INSTITUTO TECNOLÓGICO DE COSTA RICA

ESCUELA DE ADMINISTRACIÓN DE EMPRESAS

Automatización, ciberseguridad y ciencia de datos: La nueva estrategia empresarial

TRABAJO FINAL DE GRADUACIÓN PARA OPTAR POR EL GRADO DE BACHILLERATO EN ADMINISTRACIÓN DE EMPRESAS

Elaborado por:

Jimmy Ulloa Mora

Profesor Tutor:

M.Sc. Víctor Garro Martínez

San José, Costa Rica

Octubre, 2021

ÍNDICE DE CONTENIDO

Índice de ilustraciones

Índice de tablas

Índice de gráficos

Dedicatoria

Dedico este trabajo a Dios, quién es la fuerza que me sostiene para que pueda seguir día a día y quien siempre está para ayudarme.

Dedico este trabajo a mi padre y madre, quienes siempre me han apoyado y me han guiado en esta vida, a mis hermanos por su comprensión y ayuda.

Dios y mi familia es todo lo que tengo y amo; a ellos les dedico este trabajo.

Agradecimiento

Quiero agradecer al Coordinador de carrera, profesor guía y demás profesores y funcionarios de el Instituto Tecnológico de Costa Rica, quienes, de alguna forma, estuvieron presentes en mi formación profesional y me enseñaron la importancia de investigar.

Resumen

Vivimos en un mundo interconectado digitalmente, donde las empresas, servicios, productos e información no interponen barreras a la hora de comunicarse entre sí y el volumen y la importancia de los datos que se generan día con día era inimaginable tan solo unos años atrás. Actualmente muchas empresas se esfuerzan por adaptarse a esta nueva era digital y su característica evolución. Debido a los grandes avances tecnológicos que presenta la composición de la misma, inclusive los nuevos emprendimientos que, aunque a diferencia de las empresas tradicionales nacieron en pleno surgimiento de la sociedad 4.0 necesitan, sin duda alguna, estar a la vanguardia en cuanto a tecnología para poder disfrutar de las grandes ventajas competitivas que esta brinda, pero también se debe entender que por ello comparten el hecho de que la ciberseguridad sea su mayor amenaza.

Dicha situación lamentablemente puede llegar a afectar la vida cotidiana y funcionamiento de cualquier persona o compañía alrededor del mundo debido a que mientras se trata de encajar en una era digital que está en constante evolución, la apertura de mercados demanda una mayor interacción de datos en el ámbito internacional y una fuerte dependencia tecnológica para resolver problemas de distintas índoles como el manejo de macrodatos, redes sociales, seguridad, tendencias, entre otros. Todo ello nos debe poner a analizar como las amenazas cibernéticas son cada vez más frecuentes y complejas, ya que explotan en forma precisa la tecnología al usarla como plataforma principal para que la ciberdelincuencia pueda irrumpir servicios de primera necesidad, extorsionar personas o empresas de acuerdo al cargo, importancia o capital e inclusive dañar la imagen de gobiernos poniendo en duda, ante el público en general, si la información es segura, o no, ya se personal o corporativa.

Sin duda alguna, el escenario y las circunstancias donde y por qué se ejecutan varían constantemente. Por ejemplo, cuando se denotan vulnerabilidades que van desde trabajar en la comodidad de la casa –que se volvió tendencia desde inicios del 2020 debido al COVID-19– a que grupos dedicados a la ciberdelincuencia tengan como objetivo principal sectores tan importantes como el financiero. Por medio de lo que se conoce como ransomware, el sector financiero se ve altamente afectado al podérsele encriptar o cifrar información determinante a cambio de cuantiosas sumas de dinero. De esta forma, también se afectan grandes sectores gubernamentales, con lo cual se pasa de una actividad ciber criminal a lo que se conoce como

ciberterrorismo que es cuando se atenta contra la vida e integridad de las personas en busca de algún beneficio.

Actualmente, se necesitan profesionales en ciberseguridad más calificados, por lo que las empresas deben trabajar en forma conjunta con las universidades para formar gerentes, ingenieros y técnicos que conozcan del tema sin importar en el área en el que se desarrollen. Lo anterior se vuelve imperativo porque distintas disciplinas que van desde la Gestión del Talento Humano, Tecnología de la Información (TI) a sectores como el Contable y el Financiero son objetivos de alto perfil para los piratas cibernéticos y deben ser particularmente manejados cuando se trata de ciberseguridad, ya que las personas que laboran en dichos puestos cuentan con información personal identificable de los clientes y también de dinero.

Las empresas deben estar sujetas a reglas y regulaciones de ciberseguridad cada vez más fuertes y estrictas bajo un estándar de cero tolerancia. Ello con el único fin de mejorar la preparación del personal en la comprensión y uso de la información en materia de ciberseguridad y brindar al usuario o cliente no solo la atención y buen servicio que se merece, sino también la confianza de que no se expondrán sus datos ante el público en general o que no perderá alguna forma de activo a causa de un ataque cibernético. Lamentablemente se ha visto en eventos pasados ataques de este tipo, por lo que se denota que la tecnología es necesaria, pero demanda mucha responsabilidad.

Abstract

We live in a digitally interconnected world where companies, services, products, and information do not have barriers when communicating with each other and where the volume and importance of the data that is generated every day was unimaginable just a few years ago.

Currently many companies are striving to adapt to this new digital age and its characteristic evolution due to the great technological advances that its composition presents, including start-ups that, although unlike traditional companies, were born in the middle of the emergence of society. 4.0 undoubtedly need to be at the forefront in terms of technology to be able to enjoy the great competitive advantages that it offers them, but it must also be understood that therefore they share the fact that cybersecurity is their greatest threat.

This situation can unfortunately affect the daily life and operation of any person or company around the world because while trying to fit into a digital era that is constantly evolving

where the opening of markets demands a greater interaction of data to international level as well as a strong technological dependence to solve problems of different nature such as the management of big data, social networks, security, trends, etc., should make us analyze how cyber threats are increasingly frequent and complex which they exploit precisely the technology by using it as the main platform so that cybercrime can break into essential services, extort people or companies according to their load, importance or capital and even damage the image of governments by questioning before the general public if the information is safe or not either on a personal or corporate level.

Undoubtedly, the scenario and the circumstances where and why they are executed vary constantly as vulnerabilities are denoted that range from working in the comfort of the home that became a trend since the beginning of 2020 due to COVID-19 to which groups dedicated to cybercrime have as main objective sectors as important as the financial one which through what is known as malware is highly affected by being able to encrypt decisive information in exchange for large sums of money or also affecting large government sectors going from a cyber activity criminal to what is known as cyber terrorism, which is when the life and integrity of people are attacked in search of some benefit.

Today, more qualified cybersecurity professionals are needed, so companies must work together with Universities to train managers, engineers and technicians who know the subject regardless of the area in which they develop because different disciplines that go from human resources, information technology or IT to sectors such as accounting and financial are high profile targets for cyber hackers and must be particularly handled when it comes to cybersecurity by having personally identifiable information of customers and also money.

Companies will be subject to ever-increasing and strict cybersecurity rules and regulations under a zero tolerance standard with the sole purpose of improving the preparation of personnel in understanding and using information on cybersecurity and thus be able to provide the user or client not only the attention and good service he deserves but also the confidence that his data will not be exposed to the general public or that he will not lose some form of asset due to a cyber-attack as has unfortunately been seen in past events, technology is necessary but demands a lot of responsibility on our part.

Palabras clave

Ciberseguridad, seguridad, guerra cibernética, seguridad de la información (InfoSec), ataque cibernético, seguridad cibernética, vulnerabilidad, test de penetración, *pentester*, *hacker*, *hackeo*, *hackeo* ético, ataque informático, resiliencia, *malware*, *ransomware*, encriptación, llave, virus, tecnología de la información (TI), automatización, Ansible, *playbook*, YAML, nodo de control, nodos administrados, código abierto, *software*, *software* libre, repositorio, virtualización, *script*, Windows, Linux, servidor, sistema operativo, ciencia de datos, inteligencia artificial (IA), retorno de la inversión (ROI), información, ahorro, eficiencia, error humano, prevención, sociedad 4.0, cuarta revolución industrial.

Key Words

Cybersecurity, security, cyber warfare, information security (InfoSec), cyberattack, cyber security, vulnerability, pen testing, pentester, hacker, hacking, ethical hacking, computer attack, resilience, malware, ransomware, encryption, key, virus, information technology (IT), automation, Ansible, playbook, YAML, control node, managed nodes, open source, software, free software, repository, virtualization, script, Windows, Linux, server, operating system, data science, artificial intelligence (AI), return of investment (ROI), information, savings, efficiency, prevention, society 4.0, fourth industrial revolution.

Introducción

La cuarta revolución industrial será la plataforma perfecta para que la innovación tecnológica, la investigación científica y empresarial fomenten el crecimiento y el desarrollo de negocios interconectados digitalmente, concebidos en una era en la que predomina la información, la automatización, el ahorro y la eficiencia. La sociedad 4.0 planea dar una mejor calidad de vida gracias a ideas innovadoras que demuestran un impresionante crecimiento tecnológico. Por lo anterior tanto usuarios finales o consumidores y las empresas dependerán cada vez más de la tecnología debido a que se estima que, de esta forma, se experimentará un crecimiento económico sin precedente alguno.

A pesar de que esta década ha sido marcada por problemas nunca vistos –como la pandemia del COVID-19 causante del cierre de muchos negocios y el declive de la economía mundial–, la tecnología será clave para la creación de nuevos emprendimientos. A principios del año 2021, el Foro Económico Mundial (World Economic Forum) indicó que se está a las puertas de una nueva pandemia, la cual será cibernética y, si no se llegan a tomar las medidas y la seriedad del caso, esta ciber pandemia que es como se denominará, causará grandes catástrofes financieras tanto en el sector privado como en el sector público en todos los países del mundo. Se estima que dicha ciber pandemia causará daños irreversibles no solo en el ámbito económico, sino también en el histórico, en la reputación y en el prestigio de las empresas.

Esta tesis busca como mejorar la planeación, el análisis y la automatización de diversos mecanismos en el campo de la ciberseguridad con el fin de evitar que las empresas sean vulnerables y contar con un plan de acción ante estas amenazas. Este contexto evidencia que la información es, actualmente, uno de los activos más importantes que se debe proteger porque, en manos equivocadas, puede llegar a generar pérdidas económicas, de clientes y la confianza que, en el mundo de los negocios, es de suma importancia.

Actualmente, la demanda por tecnologías emergentes se incrementó especialmente en el sector de servicios financieros, en el cual la utilización de efectivo ha disminuido radicalmente gracias a los avances en banca por internet. Este avance facilita los pagos instantáneos de transacciones y servicios por medio de aplicaciones que no solo deben ser de fácil acceso y facilitar la vida para todos, sino también ser seguras debido al aumento de vulnerabilidades

cibernéticas. A su vez, esto genera una industria multimillonaria que busca, a través de las aplicaciones que usan la internet, proteger dichas transacciones contra ataques que, aunque sean un gran desafío porque se debe estar un paso delante de los piratas cibernéticos, demuestra la necesidad actual en la industria de más profesionales de seguridad que sean calificados.

¿Qué tan serias son estas amenazas? Era la pregunta que circuló por mucho tiempo hasta que, año tras año, se notó como se pasó de demostrar un alto intelecto en el manejo computacional solo para alimentar el ego del ejecutante a vivir de actividades delictivas cibernéticos. Por lo anterior, sin duda alguna, hay que preocuparse por planear no solo como se procederá ante un eventual ataque, sino también tener claro que estamos a pasos de vivir un verdadero impacto en los mercados financieros internacionales, instalaciones de generación eléctrica o en represas hidroeléctricas como posibles escenarios donde, lamentablemente, se sufrirá lo que se conoce como ciber terrorismo. La posibilidad de crear o rediseñar la seguridad es ahora y debemos hacerlo, sin importar el tamaño o tipo de empresa, por el bien de nuestra sociedad para poder asegurarnos de que continuaremos con la proyección de una mejor vida para todos.

Capítulo I. Planteamiento del problema

El presente capítulo describe la evolución de los ataques cibernéticos y sus devastadoras consecuencias tanto en empresas privadas como en instituciones públicas e incluso en las llamadas ciudades o países inteligentes, donde la totalidad de servicios, medios de transporte y seguridad poblacional es administrada por medio de la tecnología. Debido a ello, los *hackers* o piratas cibernéticos emplean métodos y técnicas cada vez más sofisticadas, por ejemplo *ransomware*, el cual desde el año 2018 ha crecido en su uso hasta en un 150%. El uso de *ransomware* ha afectado a diversos tipos de industrias mundiales como se ha visto, especialmente, durante el 2021. Con el uso de este tipo de estrategias se demanda el rescate o recuperación de datos empresariales a cambio de millones de dólares, con lo cual se daña no solo las finanzas de grandes corporaciones, instituciones gubernamentales y empresas privadas en general, sino también su integridad, reputación e imagen ante clientes, proveedores y empleados, ya que ha provocado el despido inmediato de gerentes y personal con altos cargos.

La conectividad de las distintas redes son tan altas que no podemos concebir la existencia de negocios que no se incorporen a este sistema, lo que provoca que sea innegable el impulso que brinda a las empresas, pero, a su vez, demanda una gran responsabilidad, el gran problema es que no se está tomando con la seriedad que se merece esta temática. Con lo anterior, se deja la puerta abierta a ataques a pesar de que existe la prueba inminente que se ha efectuado en diversas industrias, a grandes empresas y firmas mundiales. Por ello, se intuye que la mayoría de medianas empresas y las pymes tampoco están preparadas. A continuación, se presenta una lista de algunos ciberataques a diversas empresas que no solo terminaron en perdidas millonarias, sino también en el despido del gerente y personal especializado.

Tabla 1. Lista de algunos ciberataques en los que se perdieron puestos de mando

Año	Compañía	Actividad	Consecuencias
2014	Target	Detallista	Obtienen detalles de pago de 40 millones de clientes, se van el CIO y el director Ejecutivo
2014	Sony Pictures	Cinematográfico	Robo de documentos internos, desencadena un incidente diplomático entre Corea del Norte y Estados Unidos, despido de la CEO
2014	JPMorgan Chase	Banca y Finanzas	Acceso a 83 millones de cuentas, nombres, teléfonos, direcciones, e-mails, se movilizan al CSO y CISO
2016	Aerospace	Aeronáutica	Servicios detenidos varios días se pagan $40 millones
2017	Uber	Transporte	Robo de 57 millones de datos con nombres, teléfonos, direcciones, e-mails y licencias. Se encubre el pago de $100 mil, despido del CSO
2017	Equifax	Reporte Crediticio	Robo de 143 millones de datos con nombres, teléfonos, direcciones, e-mails y licencias, perdida de $1.35 billones, se despiden al CSO, CIO y al CEO
2019	Capital One	Banca y Finanzas	Acceso a datos de 100 millones de clientes, produce perdidas de entre $100-$150 millones, despido del CISO y CIO
2021	Colonial Pipeline	Suministro Combustible	CEO debe testificar por el cierre de seis días al oleoducto que distribuye la mitad de Diesel y gasolina de la costa este de USA y por pagar $4.4 millones
2021	JBS	Distribuidora de carne	Paga $11 millones y por varios días no pudo distribuir carne en toda la costa este de Estados Unidos

Fuente: elaboración propia.

Nuestro país no es la excepción, según *Castro, Johnny* (2020), Costa Rica registró casi 32 millones de intentos de ciberataques en los primeros tres meses del año 2020. Lo anterior desencadenó en estafas que superan los ¢500 millones, según estimaciones de el OIJ. Por lo

tanto, se debe desarrollar un plan de acción y contingencia capaz de mitigar y ayudar a las empresas costarricenses a estar mejor preparadas ante esta clase de riesgos.

1.1 Marco referencial

Actualmente, las empresas viven una etapa de transformación digital sin precedentes, lo cual ha obligado a producir una convergencia digital y transformación departamental dentro de las empresas para poder satisfacer la actual demanda en el entendimiento, buen uso, seguridad y diagnóstico de las herramientas tecnológicas. Sin duda alguna, el COVID-19 ha jugado un papel importante en dicha transformación al obligar a las empresas a adaptarse a las necesidades actuales que son brindar asistencia y servicios en forma remota y utilizar aplicaciones tecnológicas que faciliten la vida del público en general y, a su vez, aseguren la información que requieran del usuario. Lamentablemente, muchos negocios por su tipo de estructura no pueden hacerlo, otros por falta de presupuesto o de información sobre cómo se hace no pudieron migrar al formato digital mientras que otros en cambio lo hicieron exitosamente.

Al mismo tiempo en que la empresa privada y entidades gubernamentales diseñaban la migración de sus servicios al formato digital, los ciberdelincuentes que actúan en forma individual o por medio de grupos que se dedican a la piratería informática también lo hacían. De ahí que debemos aprender que no solamente las empresas se modernizan también lo hacen aquellos que son una amenaza para la seguridad. Al respecto, una investigación realizada por IBM (2020) indica que el costo comercial promedio de un ciberataque es de unos $3.86 millones y se necesitan 280 días para detectar y detener un ataque. Esto significa que el proceso de detección es extremadamente lento, ya que muchas empresas no invierten del todo en ciberseguridad ni tampoco realizan auditorias en sus sistemas y, peor aun, tampoco mantienen sus equipos actualizados, se concentran en diversas tareas y dejan la puerta abierta a un enemigo muchas veces silencioso que, en cualquier momento, ataca si es que no ha ingresado en los servidores de la empresa para la que se trabaja.

El uso de programas malignos aumentó en un 358% en el 2020 y el uso de *ransomware* aumentó en un 435% en comparación con el año anterior, según un estudio de Deep Instinct (2021). Solo en julio de 2020, se registró un aumento del 653% en la actividad maliciosa en comparación con el mismo mes de 2019. Muchos se preguntarán entonces ¿por qué este aumento

tan drástico en cuanto a las perdidas por concepto de ciberseguridad? La respuesta es porque, actualmente, la mayoría de los ciberataques en casi un 86% están motivados por la obtención de ganancias financieras, como segunda razón principal de un ciberataque incluye el espionaje estatal o privado (CSO Computerworld España, 2020, como se citó en Verizon, 2020). Es decir, los ciberdelincuentes no discriminan entre empresas o industrias, aunque sea difícil medir con precisión el costo del robo de datos que ha afectado significativamente a consumidores y empresas.

Un claro ejemplo de ello es que más del 90% de las organizaciones de atención médica sufrieron al menos una brecha de ciberseguridad en los tres años anteriores, según Yahoo! Finance (2021).

También se debe recalcar que el error humano es la principal causa de incidentes cibernéticos, debido a que las personas son el eslabón mas débil y vulnerable en sus hábitos de la cadena de seguridad. Actualmente, se reconoce que hay mucho trabajo de capacitación y educación por hacer, si se esperan grandes resultados debemos invertir en la capacitación necesaria para eliminar esa vulnerabilidad haciéndole saber al personal cómo manejar la información y, en especial, cómo se contribuye a la seguridad de la empresa en general y, por ende, de los clientes.

Si bien es cierto que existe una brecha de habilidades en seguridad de la información, también se debe alentar a las personas a estudiar y comprender la importancia de la ciberseguridad. Se puede proponer un trabajo en conjunto entre empresas para dar la capacitación, universidades para dar la formación y personal que quiera actualizarse, ya que existe una gran demanda en el mercado laboral en dicha materia.

En cuanto a la capacitación en el tema de ciberseguridad, hay que enfatizar que es esencial que hoy los gerentes de áreas como Gestión del Talento Humano, Contabilidad, Finanzas y Gerencia General también entiendan del tema. Lo anterior porque uno de los objetivos principales de la gestión de riesgos es ofrecer una seguridad óptima a un coste razonable y eso es vital en el manejo de cualquier empresa, ya que se debe pensar en el costo versus el beneficio, el manejo del riesgo y los tipos de contramedidas a desarrollar e implementar.

Los delitos cibernéticos cuestan a las organizaciones $2.9 millones por minuto y las principales empresas pierden $25 por minuto como resultado de las filtraciones de datos según la investigación de RiskIQ (2019).

Por todo lo expuesto, es vital que en las empresas existan tres diferentes anillos de seguridad en el ámbito de los colaboradores. El primero corresponde a la gerencia y personal de puestos de mando; el segundo al personal técnico de la compañía en el área de tecnología y seguridad y el tercero se asocia con el resto de personal sin importar su posición. La ayuda de todos es vital y, en conjunto con normas técnicas a recomendar, se obtendría una mayor seguridad.

1.2 Justificación del TFG

Los ciberdelitos son muy rentables, mutan con el tiempo y, además, amplifican su propio espectro de causa y razón, ya que actualmente el motivo no solo es financiero, también puede ser de índole político e, inclusive, social. El daño que puede causar un ataque cibernético a cualquier organización o empresa es extremadamente alto, importante, delicado y significativo. Afecta las finanzas, ya que puede llegar a costar millones de dólares y el grado de afectación en la capacidad para hacer negocios tanto a corto como a mediano plazo debido al detrimento en la reputación e integridad de la empresa. Cuando esta clase de situaciones llegan al conocimiento publico, sin importar el área o industria a la que se dediquen, provoca que afectaciones en la confianza por parte de clientes o usuarios.

Actualmente, la forma en que se hacen negocios es muy diferente a como se hacían tan solo hace unos años atrás. Dicha variabilidad progresa día a día, especialmente, con la integración de los modelos de negocios basados en la industria 4.0, en la que las empresas son parte de un proceso de digitalización que demandan mecanismos de autenticación sofisticados que van desde la doble autenticación del usuario o el uso de reconocimiento facial y de voz hasta el uso del internet de las cosas (Internet of Things-IOT). Todo ello demanda no solo seguridad de los datos en las empresas, sino también de sus empleados y usuarios o clientes.

