para el bien de las necesidades actuales.

Inteligencia Artificial (AI): Es un campo aparte de la ciencia computacional que trabaja con el aprendizaje por sí mismo de las computadoras, estas máquinas que las llevamos dentro de nuestros bolsillos son capaces de entrenarse a ellas mismas para realizar ciertas tareas que el usuario les haya dictado a realizar y así poder actuar como un ser humano lo haría en el mundo real proviene del inglés Artificial Intelligence combinado ligeramente con el Machine Learning.

Machine Learning: Es otro campo de la inteligencia artificial que trabaja en áreas como que las maquinas cuando las llenamos de información valiosa la misma puede aprender a identificar patrones reconocibles en el mundo real y hacer mejores tomas de decisiones con el mínimo esfuerzo humano posible hasta hoy en día.

Autenticación de Dos Pasos: En realidad aquí se refiere a obtener y garantizar que después de un primer código digitado al iniciar sesión, luego solicita la digitación de un segundo código pero en este caso es aleatorio generado por un algoritmo matemático que al digitarse permite el acceso del usuario al sistema, finalmente esto es una forma simple es decir quién soy dos veces, por ejemplo accedemos con un email y una contraseña, al pasar este paso se genera una clave lo suficientemente impredecible e aleatoria para que luego que el usuario la digite con su teclado le permita el acceso a su plataforma anhelada, esto es un milagro de Dios.

Cobit 5: Es el único entorno de negocios para regular los activos críticos conectados a Internet para maximizar el valor de su empresa como también manejar los riesgos de robo de credenciales bancarias a nivel nacional e internacional, valorar la propiedad intelectual, asegurando una buena gestión de la ciberseguridad de las organizaciones.

NIST: Este entorno de trabajo de buenas prácticas realizado por científicos innovadores consisten en estándares, líneas guías para muy bien manejar los riesgos relacionados con la ciberseguridad de hoy en día, con certeza mediante: identificar, proteger, detectar, responder y recuperar los servicios caídos de la empresa.

Magerit V.3: Es un grupo combinado de normativas que estima que el éxito de un buena gestión gubernamental y corporativa descansa en esta metodología de análisis y riesgos de filtraciones inadecuadas de los sistemas de información aplicada a ministerios, gobiernos, administraciones públicas y privadas.

ISO 270001: Es una familia de normas de seguridad de la información para asegurar los activos muy importantes para las empresas por ejemplo mantener la información segura en un entorno conectado a internet es su principal prioridad para garantizar la estabilidad cibernética de las organizaciones a nivel local, regional y global.

GDPR: Es un nuevo reglamento europeo (E U) que viene a diferenciar y reformular la forma como se piensa sobre la ciberseguridad y la privacidad de los datos de las personas que permiten quienes, como, cuando, donde, porque y que beneficios tengo si una empresa divulga o algún grupo de ciberdelincuentes roba las credenciales bancarias o información de un ciudadano europeo que tenga sus datos en internet, tiene 7 principios que hablan de la forma como es almacenada, procesada y bajo qué autorización se usa la información, las empresas u organizaciones que violen uno de estos principios tienen que pagar hasta más de 20 Millones de Euros o un equivalente al 4% de todo el producto interno bruto mundial anualmente de la empresa, lo cual es mucho más dinero todavía.

Algoritmo Aleatorio: Es un conjunto de pasos en secuencia que tiene la gran utilidad de generar códigos diferentes para prevenir en acceso de un aparentes ciberdelincuentes a plataformas utilizados por los usuarios del sistema informático.

Internet Banking: Viene del inglés y se traduce Banca de Internet el cual es un servicio ofrecido por los bancos de nuestro país y del mundo entero que funciona en la nube **(Cloud)** que permite con sencillez a los usuarios mediante un usuario y una clave entrar y consultar tus datos bancarios, verificar el estado numérico un préstamo, transferir dinero entre cuentas y pagar servicios en línea como por ejemplo tus teléfonos residenciales, entre otros.

Cloud Computing: Significa computación en la nube y es el servicio salvador mediante el cual millones de personas pueden acceder a aplicaciones que están casi siempre disponibles en internet para reducir costos de transporte por ejemplo reducir los gastos que afectan al medio ambiente por ejemplo dejando de depender del papel y más de lo digital.

Tokens: Pequeño aparato electrónico que lo único bueno que sabe hacer excelentemente es generar números aleatorios que le da una protección adicional al usuario para que mediante su usuario y contraseña o password al entrar en el Internet Banking en línea se le comunica o se le pide que digite o escriba con su teclado de computadora o teléfono inteligente en código generado para así acceder a sus servicio que ofrece su banco a través del Internet Banking (Banca Electrónica).

Computadora Tradicional: Aquí me refiero con reverencia a las computadoras personales ya sean de escritorio y portátiles están son muy usadas en nuestro país sobre todo en las provincias y con sus sistemas te permite hacen uso de internet como una persona normal y corriente.

Teléfono Inteligente: Dispositivo electrónico de lujo que tiene un sistema que permite hacer cosas más sofisticadas que un teléfono residencial tradicional como por ejemplo descargar aplicaciones de pago, de juegos, de entretenimiento, entre otros.

Ciberdelincuentes: Grupo de Hackers que funcionan en el ciberespacio que usan habilidades para destruir y romper organizaciones económicas para muy malos fines, generalmente roban información y la utilizan para maltratar en vez de aportar para buenas causas.

Introducción

Existe una Antigua broma en la industria de la Seguridad sobre cómo asegurar cualquier computadora, simplemente desconéctala, P.W. Singer, Friedman, A. Cybersecurity and Cyberwar What Do We Mean by "Security" Anyway (2014). El gobernador del Banco Central, Héctor Valdez Albizu, anunció que desde la Junta Monetaria se ha propiciado una base normativa común para todas las entidades y empresas interconectadas al sistema de pagos del país, cuyo principal pilar es el Reglamento de Seguridad Cibernética y de la Información recientemente aprobado, basado en los estándares internacionales, que permitirá tener el marco de referencia para evaluar el grado de madurez en ciberseguridad de todas las instituciones conectadas en línea.

Esta medida evitará riesgos de contagio para los sistemas financieros y de pagos, dijo.

Valdez Albizu señaló que no es un secreto que la revolución digital y el avance tecnológico en los servicios financieros ha traído consigo la transición de los delitos del mundo físico al mundo digital, lo que ha obligado a repensar las estrategias de seguridad de las entidades financieras y de sus entes reguladores.

"No es solamente prevenir, anticipar, proteger y rechazar ataques. Es necesario, en última instancia, estar preparados para responder al público, enfrentar el daño reputacional, mitigar el efecto causado y garantizar la continuidad de las operaciones", indicó el gobernador del BC al participar en la 52 Asamblea Anual de la Federación Latinoamericana de Bancos (Felaban).

De acuerdo con Valdez Albizu, los ciberdelitos surgen porque cada vez más las transacciones son electrónicas y se usan instrumentos de pago para transferir dinero de

un lado a otro sin que éste salga de las bóvedas de los bancos. Aclaró que de nada vale tener reglamentos y sistemas informáticos de última generación para protegerse del delito tecnológico si las organizaciones financieras no edifican correctamente en estos temas a los usuarios de los servicios financieros, tomando en consideración que los últimos ataques cibernéticos que han sufrido los bancos y sistemas de pago a nivel internacional de los cuales posee información tienen un punto de entrada común y es un componente humano involucrado. Por tanto, recomendó a los líderes, banqueros, empresarios e inversionistas que implementen una campaña de concientización a todos los niveles, tanto al personal interno como a los clientes, sobre el peligro de los ataques cibernéticos, pues corren riesgos, no solo los sistemas bancarios sino también el dinero y ahorros de las empresas y del público en general. Ramírez, Jhenery "Anuncia un nuevo reglamento contra ciberdelito" (2018).

El marco legal en el cual se apoya el Sistema de Pagos de la República Dominicana parte de la Ley Monetaria y Financiera 183-02 de fecha 21 de noviembre de 2002. El Artículo 27 de dicha Ley establece lo siguiente: Sistema de Pagos y Compensación: "El sistema de pagos y el de compensación de cheques y demás medios de pagos, es un servicio público de titularidad exclusiva del Banco Central. La reglamentación de la organización y el funcionamiento del sistema de pagos y compensación por parte de la Junta Monetaria, tendrán como objetivos fundamentales, asegurar la inmediación y el buen fin del pago, pudiendo establecer distintos subsistemas, teniendo como referencia los estándares internacionales en la materia. Todas las entidades de intermediación financiera estarán obligatoriamente adscritas a dicho sistema y no podrán organizarse sistemas multilaterales de compensación y liquidación de medios de pago fuera del previsto en este Artículo. Corresponde al Banco Central actuar como supervisor y liquidador final del sistema de pagos y compensación. La prestación material del

servicio podrá ser concedida a entidades privadas, en la forma que determine reglamentariamente la Junta Monetaria. En ningún caso, el Banco Central podrá cubrir una posición negativa de una entidad de intermediación financiera, por transitoria que ésta sea. La Junta Monetaria podrá establecer un régimen de fianza colectiva o de garantías adecuadas para los participantes. Las cuentas de encaje y demás fondos depositados por las entidades de intermediación financiera en el Banco Central, servirán como cuenta corriente para el sistema de compensación y de pagos, conforme lo determine la Junta Monetaria".