Debe comprenderse que toda organización tiene vulnerabilidades, las mismas pueden ser de diferente naturaleza como por ejemplo no contar con personal capacitado en el tema de la ciberseguridad o uso de equipo desactualizado. Lo recomendable es implementar y ejecutar un

plan de ciberseguridad que contemple realizar revisiones periódicas, obtener y analizar propuestas y resultados de dicha supervisión, ya que hoy en día toda empresa se vuelve una posible víctima. Además, un plan de esta naturaleza debe ser parte esencial de toda organización, con lo cual se produce un enfoque de seguridad adecuado que ayude a generar un entorno de trabajo privado, seguro y más eficiente tanto para la empresa como para el empleado y, sin duda alguna, para el usuario o cliente.

Innovar los actuales servicios de ciberseguridad en las organizaciones será fundamental para un eficiente manejo de situaciones delicadas como el *ransomware* y, en especial, servirá en la prevención de nuevos ataques cibernéticos. Estos ataques serán sofisticados delitos considerados actualmente como negocios criminales en el ámbito internacional, máxime que, de acuerdo con el World Economic Forum (2021), la próxima pandemia tendrá una exposición y propagación similar a la de un virus, pero la misma no será analizada en el campo médico o de la salud, sino más bien en el campo cibernético, ya que al igual que su contraparte no contará con restricciones geográficas y virtualmente un inmenso número de empresas presentarán muchas vulnerabilidades, lo que facilitará su contagio y la propagación del ataque al igual que un virus.

Sin duda alguna, las empresas sufrirán pérdidas y problemas porque enviarán más y nuevos trabajadores a ejercer sus labores desde casa como ya se viene haciendo, por lo que, esencialmente, los estarán convirtiendo en su propio departamento de tecnología y soporte. Sin embargo, no necesariamente esto indique que cuenten con las destrezas o medios para defenderse de un posible ataque. Lamentablemente, lo normal es que se desconozcan los requisitos para proteger a la empresa, contar con una planificación adecuada al igual que su revisión por lo que es esencial llegar a comprender las amenazas persistentes, ya que el panorama actual se complica y hay que poder identificar las amenazas realmente críticas, la infraestructura y las operaciones de seguridad de la organización.

1.3 Objetivos de la investigación

El país debe avanzar en materia tecnológica y requiere de la utilización de nuevas herramientas.

La innovación como por ejemplo el uso de código libre le permitirá a Costa Rica tener otro panorama para enfrentar los nuevos retos de este siglo y estar listo en materia de automatización, ciberseguridad y el uso de ciencia de datos.

1.3.1 Objetivo general

Mostrar las ventajas que brindan el uso de la automatización, ciberseguridad y la ciencia de datos como elementos clave de la nueva estrategia empresarial dentro del marco de la sociedad 4.0

1.3.2 Objetivos específicos

- Mostrar la importancia que tienen la investigación y la innovación en la actualidad empresarial por medio de la automatización.
- Mostrar la importancia que tiene la protección de datos por medio de la ciberseguridad.
- Mostrar los beneficios de la ciencia de datos en la toma de decisiones empresariales.
- Mostrar lo importante que es la automatización, la ciberseguridad y la ciencia de datos en la mejora de los costos e ingresos en la actualidad.

1.4 Pregunta de investigación

¿Cómo se puede realizar la transformación estratégica digital para la empresa nacional?

Capítulo II. Revisión de la literatura

El presente capítulo busca familiarizar al lector con la terminología necesaria para entender lo más relevante en ciberseguridad, automatización y administración de empresas para entender los indicadores y la información que contendrá la propuesta a desarrollar y cómo se puede implementar en cualquier empresa.

2.1 Acuerdo del nivel de servicio (Service Level Agreement-SLA)

Según Kevin, L. Jackson, Scott Goeeslin (2018), el service level agreement (SLA) o acuerdo de nivel de servicio sirve como modelo y garantía para los servicios de computación en la nube. Su propósito es documentar los niveles mínimos de servicio de los parámetros específicos y las soluciones para cualquier incumplimiento de los requisitos especificados. También debe afirmar la propiedad de los datos y especificar detalles de devolución y destrucción de datos.

2.2 Ansible

De acuerdo con Arthur Glogowski (2020), "Ansible es la plataforma de automatización de código abierto, puede administrar tareas de administración potentes, y puede adaptarse a muchos flujos de trabajo y entornos diferentes".

2.3 Aprendizaje automático (*machine learning*)

Según Aurélien Géron (2019), "el aprendizaje automático o machine learning es la ciencia (y el arte) de programar computadoras para que puedan aprender de los datos" (p. 217).

2.4 Automatización (automation)

La automatización es la tecnología que, actualmente, se utiliza en diferentes campos de la ciencia para realizar tareas en forma mas eficiente y rápida que las personas. De acuerdo a Akula Madhu "La automatización es un programa que se puede aplicar en el dominio de la seguridad de la Información" (Security Automation with Ansible 2, 2017, capítulo 2).

2.5 Automatización de la ciberseguridad (cybersecurity automation)

De acuerdo a Hsiang-Chih Hsu, Tony define la seguridad cibernética como "la automatización de la seguridad tiene como objetivo reducir la cantidad de pruebas manuales

repetidas y aumentar la cobertura de las pruebas de manera eficiente" (*Practical Security Automation and Testing*, 2019, capítulo 1).

2.6 Ciberseguridad (cybersecurity)

Calder, Alan define la ciberseguridad como "no tiene por qué costar grandes cantidades de dinero o llevar años implementarla, especialmente si se adopta un enfoque estratégico y apunta primero a la fruta mas fácil. Es una inversión que vale la pena: no importa el tamaño de su organización, mejorar la seguridad cibernética ayuda a proteger sus datos y los de los clientes, mejorando las relaciones comerciales y abriendo nuevas oportunidades comerciales" (Calder, Alan, 2020). El glosario de la NICCS por sus siglas en ingles o Iniciativa Nacional para Carreras y Estudios de Ciberseguridad del Departamento de Seguridad Nacional de los Estados Unidos de Norteamérica define la ciberseguridad "La actividad o proceso, habilidad o capacidad o estado mediante el cual los sistemas de información y comunicaciones y la información contenida en ellos están protegidos y / o defendidos contra daños, uso o modificación no autorizados o explotación." (NICCS, 2021)

2.7 Gestión del riesgo cibernético (*cyber risk management*)

De acuerdo a Hsiang-Chih Hsu, Tony explica que la automatización de la seguridad tiene como objetivo reducir la cantidad de pruebas manuales repetidas y aumentar la cobertura de las pruebas de manera eficiente. (*Practical Security Automation and Testing*, 2019, capítulo 2).

2.8 Hacker Ético

De acuerdo con EC-Council (2021), la importancia del Hackeo ético "En los albores de los conflictos internacionales, las organizaciones terroristas que financian a los ciberdelincuentes para violar los sistemas de seguridad, ya sea para comprometer las funciones de seguridad nacional o para extorsionar grandes cantidades inyectando malware y negando el acceso. Dando como resultado el aumento constante de la ciberdelincuencia. Las organizaciones enfrentan el

desafío de actualizar las tácticas de prevención de ataques, instalando varias tecnologías para proteger el sistema antes de ser víctimas del pirata informático.”.

2.9 Innovación

De acuerdo con Leiva Bonilla, Juan Carlos (2021). “La innovación muchas veces se expresa en nuevos productos y servicios o mejoras de los existentes.

Pero no es solo eso, también puede haber innovación en la forma de hacer las cosas dentro de la empresa (fabricar, distribuir, gestionar la tecnología), en la forma de comercializar los productos y servicios, en la forma de generar dinero (monetizar) o en la combinación de esos elementos, que es lo que llamamos el modelo de negocio.”.

2.10 Innovación basada en Finanzas

De acuerdo con Osterwalder, Alexander & Pigneur, Yves (2011). La innovación basada en finanzas “se trata de innovaciones basadas en nuevas fuentes de ingresos, mecanismos de fijación de precios o estructuras de costes reducidas que afectan a otros módulos del modelo de negocio”.

2.11 Instituto Nacional de Estándares y Tecnología (NIST)

El Instituto Nacional de Estándares y Tecnología (NIS National Institute of Standards and Technology) constantemente busca la innovación en relación con buenas prácticas que aseguren no solamente procedimientos correctos, sino también los necesarios para generar beneficios en las empresas. Según Alan Calder (2018), este marco de trabajo se puede utilizar para establecer un programa de ciberseguridad completamente nuevo, mejorar uno existente o simplemente brindar la oportunidad de revisar las prácticas de ciberseguridad.

2.12 Margen de Utilidad Bruta

Según Van Horne & Wachowicz (2010), esta razón "permite determinar la ganancia de la empresa relativa a las ventas, luego de descontar los costos de venta de los bienes, esta razón permite determinar la eficiencia de la empresa en minimizar sus costos de venta.".

$$\textbf{MUB} = \frac{\textbf{Utilidad Bruta}}{\textbf{Ventas}}$$

2.13 Margen de Utilidad Neta

Según Van Horne & Wachowicz (2010), esta razón "Describe la rentabilidad de las ventas realizadas por la empresa luego de descontar todos los gastos e impuestos sobre la renta. Esta razón financiera nos permite determinar el ingreso neto de la empresa por cada colon de venta.".

$$\textbf{MUN} = \frac{\textbf{Utilidad Neta}}{\textbf{Ventas Netas}}$$

2.14 Margen de Utilidad Operativa

Indicador financiero que permite visualizar el nivel de eficiencia de una empresa en un periodo dado al minimizar sus costos de operación, determinando las ganancias luego de descontar los costos.

$$\textbf{MUO} = \frac{\textbf{Utilidad Operativa}}{\textbf{Ventas Netas}}$$

2.15 Procedimientos documentados

No todos los procesos de una empresa tiene procedimientos ni tampoco se encuentran todos documentados pero si existen algunos que deben documentarse para seguir sus

lineamientos. Según la norma ISO 9000, “un procedimiento es una forma específica para llevar a cabo una actividad o un proceso. Cuando se tiene un proceso que tiene que ocurrir en una forma específica, y se especifica cómo sucede, usted tiene un procedimiento”.

2.16 Rentabilidad

La definición de rentabilidad para Gitman (2007), nos dice “rentabilidad es la relación entre ingresos y costos generados por el uso de los activos de la empresa en actividades productivas. La rentabilidad de una empresa puede ser evaluada en referencia a las ventas, a los activos, al capital o al valor accionario”.

2.17 Retorno de la inversión (Return Of Investment - ROI)

De acuerdo con Jack J. Phillips y Patricia Pulliam Phillip (2019), en el libro *ROI Basics*, el retorno de la inversión o ROI es la medida máxima de responsabilidad que responde a la pregunta: ¿existe un valor económico agregado para la organización por invertir en programas, procesos, iniciativas y soluciones de mejora del desempeño? Las organizaciones se basan en muchos indicadores económicos. El ROI se utiliza para evaluar la eficiencia o rentabilidad de una inversión o para comparar la eficiencia de varias inversiones.

2.18 Simulación Monte Carlo

De acuerdo con Azofeifa Carlos E. (2004), la simulación Monte Carlo es básicamente un muestreo experimental, cuyo propósito es estimar las distribuciones de las variables de salida que dependen de variables probabilísticas de entrada.

2.19 Utilidades antes de intereses, impuestos, depreciación y amortizaciones (EBITDA)

Según explica Gitman & Joehnk. (2009), sobre el indicador financiero EBITDA “En un esfuerzo por dar lo mejor de sí mismas, algunas empresas han comenzado a reportar la cifra

EBITDA (utilidades antes de intereses, impuestos, depreciación y amortización) que, según argumentan, es la mejor manera de medir el rendimiento. Sin embargo, las cifras EBITDA también reportan el desempeño bajo una luz más favorable. Las empresas intensivas en capital, las que involucran muchos activos intangibles, y las que se expanden sobre todo a través de la compra de otras empresas (que generan crédito comercial) muestran mejores cifras de ganancias cuando reportan sus utilidades antes de deducir la depreciación y la amortización de sus ingresos.”.

Ebitda = Utilidad Neta + Intereses + Impuestos + Amortización (o Depreciación)

Otra forma de representar el concepto es mediante esta fórmula:

Ebitda = Ingresos – Costos Operativos – Gastos Administrativos

Capítulo III. Método de la investigación

En este capítulo se presentan los diferentes métodos utilizados para el desarrollo y obtención de los resultados que se expondrán en esta investigación. Debido al impacto negativo que generan los ataques cibernéticos en las empresas, se requiere que quienes tomen las decisiones puedan realizar mejores análisis y una mejor cuantificación del riesgo para no solo saber como priorizar el uso de recursos, sino también como mejorar los mecanismos de control que se requieren y, a su vez poder calcular las potenciales perdidas en las que se pueda incurrir en un ataque. Si una empresa no tiene una evaluación de riesgos eficaz, los mecanismos de seguridad se tornan inservibles, ya que la naturaleza del entorno que asegura su operación no posee una base sólida de conocimiento y, por ende, los problemas no se corrigen correctamente ni a tiempo.

La toma de decisiones precisas y concisas para efectos de la ciberseguridad son de suma importancia, ya no solo es hacer lo correcto dentro de cualquier organización, sino que también es una práctica sana que llegó para quedarse con el fin de asegurarle al cliente, al entorno de la

empresa y a sus colaboradores que, en la forma más responsable y profesional, se toman las medidas necesarias para no sufrir daños o perdidas. Por ello, la gerencia debe apoyar lo que dicten los encargados de seguridad en vías de preservar y mejorar los mecanismos de control diseñados por si un ciberataque se cristaliza. De esa forma, se previenen costos directos que se traducirían en pérdidas de diversas formas, según el tipo de ataque, magnitud y características. Sin importar si se trata de una empresa con cierto tiempo de estar operando o en una que recién inicia, la necesidad de implementar la ciberseguridad como norma empresarial es necesaria. Es decir, se requiere un presupuesto, un análisis exhaustivo de actividades, desarrollo de normas, auditoría y apoyo de la alta gerencia para el desarrollo de una cultura cibernética que debe implementarse en toda empresa.

3.1 Enfoque de investigación

En un inicio, la industria cibernética presentaba altas deficiencias en la recolección de datos. Primero que nada, porque no se conocía mucho del tema y, dependiendo del caso, se cometían errores como eliminar accidentalmente evidencia, había pocas herramientas especializadas y se contaba con pocos profesionales en el área. Actualmente, aunque se cuenta con mas información sobre el tema, hay una gran demanda de profesionales en este sector y, aunque existe una mayor cooperación no solo entre la comunidad de encargados de la seguridad cibernética, sino también de empresas afectadas y que promueven la seguridad, buenas practicas y creación de políticas, se debe seguir investigando para el desarrollo de mejores prácticas. Todo esto ayuda en gran manera a la investigación científica, la cual se basa en el acceso compartido de datos.

Especificamente, en el campo de la ciberseguridad la investigación científica se debe nutrir de una adecuada colaboración interdisciplinaria y, aunque esto no sea simple debido a la naturaleza y composición de los diversos elementos que la estructura de la ciberseguridad presenta, se deben interconectar como si se tratase de diversos puntos de la ciencia del conocimiento. Dicha colaboración permite trazar la tan esperada línea en la que la tecnología, la sociedad y los negocios juegan un rol muy importante en la clasificación de los problemas cibernéticos.

Con base en lo expuesto, esta investigación utiliza un enfoque mixto, es decir, se utilizaran métodos de análisis de riesgos cibernéticos cualitativos y cuantitativos. El análisis de riesgo cualitativo generalmente utiliza un alto grado de conjeturas. Se basa en las opiniones de personas que completan el análisis, normalmente en el campo tecnológico son los llamados expertos en la materia o SME (*subject matter expert*) por sus siglas en ingles. Por el contrario, en el análisis de riesgo cuantitativo, se utiliza una amplia gama de datos para llegar a un resultado, aunque puede ser difícil sin las herramientas y los procesos correctos, y falta de datos históricos debido a que nunca se generaron para ser guardarlos. Sin embargo, por medio de modelos matemáticos y estadísticos, esta cuantificación es posible.

De acuerdo con Hernández, Fernández y Baptista (2014), la investigación cuantitativa "utiliza la recolección de datos para probar hipótesis, con base en la medición numérica y el análisis estadístico, para establecer pautas de comportamiento y probar teorías" (p. 4).

Por lo tanto, cabe resaltar que dentro de este enfoque puede ubicarse la investigación descriptiva, la experimental, la histórica y algunas otras que llevan a esa misma línea de acción (Barrantes Echavarría, 2013).

Gracias a este tipo de investigación, se describen las diferentes vulnerabilidades que presentan las empresas nacionales para generar un listado de recomendaciones con el objetivo de mejorar y recomendar buenas prácticas de ciberseguridad.

3.2 Diseño de la Investigación

Según Hernández, Fernández y Baptista (2014), "el diseño de la investigación es un plan que nos ayuda a poner a prueba las respuestas que se han dado inicialmente o responderlas como ya se dijo, de forma directa" (p. 194). Para esta investigación se utiliza el diseño cuantitativo no experimental es por ello que a partir de los resultados que se obtengan por medio del análisis e información que se recopile, se diseñará un plan de ciberseguridad que podrá ser implementado, modificado y adaptado según el tipo de empresa, actividad y crecimiento. De esta forma, se fomenta la estrategia, concientización, planificación e implementación de un plan de ciberseguridad para aumentar el conocimiento tecnológico, administrativo y de control con el fin de reducir los riesgos de un posible ciberataque.

3.3 Unidad de Análisis

Por medio de los avances tecnológicos actualmente las decisiones se construyen con base en datos disponibles por medio de técnicas y procedimientos, cuyos métodos de recopilación, análisis e integración son vitales para todo negocio. La recopilación de datos ayuda a resolver el problema de definición porque es un enfoque sistemático para recopilar información relevante de una variedad de fuentes. Se procede a identificar una serie de amenazas que tienen más probabilidades de seguir afectando a las empresas durante el año 2021 y el 2022. Por lo tanto, la unidad de análisis son las amenazas que se identifica en la mayoría de los ataques o debilidades en la seguridad empresarial tales como:

- Falta de entrenamiento en ciberseguridad.
- Contraseñas no seguras.
- Suplantación de identidad (phishing).
- Desconocimiento de los últimos ataques en ciberseguridad.

3.4 Población y muestra

Actualmente, la mayoría de empresas no cuentan con un departamento o programa de ciberseguridad establecido que demande la recolección de información. Las causas de ello varían según la organización, pero los escenarios comunes son:

- Falta de una cultura cibernética empresarial.
- Carencia de herramientas tecnológicas.
- Desconocimiento de cómo aplicar técnicas que recolecten información.

Lamentablemente, ese es el escenario típico, ya sea porque la empresa no mantenga o guarde información o porque es nueva, normalmente se recure a la opinión de expertos para que defina la población y muestra de estudio. En este caso, la población corresponde a los diferentes productos a utilizar para el desarrollo del plan de estrategia cibernética empresarial.

3.5 Variables de la investigación

Para este estudio, se requieren variables tanto cualitativas como cuantitativas, las cuales se trabajan en forma dependiente o independiente a la necesidad, estudio o métrica que se requiera. El análisis de riesgo cualitativo se considera un enfoque menos riguroso que el análisis de riesgo cuantitativo, pero juega un papel muy importante en el desarrollo de este plan de estrategia cibernética empresarial. No cuantifica nada, ni utiliza cálculos, sino que se basa en opiniones que se obtienen a través de los años de experiencia; dicha información se obtiene de estudios estadísticos internacionales, de reconocidas empresas o de expertos en la materia conocidos como SME por sus siglas en inglés. Por lo tanto, las variables cualitativas concluyen resultados a través de la intuición y la experiencia, es decir, generalmente utiliza un alto grado de conjeturas porque se basa en las opiniones que completan el análisis.

Por su parte, el análisis de riesgo cuantitativo asigna valores numéricos a la variable asignada para realizar el análisis de riesgo, su enfoque debe ser matemático para poder realizar los cálculos de riesgo y predecir las pérdidas monetarias por amenazas. En este tipo de análisis se utiliza una amplia gama de datos para llegar a un resultado, aunque puede ser difícil sin las herramientas y los procesos correctos.

En este caso la población a cuantificar son las amenazas cibernéticas que van a variar según la industria y empresa, además la muestra se define por medio de la opinión de experto y desde un punto de vista probabilístico valido y acertado se consideran por lo general cincuenta mil interacciones es el numero ideal de intentos en los que dicha muestra puede dar a conocer el valor a investigar.

3.6 Estrategia de análisis de los datos

Se requiere un análisis de datos cibernéticos eficiente que permita evaluar con éxito la gestión de incidentes. Lamentablemente, en la mayoría de los casos no se cuenta con datos históricos sólidos en los que confiar o utilizar, por lo que se debe emplear modelos estadísticos que permitan solventar esa clase de falencias. Por ejemplo, la utilización de un modelo de PERT (Project Evaluation and Review Techniques) o un modelo estadístico Log-Normal para poder iniciar la generación de datos capaces de proveer más información; con el tiempo estos mismos

datos llegan a ser más robustos y eficaces. De forma más confiable, gracias a esos datos se puede desarrollar un presupuesto que permita explicar el cálculo u origen de las cifras económicas en las que se considera que se debe basar, especialmente, si se solicita comprar algún equipo.

3.6.1 Estimación de un presupuesto de defensa cibernético

Para realizar estimaciones, grandes empresas utilizan programas especializados en riesgo como @RISK y, de ese modo, efectúan los cálculos en los que basan el presupuesto de sus departamentos para luego enviarlos a aprobación a su división de Finanzas. Actualmente, existen técnicas que permiten obtener resultados similares sin necesidad de comprar programas o gastar en licencias. Para ello, se utilizan herramientas ya conocidas en el mundo de los negocios como Excel y también un lenguaje de programación llamado Python que es muy popular especialmente en el campo de la ciencia de datos.

3.6.1.1 Estimación Estadística-PERT

Para este tipo de estimación, se emplea una técnica estadística llamada Programa de Evaluación y Revisión Técnica (Program Evaluation and Review Technique–PERT) que tradicionalmente se utiliza para la administración de actividades que se desarrollaran en un proyecto. Este modelo estadístico debe contar con una estimación de tres puntos conocidos como (mínimo, más probable[moda], máximo). La media de PERT se calcula utilizando la siguiente fórmula:

$$PERT = \frac{(\text{Mín.} + (4 \ * \ \text{Más probable[moda]}) \ + \ \text{Máx.})}{6}$$

PERT es una distribución perfectamente normal es decir sin sesgo, la media también es el resultado más probable (conocido también como moda) y la mediana se ubica en el percentil 50. La estimación puntual mínima representa el valor más pequeño que es factible, pero altamente improbable. La estimación puntual más probable, o moda, representa el valor que se

cree más probable, aunque existen muchos otros resultados posibles entre las estimaciones puntuales mínima y máxima. La estimación puntual máxima representa el valor más grande que es factible, pero altamente improbable. La desviación estándar o SPERT (SD) es utilizada por funciones de distribución normal en Excel como NORM.DIST y NORM.INV en las que se utiliza la desviación estándar SPERT como uno de los argumentos de entrada, se calcula utilizando la siguiente fórmula:

SPERT SD = (Máx. - Mín.) * RSM

En este caso RSM (*Ratio Scale Modeler*), por sus siglas en inglés, es el multiplicador de escala de relación asociado con la selección de confianza más probable o media de PERT.

3.6.1.2 Estimación estadística–Distribución Log Normal

Para este tipo de estimación, se emplea el lenguaje de programación Python, el cual utiliza una función de densidad de probabilidad para la distribución log-normal representada de la siguiente forma:

$$f(x) = \frac{1}{x\sigma\sqrt{2\pi}} e^{-\frac{(ln(x)-\mu)^2}{2\sigma^2}}$$

Donde σ es la desviación estándar del logaritmo distribuido normalmente de la variable, μ es la media del logaritmo distribuido normalmente. La fórmula para derivar μ y σ de las estimaciones superior e inferior es la siguiente:

$$\mu = \frac{\ln(\text{lower}) + \ln(\text{upper})}{2}$$
$$\sigma = \frac{\ln(\text{upper}) - \ln(\text{lower})}{3.29}$$

μ se calcula tomando los registros naturales de las estimaciones superior e inferior, el resultado se dividirá entre dos. En cambio, para σ se divide por 3,29, el logaritmo natural debe usar los límites superior e inferior para obtener σ para la distribución logarítmica normal.

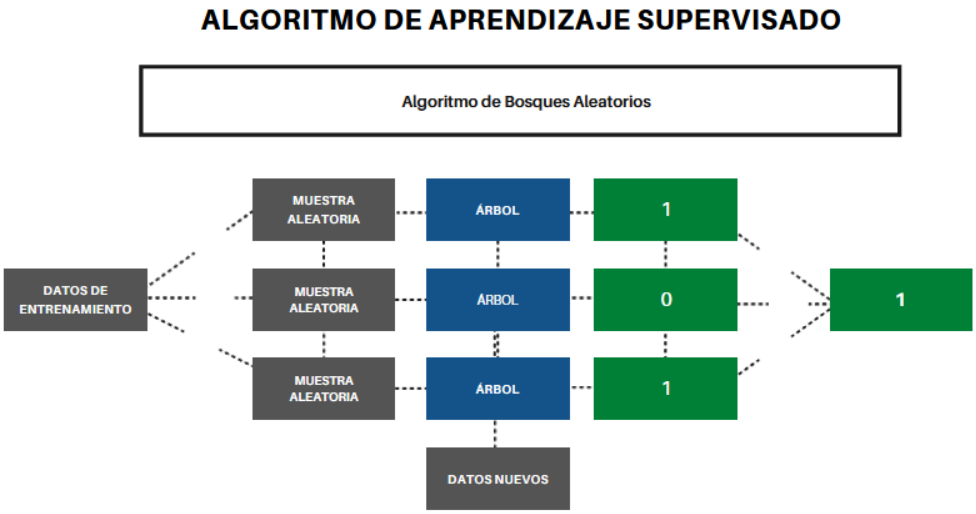
3.6.2 Predicción del comportamiento

El punto más débil de la ciberseguridad de cualquier empresa es el ser humano y, si bien es cierto que no se recomienda una gestión administrativa lleve un control y monitoreo extremo de cada colaborador, proceso o situación de la empresa, existen métodos eficaces para poder generar información de los colaboradores que permitan la mejora en la toma de decisiones en cuanto a la ciberseguridad se refiere. Para ello, se requiere una colaboración directa entre el departamento de la gestión del talento humano y los encargados de seguridad.

3.6.2.1 Identificar riesgos de personal-aprendizaje automático con Python

Por medio del aprendizaje automático o *machine learning*, se pueden analizar las razones de porque hay colaboradores insatisfechos que pueden en cualquier momento descuidarse en el uso del equipo tecnológico y que dichas desatenciones puedan ser explotadas por los ciberdelicuentes. Para ello, se utiliza Scikit-Learn, que es una de las librerías de Python más importantes para *machine learning*, y que cuenta con un modulo para implementar el algoritmo de Bosques Aleatorios Clasificación. Este algoritmo se encuentra dentro de los métodos de ensamblado de *machine learning*, por lo que se debe importar el modulo sklearn, ensemblar y, posteriormente, especificar Random Forest Classifier para poder implementarlo. Los Bosques Aleatorios es un algoritmo de aprendizaje supervisado, crea un bosque aleatorio que es un conjunto de árboles de decisión, la mayoría de las veces entrenados con el método de *bagging* o combinación de modelos de aprendizaje para mejorar el resultado global.

Figura 1. Diagrama del Algoritmo de bosques aleatorios



Nota. Adaptado de Random Forest (Bosque Aleatorio): combinando árboles, Martinez, H. Jose. (2020)

Capítulo IV. Análisis de resultados

En el presente capítulo se detallan los resultados y análisis respectivo de las diferentes herramientas disponibles para crear un plan de ciberseguridad acorde con las necesidades financieras de diversos tipos de empresas. Para el desarrollo de este análisis, los montos utilizados están expresados en colones, dólares, y como porcentajes o puntos porcentuales según corresponda.

4.1 El alcance del problema de ciberseguridad

Los ataques cibernéticos afectan a las empresas de diferentes formas, una de ellas es hacerlas incurrir en costos económicos no esperados a causa del impacto negativo que genera la

interrupción de operaciones que puede durar varias horas o días y afectar a una o varias partes o a toda la organización. Otra es la fuga y pérdida de datos los cuales pueden llegar a ser mayor que los costos directos y crear secuelas negativas, entre ellas, perdida de propiedad (extracción de datos, planos, informes, diseños), perdida de clientes, disminución de ventas, disminución de ingresos, reputación dañada, disminución en la calificación crediticia, generación de demandas a causa de la perdida de información confidencial, entre otras. Por lo tanto, se generan costos que pueden afectar la reputación, viabilidad y nombre de la empresa.

Un ataque cibernético no solo afecta la empresa objetivo del ataque, sino que, en el corto y largo plazo, las secuelas las experimentarán también sus proveedores y socios, con lo cual se convierte en un efecto multiplicador negativo que afecta la economía en general, especialmente, cuando se trata de varias empresas. Los ataques cibernéticos no conocen fronteras por lo que pueden afectar empresas de cualquier país, cualquier continente, virtualmente en todo el mundo. A continuación, se detalla tanto el panorama del ámbito internacional y el costarricense.

4.1.1 Ámbito internacional

Debido al incremento de ataques cibernéticos mundiales, se están haciendo grandes esfuerzos para mejorar los procedimientos, técnicas y reglas a favor de la ciberseguridad. Dichos esfuerzos se realizan bajo el auspicio de instituciones preocupadas por el rumbo que están tomando las amenazas y ataques. Según el Fondo Carnegie para la Paz Internacional junto con el Foro Económico Mundial (2020), trabajan en el desarrollo de "la nueva estrategia para ciberseguridad y el sistema mundial internacional (2021-2024)", donde se recomiendan medidas concretas para reducir la fragmentación, se promueve la colaboración internacional entre organismos de distintos gobiernos, empresas financieras y tecnológicas, y, de esta forma, se llegaría a proteger más eficazmente el sistema financiero mundial de las ciber amenazas.

Por su parte el Consejo de Seguridad de la ONU celebró este año 2021 su primera reunión de ciberseguridad, en la cual hubo grandes diferencias entre dos bloques de potencias, uno conformado por Estados Unidos de Norteamérica y sus aliados y el otro por Rusia y China. Esta división obedece a que la mayoría de ataques se les achaca a estos dos países mientras los mismos alegan que la formulación y propuesta de leyes siempre gira a favor de los intereses de Occidente y se posicionan muy lejos de una conciliación y una coalición mundial que permita ser equitativa en la cooperación internacional.

Según las Naciones Unidas (junio, 2021), el tema a tratar es de suma importancia debido a que es un problema mundial que va a crear cada vez más peligros y abrir la puerta a nuevos tipos de conflictos. Esta problemática no es fácil de entender o de tratar ni tampoco de solucionar, ya que se aleja de las amenazas causadas por equipo bélico, es decir, del tipo de problemas con que tradicionalmente la ONU ha tratado desde el primer día de su fundación. La dificultad reside en que este enemigo no se ve, es nuevo, sigiloso, muta con el tiempo y causa grandes estragos.

También, se debe señalar que cada país tiene su propia visión de cómo se debe tratar este tipo de problemas, especialmente porque dependen de la cantidad y administración de diversos tipos de infraestructuras tecnológicas, presupuestos y, en especial, de la cantidad de profesionales entrenados y capacitados en el campo de la ciberseguridad. En este sentido, actualmente, hay una gran brecha que deben enfrentar muchos países como los que están en vías de desarrollo, pero, al igual que los demás, corren grandes riesgos debido a que cuentan con

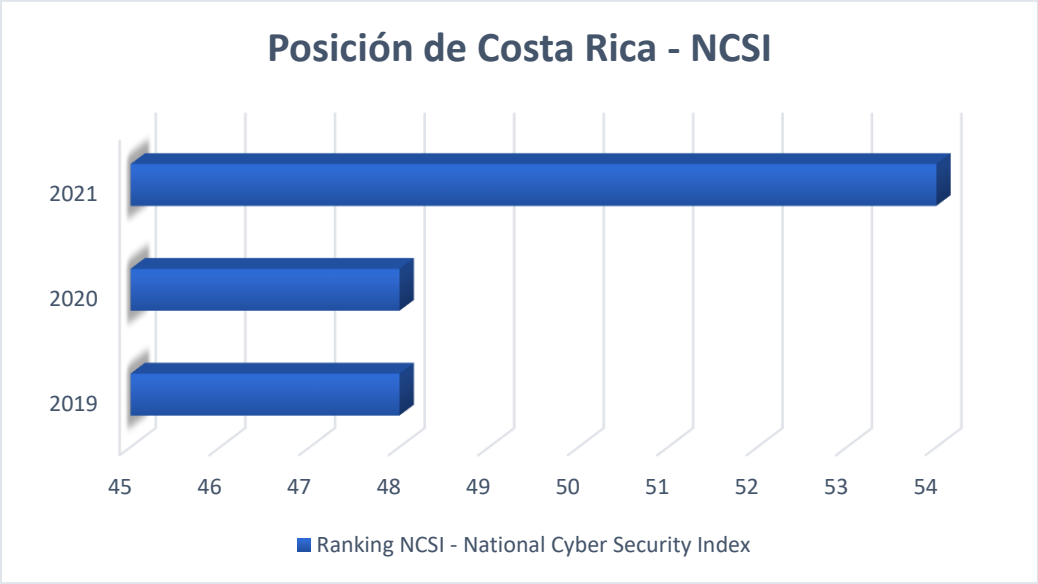
bancos, financieras y entidades gubernamentales que manejan cantidades de dinero que siempre son altamente atrayentes para potenciales ataques. Los países deben evitar que sigan ocurriendo ataques cibernéticos sistemáticos que son incidentes de grandes proporciones y que provocan costos directos significativos; los cuales generan pérdidas comerciales devastadoras. Además, gracias a la habilidad de propagación de este tipo de ataques, se puede generar una crisis financiera sin precedentes que afectaría el funcionamiento de algoritmos encargados de transacciones financieras.

4.1.2 Ámbito nacional

Costa Rica ha presentado en los últimos años un desarrollo tecnológico alto gracias a las inversiones hechas en el país por diferentes multinacionales usualmente localizadas en las llamadas zonas francas, las cuales han permitido reclutar talento nacional que se ha desarrollado en diversas áreas del conocimiento. Este desarrollo trae consigo responsabilidades nunca antes vistas y una de ellas es incrementar la ciberseguridad en territorio nacional, no solo por el bien de todos los costarricenses, sino también por la imagen que esta gran variedad de empresas y sus países de origen tienen de Costa Rica.

Si bien es cierto, nuestro país debe trabajar mucho en esta área, tiene una gran oportunidad para desarrollarse hasta poder llegar a ser un centro tecnológico en el área que le permita ser líder en el tema de la ciberseguridad. Por ello, en septiembre del año 2019 Costa Rica se integró al Índice de Ciberseguridad Nacional de Estonia (NCSI) por sus siglas en inglés, que sirve para medir el índice global y la preparación de los países ante incidentes cibernéticos, desarrollado por el e-Governance Academy de ese país y que, año tras año, brinda un reporte de los países y la región. Según el NCSI (2021), a pesar de que, en medio de la pandemia del COVID-19, el país llegó a estar en la posición 48, se descendió y, actualmente, está en la posición 54 al momento de la recopilación de la información para este estudio.

Grafico 1. Posición de Costa Rica según NCSI 2021



Fuente: Índice Nacional de Seguridad Cibernética NCSI (2021).

Grafico 2. Índice Global de Costa Rica 2020

Fuente: ITU Índice Global de Ciberseguridad v4 (2021).

Tabla 2. Puntajes del ITU Índice Global de Ciberseguridad v4, 2021

Posición en el ranking mundial	Puntaje general	Medidas legales	Medidas técnicas	Medida organizativa	Capacidad de desarrollo	Medida cooperativa
76	67.45	17.62	9.14	12.66	12.11	15.93
		88%	45.7%	63.3%	60.55%	79.65%
Nivel de desarrollo		País en desarrollo				
Área(s) de fuerza relativa		Medidas legales				
Área(s) de potencia crecimiento		Medidas técnicas				

Fuente: ITU Índice Global de Ciberseguridad v4 (2021).

4.1.2.1 Cooperación Costa Rica–Israel

Costa Rica e Israel firmaron el pasad

o 20 de mayo del año 2021 un Memorando de Entendimiento para la Cooperación en Ciberseguridad, firmado por la ministra de Ciencia, Tecnología y Telecomunicaciones (MICITT), Sra. Paola Vega Castillo y el Sr. Amir Shalom, representante de la Dirección de Cooperación Internacional de Israel. De acuerdo con el embajador de Israel en Costa Rica, señor Oren Bar El**, expresó que** "es una importante llamada a la acción, al lograr coordinar entre los equipos involucrados, y así iniciar la colaboración lo antes posible. Israel y Costa Rica se encuentran lejos geográficamente, pero es indudable la cercanía en valores, somos democracias, sociedades plurales, pertenecemos a OCDE, compartimos la vocación de mejorar el mundo y amistad histórica. Esta importante firma de cooperación es lograda entre países similares, donde se ofrecen soluciones aplicables a ambos, en innovación tecnológica israelí en favor a la competencia en la que Costa Rica es un referente mundial, el medio ambiente y medidas de economía verde para Israel. El Ciber es un mundo, un futuro lleno de desafíos. Este acuerdo también abrirá camino a posibilidades de cooperación para Costa Rica en un Hub educativo, como lo son las Academias de Ciberseguridad.". Este entendimiento entre ambas naciones abrirá camino a posibilidades de cooperación para Costa Rica en un *centro de operaciones* educativo mediante las academias de ciberseguridad**.**

4.1.2.2 Cooperación Costa Rica–Estonia

Costa Rica y Estonia firmaron el 13 de setiembre del año 2019 un Acuerdo de Cooperación en temas de Gobierno Digital y la Cuarta Revolución Industrial firmado por el Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT) y el Ministerio de Asuntos Económicos y Comunicaciones de la República de Estonia (MICITT, 2019).

4.1.2.3 CINDE Costa Rica–Zonas Francas

CINDE con casi 40 años de operación se conoce como la agencia de promoción de inversiones de Costa Rica y a guiado a más de 330 empresas de alta tecnología para establecerse en el país.

Estas empresas se establecen normalmente en el formato de zona franca generando un 72% de las exportaciones de servicios de alto valor agregado del país (CINDE, 2021).

En 2020, las empresas multinacionales generaron un total de 19.806 nuevos empleos, es decir, 18,4% más que el año 2019. La ganancia neta de empleos fue de 14.709 puestos, que representaron 45% más que en 2019. Las más de 330 empresas multinacionales atraídas por CINDE generaron un acumulado de 134.026 empleos, que representa un crecimiento del 12% más que el año 2019. (COMEX, 2020).

Las multinacionales buscan sin duda alguna posicionarse en el mercado de la mejor manera y en la actualidad es muy importante para las mismas implementar ciberseguridad, automatización y la ciencia de datos en sus tareas diarias para poder disminuir tiempo, costos de ejecución, errores de procesos y prevenir eventuales problemas.

Este tipo de empresas requieren de gerentes que tomen mejores decisiones de la mano de la tecnología para mejorar en aspectos fundamentales como los que se citaron anteriormente permitiendo la generación de mayores ganancias y la disminución de costos.

4.1.2.4 Empresas de Costa Rica–Protección de Datos (GDPR)

Las empresas costarricenses deberán mejorar y crecer en el tema de ciberseguridad, privacidad y manejo de información para garantizar la protección de datos y cumplir con normas como el reglamento general de protección de datos de la Unión Europea (GDPR) por sus siglas en inglés.

GDPR es una regulación de la Unión Europea que busca estandarizar todas las normas que se relacionen con el procesamiento y control de datos personales por toda aquella empresa y autoridad pública. Si bien es una ley perteneciente a la Unión Europea, la misma tiene un impacto directo en las empresas de todo el mundo y Costa Rica no es la excepción si es que

alguna empresa del país procesa o controla datos personales de algún ciudadano de la Unión Europea.

La GDRP protege los datos de los ciudadanos de la Unión Europea. Esto significa que, independientemente de dónde se encuentre una empresa, si procesa o controla datos que pertenecen a ciudadanos de la Unión Europea, debe hacerlo de acuerdo con la nueva regulación. Si no cumple con la regulación, está sujeto a multas de la misma manera que las empresas que se encuentran en la Unión Europea.

Empresas costarricenses pertenecientes a los sectores turístico, agricultura, salud, educación, banca y finanzas, comercio electrónico, mercadeo digital y desarrollo de software son las que comúnmente pueden tener relaciones o nexos con ciudadanos europeos y deberán acatar lo que solicita la Unión Europea si desean seguir manteniendo relaciones de negocios de lo contrario se expondrán a sanciones corporativas.

Para asegurarse de que las empresas tomen las medidas necesarias para cumplir con la norma GDPR, la regulación determina que las empresas que no cumplan con ella pueden recibir una multa de hasta el 4% de sus ventas mundiales anuales o de 20 millones de euros, la opción que sea mayor se encuentre o no en territorio de UE. En caso de que una empresa costarricense sufra un ataque cibernético, perdida de activos tangibles como lo es un servidor, disco duro o intangible como un programa, una base de datos, etc., donde se encuentre información de algún ciudadano de la UE, debe de informar las violaciones de datos y la pérdida de datos personales a la autoridad competente, dentro de las 72 horas siguientes al evento para evitar sanciones. Todo esto indica que la empresa nacional independientemente del sector en el que se encuentre si aspira a tener relaciones comerciales con la UE o ya las tiene deberá implementar las medidas necesarias que le permitan no solo comprender las reglas de la norma sino también poder implementarlas y así poder llegar a establecer las relaciones comerciales o mantenerlas sin incurrir en multas que le repararía perdidas económicas a corto y largo plazo e incluso le llegarían a prohibir totalmente continuar en operaciones con la UE, por lo que es importante que los gerentes actuales conozcan de este tipo de normas y sus implicaciones ya que otras naciones están adoptando modelos parecidos como es el caso de Canadá y para que Costa Rica siga progresando deberá estar al día con este tipo de marcos de seguridad a nivel empresarial.

4.1.3 Ámbito legal costarricense

Es importante para toda persona, y con más razón para una empresa, conocer las obligaciones y responsabilidades legales de acuerdo con la jurisprudencia local; sobre esto, el área de la ciberseguridad no es la excepción. El país viene haciendo una serie de reformas legales para poder ajustarse a los problemas y necesidades actuales con el fin de brindar la ayuda que se requiera en caso de que un individuo o empresa sufra un ataque de esta índole. En este tema, la asesoría legal es de suma importancia, por lo que no se debe descartar la asistencia técnica legal.

4.1.3.1 Código Penal Costarricense sobre Delitos Informáticos

De acuerdo al Sistema Costarricense de Información Jurídica (SCIJ, 01 de setiembre de 2021), adición de los artículos 196 BIS, 217 BIS y 229 BIS al Código Penal, Ley N° 4573 para reprimir y sancionar los delitos informáticos 8148, en nuestro país el inicio del registro de delitos informáticos fue a partir del año 2001 con la promulgación de la Ley 8148, en la cual se adicionan al Código Penal, los artículos de Violación de Comunicaciones Electrónicas (196 bis), Fraude Informático (217 bis) y Alteración de datos y sabotaje informático (229 bis). En el año 2012, se promulgó la Ley No. 9048, denominada “Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal”, la cual vino a modificar los artículos 167, 196, 196 bis, 214, 217 bis, 229 bis y 288 del Código Penal. Los cambios se dieron principalmente en el aumento de las penas y se incluyeron conductas relacionadas con el uso de redes sociales, medios informáticos, entre otros. Por otra parte, se adicionó un inciso 6) al Artículo 229, correspondiente al “Daño Agravado”, ubicado en el Título correspondiente a los “Delitos contra la propiedad”, donde también se incorpora, un artículo 229 ter, correspondiente al “Sabotaje Informático”. En la actualidad, el Código Penal tuvo una reforma muy importante sobre delitos informáticos, específicamente en las leyes No. 9048 y No. 9135.

4.1.3.1.1 Ley No. 8148

La legislación informática de la Ley No. 8148 reforma el Código Penal (Ley 4573) para reprimir y sancionar los delitos informáticos del 24 de octubre de 2001 habla sobre los delitos informáticos que se incluyeron por medio de los siguientes artículos: el artículo 196º bis., violación de comunicaciones electrónicas, artículo 217º bis., fraude informático y el artículo 229º bis, alteración de datos y sabotaje informático.