El sector financiero, en su enfoque de gestión de riesgos, en los próximos tres años, se enfrentará al impacto significativo que representan las tecnologías Blockchain, Robótica, Automatización e inteligencia artificial. "La Ciberseguridad debe ser un punto permanente de la agenda de los Consejos de Administración y la Alta Gerencia".
Rodríguez, Bismark "Experto Recomienda Sector Financiero Invertir en Tecnología para mejorar la Ciberseguridad" (2018).

Con la entrada del Reglamento de Seguridad Cibernética se necesitarán equipos, personal capacitado en dicha área. Además de información digital para ejecutar los programas satisfactoriamente. Tenemos urgentemente que implementar medios para que esa información de forma generalizada llegue a la población que usa los recursos financieros para así tener una banca más segura en la inversión.

Capítulo I: El Problema.

a. Planteamiento del Problema.

la República Dominicana se enfrenta cada vez más a amenazas cibernéticas. El gobierno del país reportó 963 casos de suplantación de identidad (phishing) en 2013, así como 432 casos de robo de datos bancarios entre 2009 y 2014, A pesar de la iniciativa "Internet Sano" (http://www.Internetsano.do) del Instituto Dominicano de las Telecomunicaciones (INDOTEL), la sensibilización del sector privado sobre seguridad cibernética es moderada y la conciencia social acerca de estos asuntos sigue siendo baja. No obstante, las empresas privadas están reconociendo la privacidad del empleado como un asunto importante y se encuentran adoptando medidas de protección.

Mi sugerencia en esta investigación es educar a la población y dar a conocer de lo que es la ciberseguridad, los riesgos a nivel financiero y cómo prevenirlos.

Para esto pretendo implementar la creación de esta fuente investigativa para hacer una verdadera conciencia a nivel poblacional en materia de ciberseguridad a nivel financiero valorando la innovación igual que la práctica para así crear un mercado económico más ciberseguro en nuestra amada República Dominicana.

A continuación, propongo las siguientes sugerencias de innovación:

1. Hay que tener más tacto y contacto con las necesidades cibernéticas del ciudadano digital de la República Dominicana, por ejemplo, es

insuficiente solo poner publicidad y educación digital por lo cual se deben formar agentes cibernéticos educadores, financieros y diplomáticos que vayan de lugar en lugar, cara a cara a educar a familias, escuelas, universidades, empresas y sociedades A nivel local, regional y global.

2. Crear encuestas digitales anónimas a nivel financiero y poblacional para conocer las principales interrogantes en esta área y así poder dar soluciones efectivas a las necesidades actuales de los clientes.
3. Hay que emprender un periódico digital e impreso que se llame "Ciberseguridad Siglo XXI" para informaciones sobre riesgos de robo de credenciales bancarias en el sistema financiero nacional de la República Dominicana.
4. Crear un sector del sistema financiero que funcione con una inteligencia artificial conectada a toda la banca electrónica que gestione la parte de incidentes cibernéticos que prevenga, intente de predecir, sea dinámica al tomar decisiones y sea adaptativa de acuerdo a la manifestación del caso incluyendo el tema de postevalucación al finalizar el ciberataque.
5. Crear dispositivos más ciberseguro y fáciles de llevar como es el uso de una pulsera digital impermeable que tiene acceso a toda la información de las tarjetas de crédito del cliente, capaz de sincronizarse con otros dispositivos, con el fin de pagar, comprar y recargar dinero en la misma; contribuyendo a la seguridad del cliente, pero, además, realizando el proceso de manera más fácil y accesible. Ayuda a la ciberseguridad del cliente financiero,

porque no necesita llevar todas sus tarjetas físicas, y en caso de un robo, sería más difícil obtener su información, porque para su acceso hay que introducir una contraseña y huella digital como también autenticación de dos pasos configurándola con una aplicación de generación de códigos gratuita o de pago. Hace más fácil y rápido el proceso y tiene mayor accesibilidad a la información bancaria. Gago, María "Asignatura de Introducción a los Negocios, Instituto Tecnológico de Santo Domingo, INTEC" (2018).

6. La mayor parte de los robos de credenciales suceden al inicio de sesión de la plataforma deseada para entrar, los probables ciberdelincuentes con sus tácticas son la creación de una excelente ingeniería social en combinación con la dedicación a programar un troyano bancario dirigido a su objetivo que pueden ser Sistemas operativos Windows como el más usado por los usuarios y algunas empresas como también Linux, Android, iOS, entre otros, estas personas harán todo lo posible por engañar o falsear la entrada de datos de parte de los usuarios que quieren acceder a su plataforma que Aman debido a que es parte de su trabajo como entes productivos. Social Security "El robo de credenciales, nuevo foco de los cibercriminales" (2017).

Formulación proposicional.

A. Prevenir el **robo de credenciales bancarias** en el sistema financiero nacional

B. Formulación Interrogativa.

1. ¿Cuáles son los métodos o técnicas que el ciberdelincuente utiliza para robar credenciales bancarias?

2. ¿Cuáles son las Instituciones Bancarias de la República dominicana que más robo de credenciales sufren en la actualidad?
3. ¿Cómo podemos identificar a un posible ciberdelincuente?

4. ¿Cómo podemos lograr que el Ciudadano Dominicano sea mas ciberseguro con sus credenciales bancarias?

5. ¿Cómo identificar y prevenir el Robo de Credenciales Bancarias en el Sistema Financiero de Nuestra República Dominicana?

En el reporte, llamado “Building Confidence: Facing the Cybersecurity Conundrum”, Accenture entrevistó a 2.000 expertos de seguridad de compañías de ingresos anuales de US$ mil millones, en más de 15 países. La encuesta consultó sobre temáticas y sus percepciones en temas de ciberataques, la efectividad de sus esfuerzos actuales de seguridad, y sus actuales inversiones en seguridad. Asimismo, revela que el tiempo que les toma a las compañías en detectar estas violaciones de seguridad agrava el problema, ya que más de la mitad de los ejecutivos consultados (51%), afirma que les toma meses detectar ataques sofisticados de seguridad, y más de un tercio de los ataques exitosos de

seguridad no son detectados. “La transformación digital es y debe ser una realidad para las empresas en tanto constituye una herramienta fundamental para el crecimiento y el aumento de la productividad”.

Lo que se ha hecho en el pasado no está funcionando

- Dejar de lado lo antiguo y adoptar lo nuevo es algo más fácil de decir que de hacer, especialmente cuando se trata de adoptar nuevas tecnologías y herramientas de defensa de ciberataques, solo en este caso, sin embargo, los cambios son beneficiosos siempre que ambas partes estén completamente felices, solo así, significa que hemos logrado despertar de nuestro sueño profundo.

– Mientras los encuestados por el estudio de Accenture afirman que los ataques internos tienen el impacto más grande, 58% prioriza los controles perimetrales, en vez de enfocarse en las amenazas internas.

– La mayoría de las compañías no cuenta con la tecnología efectiva para monitorear los ciberataques y está enfocada en riesgos no asociados con las amenazas.

– Sólo 37% de los consultados dice que confía en su habilidad para desarrollar un monitoreo esencial de posibles ataques de seguridad y 36% sostiene lo mismo respecto de minimizar disrupciones.

- Mayor efectividad en la inversión para seguridad

Recientes ciberataques de alto perfil han llevado a las compañías a aumentar sus inversiones en seguridad. Sin embargo, la encuesta muestra que las empresas seguirán invirtiendo en las mismas medidas, en vez de invertir en controles nuevos y diferentes para mitigar las amenazas.

– Por ejemplo, entre 44% y 54% dice que doblará sus gastos actuales en ciberseguridad, aunque las tecnologías específicas en uso no han detectado ni reducido de forma significativa ataques de seguridad en desarrollo.

– Estas prioridades incluyen proteger la reputación de la compañía (54%); resguardar la información de la compañía (47%); y proteger la información de los clientes (44%).

– Sin embargo, pocas compañías invertirán en mitigar sus pérdidas financieras (28%) o en entrenamiento de ciberseguridad (17%)

Diario TI "Building Confidence: Facing the Cybersecurity Conundrum" (2017).

Objetivos de la investigación.

a. Objetivo general.

Prevenir el robo de credenciales bancarias en el sistema financiero nacional dominicano.

b. Objetivos específicos.

- Identificar y Analizar las características que provocan el robo de credenciales bancarias.
- Crear conciencia de cultura digital y de ciberseguridad en la República Dominicana.

Justificación de la investigación.

La presente Investigación propone crear conciencia preventiva sobre el **robo de credenciales bancarias** en tiempos globalizados y en los Ciudadanos Dominicanos del Sistema Financiero Nacional de la República Dominicana, es decir, todos.

Alcance.

La Presente Investigación tendrá como techo el **Robo de Credenciales Bancarias** en el Sistema Financiero Nacional Dominicano contemplando la situación global, regional y local de la ciberseguridad como tema clave en estos tiempos modernos.

Limitaciones.

Ninguna

Capitulo II: Referencias Conceptuales.