4.1.3.1.2 Ley No. 9048

La Ley No. 9048 del 7 de junio de 2012. Reforma varios artículos y modificación de la Sección VIII, denominada delitos informáticos y conexos, del Título VII del Código Penal incluye la reforma de los artículos 167, 196, 196 bis, 214, 217 bis, 229 bis y 288 de la Ley No. 4573 para reprimir y sancionar diversos tipos de delitos informáticos como la violación de correspondencia, violación de datos personales, estafa informática, sabotaje informático, espionaje informático, instalación de programas maliciosos, difusión de información falsa y suplantación de páginas electrónicas.

4.1.3.1.3 Ley No. 9135

Por medio de la Ley No. 9135, la Asamblea Legislativa de la Republica de Costa Rica decreta una reforma en la que se hacen cambios a artículos relacionados con violación de correspondencia o comunicaciones; violación de datos personales; suplantación de identidad; revelación de secretos de Estado; espionaje; seducción o encuentro con menores por medios electrónicos.

4.1.3.1.4 Proyecto de Ley No. 21187: para combatir la ciberdelincuencia en Costa Rica

Este proyecto nace a raíz de la necesidad de reforzar el compromiso que adquirió Costa Rica al haberse ratificado el convenio Europeo sobre ciberdelincuencia. La importancia del proyecto es la proteccion de la libertad de expresión y proteger al país de los ataques más conocidos según fuentes reconocidas de la industria.

4.1.4 Denuncias informáticas en Costa Rica

En este país, el Organismo de Investigación Judicial (OIJ) cuenta con una unidad dedicada a investigar crímenes cibernéticos. De acuerdo con el OIJ (2021), la sección especializada contra el cibercrimen fue creada en 1997, por la necesidad de procesar información contenida en computadoras y servidores decomisados en casos importantes. Se realizan investigaciones de Delitos Informáticos y de otros delitos donde la informática es utilizada para el acto delictivo o como medio de prueba.

> En el 2004 se constituye como Sección de Delitos Informáticos. Se utilizan técnicas de Computación Forense, en la recolección, preservación y análisis de indicios para garantizar la cadena de custodia de los indicios en computadoras, discos duros, llaves USB, dispositivos móviles, entre otros dispositivos de procesamiento y almacenamiento de datos (párrs. 1-2).

Como parte de la indagatoria de esta investigación se solicitó al OIJ un informe incluido en los anexos de este documento, el cual indica que el año en el que más se reportaron delitos cibernéticos fue durante el 2019 con un total de 1208 denuncias, pero a setiembre del 2021 se contabilizaban un total de 927. Con ello, se proyecta que, al finalizar el año 2021, se superarán los registros de denuncias. Además, dicho informe revela que de los últimos cuatro años la mayoría de las denuncias provienen de la provincia de San José con un total de 2307 para el periodo del 2018 hasta el mes de setiembre del 2021; mientras que la provincia que genera la menor cantidad de denuncias es la de Guanacaste con un total de 147. La información de dicho informe también nos indica que el delito que más reportan los costarricenses es el de suplantación de identidad. En la pagina del OIJ se indica que

> Para interponer una denuncia de cualquier tipo, la persona denunciante u ofendida, debe de presentarse ante una de las oficinas del Organismo de Investigación Judicial, dispuestas a lo largo del país, en el enlace a continuación se puede observar un video oficial sobre el proceso de recepción de denuncias (párr. X).

La página web indica que se puede interponer una denuncia llamando al teléfono (506) 2295-4130. Cabe recalcar que las estadísticas brindadas solo representan los ataques cibernéticos que fueron denunciados. Sin embargo, lamentablemente, la gran mayoría nunca se reporta, ya sea por miedo a represalias, vergüenza de lo ocurrido u otra razón. Lo anterior aplica en los casos en los que el afectado es un individuo, pero en el caso de una empresa, típicamente, no se denuncia por el tema de la confidencialidad, reputación y evitar la irrupción de recolección de información.

4.1.5 Ámbito gerencial

Es de suma importancia que las empresas comprendan que significa el riesgo no solo financiero, de inversión o de decisiones administrativas. El riesgo cibernético es muy importante hoy y comprender el grado de riesgo que implica un ataque cibernético, aunque nunca se haya tratado de medir en el pasado, es una práctica sana y recomendada que se debe hacer continuamente para evaluar y, al mismo tiempo, evitar el riesgo. La gestión de riesgos afecta positivamente la generación de ingresos y el impacto en el EBITDA por sus siglas en inglés (Earnings Before Interest, Taxes, Depreciation, and Amortization) es inminente.

El EBITDA es el indicador que nos muestra el beneficio antes de restar los intereses que se deben pagar por deuda contraída, impuestos y depreciaciones.

4.1.5.1 Gestión del riesgo

La gestión de riesgos es el mecanismo que permite identificar, evaluar y controlar las amenazas al capital y las ganancias de una organización. Las fuentes de riesgo son muy variadas y pueden incluir temas que implícitamente se involucran con otras disciplinas. La gestión de riesgos exitoso meticulosamente debe examinar la relación entre los diferentes tipos que hayan identificado durante un periodo dado con respecto al impacto que podría llegar a tener en los objetivos estratégicos de la empresa. Es necesario que administrativamente se cuantifique el riesgo para que, tanto a la alta gerencia como a los departamentos contable–financiero, les quede claro el escenario de cuánto le puede costar a la empresa un ataque y cuánta ganancia se obtiene con medidas y controles que identifiquen, mitiguen, solucionen y detengan posibles ataques.

4.1.5.2 El mayor riesgo del siglo XXI: el cibernético

Es el riesgo que se cuantifica a partir del análisis de probabilidad de pérdida en un período de tiempo determinado, a su vez, dicho análisis incluye una serie de variables necesarias como las incertidumbres financieras, las responsabilidades legales, los desastres naturales, la negligencia, los errores de gestión, los accidentes y el error humano entre otros. El riesgo

cibernético debe gestionarse de forma objetiva para medir correctamente los eventos que conducen a una adecuada o mala gestión del riesgo.

4.1.5.3 Intangible, mas no imposible: cuantificando los riesgos cibernéticos

Es difícil estimar con exactitud los riesgos cibernéticos especialmente si se trata de empresas privadas debido a la rigurosidad de su confidencialidad. Normalmente dicha información se puede extraer de reportes por parte de empresas especializadas en la materia, consultores expertos en el tema, registros públicos de algún ente gubernamental. Sin embargo, los riesgos siempre van a varias áreas según la actividad de la empresa, ya que eso la puede convertir en un objetivo de alta relevancia comparado a otros como el país o región donde se localiza, estructura tecnológica y equipo de soporte que tenga.

4.1.5.3.1 Método de la matriz de riesgos

Los encargados de la ciberseguridad y de la industria observaron cómo las instituciones financieras realizaban evaluaciones de riesgo para la toma de decisiones por lo que tomaron de ella el uso de la matriz de riesgos o mapa de calor para poder hacer un análisis de amenazas, vulnerabilidades y probabilidad de ocurrencia, mediante la siguiente fórmula:

$$\text{Riesgo} = \text{Amenaza} * \text{Vulnerabilidad}$$

Esta herramienta de gestión del riesgo de la ciberseguridad permite la clasificación de riesgos bajo la relación de probabilidad y consecuencia, con lo cual se determinan los riesgos a los que se enfrentaran las organizaciones. En teoría, este modelo llena el vacío a la hora de cuantificar los riesgos cibernéticos. A continuación, se muestra una representación de ese modelo que se basa en el análisis, criterio y subjetividad de lo que se considere en una escala de valores como un peligro menor, moderado, mayor o crítico.

Tabla 3. Matriz de riesgo cibernético

Casi Seguro	Moderado	Mayor	Crítico	Crítico	Crítico
Moderado	Moderado	Mayor	Mayor	Crítico	Crítico
Posible	Moderado	Moderado	Mayor	Mayor	Crítico
Improbable	Menor	Moderado	Moderado	Mayor	Crítico
Raro	Menor	Menor	Moderado	Moderado	Mayor
	Insignificante	Menor	Moderado	Mayor	Crítico

Fuente: elaboración propia.

La probabilidad de que ocurra un daño puede clasificarse como "Casi Seguro", "Moderado", "Posible", "Improbable" y "Raro". Sin embargo, debe considerarse que las probabilidades muy bajas pueden ser no muy fiables. Con el paso del tiempo, se notó que este modelo no era tan preciso como se creía al menos en el campo de la ciberseguridad. El principal problema es que se basa en la opinión de un experto en la materia o SME (*Subject Matter Expert*) por sus siglas en ingles.

Su experiencia puede basarse en empresas muy pequeñas o grandes, las cuales no se adapten al momento que brinde una asesoría o que conozca de ciertos ataques o vulnerabilidades que puedan ser conocidos, pero no todos los que se requiera. Puede asignar calificaciones idénticas a riesgos cuantitativamente muy diferentes ("compresión de rango"), puede también lidiar con riesgos internos que le sean familiares como los riesgos que una organización puede controlar. Por ejemplo, una organización puede evaluar el riesgo de implementar un antivirus para asegurarse de que las computadoras no estén directamente expuestas a internet. Pero, por otro lado, tanto la organización como el experto no pueden controlar los riesgos externos.

Un ejemplo de riesgo externo son los desastres naturales, normalmente estos podrían afectar los sistemas de la organización. Es decir, hay un sinfín de razones por las que se puedan cometer errores a la hora de adjudicar un valor. Las matrices de riesgo pueden asignar erróneamente calificaciones cualitativas más altas a riesgos cuantitativamente más pequeños.

Se concluye que los riesgos con frecuencias y severidades correlacionadas negativamente pueden ser peores que las calculaciones aleatorias. Es decir, la asignación eficaz de recursos a los valores para reducir el riesgo no puede basarse en las categorías proporcionadas por la matriz de riesgo. Por tanto, el mapa de calor o matriz de riesgo genera entradas y salidas ambiguas. Las categorizaciones de gravedad no se pueden hacer objetivamente para consecuencias inciertas. Las entradas a las matrices de riesgo requieren una interpretación subjetiva, por lo que se pueden obtener calificaciones opuestas en los mismos riesgos cuantitativos.

Estas limitaciones sugieren que las matrices de riesgo deben usarse con precaución y solo con explicaciones cuidadosas de los juicios implícitos. La participación de un mayor número de partes aumenta el impacto de los riesgos, ya que cada parte tiene diferentes objetivos. Es posible que las técnicas convencionales de gestión de riesgos no sean la solución para los riesgos de múltiples partes.

La mayoría de las profesionales en el campo de la ciberseguridad utilizan algún tipo de matriz de riesgo, esto puede ser un problema grave debido a que se varía el rango de apreciación de un error. Es decir, se consideran los problemas desde el contexto de otros errores humanos medidos por lo que los errores de los expertos simplemente se ven agravados por la óptica con la que se mida o aprecien los errores variando la asignación brindada a las escalas y matrices mismas.

Actualmente este es el modelo mayormente utilizado en las empresas para, no solo medir el riesgo cibernético y tener un monto total, sino también individualmente para conocer cuáles son los riesgos que componen la estructura de riesgos y sus costos individuales. La gran duda no solo es qué tan preciso es el modelo en términos de seguridad, sino también en el económico, ya que se considera que no le da al departamento financiero información veraz para asignar un presupuesto que se destine a la seguridad de la empresa en general.

4.1.5.3.2 Manejo de riesgos

El manejo de los riesgos va a variar según la experiencia y apreciación de los expertos involucrados, ya que puede haber riesgos que se acepten siempre y cuando no se tome ninguna acción contra el riesgo que se llegue a identificar y aceptarlo tal como es, ya que, a juicio de los

involucrados, no causara mayor problema. Para que una empresa consiga gestionar con éxito cada riesgo, manejarlo y tomar decisiones que, para algunos pueden ser drásticas, y hacerlo con las condiciones adecuadas se debe revisar, analizar y utilizar normas reconocidas internacionalmente como el ISO 31000:2018 o el ISO/IEC 27005:2001 debido a que ellas ofrecen un marco de referencia para el estudio, identificación y mitigación de los riesgos de ciberseguridad.

Estos marcos de trabajo dictan que, para determinar los riesgos, se debe establecer cuál es el alcance sobre la base de los procesos y objetivos del negocio, ya que siempre será esencial trabajar alineados con ellos. Una vez que se haya fijado y determinado el alcance y los objetivos, la empresa procede a realizar un inventario de sus activos tanto físicos como equipo de *hardware*, servidores, *router*, entre otros; como los activos intangibles como el *software*, licencias del sistema operativo Windows, licencia de la base de datos Oracle o de SAP, entre otros para realizar una evaluación de los mismos teniendo en cuenta la confidencialidad, disponibilidad e integridad.

Posteriormente, se ejecuta la detección de las amenazas y de las vulnerabilidades, a partir de eso, se definen los criterios de aceptación de los riesgos en los que se debe calcular cada uno de ellos analizando impacto, probabilidad y posibilidad de ocurrencia. La gestión de riesgos en el campo de la ciberseguridad es esencial, ya que vela por proteger los activos, controles y reglas de la empresa con el objetivo de poner el fin a la actividad que introduce el o los riesgos. Una vez que se detiene el problema se mitiga el riesgo, también puede haber un rechazo al riesgo que básicamente es no tomar ninguna acción para detenerlo y se considera una práctica negligente.

4.1.5.4 Innovar: La llave del éxito empresarial

La empresa costarricense debe innovar más para poder competir con otras industrias, en esto juega un papel clave la investigación. El gerente actual debe comprender que es vital conocer no solo las nuevas tendencias y practicas administrativas sino también que tipo de tecnología están utilizando las empresas.

La combinación del conocimiento es esencial para poder llevar acabo una ruta de vida para la compañía donde se determine como modernizarla sin incurrir en grandes gastos y

verificar que esto permita generar una mejor reputación, mejores prácticas y mejores procesos que deberán permitir mayores ganancias, ventas, etc.

Por medio de la innovación se pueden cumplir diferentes metas que desde el punto de vista administrativo a veces no se contemplan pero que hoy en día es necesario en un mercado cada vez mas exigente ya que no es solo local sino también internacional.

Al innovar podemos cumplir con normas internacionales que le permitirán a la compañía incurrir en nuevos mercados o asegurar su permanencia, ahorrar tiempo en las diversas actividades y ahorrar en costos, proyectando una mejora en un tiempo determinado según la industria en la que se encuentre.

El buen manejo y control de los costos permitirá que el tipo de innovación que se vaya a utilizar o desarrollar cumpla con los objetivos propuestos por la empresa.

De acuerdo con los datos que tanto CINDE como COMEX brindan en cuanto a cantidad de puestos generados y actividad a la que se dedican las empresas que se establecen en el país, se debe de innovar utilizando la ciberseguridad, la automatización y la ciencia de datos para que la empresa nacional también este a la altura y nivel de las multinacionales, esto generara más confianza en el inversor y sin duda alguna generar mejores ganancias para la industria o empresa nacional

4.1.5.5 Disminución de Gastos: Ahorrar en tiempo de crisis

Actualmente la empresa nacional debe de cumplir con normas internacionales que contemplan la protección y buen uso de los datos, ser capaz de informar si una fuga o pérdida de dichos datos se produce y al mismo tiempo se le solicita acortar gastos en tiempos de crisis donde la pandemia del Covid-19 a afectado a las empresas en general.

Para poder cumplir con los objetivos que se requieren para modernizar la empresa y al mismo tiempo cumplir con los diversos requerimientos es muy importante que a nivel gerencial se considere el desarrollo e implementación de la hoja de ruta empresarial a la sociedad 4.0 y así poder cumplir con los diversos objetivos ya que será esencial para continuar y mantener las operaciones.

Hay muchas formas de disminuir gastos, pero específicamente para industrias prominentes en Costa Rica como son la turística, agricultura, tecnológica y la de servicios abre

las puertas para que los gerentes se interesen más en utilizar plataformas de código abierto para agilizar ciertos procesos sin incurrir en gastos extras y evitando al mismo tiempo potenciales problemas que harían a la empresa en incurrir en cuantiosas pérdidas

4.1.6 Ámbito de la gestión del talento humano

El departamento de la gestión del talento humano se preocupa por captar el personal más capacitado, crear un ambiente laboral idóneo y velar por las necesidades no solo de los integrantes de la línea gerencial, sino también de aquellos en los que recaen las responsabilidades operativas. Sin embargo, la mayoría de las empresas no sabe que el punto más débil de la seguridad de una empresa es el colaborador y es a quien se le debe analizar bajo el prisma de nuevos elementos, los cuales son la tecnología y la ciberseguridad. Esto difiere mucho de lo que se hacía tradicionalmente, y es que hoy por hoy es cuando más se necesitan empleados que comprendan los riesgos y amenazas de la empresa moderna de la sociedad 4.0

De nada vale contratar, por ejemplo, a un gerente de seguridad de la información con basta experiencia, contar con analistas cibernéticos e, inclusive, comprar equipo tecnológico que respalde sus acciones si los empleados en general no conocen sobre ciberseguridad, no reciben capacitación alguna y, peor aun, no son consientes de la importancia que tienen dentro de la misma empresa para lograr implementar con éxito un programa de ciberseguridad. El activo más importante es y deberá siempre ser el colaborador. Su importancia no solo radica en que es el encargado de generar ventas, de innovar o atender al cliente; también es quien, al final de cuentas, es quien tiene acceso a la tecnología, los equipos, la información e, inclusive, a la comunicación con los clientes. Por ende, el empleado se convierte en esa mano que puede abrir una puerta que podría ser la causa del ingreso de vulnerabilidades.

4.1.6.1 La mayor amenaza no es una maquina, más bien, es humana

El ser humano es capaz de conectar un dispositivo de almacenamiento portatil, llámese llave USB, disco duro externo o, simplemente, una memoria flash al computador de la empresa para ver su contenido, aunque se haya encontrado el dispositivo tirado o desatendido tan solo unos instantes atrás, sin sospechar que puede contener algún virus o un programa malicioso lo

que no solo le causaría daño a quien lo ingresó y utilizó, sino también a la empresa en general. Lamentablemente, muchas organizaciones están pasando por alto el aspecto más importante de la integridad de la seguridad dentro de una organización: sus empleados. ¿Por qué los colaboradores son la mayor amenaza de ciberseguridad y qué se debe hacer al respecto? Porque los hackers o piratas informáticos se aprovechan de diversos factores psicológicos que influyen con las personas, que, al verse inmersos en un ambiente laboral lleno de reglas, en algún momento, bajarán la guardia y cometerán errores que, con las herramientas adecuadas, será el equivalente a entregar las llaves de la puerta que conduce a información confidencial, malas prácticas, secretos industriales, entre otros. Esos errores varían desde perder el celular de la empresa sin utilizar el doble factor de autenticación, es decir contraseña y huella a generar, o utilizar contraseñas muy débiles y fáciles de adivinar.

4.1.6.2 El oscuro arte de la persuasión

La persuasión es la base de la ingeniería social que, a su vez, es un método muy eficaz para obtener información de empresas, grupos, personas e, inclusive, sistemas informáticos a través de medios no técnicos. Si bien es cierto que muchas empresas víctimas de los cibercriminales cuentan con una seguridad en los sistemas muy alta, los mismos siguen siendo vulnerables a medios empleados por los *hackers* como la ingeniería social. Se debe comprender que la ingeniería social es una técnica que no requiere del uso o comprensión de herramientas técnicas, esto permite que cualquier persona pueda emplearla y requiere de mucha confidencia por parte de su ejecutor para engañar a otros al hacerse pasar por alguien que no es, mostrar que sabe algo que se conoce o pertenecer a algo de lo que no se es parte.

Según análisis hechos por expertos en la materia, la mayoría de las empresas gastan en presupuesto de ciberseguridad en la contratación de servicios, compra de equipo y en diagnósticos. Sin embargo, olvidan que sus colaboradores son el punto débil y que mediante la persuasión pueden develar secretos que permitirán que los ciberdelincuentes tomen control de la infraestructura tecnológica de la empresa. Son realmente escasos lo enfoques que consideran la explotación de colaborador a través de la ingeniería social y tratan de reforzar ese punto tan vital. A pesar de que está más que comprobado que los ataques de ingeniería social aumentan año tras año, lamentablemente la conciencia sobre el rol fundamental que tiene el empleado sobre la

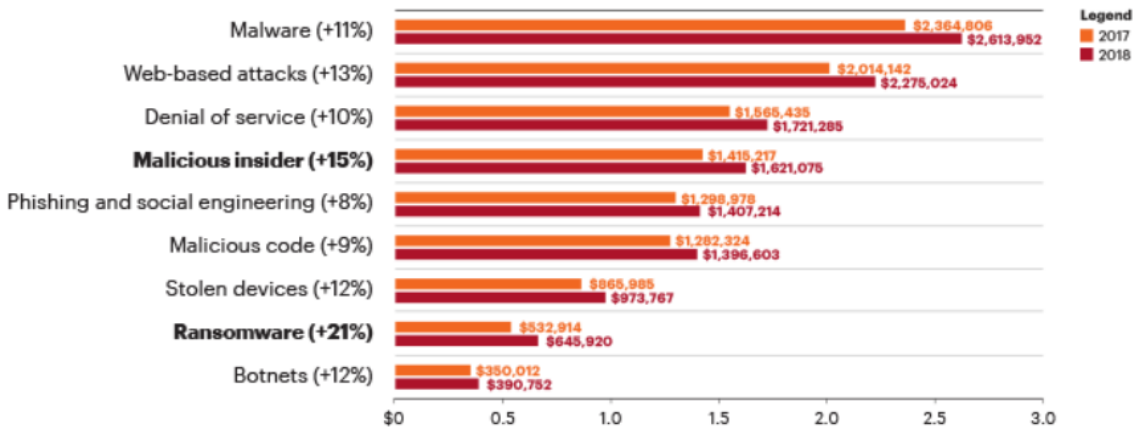
seguridad y cómo evitar este tipo de ataques ya sea abriendo correos o documentos de extraña procedencia, generar y usar contraseñas relacionadas a temas de interés, familiares, gustos personales que sean muy fácil de deducir por parte del atacante, provoca que este tipo de prácticas riesgosas aún sea común. Psicológicamente, la ingeniería social llega a dominar la persuasión en grados aplicables únicos donde mostrar actitud y tener confidencia influyen sin duda alguna en la toma de decisiones de quien llega a ser el objetivo, quien llega a sucumbir ante el engaño que puede darse bajo circunstancias y formas inesperadas.

4.1.6.3 El rostro de un punto sin retorno

La naturaleza de muchas personas es inclinarse a ayudar a quien lo requiera y, en especial, si el que requiere la ayuda demuestra estar en una situación de desventaja, peligro o gran necesidad. Esta premisa se hace cierta especialmente si a simple vista nos da la impresión de que lo que se requiere o lo que se nos pide no es dañino o demande gran cosa de nuestra parte según nuestro propio juicio o criterio. Pero la verdad es que existen reglas y estatutos que las empresas se esfuerzan por crear y establecer, pero que no necesariamente logran su cometido y es lograr que, efectivamente, los colaboradores lleguen a cumplir los lineamientos establecidos. En escenarios menos afortunados, las empresas no poseen dichos reglamentos.

Ya sea por una razón u otra, según estudios en la materia como el que se muestra en el Grafico 3 de Cyber insights, demuestra que siempre hay alguien que no cumple con las normas y provoca, en muchos casos, problemas no esperados de un punto sin retorno, cuyo rostro es el engaño. Ejemplos típicos de engaños son darle acceso a alguien que no estamos seguros si realmente pertenece, o no, a la empresa, si es, o no, del departamento de cómputo, si la información requerida es confidencial, o no, si el remitente del correo electrónico es, o no, correcto. El engaño es tan poderoso que, en la ingeniería social, ha logrado tener como víctimas desde colaboradores de puestos operativos hasta altos ejecutivos de grandes corporaciones, quienes, a causa de ello, terminan perdiendo su empleo. A continuación, podemos ver la tabla de ataques mas comunes.

Gráfico 3. Lista de ataque reconocidos a empresas



Fuente: Accenture (2018).

4.1.6.4 El nuevo lema: entrenamiento, entrenamiento, entrenamiento

La capacitación es fundamental para fortalecer el conocimiento de los colaboradores, analizar sus áreas de mejora y sus fortalezas. Por tanto, se puede afirmar que la formación del campo de la ciberseguridad debe estar presente en todas las operaciones de la organización porque, sin importar el puesto que se ejerza, está confirmado que nadie está exento de ser engañado por delincuentes cibernéticos.

Si no existe un programa de inducción dirigido por el equipo de recursos humanos es vital crearlo y/o fortalecerlo. Este programa se debe ofrecer junto al el equipo de tecnología de la información; se puede crear una capacitación en seguridad en la que se explique cómo proteger la información. Dicha información, que debe ser protegida, incluye documentos financieros, reportes de compras o ventas, resultados de estrategias de mercadeo. Por otro lado, también se debe proteger los activos tecnológicos físicos como computadoras de escritorio, computadoras portátiles, tabletas, celulares, los cuales deben guardarse en lugares seguros y estar bloqueados

en caso de que el usuario se retire por alguna razón. Finalmente, deben cuidarse los activos intangibles como el *software* para que se bajen solo programas autorizados por la empresa y no de páginas o lugares no aprobados o testeados por la empresa. Por tanto, el departamento de la gestión del talento humano puede utilizar diferentes tipos de métodos de formación, algunos de los métodos de capacitación clave son:

4.1.6.5 Tipos de entrenamiento

La capacitación es fundamental para fortalecer el conocimiento de los colaboradores, analizar sus áreas de mejora y sus fortalezas. Por tanto, se puede afirmar que la formación en el campo de la ciberseguridad debe estar presente en todas las operaciones para todos los colaboradores de la organización, ya que sin importar el puesto que ejerza debe evitar ser víctima del engaño que pueda intentar un delincuente cibernético.

Actualmente existen diversos tipos de entrenamiento ajustados para diferentes tipos de organización, de puestos y de colaboradores. Uno de los objetivos del entrenamiento es que este no se considere como una carga, sino más bien como algo positivo que no solo les será útil en el trabajo, sino también en sus vidas cotidianas gracias a que la tecnología está al alcance de la mayoría de las personas.

4.1.6.5.1 De vuelta a los juegos: gamificación

La gamificación es una técnica de aprendizaje que se cataloga como uno de los últimos métodos de entrenamiento. Actualmente, tiene un uso difundido, ya que logra trasladar la mecánica de un juego común y corriente al ámbito educativo-profesional. En este tipo de

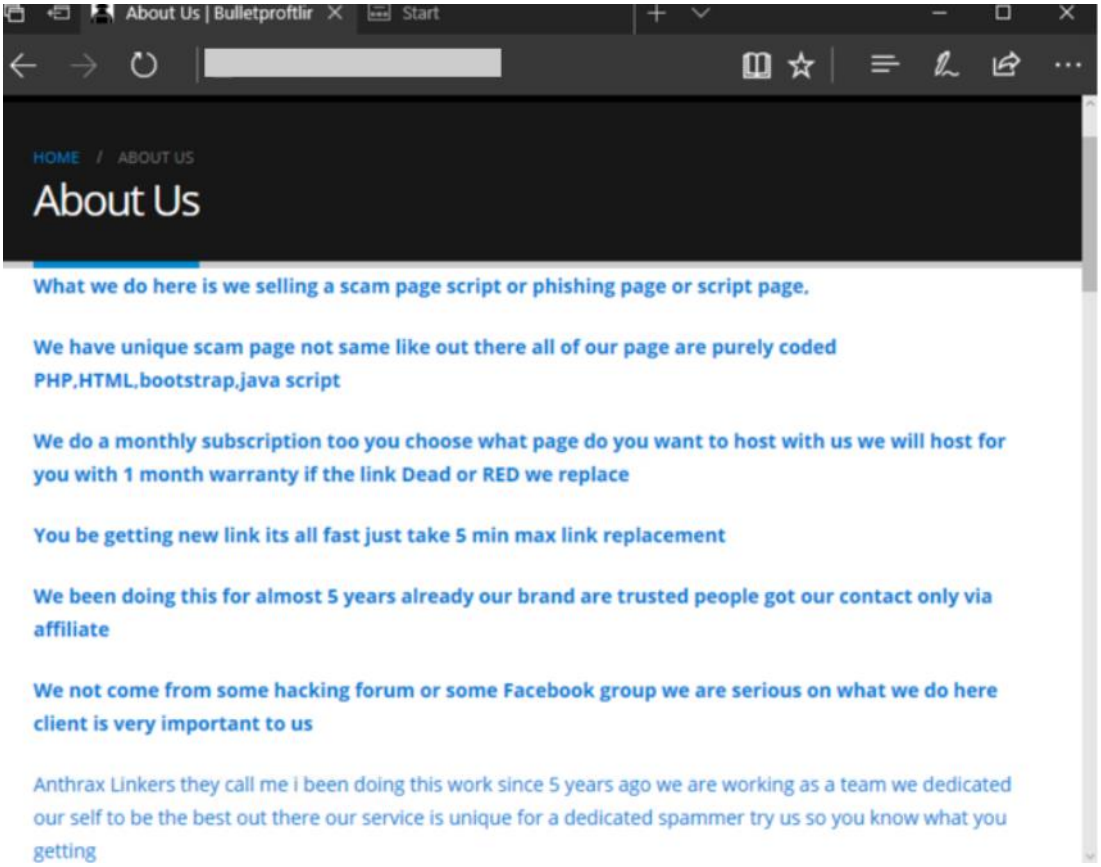
formación se debe responder algunas preguntas en función del rendimiento que se vaya obteniendo en el entrenamiento con el fin de conseguir mejores resultados, ya sea para confirmar que se obtuvo el conocimiento, mejorar alguna habilidad o, bien, recompensar acciones concretas, entre otros muchos objetivos. Se puede utilizar para hacer énfasis en temas de mucha importancia sobre seguridad como los accesos, el uso correcto de contraseñas, la protección del equipo, identificar que es una amenaza cibernética, como reportar un ataque cibernético, entre otros.

4.1.6.5.2 Es la hora de *phishing*

Gracias a los resultados de los últimos estudios sobre los ataques más comunes las organizaciones comenzaron a probar la postura de seguridad de sus usuarios al realizar entrenamientos y campañas de *phishing*. Esto consiste en enviar un correo electrónico de falso a los empleados internos, los cuales pretenden ser reales emulando la dirección o el nombre de una empresa reconocida o de una que aparente que sí existe y, usualmente, muestra un enlace engañoso para que el colaborador lo utilice. Una vez que algún colaborador le haga clic, puede ser llevados a una página web en la que se le pedirá que ingrese su usuario y contraseña; automáticamente se le mostrara un mensaje que indique que debe realizar un entrenamiento para que pueda entender en que parte falló y porque es peligroso caer en un engaño de este tipo.

En el 2021 la empresa Microsoft descubrió una empresa fraudulenta llamada BulletProoflink la cual se dedicaba al *phishing* como servicio o (PhaaS – Phishing as a service) por sus siglas en inglés. La empresa vendía plantillas web y plantillas de correo listas para ser usadas o enviadas con el único fin de engañar y estafar otras empresas. Gracias a la empresa Microsoft, este servicio dejó de funcionar, ya que promovía prácticas ilegales penadas por la ley, las cuales potencialmente no solo afectan a empresas, sino también a los usuarios que compraban sus servicios.

Figura 2. Captura de la página de BulletProoflink



Fuente: Microsoft. (2021). The BulletProof Link's 'About Us' page provides potential customers an overview of their services

4.1.6.5.3 Entrenamiento basado en computadora (CBT–*Computer Base Training*)

Este tipo de entrenamiento o capacitación por computadora es uno de los mas utilizados actualmente; su popularidad no nació durante la pandemia del Covid-19, en realidad ya era y sigue siendo popular. El éxito radica en varias ventajas, la primera es que el colaborador en un rango amplio de tiempo decide cuando llevarlo, por ejemplo, la empresa puede definir que el curso de fundamentos de ciberseguridad para el año 2022 debe completarse entre el 2 de enero del 2022 y el 15 de febrero de ese mismo año, también permite que el usuario pueda comprar otros cursos en línea para una mayor capacitación. Otra de las ventajas es que, gracias a la

edición del video, todas las demostraciones corren a la perfección, se ahorra mucho tiempo y se va al punto en cuanto a las explicaciones. Además, si se presentara la eventualidad de que un tema no haya quedado claro, se puede volver a ver para repasar, ya sea una parte en específico o todo el video, eso queda como alternativa para el colaborador.

4.1.6.5.4 Entrenamiento a la medida

Este tipo de entrenamiento es de suma importancia, ya que la capacitación se puede estructurar según la cantidad de departamentos, número de colaboradores y, en especial, con base en las funciones que desempeñen los usuarios dentro de la organización. En este punto, la capacitación tanto en tecnologías de la información como en ciberseguridad puede aumentar o disminuir según el nivel de complejidad que requiera el puesto del colaborador y, así, poder garantizar que siga los procesos y procedimientos definidos por la empresa para que apoye y guíe a otros en la batalla contra las malas prácticas cibernéticas.

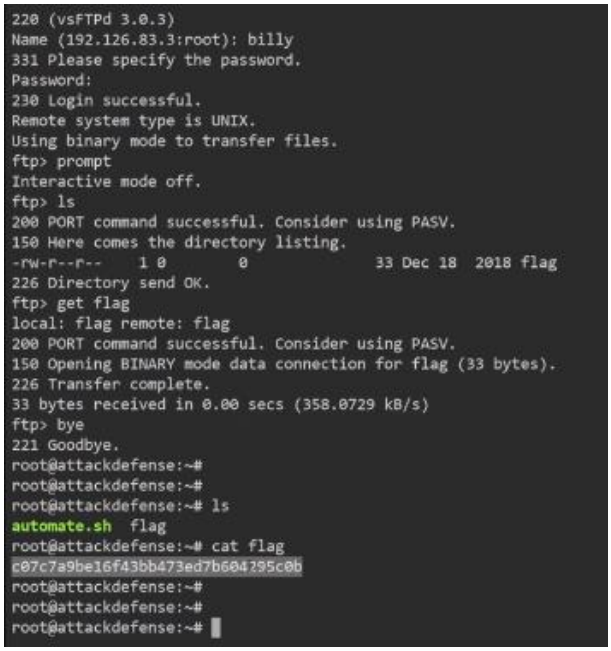
Por tanto, los diferentes tipos de colaboradores y sus puestos dentro de una organización pueden tener diferentes necesidades o grados de formación. Si un colaborador externo que su puesto demanda mucha interacción con clientes, ya sea por llamadas, video conferencias, entre otros, pueda ser que, para esta persona el entrenamiento basado por computadora o CBT sea el ideal para capacitar al usuario. Puede ser que la mejor opción sea una prueba de *phishing* inesperado, pero lo más importante es que la empresa tenga diferentes métodos de capacitación para poder entrenar a sus colaboradores.

4.1.6.5.5 Capturar la bandera (CTF–*Capture The Flag*)

Los entrenamientos no solo deben ser dirigidos a aquellas personas que no tienen conocimiento técnico en el campo de la computación o en el de la ciberseguridad, sino también para aquellos que implícitamente trabajan en él. Es muy recomendable que se lleven acabo entrenamientos de capturar la bandera o CTF. Estos consisten en competencias de seguridad informática en las que todos sus participantes compiten en desafíos con temas de seguridad con el fin de obtener la puntuación más alta. Esto ayuda a simular escenarios reales de como

ciberdelincuentes pueden violentar el ingreso al sistema de una empresa. Utilizar ese tipo de prácticas es importante no solo para reforzar el aprendizaje, sino también para asegurar más eficientemente a la empresa. Cada vez que los participantes logren cumplir con una tarea, "capturan una bandera" para aumentar su puntuación, de ahí el nombre del evento. Las banderas suelen ser numeraciones aleatorias que serán reveladas al participante en los desafíos si logra cumplir con lo requerido.

Figura 3. Captura de la línea aleatoria representación de un evento CTF



Fuente: adaptación de demostración. Autor: attackdefense (2021)

4.1.7 Ámbito de la gerencia de tecnología de la información-GTI

El departamento de tecnología de la información debe trabajar en conjunto con la gerencia general y con el departamento de finanzas y el de gestión del talento humano para informar sobre el estado de la ciberseguridad de la empresa, solicitar equipo que se deba obtener para dicho fin o diseñar un entrenamiento que se requiera. El departamento de tecnología de la información se encarga de desarrollar, probar e implementar una cultura de ciberseguridad en la que sea natural hablar de este tema y no proyectarlo como algo que sea exclusivo de personas que solo trabajan en el área de computación, o algo muy complicado de comprender. Las

empresas que se esfuerzan por implementar una cultura de ciberseguridad han experimentado una gran mejora en esa área hasta un punto en el que se sienten cómodos para investigar potenciales problemas y actualizar sus planes de contingencia según las necesidades que se dan a conocer con base en los ataques actuales.

4.1.7.1 Eliminando fronteras, el trabajo es de todos no solo de TI

Desafortunadamente, en muchas empresas se cree que el trabajo del departamento de tecnología de la información es solo velar por que el equipo, los sistemas y los reportes de todo lo relacionado a los sistemas de cómputo y que estos funcionen según lo esperado tanto por sus colegas como por clientes. Esta apreciación es parcialmente correcta, ya que, si bien es cierto ese era el modelo que se conoció y bajo el que se ha trabajado por años, no necesariamente es el correcto actualmente. Debido a que los ataques cibernéticos son constantes e impredecibles, se requiere que el departamento de tecnología de la información sea mas dinámico y permita la apreciación, ayuda y colaboración de los demás departamentos dentro del organigrama empresarial.

Al respecto, la gran pregunta es ¿por qué se deben eliminar las fronteras departamentales? La respuesta radica en que todo departamento este sujeto a un ataque cibernético y, si no se toman medidas generales que abarque a toda la empresa, medidas especial y estratégicamente diseñadas para un determinado departamento siempre se estará expuesto a las vulnerabilidades cibernéticas. Los ataques son constantes alrededor del mundo y crecen exponencialmente día con día. A continuación, ejemplos en vivo de reportes sobre este tema.

Figura 4. Mapa interactivo con mas de 46 millones de ataques en un solo día

Fuente: Check Point (2021).

Figura 5. Mapa interactivo de ataque por tipo de industria

Fuente: FireEye (2021).

4.1.7.2 SOS: la ayuda internacional siempre es bienvenida

La gran discordancia en el departamento de tecnología de la información fue la bifurcación de ideas o estilos de trabajos por la diferencia de opinión sobre la importancia de diferentes aspectos. De dichas diferencias se fueron analizando y desarrollando políticas, reglas y estatutos laborales para velar por la seguridad de las empresas. En muchos casos, esas normas debieron ser aplaudidas por la comunidad tecnológica en general porque eran no solo fáciles de entender, sino que también eran fáciles de aplicar y ajustables a cualquier tipo de organización. Sin embargo, en otros casos dejaban mucho que desear porque su implementación no era sencilla en otras organizaciones.

El problema es que no siempre el caso anteriormente expuesto fue lo que vivieron la mayoría de las empresas, ya que luego de un ataque cibernético se concluyó que las normas aplicadas solo estaban en papel y, en realidad, no se cumplían debido a su complejidad, falta de interés o falta de conocimiento o experiencia por parte de los encargados del departamento de tecnología de la información. Ante esta evidente problemática, se decidió adoptar marcos de trabajo internacionales desarrollados por un gran numero de expertos en la materia, en los que se pone a disposición no solo del público en general, sino de toda empresa sin importar si es pública o privada. Se trata de una serie de normas vitales para la estructura de una cultura cibernética resiliente y que pueda ser implementada en forma práctica.

4.1.7.2.1 Marco de riesgo cibernético: controles del Centro de seguridad de Internet (CIS)

Este marco de trabajo se desarrolla en el Centro de Seguridad de Internet o CIS (Center for Internet Security), por sus siglas en inglés. El marco de seguridad es prescriptivo y ayuda a gestionar las mejores prácticas en seguridad cibernética y acciones defensivas dentro de una empresa, con lo cual se ayuda a prevenir ataques y cumplir con las normas requeridas. Estas mejoras son un compedio realizado por un grupo de expertos en tecnología de la información en base a ataques reales y métodos comprobados de defensa efectivos. Funcionan como una base preliminar en el reforzamiento de seguridad de cada empresa. Este marco es gestionado y desarrollado por los Controles del Centro de Seguridad de internet o CIS por sus siglas en inglés.

Figura 6. Controles del Centro de Seguridad de Internet (CIS)

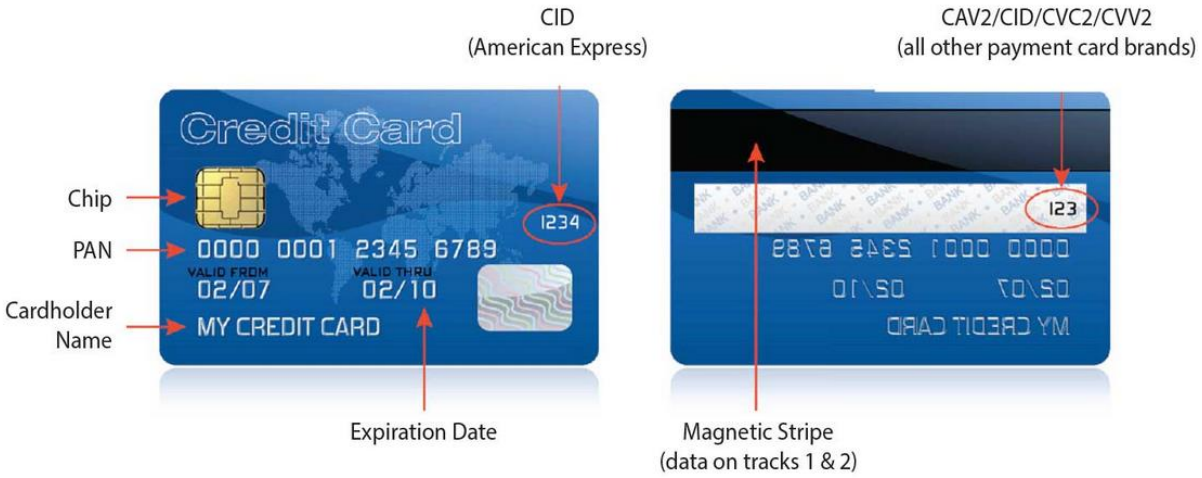
Fuente: SANS. (2021). CIS Controls Version 8. [foto].

4.1.7.2.2 Marco estándar de seguridad de datos: industria de tarjetas de Pago (PCI DSS)

El estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS) es un conjunto de estándares de seguridad recomendado para todas aquellas empresas que realizan transacciones financieras. Esto adquiere una relevancia especial actualmente, ya que la gran mayoría utiliza una página web como herramienta principal en el engranaje de diseño comercial que posee, con ello se garantiza a las empresas que lo aceptan, procesan, almacenan o transmiten información de tarjetas de crédito un entorno seguro. Este marco de trabajo se inicio el 7 de septiembre de 2006 y ha llegado, sin duda alguna, a gestionar la evolución continua de los estándares de seguridad de la Industria de Tarjetas de Pago (PCI) con un enfoque en mejora de la seguridad de las cuentas de pago durante todo el proceso de transacción. PCI DSS es administrado y gestionado por PCI SSC (PCI Security Standards Council 2021). Este es un

organismo independiente creado por las principales marcas de tarjetas de pago (Visa, MasterCard, American Express, Discover y JCB).

Figura 7. Tipos de datos en una tarjeta de pago (PCI DSS)



Fuente: PCI Security Standards Council PCI DSS. (2021). Types of Data on a Payment Card [foto]

.