2.1 **Marco Teórico: Antecedentes de la Investigación.**

Situación a Nivel Mundial:

"El aspecto más triste de la vida en este preciso momento es que la ciencia reúne el conocimiento más rápido de lo que la sociedad reúne la sabiduría" (**Asimov, Isaac).** Hoy en día a pesar de estar cubiertos de buena ciberseguridad, existe una situación clásica a nivel mundial que los posibles ciberdelincuentes utilizan para robar credenciales bancarias y es el empleo de troyanos y al usar en combinación sus familias, no hace falta mencionar sus nombres, pero si su modo de operar, al abordar con sabiduría equilibrada, es muy necesario y objetivo que los equipos que alojan malware

bancario no necesariamente terminan en una situación de fraude. Para que un fraude se produzca se han de dar tres probables circunstancias:

1. El Equipo del usuario ha de estar infectado por este tipo de troyanos.
2. El espécimen que infecto la máquina del usuario ha de aclarar a la entidad bancaria con la que opera el usuario.
3. El usuario ha de iniciar sesión en su espacio de banca electrónica y rellenar los datos adicionales que se le soliciten.

Además, en la programación interior de todo malware, familia de troyanos, entre otros, existe el filtrado de los datos de los usuarios en cual se lleva a cabo mediante listas de entidades bancarias a monitorizar. Estas listas contienen cadenas de textos (Strings) que suelen ser:

- La propia URL del banco objeto de suplantación: http://www.Bitcorp.com
- Subcadenas de la URL del banco: *Bitcorp.com
- El título de la ventana de la página de banca en línea: Bitcorp – Vivaldi Browser.
- Cadenas particulares del cuerpo de la página de banca en línea: Bitcorp 2009. Todos los derechos reservados.
- Cadenas del código HTML de la página relacionadas con los formularios de ingreso de cuenta personal: <label for=" lg_username" class=" labuser_01" >

Para llegar a su propósito de "Robar Credenciales Bancarias" se usan:

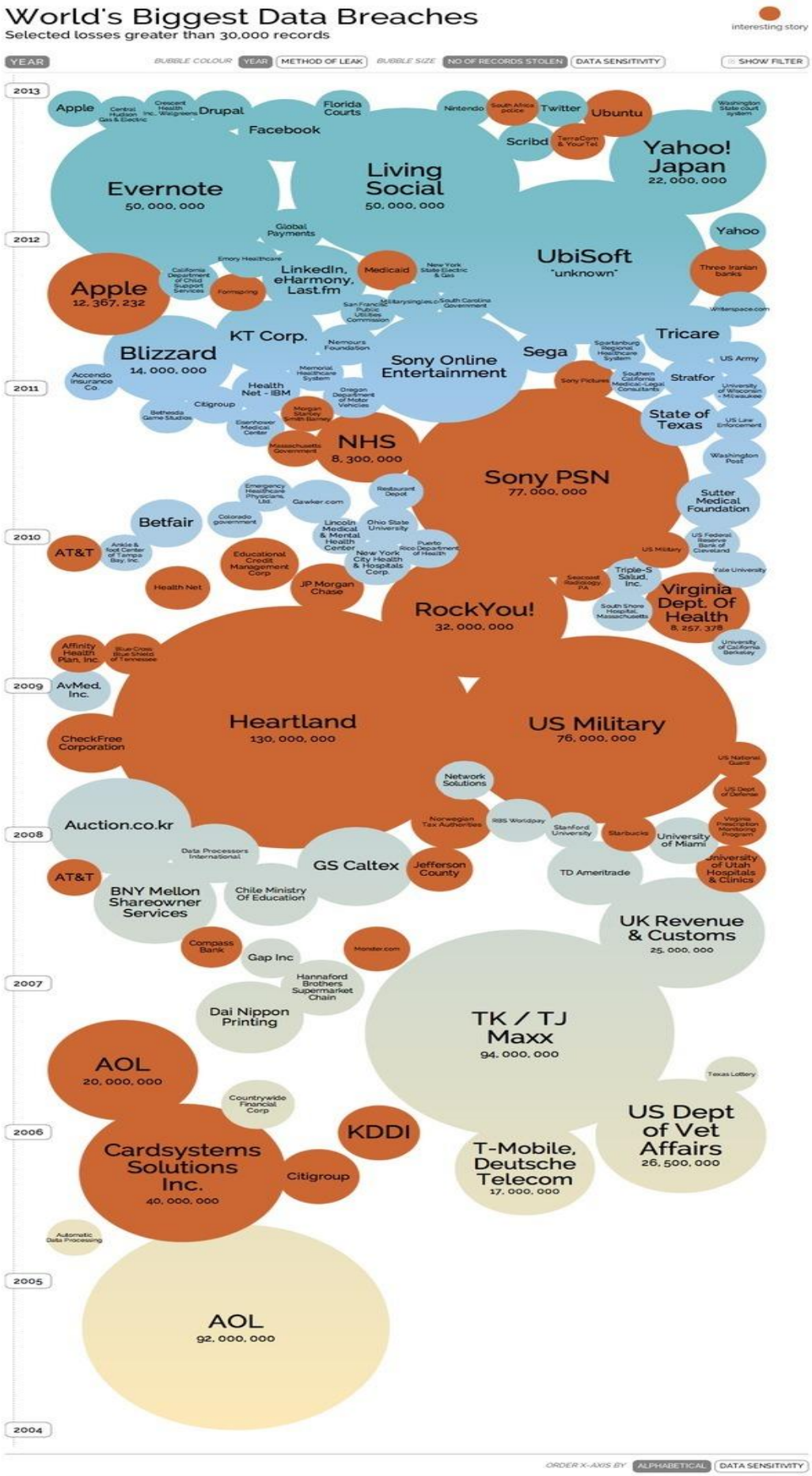
1. Registro de teclas pulsadas
2. Captura de formularios
3. Capturas de pantalla y grabación de video
4. Inyección de campos de formulario fraudulentos
5. Inyección de páginas fraudulentas

6. Redirección de páginas bancarias
7. Hombre en el medio (Man in The Middle)

INTECO “Instituto Nacional de Tecnologías de las Comunicaciones”, Cuaderno de Notas del Observatorio ¿Qué son y cómo funcionan los troyanos bancarios? (2015).

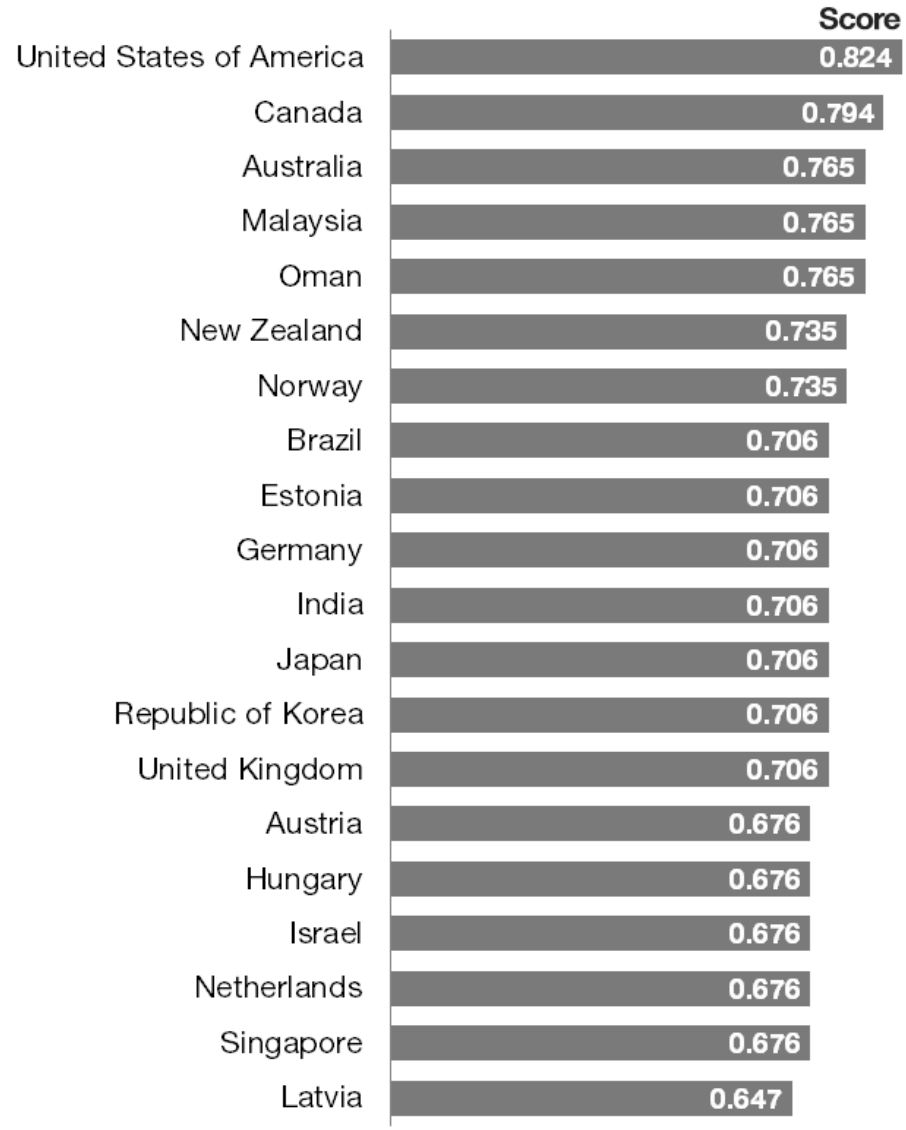
En el mundo moderno que hoy estamos viviendo tenemos una identidad digital que nos permite ser autenticados o reconocidos en Internet para acceder a Aplicaciones móviles, Aplicaciones industriales, Servidores Remotos, entre otros, además tenemos varias identidades digitales dependiendo si es para redes sociales, correos electrónicos, es un activo muy valioso y codiciado hoy en día por simple hecho que le da poder a las personas malintencionadas aparentemente para perpetrar sus propósitos malévolos, sin embargo, existe una luz dorada al final de todo, según un informe de Symantec. Se declaran más de 300 incidentes de robo de datos personales al año, pero sólo los operadores de telecomunicaciones están obligados a declararlos, y se estima que entre el 80% y el 90% no se declaran, por un asunto reputacional y de crear una imagen ficticia de son empresas poderosas e infalibles. En cada incidente se exponen una media de más de 1 millón de identidades, aunque la mediana se está reduciendo a unas 5,000, porque la mayoría de ataques son a pequeños comercios o empresas. También tenemos identidades de organizaciones que operan en internet que al ser robadas son muy lucrativas para los aparentes ciberdelincuentes por el ejemplo del coste medio de una brecha de datos es de unos 4 M USD, unos 150USD/registro robado, aunque en los ataques más voluminosos el coste se dispara, por el impacto que puede tener en la valoración de la empresa en bolsa. Por ejemplo, el robo de credenciales de usuarios de PlayStation de Sony en 2011, provocó pérdidas en la compañía superiores a las que le causó el Tsunami de ese mismo año en Japón, que le obligó a interrumpir la producción en 5 plantas. El robo de credenciales está relacionado con el acceso ilegal a Documentos