4.1.7.2.3 Marco de ciberseguridad: (CSF) Instituto Nacional de Tecnologías (NIST)

El marco de ciberseguridad, desarrollado por NIST, es una excelente herramienta que permite elaborar, organizar y mejorar el programa de ciberseguridad que se requiera implementar dentro de una empresa. Este marco de trabajo en el área de ciberseguridad es un conjunto de mejores prácticas para ayudar a las organizaciones a construir y mejorar su postura en temas de ciberseguridad. Asimismo, da recomendaciones y estándares que permiten preparar a las empresas para que puedan identificar y detectar ataques cibernéticos y que sepan recuperarse en caso de un incidente. Fue creado por el Instituto Nacional de Estándares y Tecnología NIST por sus siglas en inglés y vino a llenar el vacío de la falta de estándares de ciberseguridad, por ello ha sido adoptado ampliamente en el ámbito internacional.

Figura 8. Marco de ciberseguridad NIST

Fuente: N. Hanacek/NIST (2018).

4.1.7.2.4 Marco de ataque: MITRE ATT & CK

MITRE ATT & CK son siglas que significan: Tácticas, técnicas y conocimientos comunes contra los adversarios o ATT & CK (Adversarial Tactics, Techniques and Common Knowledge) por sus siglas en inglés. MITRE desarrolló ATT & CK como modelo para documentar y rastrear numerosas técnicas que los atacantes utilizan durante las diferentes etapas de un ciberataque para penetrar en una red y ex filtrar datos. Fue creado en 2013 como resultado del experimento Fort Meade (FMX) de MITRE, en el cual los investigadores emularon el comportamiento tanto del adversario como del defensor en un esfuerzo por mejorar la detección de amenazas. La pregunta clave que llevo a los investigadores a desarrollar este marco de ciberseguridad fue ¿qué tan bien lo estamos haciendo en la detección del comportamiento del adversario documentado? Para responder a esa pregunta, los investigadores desarrollaron ATT & CK, que se utilizó como una herramienta para categorizar el comportamiento del adversario.

Figura 9. Diagrama del Marco de ciberseguridad MITRE ATT & CK

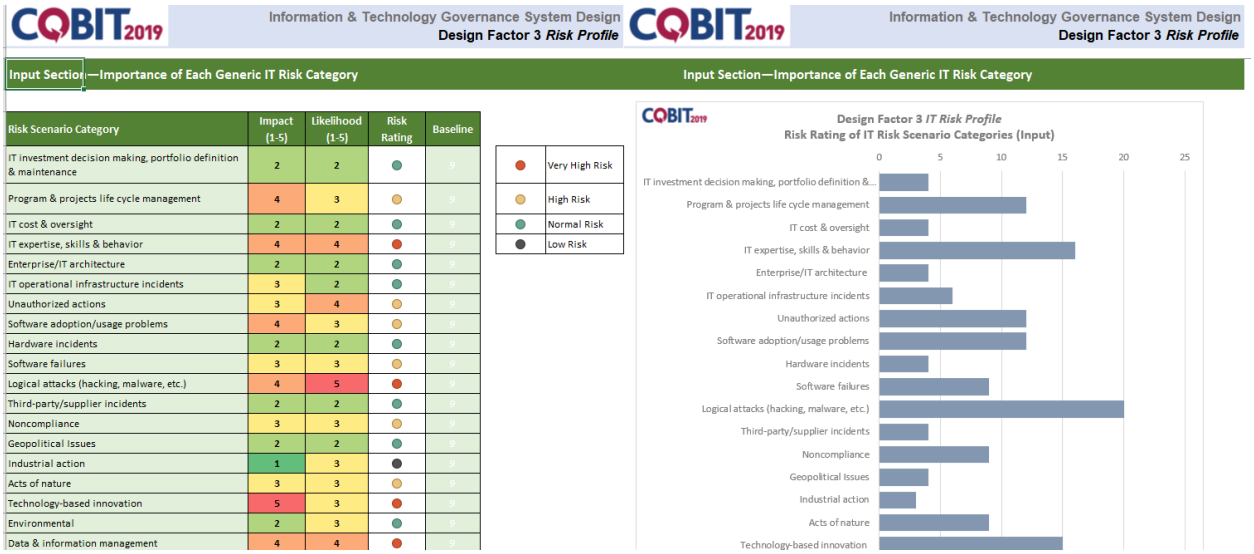
Fuente: MITRE (2021).

4.1.7.2.5 Objetivos de control para tecnologías de la información (COBIT)

COBIT 2019 es un marco de trabajo creado por ISACA-Asociación de Auditoría y Control de Sistemas de Información (Information Systems Audit and Control Association) por sus siglas en inglés, la cual está enfocada en el desarrollo de metodologías y certificaciones para la ejecución de actividades de auditoría y control de sistemas de la información. Es de suma importancia debido a la cultura de controles y normas que establece, los cuales permiten conocer a fondo la situación de la empresa en términos de ciberseguridad y seguridad en general.

Entre sus principales atributos se encuentra que ayuda a alinear los objetivos de la empresa con los del departamento de tecnología de la información. Esta función de puente permite no solo una mejora comunicación entre las partes, sino también una mayor confianza que, a lo largo del tiempo, le hará comprender al personal que ambos objetivos son fundamentales en el buen desarrollo y comportamiento de la empresa en materia de ciberseguridad.

Figura 10. Marco de Trabajo COBIT2019



Fuente: ISACA (2021).

4.1.7.2.6 Oficina Internacional de Normalización (ISO) 27001

Es el estándar internacional para la seguridad de la información ISO (2020) que permite la especificación de un sistema de gestión de seguridad de la información o (SGSI) por sus siglas en inglés. La última versión del estándar de seguridad de la información ISO 27001 se publicó en septiembre de 2013, el cual reemplazó la iteración de 2005. Se enfoca en las mejores prácticas del estándar del sistema de gestión de seguridad de la información, de esta forma, ayuda a las organizaciones a gestionar su seguridad de la información dirigiéndose a las personas, los procesos y la tecnología. La certificación de la norma ISO 27001 es reconocida en todo el mundo como una indicación de que se cumple con las mejores prácticas de seguridad de la información. Como parte de la serie ISO 27000 de estándares de seguridad de la información, se incluye un marco que ayuda a las organizaciones a establecer, implementar, operar, monitorear, revisar, mantener y mejorar continuamente.

4.1.8 Ámbito financiero

El departamento de finanzas o los servicios financieros deben enfrentar muchas amenazas cibernéticas día con día. Debido a la creciente amenaza de fraude, filtración de datos y

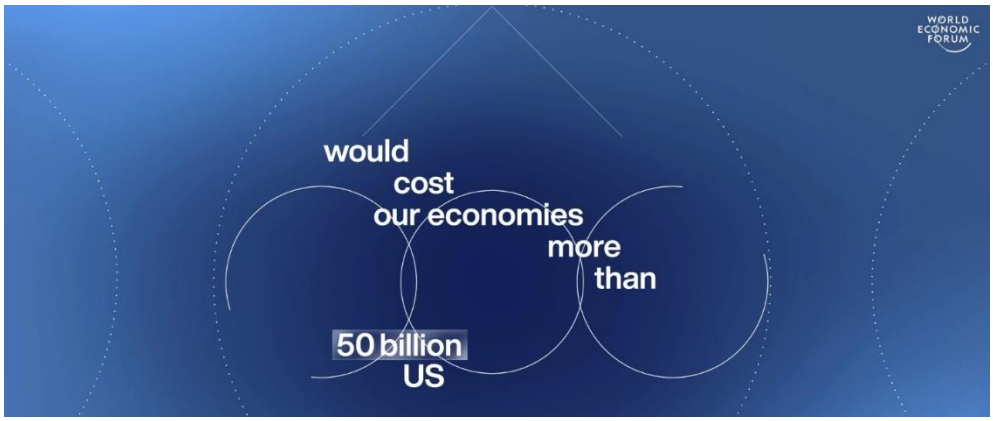
robo de identidad, las empresas tratan de redoblar esfuerzos para mejorar la privacidad de los datos. El problema de las filtraciones de datos es una preocupación en todas las industrias; sin embargo, en la industria de servicios financieros es un objetivo principal debido a la inherente relación entre los datos y su valor, entre los datos y el precio que estarían dispuestos a pagar a causa de un ataque cibernético exitoso. De acuerdo con el Instituto Ponemon (IBM, 2021),

> El aumento en el trabajo desde la casa o remoto, combinado con una adopción lenta de la automatización de la seguridad y las tecnologías modernizadas, aumentó los costos generales de identificar y contener una violación de datos. En 2021, el costo total promedio de una violación de datos aumentó a $ 4.24 millones. La industria financiera sufrió perdidas por alrededor de $ 5,72 millones (párr. 1).

4.1.8.1 Teoría del caos en las finanzas: ¿se aproxima su invierno?

En el mundo empresarial muchos aun no tomaban en consideración las posibles consecuencias desastrosas que pueden tener las finanzas mundiales a causa de fallas de seguridad cibernéticas. De hecho, normalmente no hay tiempo para pensar en eso, ya que cada minuto cuenta presenta un volumen muy alto de transacciones y cada transacción es dinero que fluye y donde hay dinero los mercados adquieren dinámica; la cual provoca que la oferta y la demanda continúen como se hizo desde los orígenes de la humanidad hasta que ocurrió la inesperada falla de los sistemas en Wall Street. Llama la atención que, durante la reunión de Davos en febrero del 2021, el tema principal fue el de la ciberseguridad; se discutió sobre el temor que ellos contemplan de que haya una falla mundial en el internet que podría provocar perdidas de hasta $50 billones de dólares.

Figura 11. Costo de un día sin internet en el mundo

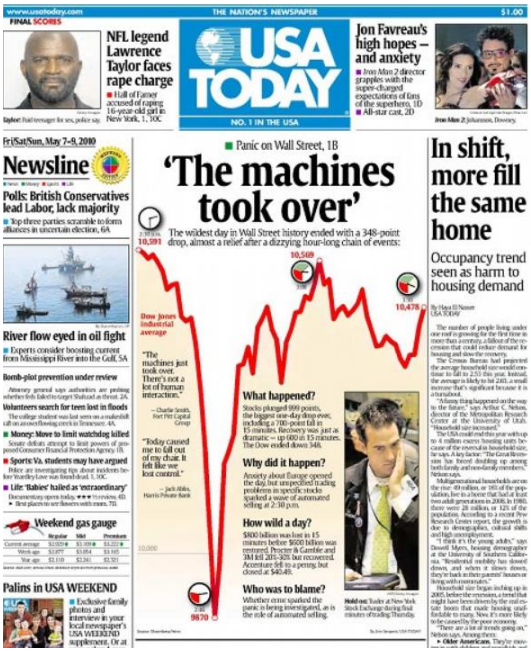


Fuente: Foro Económico Mundial (2021).

4.1.8.2 Caída 2:45 – Sin tiempo para errores

En la actualidad, no hay tiempo para errores porque eso automáticamente se traduce en cuantiosas perdidas financieras si la magnitud del problema es grande, y aunque se sabe que existen probabilidades de riesgo hay muchas empresas que no toman las medidas respectivas. Recordemos que en el año 1999 se hablaba sobre el error del milenio, conocido también como Y2K que consistía en una falla mundial en los sistemas, pero se pudieron tomar acciones que permitieron evitar el problema. En ese caso el error se descubrió con tiempo suficiente como para que se tomaran acciones apropiadas, pero no siempre este será el escenario. En el año 2010 ocurrió lo inesperado: una falla en los sistemas financieros de la bolsa en Nueva York y, aunque no fue un problema que duró meses, semanas o días, en tan solo unos minutos afectó el mercado financiero.

Figura 12. Las máquinas se apoderaron (Wall Street) - The Machines Took Over (Wall Street)



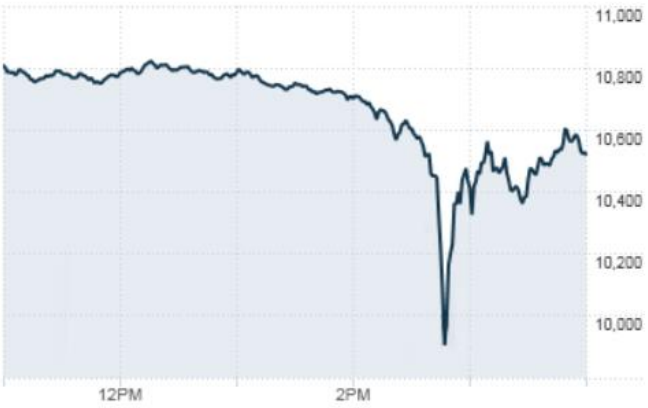
Fuente: USA Today print edition, May 7, 2010 (*Kiosko.NET* 2021).

Incluso hoy, la causa no es tan clara como se hubiera esperado, pero es evidente que las finanzas mundiales son vulnerables porque, aunque hoy se vive en un mundo tecnológico de alta gama como nunca se vio, no estamos anuentes a las fallas. Las fallas tecnológicas muchas veces están entrelazadas y, aunque hay actividades de mantenimiento, continúan siendo parte de la seguridad informática, por lo que la falta de diagnóstico y monitoreo fue evidente cuando esta gran falla ocurrió.

4.1.8.3 El mundo financiero – su majestad el algoritmo, su padre un defectuoso humano

De acuerdo con el informe que se brindó, la falla fue causada por un algoritmo, el cual no deja de estar exento a problemas debido a que es, de todos modos, hecho e implementado por un ser humano y, obviamente, está expuesto a fallos al no poder controlar por completo el ambiente que lo rodea. Este tipo de situaciones debe alertarnos y evidencia la necesidad de que en las empresas se hable y se considere este tipo de vicisitudes porque, al final, se traduce en perdidas inimaginables.

Figura 13. Caída 2:45, el mercado cae por un valor de un trillón de dólares



Fuente: DOW (DJIA) 6 de mayo de 2010 (11:00 AM – 4:00 PM EDT).

El mundo de las finanzas depende de equipo de cómputo capaz de procesar miles de transacciones por minuto, pero como toda maquina va a requerir mantenimiento para evitar fallos. Además, pueden existir fallas debido al error humano y otras múltiples formas de fallos que no pueden ser controlados, como los del ambiente externo o natural. Asimismo, la falta de actualizaciones y mantenimiento tanto en el área de *software* como en la de hardware pueden causar este tipo de problemas. En la actualidad, existen esquemas de respaldo y de balance de cargas que permiten continuar operando ante problemas, por ello es vital que, en el ámbito administrativo en conjunto con el técnico, se discutan este tipo de escenarios y modulen cuál sería el plan a seguir para evitar problemas o, al menos, mitigarlos para que el impacto sea lo menos fuerte posible.

4.1.9 Ámbito Empresarial Costarricense

La empresa nacional debe asumir grandes retos no solo para mantenerse vigente sino también para poder ser aceptada en nuevos mercados.

Las exigencias internacionales cada vez son mayores y tiene que haber una adaptación rápida y fácil de implementar que le permita hacerlo sin incurrir en grandes inversiones de

tiempo y económicas, es por ellos que debe de haber un mapa conceptual que permita comprender las áreas claves de mejora para que un gerente pueda tomar las decisiones pertinentes que le permitan cumplir los objetivos en un tiempo dado.

Figura 14. Mapa conceptual: Retos de la empresa costarricense

Fuente: elaboración propia.

El mundo empresarial a nivel internacional esta aprovechando el uso de la tecnología como nunca antes lo hizo y aunque mucha empresa se vio forzada a hacerlo debido a las circunstancias que se desarrollaron en el 2020 y en este año 2021 lo importante es que se pueda adaptar y cumplir con las demandas actuales.

El país tiene en sus manos una gran oportunidad para desarrollar el talento nacional por medio de la innovación y la investigación y de esta forma impulsar a la industria costarricense para que pueda abarcar mercados que requieren de ciertas normas, requerimientos y procesos.

El objetivo de este mapa conceptual es que a nivel gerencial se comprenda que la única forma de crecer y ser aceptados internacionalmente es involucrando una serie de pasos y términos que hasta no hace mucho tiempo eran totalmente desconocidos en el área de las ciencias sociales pero que hoy sin duda alguna son requisitos necesarios para la toma de decisiones clave basándose en analizar "quién, qué, cómo y dónde" en relación con los productos, servicios, clientes y empresas internacionales.

Capítulo V. Propuesta

En el presente capítulo se detallan una serie de propuestas que pueden ser implementadas con un costo mínimo o libre de pagos. Se trata de herramientas disponibles que permiten comprender como la automatización, la ciberseguridad y la ciencia de datos pueden ser utilizadas e implementadas en la nueva estrategia empresarial que consiste en incluir la empresa costarricense en la sociedad 4.0.

Para el desarrollo de las herramientas y sus análisis, los montos utilizados están expresados en colones y dólares, así como en porcentajes o puntos porcentuales según corresponda. La propuesta utiliza un conjunto de métricas y cálculos que se desarrollaron en una herramienta conocida o al alcance de la mayoría de empresas: Excel. Opcionalmente, también se puede utilizar la hoja de cálculo que ofrece Google o en libre office. También, se utilizan modelos desarrollados en el lenguaje de programación PYTHON, el cual posee una licencia de *software* permisiva de estilo BSD que es compatible con la GNU General Public License (GPL) por la que no hay que pagar por su uso para la automatización.

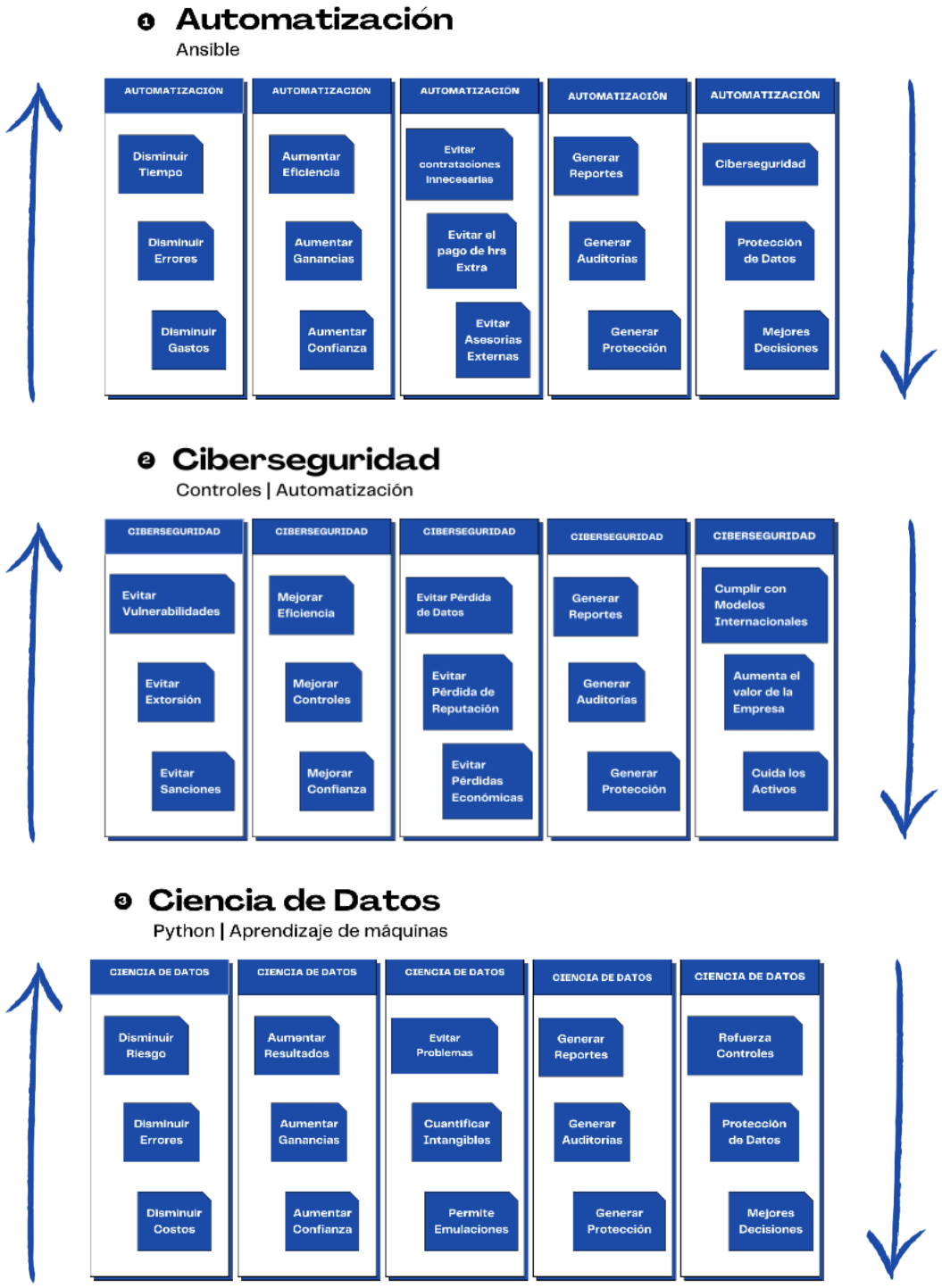
5.1 Herramientas que permiten la innovación.

Las empresas costarricenses pueden innovar en diferentes maneras por medio de la automatización, la ciberseguridad y la ciencia de datos.

Se debe mantener en todo momento la idea de que se puede innovar desde un punto de vista financiero, es decir ya sea logrando una disminución en los costos o un aumento en los ingresos e inclusive logrando ambos objetivos.

Es muy importante para toda compañía lograr una mayor rentabilidad y sin duda alguna la mejora de sus operaciones, buscando en todo momento nuevos mercados donde se logre demostrar que se puede satisfacer las mas altas demandas y estándares internacionales con el objetivo de tener más ganancias.

Figura 15. Beneficios de la automatización, ciberseguridad y ciencia de datos en la empresa



5.1.1 Paso 1: disminuir el error humano

Un simple descuido puede verse como algo pasajero, pero la magnitud de ciertas prácticas puede hacer que se incurra en cuantiosas perdidas económicas. Se debe comprender que todos los seres humanos cometen errores, pero los mismos se pueden evitar si existen los mecanismos correctos. En cuanto a la ciberseguridad, el mayor punto débil de las empresas es el comportamiento de los colaboradores, quienes permiten que la organización sea vulnerable. Debe de haber unión y trabajo en conjunto entre gerencia, ciberseguridad y el personal para que se detecten las debilidades y estas puedan ser corregidas a tiempo.

5.1.1.1 Gestión del talento humano (GTH): es la hora de auditar

Para garantizar el funcionamiento esperado, no se debe dejar guiar únicamente por el criterio de algunas personas, se requiere auditar, tener control cruzado para evidenciar datos y resultados transparentes que indiquen la verdadera situación de la organización. Al auditar podemos observar, encontrar e identificar prácticas, situaciones y circunstancias que probablemente no era de nuestro conocimiento y que es la fuente de muchos problemas. Gracias al código abierto y a las licencias públicas, se pueden realizar una serie de herramientas simples en uso y en naturaleza, pero eficaces para lograr el objetivo que se busca.

5.1.1.1.1 Auditoría: revisión de contraseñas con PYTHON

Los últimos informes de ciberseguridad muestran que el punto más débil de la seguridad cibernética es el humano. Lo preocupante es que el mismo colaborador es el responsable de utilizar contraseñas e inclusive generarlas. A continuación, se muestran algunas de las métricas recopiladas.

De acuerdo al secplicity (2021) el informe de investigaciones de violaciones de datos de Verizon para el 2020, el 81% del número total de violaciones de ciberseguridad se aprovecharon de contraseñas robadas o débiles. Igualmente de acuerdo a secplicity (2021) se roban 1 millón de contraseñas cada semana en el informe de Breach Alarm 2019. Debido a esta situación, el Marco de Seguridad del Instituto Nacional de Estándares y Tecnología (NIST)

realizó una publicación especial llamada: NIST 800-63B, la cual contiene una serie de políticas y lineamientos para entender que requisitos se deben cumplir para generar o tener una contraseña segura (NIST 2021).

Hoy es necesario crear contraseñas seguras para iniciar una sesión y disfrutar de los beneficios de una computadora, una cuenta bancaria, inclusive para usar la biblioteca de la universidad. Lamentablemente, muchas personas no crean contraseñas seguras que sean difíciles de descifrar y, así, evitar ser víctimas de un ciber ataque a causa del uso incorrecto de una contraseña. Para muchos definir qué es o cómo se hace una contraseña segura es complicado, pero el documento desarrollado por el NIST lo explica a la perfección, por tanto, se procede a utilizar por medio del lenguaje de programación PYTHON.

El departamento de gestión del talento humano debe trabajar en conjunto con el departamento de tecnología de la información para poder reducir al máximo este grave problema que es considerado uno de las mayores causas de ingresos no autorizados a los sistemas de una empresa para la extracción de información. En el anexo 5 se muestra una "Auditoría de Contraseñas" y se expone un modelo desarrollado con el lenguaje PYTHON que permite analizar las contraseñas utilizadas por cada usuario con el fin de determinar si cumple con el estándar de ciberseguridad creado por la NIST.

Al respecto, se requiere que el departamento de la gestión del talento humano le envíe la lista de colaboradores activos a el departamento de tecnología de la información para un control cruzado de los usuarios existentes, si hubiese alguna diferencia se investigara hasta que ambos departamentos tengan la misma información. Asimismo, se debe detallar tanto en la lista como en el informe final quienes están de vacaciones, presentan una ausencia justificada por enfermedad, incapacidad o cualquier otra excepción. Esta auditoría se puede realizar sin importar que el colaborador esté presente en las instalaciones físicas de la empresa, trabajando en forma remota o ausente por alguna de las causas anteriormente mencionadas. La justificación es para tener pendiente el reingreso a actividades del colaborador para que la notificación tome efecto hasta el día que vuelva.

Sobre como obtener las contraseñas, eso se hace solo en la auditoría como se propone en este caso, con las aprobaciones pertinentes de los gerentes de cada departamento y su resultado siempre es confidencial. En caso de que se determine que algún colaborador no logra pasar la auditoría en el informe se debe detallar quién o quiénes son los colaboradores para que

el departamento de la gestión del talento humano programe el entrenamiento correspondiente para reforzar esa área de aprendizaje y, al mismo tiempo, el departamento de tecnología de la información podrá generar una nueva contraseña para el colaborador o solicitarle que genere una con base en las reglas de la empresa. El beneficio de esta propuesta es muy alto porque no se requiere pagar por concepto de licencia alguna para poder utilizar PYTHON, este modelo puede implementarse en cualquier empresa y en cualquier plataforma de computación, ya sea en el sistema operativo Linux como en el de Windows; el tiempo que se tarda para ejecutarlo es sumamente corto.

5.1.1.1.2 Auditoría: generador de contraseñas con PYTHON

Esta herramienta es muy simple, pero de gran necesidad. Genera una contraseña que cumple con todos los requisitos que se expusieron anteriormente, lo cual permite que, al colaborador, se le simplifique entender que se requiere. Al mismo tiempo, mejora los resultados de la auditoría y, finalmente, ante un caso de emergencia en el que se debe utilizar una nueva contraseña, esta se puede tener rápidamente. En el anexo 6 se encuentra un "Generador de Contraseñas con Python", en el cual se muestra el modelo desarrollado con el lenguaje PYTHON que permite generar las contraseñas utilizando módulos que las generaran con base en lo que recomienda el marco de ciberseguridad creado por la NIST.

5.1.1.1.3 Auditoría: revisión de entrenamiento con PYTHON y *machine learning*

Este modelo desarrollado en PYTHON permite determinar a través de datos históricos recopilados por el departamento de gestión del talento humano, quienes han renunciado, se mapean las posibles razones de las salidas y el número de colaboradores que continúan. La primer ventaja que nos da es que brinda información como la cantidad de colaboradores que trabajan desde casa por lo que pueden identificar para darles entrenamiento en ciberseguridad por ser más vulnerables que el resto de sus colegas por no estar utilizando las instalaciones de la empresa cuya red debería estar asegurada.

Otro punto es que se puede comprobar si las personas que trabajan desde casa utilizan o no la red virtual privada (vpn *virtual private network* por sus siglas en inglés) que les daría más seguridad. El modelo utiliza aprendizaje automático (*machine learning*) para comprender las

causas del porqué esas personas renunciaron, lo que se busca es una alternativa para que, en este caso, cuando el departamento de gestión del talento humano identifique colaboradores que están ingresando en esa área no solo lo puedan evitar, sino que se identifican como sujetos que puedan bajar la guardia en cuanto a la utilización de los mecanismos de seguridad por lo que se les puede reforzar con entrenamiento este tema. Además, se pueden monitorear sus prácticas de seguridad con el fin de evitar que puedan caer en faltas que abran las puertas a potenciales vulnerabilidades.

5.1.1.1.4 Auditoría: revisión de controles internos

Es esencial utilizar controles internos no solo para asegurar el obtener mejores resultados, sino también para poder estandarizar el trabajo y llegar a hacer o cumplir nuestras obligaciones en forma más rápida y eficiente. Los controles generan información y, con el tiempo, esta información nos genera indicadores que ayudan a mejorar las estimaciones y los resultados de lo que se mida. Los detalles hacen la diferencia en todo y los controles no son la excepción, ya que los mismos permiten evitar el error humano, agilizan la ejecución de muchas tareas y, en general, permiten la mejora. A continuación, se presentan las recomendaciones de controles esenciales para la seguridad con base en las últimas métricas de fallas en la ciberseguridad.

5.1.1.1.4.1 Control 1: ingreso de personal - *onboarding*

Muchas empresas no tienen un proceso adecuado para recibir un colaborador, dicho proceso se conoce según el departamento de la gestión del talento humano como inducción, el cual consiste en darle no solo la bienvenida al nuevo colaborador al equipo, sino tambien en brindar explicaciones para que entienda y conozca los pormenores de la empresa en un período corto con el fin de que pueda estar en producción lo más pronto posible. Esa descripción teórica suena muy bien, pero en la práctica muchos colaboradores ingresan y pasan a veces no días y hasta semanas para que produzcan por no contar con lo necesario para poder trabajar. El problema nace a raíz de que no existe un control adecuado para asegurarse que el nuevo colaborador cuente con todo lo necesario para que pueda trabajar lo más pronto posible.

El departamento de tecnología de la información juega un papel fundamental ante esta situación, por ello, cuando se completan los trámites de afiliación, el equipo de TI debe crear la cuenta de usuario, proporcionar los permisos basados en roles y asignar un sistema que puede ser una computadora de escritorio o portátil. La propuesta es utilizar un documento que sirva de control cruzado (ver anexo 7. Control de verificación de ingreso a la empresa) por parte de el departamento de GTH y el de TI válido para los casos en los que los colaboradores deban utilizar equipo tecnológico y no dejar una impresión negativa de la organización. Este tipo de control disminuye e influye positivamente en la métrica de riesgo, producción y satisfacción. En el anexo 7 “Control de verificación de ingreso a la empresa” se muestra el modelo desarrollado para cubrir los puntos más importantes y agilizar la bienvenida del nuevo personal.

5.1.1.1.4.2 Control 2: salida de personal - *offboarding*

Muchas empresas no tienen un proceso adecuado para dar de baja a un colaborador y, en otras, el departamento de GTH delega esta responsabilidad al gerente en turno por estar encargado. Sin embargo, posteriormente, el gerente solicita a algún líder de equipo que se encargue de la salida de la persona que deja de ser un colaborador. Este es el panorama que normalmente se vive en la mayoría de las empresas, lo cual genera un problema de seguridad potencial, ya que la problemática radica en que no se aseguran totalmente de que la persona salga adecuadamente.

Ante esta situación el departamento de TI juega un papel fundamental y debe poner a disposición la experiencia en seguridad tradicional y ciberseguridad la importancia de que alguien que deje de ser un colaborador no tenga ningún acceso, ni vínculo alguno con la empresa. Por ejemplo, el equipo de TI debe deshabilita o eliminar las cuentas del usuario, revisar su sistema y otros dispositivos asociados. De esta forma, se propone que, como parte del proceso de baja, el procedimiento se haga contra una lista requerida para control cruzado en el que, tanto el departamento de GTH como el de TI estén seguros de que se hizo lo correcto.

Un ejemplo que se propone para este tipo de control es el que se encuentra en el anexo 8. Control de verificación de salida de la empresa. Este control es muy importante porque la empresa se asegura que la persona se despida en forma honorable y respetable por gratitud a su

servicio, estando la persona conforme de que deja todo en orden. Al mismo tiempo, la empresa se asegura de que la persona que sale no tenga nada que potencialmente le permita todavía utilizar o accesar algún servicio, programa o recurso que comprometa la integridad y reputación de la empresa y de la persona misma.

Tristemente, no todas las personas que han salido de una empresa lo han hecho de forma satisfactoria, muchos casos son por circunstancias delicadas e, incluso, puede radicar en un comportamiento no adecuando que indique que es prioritario ejecutar el procedimiento de salida lo más pronto posible, cumpliendo con el protocolo para evitar problemas como la fuga de información o, inclusive, daño a algún activo. Este tipo de control disminuye e influye positivamente en la métrica de riesgo. En el anexo 8. "Control de verificación de salida de la empresa" se muestra el modelo recomendado, en el cual se abarcan los puntos más críticos para agilizar la salida de las personas.

5.1.1.1.4.3 Control 3: acuerdo de confidencialidad

Es posible que algún colaborador trabaje para un cliente perteneciente a la empresa que solicite un acuerdo de confidencialidad, por lo que la gerencia y el departamento legal deben revisar lo solicitado. Si este no fuera el caso, se propone revisar si se emplea o se utiliza proveedores externos que trabajen en conjunto con la empresa, por lo que, si se comparte cualquier tipo de información con el proveedor, se debe de firmar un acuerdo de confidencialidad. Ambas partes, deben de acordar que no se divulgara ninguna información confidencial, también puede requerirse la eliminación de información después de que se finalice un proyecto. Con este control, se influye positivamente en la métrica de riesgo al evitar la pérdida de credibilidad, daños a la imagen y reputación, sanciones legales y financieras.

5.1.2 Paso 2: cuantificar el riesgo

La seguridad cibernética se ha convertido en un problema que no es común en el ámbito administrativo, con lo cual se genera una necesidad creciente para medir e informar el riesgo cibernético en términos financieros para poder entender y justificar el presupuesto que se

vaya a requerir por concepto de planilla, compra de equipo que inclusive incluye activos intangibles como los antivirus, programas o *software*. Los mapas de calor en su forma tradicional ya no nos proporcionan información suficiente para calcular los costos como se debe, por ejemplo, para justificar la compra de un antivirus no basta con decir que los virus y el *malware* nos ponen en un riesgo alto o en zona roja y pretender que el departamento de finanzas otorgue el dinero.

Es por lo que Peter F Drucker dijo “lo que se mide se gestiona” (The Practice of Management, 1954) y, actualmente, no solo es una gran necesidad, sino que pasó a ser un requisito. Tomando como ejemplo la planilla, ya no solo basta emplear ingenieros en computación, sino que también se requiere contratar expertos en ciberseguridad que, por lo general, son escasos y su sueldo es bastante alto, con ello se aumenta, sin lugar a duda, el costo de planilla sin todavía hablar del equipo físico o *hardware* y el intangible o *software* que se va a requerir para mejorar la seguridad. Solo cuantificando y justificando el valor de los elementos que giran en torno a este ambiente, se permite no solo una mejor comprensión y gestión de la parte financiera de los riesgos cibernéticos, sino también en ayudar a identificar y priorizar las actividades de remediación en función de la exposición al riesgo financiero.

5.1.2.1 Finanzas: es la hora de cuantificar

El departamento de finanzas normalmente asigna un presupuesto a cada departamento, sino que se cuantifican los eventos dentro del departamento de ciberseguridad no habrá claridad con los eventos. Por ello, se recomienda iniciar o implementar con la cultura de cuantificar para poder tener un mejor control del ambiente y, así, poder dar las razones financieras correctas para justificar un presupuesto y, a la vez, tener los datos para cuantificar la realidad económica y financiera de el departamento de TI con respecto a su capacidad para asumir las diferentes obligaciones con el fin de poder desarrollar sus labores lo mejor posible.

5.1.2.1.1 Análisis: cuantificar el riesgo con PYTHON

Como se expuso anteriormente en materia de ciberseguridad se ha utilizado la matriz de riesgo como único instrumento para poder medir o cuantificar cuánto cuesta un riesgo. El problema es que decir que el eminente riesgo de ransomware era alto no calculaba el costo en

términos monetarios, entonces se comenzó a utilizar la estadística para poder medir en forma mas científica cuánto cuesta un riesgo y, así, poder determinar cuánto sería el potencial total de los riesgos. La técnica del uso de la matriz del riesgo presenta sesgos para medir el riesgo de seguridad cibernética. Se propone entonces reemplazar las matrices de riesgo con enfoques más cuantitativos para poder contar con un método diferente para la toma de decisiones.

Por ello, en el anexo 9 “Cuantificación de riesgos cibernéticos con PYTHON” se muestra un modelo que genera una curva de excedencia de pérdida con simulaciones de Monte Carlo en PYTHON. Por tanto, este enfoque cuantitativo mide el riesgo de los ataques cibernéticos de la misma forma en que las compañías de seguros y las administradoras de fondos de pensiones miden el riesgo, ya que no es suficiente decir que un riesgo es "bajo", "medio" o "alto". En lugar de eso, con la ayuda de la información que brindan los estudios profesionales en el campo de la ciberseguridad o por medio del análisis de los mismos expertos del medio local, se puede indicar que porcentaje de posibilidad que tiene la empresa de experimentar un ataque en determinado periodo del año. Se utiliza una estimación de pérdida monetaria que, en términos financieros es lo más adecuado para evitar estimaciones descriptivas como lo hace la matriz de riesgo que solo diría “riesgo alto”. El modelo permite utilizar una serie de iteraciones que provoca que la técnica de Monte Carlo sea, o no, más efectiva en el ejemplo vemos que 1000 iteraciones no es tan precisa como si se utilizan 1000 o 50000 que definitivamente brindan una aproximación mejor.

5.1.3 Paso 3: implementar métricas

La evolución de la ciberseguridad es inminente y ha ido de la mano con los cambios empresariales y de los avances tecnológicos. En la actualidad, las empresas se ven inmersas en un ambiente global altamente competitivo, en el cual es primordial tomar decisiones estratégicas de alto nivel y de impacto con el único fin de provocar que la empresa sea rentable, es decir, que sea eficiente como para una optimizar sus propios recursos financieros. La única forma de hacerlo es por medio de una gerencia sostenible, resiliente, moderna y sana en términos financieros, que pueda utilizar la información eficientemente, ya que la información es poder si, y solo si, el que la tiene la puede entender. Cuando se usan métricas, estas generan datos y, si se mantienen con esas prácticas en una línea de tiempo, esa información brinda una mayor

capacidad y precisión suficiente para hacer predicciones financieras muy acertadas. La recomendación general es utilizar las métricas para generar datos e información que permita a la alta gerencia tomar mejores decisiones.

5.1.3.1 Gerencia general: es la hora de tener métricas

Las métricas son muy importantes porque ayudan a conocer el rendimiento del programa de ciberseguridad que, actualmente, puede tener una organización o el que vaya a implementar, lo cual ayuda a tomar las decisiones correctas, pertinentes y acordes al programa. Las métricas de rendimiento de ciberseguridad permiten tanto al equipo gerencial como a la administración de la ciberseguridad, analizar con mayor profundidad el riesgo, las amenazas, que se requiere para proteger, mitigar, mejorar y que los cambios sean efectivos con el tiempo. Asimismo, permiten probar los marcos de seguridad y entender si es el apropiado, o no, si se le debe implementar cambios o actualizaciones o si del todo se debe cambiar por otro más efectivo. Se propone usar métricas que respalden las decisiones que se vayan a tomar especialmente cuando se trata de presupuestos y gastos. El uso de métricas brinda al departamento de TI la capacidad de comparar no solo su postura de seguridad, sino también la económica delante del análisis exhaustivo que debe hacerse para el departamento financiero para justificar sus requerimientos. Se debe dedicar una gran cantidad de esfuerzo y tiempo a la preparación de las métricas de seguridad cibernética que se vayan a utilizar para que se adapten individualmente a las necesidades de una empresa sin que generen sesgos de apreciación.

Por otro lado, la gerencia general debe promover el uso de las métricas como cultura interna de la organización sin olvidar que, probablemente, el departamento de la TI vaya a requerir ayuda a la hora de confeccionarlas, especialmente, en el momento de asignar valores económicos. El uso de métricas permite a los miembros de la junta administrativa comprender el estado actual de la seguridad cibernética de una empresa y el de sus proyectos en esa materia, permiten influir en la toma de decisiones al proporcionar valores de referencia tangibles y puntos de discusión que, normalmente, no son claros o, peor aun, ni siquiera se sabe de donde se obtienen los datos ni que los respalda. La gerencia general debe justificar la asignación de recursos de seguridad por parte de una empresa especialmente si es objeto de una auditoría que exige un control más minucioso y debe justificar lo que pase en la empresa.

5.1.3.1.1 Análisis: creando métricas con Excel

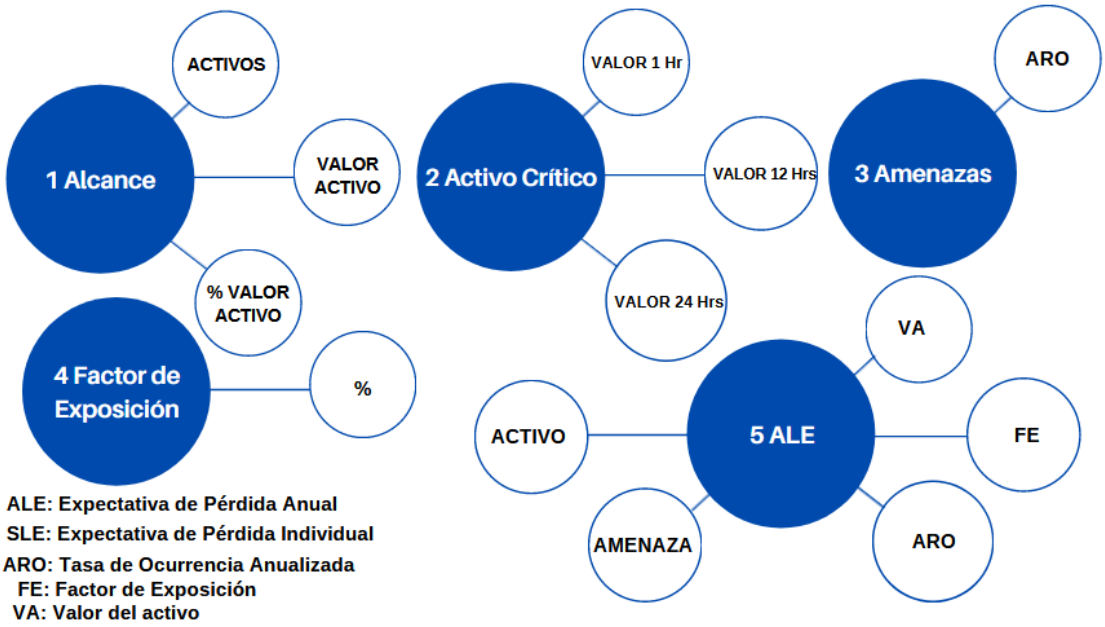
Por lo general, las empresas gastan mucho dinero en programas que monitorean en tiempo real las actividades de ciberseguridad que son utilizadas por los técnicos del área de ciberseguridad. En el ámbito gerencial, se puede utilizar Excel perfectamente para cumplir con el mismo objetivo y sin recaer en altos costos. Además, se puede aprovechar que también permite generar los llamados *dashboards* si se requiere.

Se recomienda la utilización de Excel para generar una serie de calculaciones simples en naturaleza, pero muy efectivas a la hora de generar información que es pertinente para la toma de decisiones en el campo de la ciberseguridad. Estas métricas son reconocidas internacionalmente, la recomendación de su uso es alta, ya que permite la generación de datos históricos que mejoraran con el paso del tiempo la precisión de los resultados, los cuales podrán ser determinantes a la hora de tomar decisiones, en especial, por su naturaleza práctica debido a que se encadenan en una serie de fases las cuales dependen una de otra en términos de resultados hasta lograr el final, el cual permite conocer la situación con más claridad.