gubernamentales (declaraciones de beneficios o pago de impuestos) (aprox. 49%), fraudes de tarjetas de crédito (15%), fraude telefónico o de otros suministros (10%), Fraude bancario (6%), intento de robo de identidad (aprox. 3.7%), Fraude de Préstamos (3.5%), relacionado con empleo (aprox. 3,3%), Otros (aprox. 19%). Curiosamente, las estadísticas son una verificación de la tendencia de monetización (precio en el mercado negro) de estas credenciales. Otra operación de Anonymous que tocó a países hispanohablantes fue la #Oplcarus, orquestada para atacar los bancos de todo el planeta y nuestro Banco Central de la República Dominicana, junto a el Banco Central de las Maldivas, el Banco Nacional de Panamá y el Banco Central de México, entre otros. Informe VIU Ciberseguridad: Tendencias (2017).


World's Biggest Data Breaches
Selected losses greater than 30,000 records
interesting story
YEAR
BUBBLE COLOUR
YEAR
METHOD OF LEAK
BUBBLE SIZE
NO OF RECORDS STOLEN
DATA SENSITIVITY
SHOW FILTER
2013
Apple
Central Hudson Gas & Electric
Crescent Health Inc.
Walgreens
Drupal
Florida Courts
Facebook
Nintendo
South Africa police
Twitter
Ubuntu
Washington State court system
Scribd
TerraCom & YouTel
Yahoo! Japan
22, 000, 000
Evernote
50, 000, 000
Living Social
50, 000, 000
2012
Global Payments
Yahoo
Emory Healthcare
California Department of Child Support Services
LinkedIn, eHarmony, Last.fm
Medicaid
New York State Electric & Gas
UbiSoft
"unknown"
Three Iranian banks
Apple
12, 367, 232
Formspring
San Francisco Public Utilities Commission
Militarysingles.com
South Carolina Government
Winterspace.com
KT Corp.
Nemours Foundation
Tricare
Blizzard
14, 000, 000
Sony Online Entertainment
Sega
Spartanburg Regional Healthcare System
US Army
Accendo Insurance Co.
Memorial Healthcare System
Health Net - IBM
Oregon Department of Motor Vehicles
Sony Pictures
Southern California Medical-Legal Consultants
Stratfor
University of Wisconsin - Milwaukee
2011
Citigroup
Morgan Stanley Smith Barney
Bethesda Game Studios
Eisenhower Medical Center
State of Texas
US Law Enforcement
NHS
8, 300, 000
Massachusetts Government
Washington Post
Sony PSN
77, 000, 000
Emergency Healthcare Physicians, Ltd.
Gawker.com
Restaurant Depot
Sutter Medical Foundation
Betfair
Colorado government
Lincoln Medical & Mental Health Center
Ohio State University
2010
AT&T
Ankle & foot Center of Tampa Bay, Inc.
Educational Credit Management Corp
Puerto Rico Department of Health
New York City Health & Hospitals Corp.
US Military
US Federal Reserve Bank of Cleveland
Yale University
Triple-S Salud, Inc.
Health Net
JP Morgan Chase
Seacoast Radiology, PA
Virginia Dept. Of Health
8, 257, 378
RockYou!
32, 000, 000
South Shore Hospital, Massachusetts
Affinity Health Plan, Inc
BlueCross BlueShield of Tennessee
University of California Berkeley
2009
AvMed, Inc.
Heartland
130, 000, 000
US Military
76, 000, 000
CheckFree Corporation
US National Guard
Network Solutions
US Dept of Defense
Auction.co.kr
Norwegian Tax Authorities
RBS Worldpay
Stanford University
Starbucks
University of Miami
Virginia Prescription Monitoring Program
2008
Data Processors International
GS Caltex
Jefferson County
TD Ameritrade
University of Utah Hospitals & Clinics
AT&T
BNY Mellon Shareowner Services
Chile Ministry Of Education
UK Revenue & Customs
25, 000, 000
Compass Bank
Gap Inc
Monster.com
2007
Hannaford Brothers Supermarket Chain
Dai Nippon Printing
TK / TJ Maxx
94, 000, 000
AOL
20, 000, 000
Texas Lottery
Countrywide Financial Corp
US Dept of Vet Affairs
26, 500, 000
2006
KDDI
Cardsystems Solutions Inc.
40, 000, 000
Citigroup
T-Mobile, Deutsche Telecom
17, 000, 000
Automatic Data Processing
2005
AOL
92, 000, 000
2004
ORDER X-AXIS BY
ALPHABETICAL
DATA SENSITIVITY

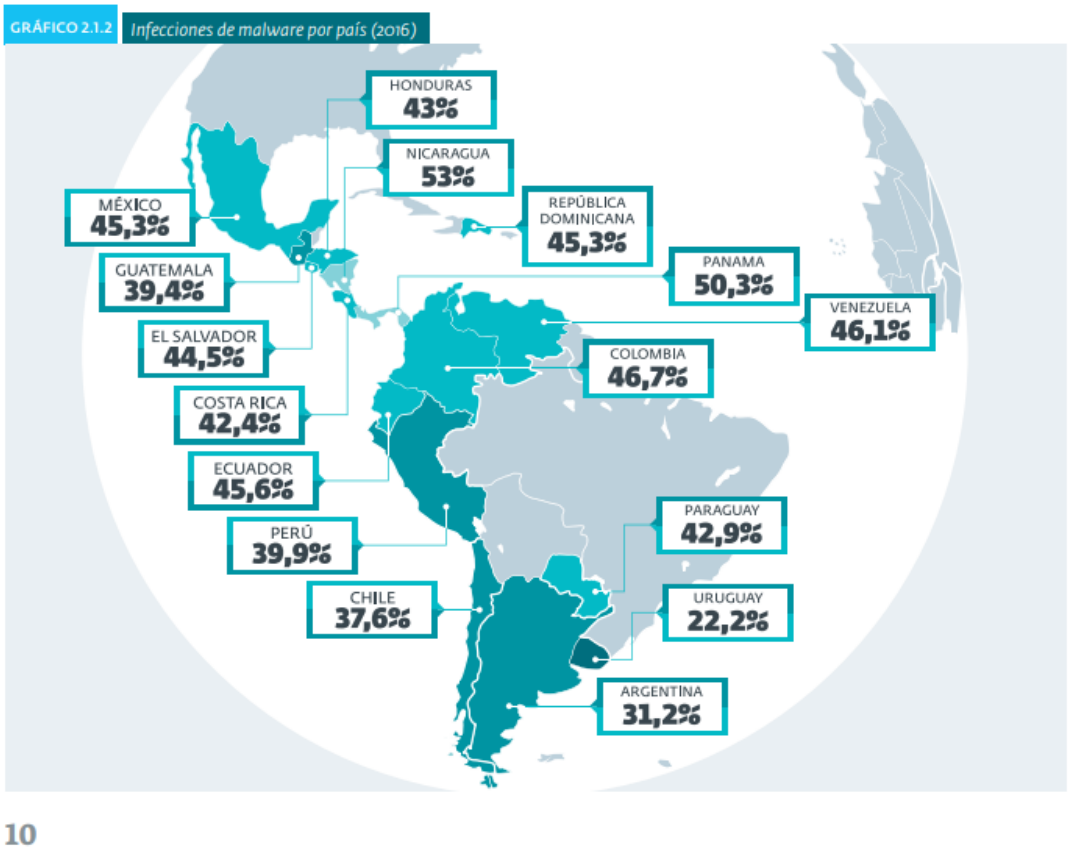
Countries best prepared against cyberattacks

WORLD ECONOMIC FORUM
COMMITTED TO IMPROVING THE STATE OF THE WORLD



Source: ABI Research, ITU, Global Cybersecurity Index

Situacion a Nivel Regional:



Hoy en día a pesar de estar cubiertos de buena ciberseguridad, existe una situación clásica a nivel mundial que los posibles ciberdelincuentes utilizan para robar credenciales bancarias y es el empleo de troyanos y al usar en combinación de virus informáticos, sin embargo, hay una necesidad latente de mejorar la ciberseguridad de las organizaciones tomando en cuenta la labor de crear niveles de conciencia óptimos para los gobernantes y otras comunidades que puedan adquirir información valiosísima para lograr mejores familias y empresas, la ciberseguridad es un tema más que importante para la humanidad, dará mucho de qué hablar a lo largo y ancho de todo el globo terráqueo. ESET Security Report Latinoamérica (2017).

Si los lectores han de llevarse un sólo mensaje de este Informe 2016 del Observatorio de la Ciberseguridad en América Latina y el Caribe, es que una enorme mayoría de nuestros países aún están poco preparados para contrarrestar la amenaza del

cibercrimen. Su análisis es un llamado a la acción para empezar a hacer todo lo necesario por proteger esta infraestructura clave para el siglo XXI. Hay mucho en juego, el cibercrimen le cuesta al mundo hasta US$575.000 millones al año, lo que representa 0,5% del PIB global. Eso es casi cuatro veces más que el monto anual de las donaciones para el desarrollo internacional. En América Latina y el Caribe, este tipo de delitos nos cuestan alrededor de US$90.000 millones al año. Con esos recursos podríamos cuadruplicar el número de investigadores científicos en nuestra región. Las ventajas de la conectividad son innegables, y los latinoamericanos y caribeños adoptan estas nuevas tecnologías con entusiasmo. Hoy somos el cuarto mayor mercado móvil del mundo, la mitad de nuestra población usa el Internet y nuestros gobiernos emplean cada vez más medios digitales para comunicarse y brindar servicios a los ciudadanos.

Pero en donde nos quedamos cortos es en prevenir y mitigar los riesgos de la actividad delictiva o maliciosa en el ciberespacio. Un análisis de sus 49 indicadores demuestra que muchos países de la región son vulnerables a ataques cibernéticos potencialmente devastadores. La gran mayoría de las fiscalías carece de capacidad para perseguir los delitos cibernéticos.

Si vamos a sacarle la mayor ventaja posible a la llamada cuarta revolución industrial, tenemos que crear una infraestructura digital no sólo moderna y robusta sino también segura. Proteger a nuestros ciudadanos del cibercrimen no es una mera opción: es un elemento clave para nuestro desarrollo.

Como tantos de los desafíos que enfrentamos en pos de ese desarrollo, este es un reto que excede la capacidad de cualquier institución. Nuestros esfuerzos individuales se potencian cuando trabajamos con aliados que comparten nuestros objetivos y valores. Este informe se benefició de ese tipo de colaboración gracias a los aportes de la Organización de los Estados Americanos, la Universidad de Oxford, el Center for

Strategic International Studies, la Fundación Getúlio Vargas, la organización FIRST, el Consejo de Europa, Potomac Institute y el Foro Económico Mundial. Espero que esta evaluación rigurosa y sistemática, con sus útiles indicadores, sirva de guía y aliciente a los responsables de la ciberseguridad de nuestra región para avanzar rápidamente en el camino correcto. Quienes son engañados y luego supuestamente aliados con el cibercrimen no nos darán tregua, sin embargo, el mal siempre anhela el bien, es decir estar en la luz, ha sido así desde un principio, para aquellos que deciden seguir haciendo el mal aun sabiendo que tienen que hacer el bien, Dios se encargara de hacer justicia porque Dios ama aquellos que se entregan por Amor a él.

Un número de entidades trabajan conjuntamente para abordar las cuestiones de seguridad cibernética en virtud de la Comisión Interinstitucional contra Crímenes y Delitos de Alta Tecnología (CICDAT). Con la aprobación de la Ley 53-07 y la Ley 310-13, así como la adhesión al Convenio sobre Delincuencia Cibernética (Convenio de Budapest), la República Dominicana ha desarrollado un marco legislativo global para la penalización de la delincuencia cibernética y el manejo de evidencia electrónica, la regulación de correo SPAM y el establecimiento de cooperación internacional. Por otra parte, los tribunales tienen la formación y capacidad suficientes para procesar los casos de evidencia electrónica. Sin embargo, solo existe una legislación parcial en lo que respecta a la privacidad en Internet y la libertad de expresión. El Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (DICAT) de la Policía Nacional y la División de Investigaciones de Delitos Informáticos (DIDI) del Departamento Nacional de Investigaciones (DNI) son las dos principales entidades de investigación de crímenes cibernéticos en el país. el DICAT también maneja la respuesta a incidentes cibernéticos y coordina regularmente con INTERPOL y los

CSIRT de otros países. Por último, el gobierno está mejorando la colaboración con el sector privado al divulgar infracciones cibernéticas y proporcionar informes de vulnerabilidad. Dada la creciente cantidad de usuarios de Internet y disponibilidad de servicios de comercio electrónico, la República Dominicana se enfrenta cada vez más a amenazas cibernéticas. El gobierno y sus conformantes también están trabajando para crear programas pertinentes, dadas las limitadas oportunidades para educación y formación en seguridad cibernética del país. En el caso de nuestro país vecino Haití, Aunque se encuentran con recursos limitados y ha habido algunos reveses en los últimos años, las entidades del Gobierno de Haití continúan trabajando hacia la elaboración de una estrategia nacional de seguridad cibernética. Un grupo de trabajo conformado por la unidad de gobierno electrónico del Gabinete del Primer Ministro (PRIMATURE), el Consejo Nacional de Telecomunicaciones (CONATEL), la Policía Nacional y la Secretaría para la Seguridad Nacional se ha reunido para establecer el marco para una estrategia nacional y han recibido asistencia de la OEA, la Unión Internacional de Telecomunicaciones y otros socios internacionales. Recientemente se estableció un grupo de trabajo dentro del CONATEL con el mandato de elaborar un plan estratégico y un plan de trabajo para la seguridad cibernética y la lucha contra el delito cibernético. Si bien el conocimiento sobre la seguridad cibernética en el gobierno es cada vez mayor, la preparación varía según las agencias. Esto es notorio en la falta de aplicación uniforme de las normas de seguridad a través de las infraestructuras de TI. Sin embargo, la principal preocupación del CONATEL ha sido la necesidad de tener una capacidad de respuesta a incidentes cibernéticos y se ha coordinado con el sector privado para abogar por la creación de un CSIRT de calidad. Como parte del Proyecto HIPCAR de la Unión de Telecomunicaciones del Caribe (CTU) y la Comunidad del Caribe (CARICOM), las partes interesadas haitianas han propuesto legislación sobre la

delincuencia cibernética y leyes de privacidad de Internet que se encuentran actualmente en la fase de consulta. Sin embargo, las gestiones legislativas se han estancado dado el desacuerdo sobre las elecciones que llevó a la disolución de la mayoría del Parlamento de Haití en enero de 2015. Hasta que se resuelva esta crisis política, será muy difícil que el país adopte un marco jurídico integral para la delincuencia cibernética. No obstante, la Dirección Central de la Policía Judicial (DCPJ) ha tenido un éxito considerable en la investigación y detención de la delincuencia cibernética por medio de la captura de 69 delincuentes en 2014, de los cuales 11 fueron declarados culpables de delitos relacionados con la cibernética. Con una tasa de penetración de Internet del 11%, la conciencia de seguridad cibernética en la Sociedad haitiana es predominantemente baja Para solucionar esto, el CONATEL ha llevado a cabo una serie de eventos para brindar conocimientos a las partes interesadas y al público en general sobre la seguridad cibernética. Así mismo algunas universidades ofrecen cursos relacionados con la seguridad cibernética, pero actualmente no hay programas de grado formales. Áreas del sector privado, como los bancos y los operadores de telecomunicaciones, están bien informados de la importancia de la seguridad cibernética y han invertido en oportunidades de formación para los empleados. Mientras que los servicios de gobierno electrónico están empezando a llegar al país recientemente, los servicios de comercio electrónico están ampliamente disponibles y por lo general son confiables y seguros.

El Consejo Nacional de Política Económica y Social del Gobierno de Colombia estableció la política nacional de seguridad cibernética CONPES 3701 bajo el auspicio del Ministerio de Tecnologías de la Información y las Comunicaciones (mintic), el Ministerio de Defensa, el Departamento Nacional de Planeación y otras instituciones

nacionales clave. Además, en 2014 una Misión de Asistencia Técnica de la OEA al país ayudó a construir la capacidad de las partes interesadas de desarrollar marcos y políticas institucionales. Si bien está muy extendida la conciencia sobre el CONPES 3701, no se han definido claramente mandatos específicos. El Grupo de Respuesta de Emergencias Cibernéticas de Colombia (colcert) es una institución clave en defensa y seguridad cibernética y se muestra competente para la coordinación con otros organismos y el sector privado. El programa CERT de Colombia funciona principalmente como un mecanismo de respuesta a incidentes cibernéticos específicos de la organización, y los programas de gestión del riesgo han comenzado a surtir efecto.

Últimamente, el Ministro de TIC de Colombia ha informado que una nueva estrategia de seguridad cibernética y defensa cibernética estará lista para finales de 2015 o inicios de 2016. Colombia ha aprobado una legislación procesal penal integral y de efectiva penalización (Ley 1273 y Ley 906) para abordar los delitos cibernéticos y reconoce los tratados internacionales con Interpol y Europol. Las fuerzas del orden y el Poder Judicial tienen la capacidad de investigar y manejar casos de delincuencia cibernética, pero carecen de la formación y capacidad para lograr los mismos resultados en los tribunales. Asimismo, si bien la Ley 1581 establece un marco básico para la protección de datos y divulgación y denuncia de las violaciones de seguridad, a menudo los casos de los sectores público y privado no se informan. La conciencia social sobre la importancia de la privacidad y la seguridad en Internet y la confianza en los sistemas digitales del país ha crecido notablemente, en parte debido a las campañas nacionales, como en la campaña “en TIC Confío” del mintic. Colombia cuenta con más de 2.000 oportunidades de comercio electrónico y servicios de gobierno electrónico que se realizan en su mayoría en un entorno seguro. Aun así, la mayoría de ciudadanos y

empleados privados cuentan con por lo menos un nivel mínimo de infraestructura de privacidad y hay leyes en vigor que obligan a las empresas a implementar políticas de protección de datos en el lugar de trabajo como la Ley 1581 de 2012 y el Decreto 1377 de 2013. El desarrollo de educación de seguridad cibernética nacional ha experimentado un crecimiento notable y los foros público-privados y centros de excelencia financiados por el gobierno han comenzado a gestarse en el país. Numerosas universidades, organismos policiales y de defensa y las empresas privadas ofrecen cursos y capacitaciones, incluyendo maestrías y programas de acreditación OEA "¿Estamos preparados en América Latina y el Caribe?" Ciberseguridad (2016).

Situación a Nivel Local:

A miles de personas en cualquier parte del mundo les han robado su identidad. Simplemente, alguien que ha robado su información personal a través de su correo electrónico, tarjeta de crédito, de su seguro médico, de su estado de cuenta bancaria u otras cuentas, para utilizarla en su provecho personal, se llama robo de identidad. Esa práctica del robo de identidad, le puede afectar sus finanzas, su reputación, su historial financiero, o poner en duda su moral, sus valores y la ética con que una persona ha funcionado en sus negocios y en su vida. Es angustiante recibir la noticia de que en otro país alguien ha consumido su dinero, o ha usado su tarjeta de crédito sin usted viajar, y tener que estresarse en un banco queriendo demostrar que usted no ha viajado, no realizó ninguna transferencia; ante todo, le piden tiempo, paciencia, ¿Cómo se roba la identidad? Los ladrones de identidad usan todo tipo de recursos para dar con su información financiera, ejemplo: buscar en los basureros frente a su casa para obtener facturas, documentos o informes sobre sus estados de cuentas o tarjetas; otros le llaman a su casa

> pidiendo informaciones, simulando una oficina, banco, instituciones del gobierno, empresas o seguros médicos, para luego engañarlo y robarle su identidad. La otra modalidad es a través del robo de carteras, bolso, mochila, para apoderarse de sus tarjetas de crédito, seguros médicos, cédula de identidad; pero en este país, es decir nuestra República Dominicana hasta de los cementerios roban la identidad de los muertos para obtener beneficios. Sin importar la vía que usen, los delincuentes cibernéticos, saben cómo robar la identidad, transferir dinero, o usar los ahorros y tarjetas, sin piedad y sin resaca moral, dañando la vida o poniendo en riesgo a las personas.

En el mundo globalizado, tecnológico, donde se usa el dinero plástico, y las informaciones personales están en las redes sociales; o peor aún, donde tantas personas son ingenuos, poco precavidos o desconocen sobre estos temas, se convierten en las víctimas o presas fáciles del delincuente que roba identidad. La pregunta sería ¿Cómo evitar o prevenir el robo de identidad? Y la contesta es la siguiente: No responda llamadas, correo electrónico o no de información por teléfono en las que le pidan informaciones personales sobre sus negocios, finanzas o cuentas bancarias, Cuando pague un estado de cuenta de su tarjeta o préstamo, o informaciones sobre sus finanzas no la tire a la basura sin romperla y asegurarse que nadie puede obtenerla para leerla; no responda correo electrónico desconocido donde le pidan informaciones personales o de su familia; elimine todo correo que no tiene fuente segura de sus contactos personales, nunca informe en las redes sociales todos sus movimientos, dónde compra, almuerza, viajes, o realice sus operaciones de negocios. Los ladrones de identidad saben buscar en cualquier lugar y viven acechando sus víctimas.

¿Qué siente la persona que le roban la identidad? Entra en estado de angustia, ansiedad, nerviosismo, intranquilidad, dificultad para dormir, impotencia, desesperación, depresión, miedo e inseguridad. Pero también puede tener síntomas de paranoia, hasta presentar ataques de ansiedad o estrés postraumático. Cada situación estresante por el robo de identidad le cambia la vida a una persona. Una gran pena es tener que vivir la dura realidad que nadie como persona o institución está cien por ciento seguro o blindado para evitar el robo de identidad. Sin embargo, se puede prevenir, o si le sucede puede dirigirse a su banco, la policía, poner en alerta a la familia o negocios. Hoy estamos expuestos a todo, desde la grabación de las llamadas telefónicas, hasta el acceso que pueden tener otras personas de tu perfil personal y financiero. Hay que tomar el control y timón de nuestras vidas, previniendo y aprendiendo a cuidar nuestra identidad y las informaciones que pueden usar sin su permiso. Por su salud mental y financiera prevenga el robo de identidad Gómez, José Miguel "Robo de Identidad y Sus Consecuencias" (2017).

Entre enero y marzo de 2018 los usuarios de los servicios financieros realizaron 150,009 reclamaciones, según los datos disponibles en la Superintendencia de Bancos (SIB). Los principales motivos fueron no reconocimiento de cargos aplicados, no los tenían estipulados o autorizados. Por esto se hicieron 36,159 reclamaciones y estas representaron el 24.10% del total. La siguiente causa más frecuente de los reclamos es que el cajero no dispensa el efectivo solicitado, por lo que se hicieron 30,361 para representar un 20.24%. También se realizaron 12,589 reclamaciones por transferencia no aplicada, las cuales representaron el 8.39%. Otros motivos son error en el cobro de intereses, consumo duplicado, no reconocimiento del consumo en la tarjeta de crédito, prestamos informales, falta de regulación en lugares no oficiales, errores detectados en

el estado de cuenta, cobro de penalidad no estipulada y transacción fraudulenta; También por débitos automáticos por pago de facturas, bloqueo de cuentas sin justificación, además se hicieron 28 reclamos porque el cajero dispensó dinero falso, entre otras más. Las reclamaciones abarcan los bancos múltiples, las asociaciones de ahorros y préstamos, los bancos de ahorro y crédito, las corporaciones de crédito y las entidades públicas de intermediación financiera Tejeda, Lilian Listín Diario "En tres meses usuarios del sistema financiero realizan más de 150,000 reclamaciones" (2018).

Muchos usuarios del sistema financiero desconocen cuáles son sus derechos al adquirir determinado producto o servicio y pasan por alto ciertas irregularidades porque desconocen cómo pueden hacer sus quejas o reclamaciones y los motivos por los que pueden hacerlas. La Superintendencia de Bancos (SIB) les concede a los usuarios la facultad de reclamar siempre que sus derechos no sean respetados, y establece que usted puede hacer sus denuncias de manera gratuita (dependiendo del caso) y obtener respuesta en los plazos establecidos, así como la corrección inmediata de la situación que originó la reclamación. Hay personas que sí están al tanto de esto y realizan sus denuncias. Algunos obtienen respuestas favorables, otros no. Pero lo importante es que muchos recuperaron su dinero porque no perdieron la oportunidad de reclamar.

Muestra de ello es que en el 2017 la SIB atendió 812 reclamaciones de los usuarios de los productos y servicios financieros, de las cuales 354 (43.6%) recibieron respuestas favorables, lo que significó la devolución de RD$5.54 millones y USD$31,307.19

La entidad destaca que el tiempo de respuesta se redujo en 5 días con relación al 2016, al registrar un promedio de 23 días calendario por caso, cuando el plazo reglamentario

es de 60 días calendario. Las reclamaciones fueron respondidas 37 días antes de lo establecido, para una reducción de un 60% del plazo, establece la entidad en su informe.

Motivos de las reclamaciones: Los principales motivos de las reclamaciones son regularmente que el cajero no dispensa el efectivo solicitado, por lo que entre enero y marzo se realizaron 30,361 reclamaciones, y no reconocimiento de cargos aplicados, por lo que se hicieron 36,159. Otras razones son error en el cobro de intereses, consumo duplicado, que el usuario no reconoce el consumo en la tarjeta de crédito, cobro de penalidad no estipulada, débitos de cuentas no autorizados, cobro erróneo del impuesto de 0.15%, que se aplica a los cheques y a los pagos realizados a través de transferencias electrónicas, entre otros. Es por esto que usted debe estar pendiente de todos los cargos, descuentos y movimientos de las cuentas que posea en bancos múltiples, asociaciones de ahorros y préstamos, bancos de ahorro y crédito, corporaciones de crédito o entidades públicas de intermediación financiera Tejeda, Lilian Listín Diario "¿Cuáles son las quejas más comunes de los usuarios en el sistema financiero?" (2018).

El Daño Vital

En la economía digital que crece sin cesar, los ejecutivos responsables de la infraestructura de tecnología de la información (TI) de las organizaciones se esfuerzan por encontrar ventajas de mercado. Su rol ya no se circunscribe a la tecnología: hoy, los líderes de TI están posicionados para convertirse en proveedores de servicios hábiles para sus organizaciones. Para ello, deben innovar rápidamente, ofrecer experiencias únicas al cliente, y maximizar sus conocimientos de los clientes y el mercado. Ahora, las infraestructuras de TI deben conectarse con socios en el ecosistema, mejorar los servicios de transacciones y analítica, y construir capacidad lo cual exige para abordar condiciones de negocio muy dinámicas. El éxito también depende de que la

organización replantee su mentalidad en el área de TI, lo cual incluye reflexionar sobre cuál sería la mejor manera de anunciar la tecnología, cómo aprovechar fuentes de innovación y cómo prepararse para lidiar con un futuro incierto. La llegada de la revolución digital cambió la naturaleza de la conversación de TI: de ser meramente técnica pasó a ser estratégica. Los clientes reclaman mayor personalización, y las empresas enfrentan nuevos competidores de industrias advenedizas, así como una presión sin precedentes para innovar. Ahora, la conversación sobre la infraestructura de TI cubre mucho más que "reducir costos y mantener las luces prendidas": también implica convertirse en un proveedor de servicios confiable para la organización. Las capacidades de negocio emergentes –como la creación de experiencias diferenciadoras para los clientes, la incorporación de conocimientos de los clientes en nuevos productos y servicios, y la habilitación de una ágil experimentación– están transformando las decisiones de infraestructura del back-office a un componente clave de la estrategia de negocios de una organización. Y con estas nuevas capacidades viene un conjunto nuevo de elecciones estratégicas sobre iniciativas de hardware, software e interconexión necesarias para impulsar esta transformación digital. Las investigaciones previas del IBM Institute for Business Value (IBV) destacan que siete de cada diez organizaciones reconocen que la infraestructura de TI desempeña un papel significativo para impulsar los resultados de negocio. Además, más del 60% de los encuestados se proponen aumentar su inversión en infraestructura tecnológica en los próximos 12 a 18 meses. Al mismo tiempo, menos del 10% de las firmas dijo estar plenamente preparada para satisfacer las demandas del negocio digital para dar soporte a tecnología de nube, analítica, móvil y social. Las organizaciones se enfrentan a una serie de fuerzas que las Impulsan a formas de participación más basadas sobre lo digital. Además de las implicancias tecnológicas para la infraestructura de TI, descubrimos que se ha

producido un cambio fundamental en la mentalidad. ¿Qué capacidades centrales necesitan estas organizaciones para promover la transformación digital? ¿Qué cambios de mentalidad se necesitan para liderar a una organización de TI en tiempos turbulentos? “IBM Whitepaper” - Nueva Tecnología, Nueva Mentalidad, (2016).

Medidas básicas

Para prevenir los ciberataques las organizaciones deben contar con:

- Equipo de TI capacitado y una infraestructura adecuada que permita enfrentar los riesgos cibernéticos.
- Compromiso de alta gerencia y juntas directivas.
- Políticas para guiar a los colaboradores para compartir los ciberataques.
- Información actualizada sobre las amenazas cibernéticas y sus posibles repercusiones en la organización.
- Recursos suficientes para implementar planes de gestión de amenazas de riesgo.
- Monitoreo de legislación actual y potencial sobre Ciberseguridad y regulación.

Ramírez, Alonso “Un paso adelante en la era de las amenazas cibernéticas” (2016).

Hipótesis y variables de estudio.

1. El Robo de Credenciales Bancarias.
2. El Crimen Globalizado en América Latina.
3. La Adopción a la Era del Cibermundo.
4. La Preocupación de los Profesionales del Área.
5. El Futuro de la Gobernabilidad de la Ciberseguridad.
6. Predicciones de Ciberseguridad para la Globalización.
7. La Salud de Internet.

Variables: Independiente, dependiente.

Variable Independiente: Estabilidad del Sistema Nacional Financiero

Variable Dependiente: Impacto.

Operativización de variables + Indicadores.

Variable + Impacto.

Indicadores +

- Integridad de los Datos: La Integración de Grandes Cantidades de Datos es tan importante para mantener todo en orden.
- Disponibilidad: En toda organización incluyendo los Bancos necesitan tener los Datos disponibles en todos los puntos de acceso para desempeñar un mejor trabajo y cantidad de atención.
- Accesibilidad: El Manejo de la accesibilidad a los Datos de una organización va a garantizar la trascendencia de nuestros clientes.
- Ciberespionaje: Gran variedad de Crimeware Kits para extraer credenciales bancarias en instantes.

Variable + Estabilidad de los Sistemas de Información.

Indicadores +

- Pruebas de Malware: Diferentes Pruebas de Malware en Acción con el Pwnie Express Phone, Teléfono Inteligente para Pruebas de Malware con comportamiento en la Red Corporativa.
- Pruebas de Penetración: Diferentes Pruebas de Penetración con el Pwnie Express Phone, Teléfono Inteligente para Pruebas de Penetración a Redes, Servidores y Dispositivos.

- Pérdida de Información: Infografía sobre la Perdida de Datos en las organizaciones de acuerdo a Intel Security and Mcafee.
- Secuestro de Información: Publicación Científica sobre el Ransomware en las Entidades Bancarias o Secuestro de Información Sensitiva o Confidencial para la Operación del Sistema Financiero Nacional.
- Ciberseguridad de la Información: La Importancia de la Seguridad Cibernética en la Organización y los Dispositivos donde llevamos Datos Sensibles.
- Ciberseguridad de la Base de Datos: Virus como Stuxnet pueden corromper cualquier Base de Datos, lo que hace necesario Pelear con los Virus y Defender la Red.
- Ciberseguridad de los Dispositivos: Diferentes tipos de ataques basados en Ingeniería Social, Spam y la Preocupación del comportamiento de los Usuarios en la Red de Redes.

Interpretación Variables e Indicadores:

1. En toda organización conformada por personas y tecnologías se hace necesario mantener el Big Data en Gestionar que los datos estén intactos para su uso en hospitales, escuelas, Bancos, Empresas, Así prevenir, mitigar y tratar de anticipar el robo de credenciales bancarias, entre otros.
2. Si los datos no están disponibles dentro o desde fuera la empresa u organización se vuelve imposible acceder a la Información que se busca.
3. Tanto la Integridad de los Datos, la Disponibilidad de los mismos y por último la accesibilidad es la espina dorsal de las tomas de decisiones, tenemos que tener acceso a la información para tratar de mejorar a las personas y conectar con sus necesidades, el acceso es Poder, La conexión es Poder. Ubisoft “Watch Dogs Videogame” (2012).

4. El Ex Director de Google Eric Schmidt desde el 2001 hasta 2011 dijo: “La Naturaleza del Internet es el Espionaje” la recolección a gran escala es más que necesaria para poder brindar mejores servicios tecnológicos.

5. El Pwnie Express Phone es un dispositivo real para Espionaje y pruebas de Malware a equipos conectados a internet, Pwnie Express Phone se hizo llamativo en la Serie de USA Network Mr. Robot (2015).

6. Cuando visualizamos los altos precios de las tecnologías de Ciberseguridad nos damos cuenta que es necesario un cambio radical con respecto a cómo funcionamos como organización.

7. Si algo necesitamos saber es que cada país tiene un gran reto con respecto a la adopción segura hacia el Cibermundo, Por ejemplo, en Singapur se protegen dando un enfoque o prioridad a los datos y no a los Dispositivos.

Capitulo III: Metodología.

a. Nivel de Investigación.

Trabajo de Investigación: Caso de Estudio

b. Diseño de Investigación.

Método de lo General a lo Particular

1. Planteamiento del Problema.
2. Creación de Hipótesis.
3. Testimonios.
4. Cuestionarios.
5. Respuestas Anónimas.

c. Población y Muestra.

Población: 1,000 Empleados

Muestra: 16

d. Técnicas e Instrumentos de Recolección de Datos.

1. Informes Oficiales.
2. Infografías.
3. Cuestionarios.
4. Artículos de Periódicos y Revistas.
5. Videos, Cortometrajes, Documentales, Películas.
6. Papeles Científicos.

e. Técnicas de Procesamiento y Análisis de Datos.

Google Forms – Crea y Analiza Encuestas de Forma Gratuita.

https://docs.google.com/forms/d/e/1FAIpQLSf1v0xVOeKT17FzhQiCxthRK-9U7pzN1NVE54gyGndbESoukA/viewform?vc=0&c=0&w=1

Capitulo IV: Aspectos Administrativos.

+Recursos

Humanos: Sistema Financiero Nacional de la República Dominicana

Materiales:

1. Computadora de Escritorio Optiplex.
2. Computadora Portátil Lenovo Ideapad 110.
3. Memoria USB de 32 GB.
4. Disco Duro Portátil de 1TB.

5. Conexión 4G LTE Wind Telecom 3 Mbps.
6. Impresora Epson L220.
7. Hojas.
8. Pixeles.
9. Colores.
10. Folders.
11. Cuadernos.
12. Mochilas.
13. Maletines.
14. Libros de Ciberseguridad.
15. Amor a Dios y la Familia.

Financieros:

Presupuesto Personal de RD$12,100.00

Cronograma de Actividades: Diagrama de Gantt.

1. Presentación Profesional del Maestrante, Entrega de Certificación Como Estudiante Activo de INTEC y Solicitud de Aprobación de Caso de Estudio: Aug 21, 2018, 11:24 PM.
2. Solicita la Respuesta de 3 Preguntas:

Aug 22, 2018, 9:02 AM.

3. Solicitud de Asesoría A Miguel María Árias Romero: Aug 22, 2018, 11:53 PM.
4. Excelentes Recomendaciones de Miguel María Árias Romero:

Sep. 09, 2018, 9:06 PM.

5. Cuestionarios y Declaraciones sobre Ciberseguridad a Nivel Global, Regional Latinoamérica y Nacional de la República Dominicana:

Sep. 09, 2018, 9:20 PM.

6. Ultima Corrección del Trabajo Final de parte Ing. Miguel María Arias Romero

Nov. 28, 2018, 11:20 PM.

Capitulo IV: Análisis, Síntesis y Desarrollo de la Investigación.

Como resultado final la única solución a esta problemática de identificar, analizar y cómo prevenir el **robo de credenciales bancarias** es ir al problema antes que el problema llegue a las empresas. Mi Investigación fue basada en la creación de una encuesta digital **"Ciberseguridad Siglo XXI 2"** la cual fue anónima y dirigida a las principales personas que trabajan en el área financiera; ya que el Banco Central de la República Dominicana y la Superintendencia de Bancos (SIB) han colaborado en profundidad en dicho tema. En esta encuesta tenemos un total de 5 preguntas y añadimos las principales respuestas más destacadas con sus respectivos análisis.

Capítulo V: Conclusiones y Recomendaciones.

Los delitos cibernéticos se han convertido en el pan de cada día para muchas organizaciones. Aunque algunos son imperceptibles otros estallan en diferentes direcciones afectándolas considerablemente al no contar con una infraestructura de gestión de riesgos que les permitan enfrentar acertadamente esas amenazas. Al tratarse de un fenómeno relativamente nuevo y en constante evolución, los hackers hacen de las suyas en las redes para manipular la información ante las debilidades que presentan las empresas en sus plataformas tecnológicas. Para derrotar a los cibercriminales es que se hace necesario la aplicación de un marco de gestión de riesgo inteligente en las empresas.

Bajo ese panorama, cada nivel de la organización asume las responsabilidades específicas de gestión de riesgos aplicando una madurez tecnológica en torno a la gestión de riesgo de amenaza cibernética.

Para ello es que se hace necesario aplicar un uso efectivo de la tecnología para apoyar la ejecución del proceso. La automatización puede hacer que los procesos sean más eficaces y eficientes.

Además, las plataformas tecnológicas se utilizan para disuadir, detectar y defenderse contra las amenazas informáticas propias que abarcan desde aplicaciones de protección, contraseñas para el seguimiento automatizado de datos, la minería y técnicas analíticas.

Existen grandes potenciales para lograr una excelente ciberseguridad en nuestra amada República Dominicana, por lo tanto, para lograr estas cuestiones debemos muy enfáticamente desarrollar el personal humano para que actué de forma dinámica por sí mismo, refiriéndome muy imperativamente a la capacidad que debe impregnarse en el usuario y empleado de nuestras organizaciones, sin embargo, la única solución para obtener una situación clara y óptima de nuestro estado actual de debilidad en materia de ciberseguridad, es que por disciplina la ciberseguridad es más educación cibernética que emplear tecnología de punta, tenemos que entender que el enfoque es obligatorio que vaya dirigido a enseñar profundamente a los usuarios y empleados como prevenirse un robo de credenciales bancarias, es totalmente ineficiente que solo se hagan esfuerzos mínimos solo creando una humanidad solo enfocada en los jóvenes, hace mucha falta que se enseñe primero a padres y luego a los jóvenes la gran importancia de prevenir incidentes dañinos sobre todo lo básico de la ciberseguridad como son la confidencialidad, integridad, disponibilidad asuntos muy delicados y que nuestro país

cumple de forma muy ambivalente, por asuntos de pura corrupción, pobreza mental y pobreza económica, no hace falta tener muchas certificaciones ni tampoco estar excesivamente preparado o esclavizado a maquinas cuando en realidad las cosas son simples y sin complicaciones. Vivimos en un país que tenemos que trabajar el pensamiento en conjunto en hacer cosas buenas que se puedan hacer para el ciudadano digital de la República Dominicana; debemos de dejar de crear en el ser humano de que la tecnología es infalible e impenetrable cuando se crea una solidez ficticia de que siempre estaremos disponibles en nuestros servicios. En nuestro país tenemos que ir pensando muy bien en cómo vamos a lograr una República Dominicana desarrollada camino al 2030; lo único que podemos hacer por ahora es transparentarnos y crear una tecnología de una forma diferente lo cual podemos acoplar en este mundo moderno que nos ha tocado vivir a todos. Mi recomendación es que si quieres tener una excelente ciberseguridad para prevenir el riesgo de robo de credenciales bancarias en el sistema financiero nacional de la República Dominicana debe implementarse más educación a nivel del cliente financiero para así evitar pérdidas millonarias en el sector económico de nuestro país. Además, crear a largo plazo depósitos electrónicos más seguros y una inteligencia artificial que maneje las instituciones financieras desde el Banco Central de nuestra República Dominicana en conjunto con la Superintendencia de Bancos (SIB) junto a las empresas del país conectadas a internet.

Bibliográfica:

USA Network Mr. Robot (2015).

INTECO "Instituto Nacional de Tecnologías de las Comunicaciones", Cuaderno de Notas del Observatorio ¿Qué son y cómo funcionan los troyanos bancarios? (2015).

Merejo, A. (2015). La era del Cibermundo. República Dominicana: Editorial Nacional, ISBN: 978-9945-492-46-0.

República Dominicana: hacia una regulación para fomentar el teletrabajo, Arango, Amparo Coordinadora Técnica de la Comisión Nacional para la Sociedad de la Información y el Conocimiento (CNSIC) 2015.

The Research Brief of the Future of Government Cybersecurity, (2015-2016).

Un paso adelante en la era de las amenazas cibernéticas Ramírez, Alonso Socio de consultoría y asesoría Deloitte & Touche S.A, (2016).

Ciberseguridad ¿Estamos Preparados En América Latina y el Caribe? Banco Interamericano de Desarrollo (BID); Organización de Estados Americanos (OEA), Mar 2016.

IBM Whitepaper - Nueva Tecnología, Nueva Mentalidad, (2016).

Un paso adelante en la era de las amenazas cibernéticas Ramírez, Alonso Socio de consultoría y asesoría Deloitte & Touche S.A, (2016).

Privatewatershousecoopers: The Global Economic Crime Survey, 2016. México D.F. Firma de Consultoría de las Big Four Entidades Gubernamentales. Recuperado de Www.Pwc.com/crimesurvey

Gómez, José Miguel “Robo de Identidad y Sus Consecuencias” (2017).

Social Security “El robo de credenciales, nuevo foco de los cibercriminales” (2017).

Cisco Annual Cybersecurity Report, (2017).

Diario TI “Building Confidence: Facing the Cybersecurity Conundrum” (2017).

S21sec Cyberpredictions for 2017, https://www.s21sec.com/en/cyber-predictionsfor-2017/.

The Internet Health Report V.01, 2017. Mozilla Foundation. Recuperado de https://internethealthreport.org/v01/es/

Informe VIU Ciberseguridad: Tendencias (2017).

ESET Security Report Latinoamérica (2017).

Tejeda, Lilian Listín Diario “¿Cuáles son las quejas más comunes de los usuarios en el sistema financiero?” (2018).

Rodríguez, Bismark “Experto Recomienda Sector Financiero Invertir en Tecnologia para mejorar la Ciberseguridad” (2018).

Ramírez, Jhenery “Anuncia un nuevo reglamento contra ciberdelito” (2018).

Reglamento de “Seguridad Cibernética y de la Información” para nuestra República Dominicana (2018).

Tejeda, Lilian Listín Diario “En tres meses usuarios del sistema financiero realizan más de 150,000 reclamaciones” (2018).

Apéndice y/o Anexos

Gracias aquellos héroes desconocidos que decidieron colaborar con esta Idea de Hoy que se hace realidad.

INSTITUTO TECNOLOGICO DE SANTO DOMINGO, INTEC

MAESTRIA EN CIBERSEGURIDAD

EVALUACION DEL TRABAJO DE GRADO DE
[ING. MIGUEL ALFONSO PEÑA GAGO]
ID 1073505

[Riesgos de Robos de Credenciales Bancarias en el Sistema Financiero Nacional de la República Dominicana]

FECHA _____

ASESOR _____ FIRMA_____

LECTOR _____ FIRMA_____

_____	_____
ING. ARTURO DEL VILLAR DECANO DE INGENIERIA	ING. MIGUEL MARIA ARIAS COORDINADOR DE MAESTRIA