5.1.3.1.1.1 Expectativa de la pérdida anualizada (Annualized Loss Expectancy o ALE)

A continuación se muestra las fases del modelo Expectativa de pérdida anualizada (Annualized Loss Expectancy o ALE por sus siglas en inglés).

Figura 16. Fases de la Expectativa de pérdida anualizada



Fuente: elaboración propia.

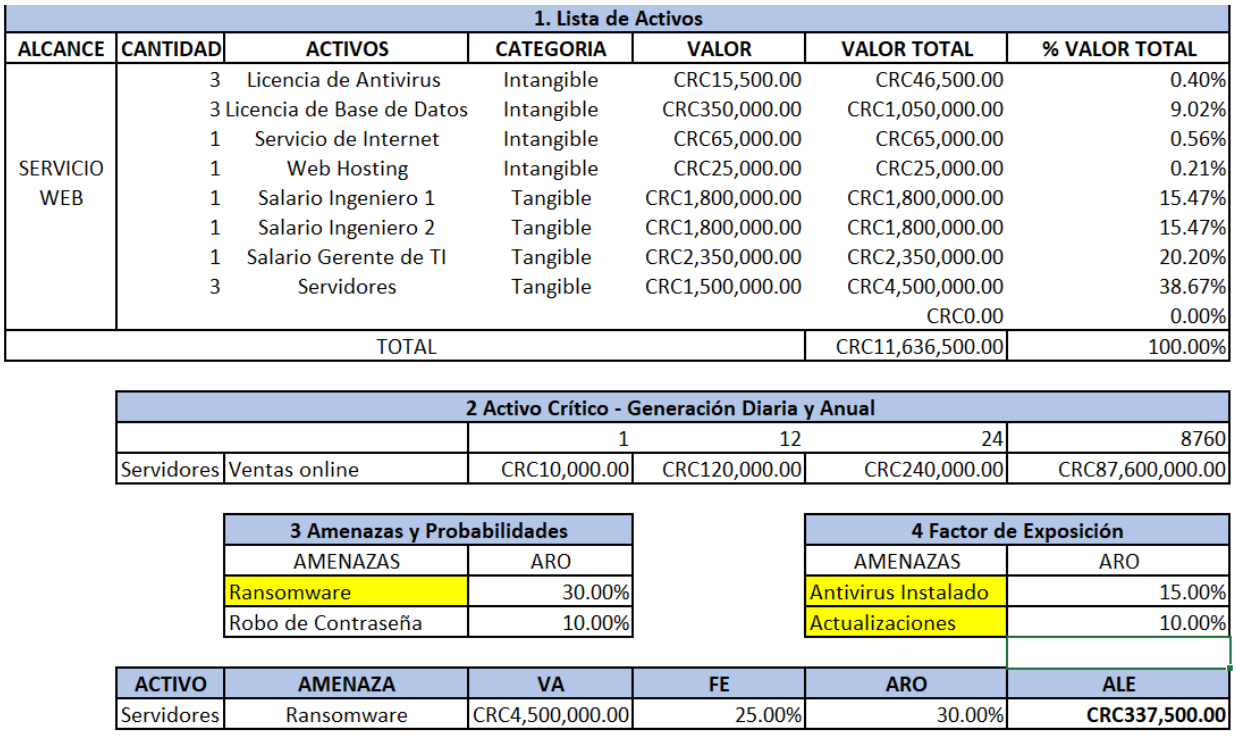
ALE en un análisis de costo-beneficio que se utiliza para destinar recursos al área de seguridad de la información. La formula para su cálculo es la siguiente:

ALE = SLE x ARO

SLE = FE x VA

La formula lo que nos indica es que se debe multiplicar el valor de la Expectativa de Pérdida Individual (SLE por sus siglas en ingles) por la Tasa de Ocurrencia Anualizada (ARO por sus siglas en ingles), pero antes de llegar a ese punto se debe conocer o tener primero el valor de la Expectativa de Pérdida Individual. Por lo tanto, SLE es el resultado de la multiplicación entre el Factor de Exposición por el Valor de un Activo. A continuación, se muestra un ejemplo aplicado.

Figura 17. Calculadora para la Expectativa de Pérdida Individual



1. Lista de Activos

ALCANCE	CANTIDAD	ACTIVOS	CATEGORIA	VALOR	VALOR TOTAL	% VALOR TOTAL
SERVICIO WEB	3	Licencia de Antivirus	Intangible	CRC15,500.00	CRC46,500.00	0.40%
	3	Licencia de Base de Datos	Intangible	CRC350,000.00	CRC1,050,000.00	9.02%
	1	Servicio de Internet	Intangible	CRC65,000.00	CRC65,000.00	0.56%
	1	Web Hosting	Intangible	CRC25,000.00	CRC25,000.00	0.21%
	1	Salario Ingeniero 1	Tangible	CRC1,800,000.00	CRC1,800,000.00	15.47%
	1	Salario Ingeniero 2	Tangible	CRC1,800,000.00	CRC1,800,000.00	15.47%
	1	Salario Gerente de TI	Tangible	CRC2,350,000.00	CRC2,350,000.00	20.20%
	3	Servidores	Tangible	CRC1,500,000.00	CRC4,500,000.00	38.67%
					CRC0.00	0.00%
TOTAL					CRC11,636,500.00	100.00%

2 Activo Crítico - Generación Diaria y Anual

		1	12	24	8760
Servidores	Ventas online	CRC10,000.00	CRC120,000.00	CRC240,000.00	CRC87,600,000.00

3 Amenazas y Probabilidades

AMENAZAS	ARO
Ransomware	30.00%
Robo de Contraseña	10.00%

4 Factor de Exposición

AMENAZAS	ARO
Antivirus Instalado	15.00%
Actualizaciones	10.00%

ACTIVO	AMENAZA	VA	FE	ARO	ALE
Servidores	Ransomware	CRC4,500,000.00	25.00%	30.00%	**CRC337,500.00**

Fuente: elaboración propia.

El experto de ciberseguridad debe hacer una lista de los activos tangibles e intangibles que se tiene. Los mismos se pueden agrupar por alcance o servicio. En el ejemplo se utiliza como primer paso el servicio web, el cual permite a la empresa vender en línea, el valor individual es información que contabilidad debe tener registrada por concepto de compras. El segundo paso es decidir cuál o cuáles son los elementos críticos del servicio escogido; luego, debe calcular lo que ese elemento genera por hora, por día o por año, esa información la tiene contabilidad y finanzas por concepto de la relación ventas/ganancias. La razón de hacerlo de esa forma es porque habrán otros elementos críticos, por tanto se deben sacar los esenciales de esa lista.

El tercer paso es identificar todas las posibles amenazas que pueda tener el activo escogido junto a la Tasa de Ocurrencia Anualizada, para la cual la opinión de los expertos o datos de estudios en ciberseguridad pueden brindar dicha información. Lo mismo aplica para el cuarto paso, en el cual los porcentajes se dan con base en esos estudios o la opinión del experto. Es importante recalcar que para cada periodo en que se ejecute esta técnica la precisión

aumentará gracias a los datos históricos que se vayan construyendo. Finalmente se aplica la formula para conocer el ALE o la Expectativa de Pérdida Anual de un evento individual o una serie de eventos.

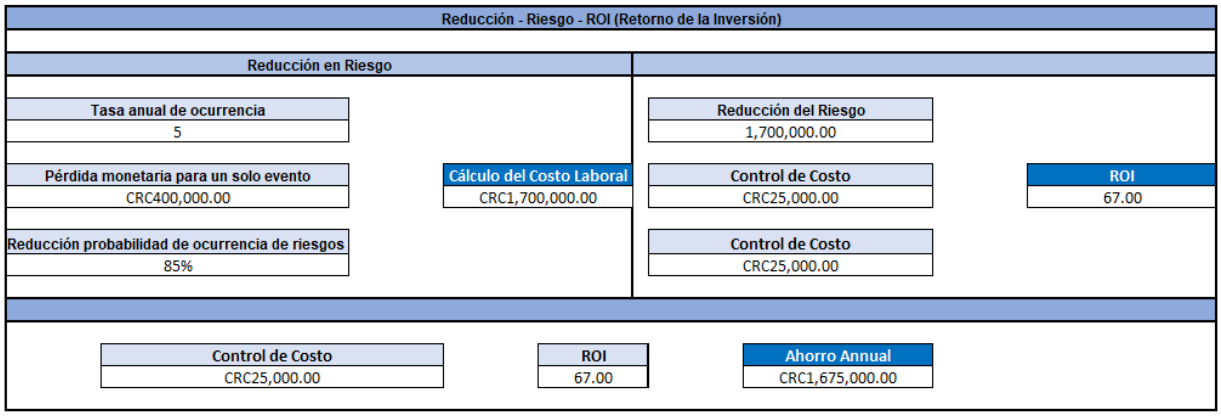
5.1.3.1.1.2 Retorno de la Inversión (Return of Investment o ROI)

Con la mejora de un plan existente de ciberseguridad o con la implementación de este, se tendrán que tomar decisiones sobre los temas de seguridad, la implementación de nuevas soluciones y controles. Como cualquier otro departamento va a requerir de inversiones monetarias, por tanto, es de suma importancia poder tener la capacidad de determinar el costo de un riesgo potencial versus el costo de un control. Por tanto, se recomienda utilizar una herramienta que le permita calcular el retorno de la inversión (ROI) para tener en cuenta el costo del riesgo frente al costo del control y entender, en términos financieros, la situación de todo lo relacionado en ciberseguridad no solo técnicamente.

Figura 18. Retorno de la Inversión (ROI)

Fuente: elaboración propia.

Figura 19. Calculadora para la Reducción del Riesgo – Retorno de la Inversión (ROI)



Fuente: elaboración propia.

Podemos suponer que la organización espera recibir un ataque cibernético, el cual será *phishing* cinco veces al año, a un costo estimado de ₡ 400,000.00 por ataque exitoso. Se espera que el costo de capacitar a los empleados para detectar y evitar correos electrónicos de *phishing* sea de ₡ 25,000, por lo que monetariamente sí da resultado invertir ₡ 25,000.00 por concepto de capacitación para poder reducir el riesgo de un ataque de *phishing*.

5.1.3.1.1.3 Reducción de la inactividad (*downtime reduction*)

Comprender el impacto financiero de los incidentes cibernéticos es de suma importancia, pero se debe aclarar algo muy importante: no se puede deducir que cada vez que un servidor deje de funcionar y esté fuera de servicio se trata de un ataque de ciberseguridad. En términos técnicos, los servidores deben actualizarse y, normalmente esta sana y recomendada práctica requiere que el servidor se reinicie por lo que estará fuera de servicio por unos pocos minutos. Sin embargo, hay situaciones que provocan que el servidor no vuelva después de la orden de reinicio y esta práctica se debe ejecutar porque actualizando los servidores es una forma en que podemos proteger los equipos. A continuación, algunos ejemplos que nos retratan la importancia de esta métrica:

En marzo de 2015, una interrupción de 12 horas en una tienda de Apple le costó a la empresa 25 millones de dólares.

En agosto de 2016, un apagón de cinco horas en un centro de operaciones provocó la cancelación de 2.000 vuelos y una pérdida estimada de 150 millones de dólares para Delta Airlines.

En marzo de 2019, una interrupción de 14 horas le costó a Facebook perdidas estimadas en $90 millones.

En el mundo, el costo promedio del tiempo de inactividad es de $5,600 por minuto, según un estudio de 2014 de Gartner. Sin embargo, un informe de Avaya del mismo año encontró que los promedios oscilaron entre $2,300 y $9,000 por minuto, dependiendo de factores como el tamaño de la empresa y la industria. Lamentablemente, esa cifra ha ido en aumento. Esta métrica demuestra la importancia financiera de tener datos económicos que respalden la inversión en equipo técnico y de ciberseguridad porque los costos de cada evento son cuantiosos y, anualmente, pueden ser alarmantes.

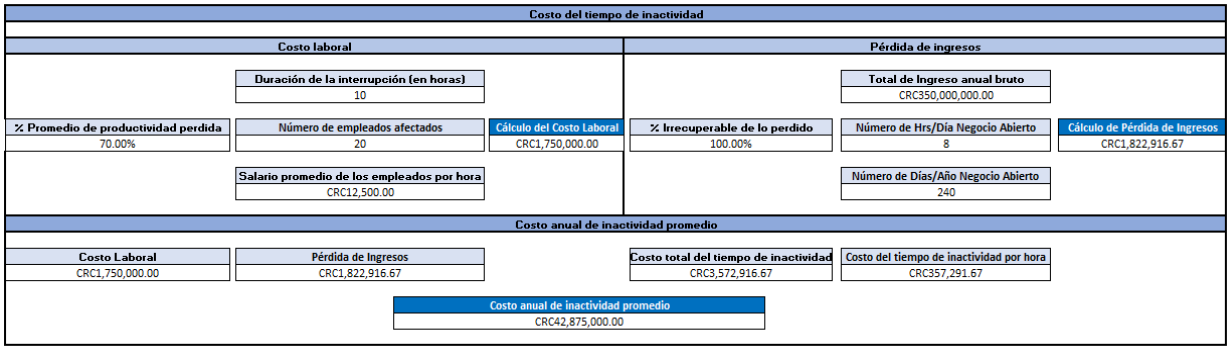
Figura 20. Costo anual de inactividad promedio

Fuente: elaboración propia.

El modelo rescata que, dependiendo del tipo de empresa, tamaño e industria, el costo o magnitud del impacto es variable debido a que el problema se puede presentar en solo una

unidad o departamento o en toda la organización; lo cual afecta grandemente a la empresa. El modelo que se recomienda permite que se conozcan a la perfección los costos departamentales y globales como organización los impactos por concepto de inactividad.

Figura 21. Calculadora anual de inactividad promedio



Fuente: elaboración propia.

5.1.4 Paso 4: hacer un presupuesto

En muchos casos, se encuentran problemas en el departamento de TI a la hora de crear un presupuesto debido a que, al enviarse la justificación al departamento de finanzas en caso de que la soliciten, muchos encargados viven momentos difíciles para calcular los riesgos que se tienen y poder demostrar la importancia de invertir en ciberseguridad. Por ello, se recomiendan técnicas que se pueden utilizar para dichos fines y, así, lograr crear un presupuesto fiable y que pueda ser aprobado por el departamento financiero.

5.1.4.1 Finanzas: es hora de hacer el presupuesto

Ciberseguridad debe crear presupuestos como cualquier otro departamento dentro de la organización, en los que se pueda cuantificar los eventos, necesidad y requerimientos de la empresa, cuya presentación sea entendible por las personas del departamento financiero. El presupuesto se puede hacer anual para construir los datos y hacer las proyecciones a varios anos en caso de que se requiera.

5.1.4.1.1 Análisis: creando un presupuesto con Excel

Por medio de Excel es posible generar un presupuesto que pueda ser presentado ante el departamento de finanzas para su evaluación. Como se explicó anteriormente, se puede utilizar también en otros tipos de hoja de cálculo previniendo que se tenga que hacer gastos especiales o pagar licencias.

Figura 22. Planificador de presupuesto

PLANIFICADOR DE PRESUPUESTO PARA CIBERSEGURIDAD		SEPTIEMBRE		OCTUBRE		NOVIEMBRE		DICIEMBRE		MONTO TOTAL	
NOMBRE DEL ENCARGADO		Monto Planificado	Monto Real	Monto Planificado	Monto Real	Monto Planificado	Monto Real	Monto Planificado	Monto Real	Monto Planificado	Monto Real
DEPARTAMENTO	TI	CRC15,407,180.00	CRC15,407,180.00	CRC15,907,180.00	CRC15,907,180.00	CRC12,032,430.00	CRC11,957,430.00	CRC11,907,430.00	CRC11,907,430.00	CRC179,662,460.00	CRC178,457,460.
ÁREA	CIBERSECURITY	CRC0.00		CRC0.00		CRC75,000.00		CRC0.00		CRC1,205,000.00	
FECHA		4402%	4402%	4545%	4545%	3438%	3416%	3402%	3402%	51332%	50988%
PRESUPUESTO PARA EL AÑO	2021	CRC15,400,000.00	CRC15,400,000.00	CRC15,900,000.00	CRC15,900,000.00	CRC11,900,250.00	CRC11,900,250.00	CRC11,900,250.00	CRC11,900,250.00	CRC179,450,500.00	CRC178,300,500.
TOTAL DE PRESUPUESTO ₡	CRC350,000.00		1	4 Q						Planilla del Personal	
TOTAL DE PRESUPUESTO US$	$350,000.00										
Planilla del Personal		SEPTIEMBRE		OCTUBRE		NOVIEMBRE		DICIEMBRE		TOTAL	
Nombre del Colaborador	Nombre del Puesto	Monto Planificado	Monto Real	Monto Planificado	Monto Real	Monto Planificado	Monto Real	Monto Planificado	Monto Real	Monto Planificado	Monto Real
	Director de Seguridad	CRC3,500,000.00	CRC3,500,000.00	CRC4,000,000.00	CRC4,000,000.00	CRC250.00	CRC250.00	CRC250.00	CRC250.00	CRC35,500,500.00	CRC35,500,500.0
	Ingeniero en Redes	CRC2,500,000.00	CRC2,500,000.00	CRC2,500,000.00	CRC2,500,000.00	CRC2,500,000.00	CRC2,500,000.00	CRC2,500,000.00	CRC2,500,000.00	CRC30,000,000.00	CRC30,000,000.0
	Administrador de Sistemas	CRC2,500,000.00	CRC2,500,000.00	CRC2,500,000.00	CRC2,500,000.00	CRC2,500,000.00	CRC2,500,000.00	CRC2,500,000.00	CRC2,500,000.00	CRC30,000,000.00	CRC30,000,000.0
	Administrador de Sistemas	CRC1,700,000.00	CRC1,700,000.00	CRC1,700,000.00	CRC1,700,000.00	CRC1,700,000.00	CRC1,700,000.00	CRC1,700,000.00	CRC1,700,000.00	CRC20,400,000.00	CRC20,400,000.0
	Administrador de Sistemas	CRC1,350,000.00	CRC1,350,000.00	CRC1,350,000.00	CRC1,350,000.00	CRC1,350,000.00	CRC1,350,000.00	CRC1,350,000.00	CRC1,350,000.00	CRC16,200,000.00	CRC16,200,000.0
	Analista de Ciberseguridad	CRC1,350,000.00	CRC1,350,000.00	CRC1,350,000.00	CRC1,350,000.00	CRC1,350,000.00	CRC1,350,000.00	CRC1,350,000.00	CRC1,350,000.00	CRC17,350,000.00	CRC16,200,000.0
	Analista de Ciberseguridad	CRC2,500,000.00	CRC2,500,000.00	CRC2,500,000.00	CRC2,500,000.00	CRC2,500,000.00	CRC2,500,000.00	CRC2,500,000.00	CRC2,500,000.00	CRC30,000,000.00	CRC30,000,000.0
		CRC0.00	CRC0.00	CRC0.00	CRC0.00	CRC0.00	CRC0.00	CRC0.00	CRC0.00	CRC0.00	CRC0.00
		CRC0.00	CRC0.00	CRC0.00	CRC0.00	CRC0.00	CRC0.00	CRC0.00	CRC0.00	CRC0.00	CRC0.00
		CRC0.00	CRC0.00	CRC0.00	CRC0.00	CRC0.00	CRC0.00	CRC0.00	CRC0.00	CRC0.00	CRC0.00
		CRC0.00	CRC0.00	CRC0.00	CRC0.00	CRC0.00	CRC0.00	CRC0.00	CRC0.00	CRC0.00	CRC0.00
		CRC0.00	CRC0.00	CRC0.00	CRC0.00	CRC0.00	CRC0.00	CRC0.00	CRC0.00	CRC0.00	CRC0.00
		CRC0.00	CRC0.00	CRC0.00	CRC0.00	CRC0.00	CRC0.00	CRC0.00	CRC0.00	CRC0.00	CRC0.00
		SEPTIEMBRE		OCTUBRE		NOVIEMBRE		DICIEMBRE		Capacitación	
		Monto Planificado	Monto Real	Monto Planificado	Monto Real	Monto Planificado	Monto Real	Monto Planificado	Monto Real	Monto Planificado	Monto Real
Capacitación		CRC0.00	CRC0.00	CRC0.00	CRC0.00	CRC125,000.00	CRC50,000.00	CRC0.00	CRC0.00	CRC125,800.00	CRC50,800.00
Nombre del Curso	Grupo										
Phishing	Colaboradores en General	CRC0.00	CRC0.00	CRC0.00	CRC0.00	CRC125,000.00	CRC50,000.00	CRC0.00	CRC0.00	CRC125,000.00	CRC50,000.00
		CRC0.00	CRC0.00	CRC0.00	CRC0.00	CRC0.00	CRC0.00	CRC0.00	CRC0.00	CRC0.00	CRC0.00

Fuente: elaboración propia.

Se recomienda el uso de este planificador para controlar y entender desde una perspectiva financiera lo que sucede con todo lo relacionado con la ciberseguridad. Contempla no solo la planilla, sino también la contabilización de todo lo relacionado con la capacitación, el equipo y los servicios que se requiere.

5.1.5 Paso 5: automatizar las tareas de ciberseguridad

La automatización de tareas es de suma importancia debido a que no solo permiten ahorrar tiempo, sino también ayudan a evitar el error humano lo que conllevaría a estar creando análisis de la causa raíz o RCA (*root cause analysis* por sus siglas en inglés). La automatización permite que las empresas cumplan con los compromisos que se hacen con sus usuarios o clientes y, pensando en ellos, se deben hacer las siguientes preguntas: ¿Con qué frecuencia estarán disponibles nuestros sistemas?, ¿Con qué rapidez se responderá si experimentamos fallas o

vulnerabilidades en el equipo?, ¿Qué tipo de promesas se hacen en temas de funcionalidad? Los usuarios quieren saber muchas veces qué tan eficiente es una empresa y como se diferencia de la competencia, por lo que se necesita una métrica como el acuerdo de nivel de servicio (SLA Service Level of Agreement por sus siglas en inglés) para cumplir las expectativas de los clientes sin importar si la empresa da servicios o si internamente el departamento de TI cuenta con esta métrica y sus clientes son los mismos empleados internos. Todo ello con el fin de responder más eficientemente ante los problemas computacionales de la organización.

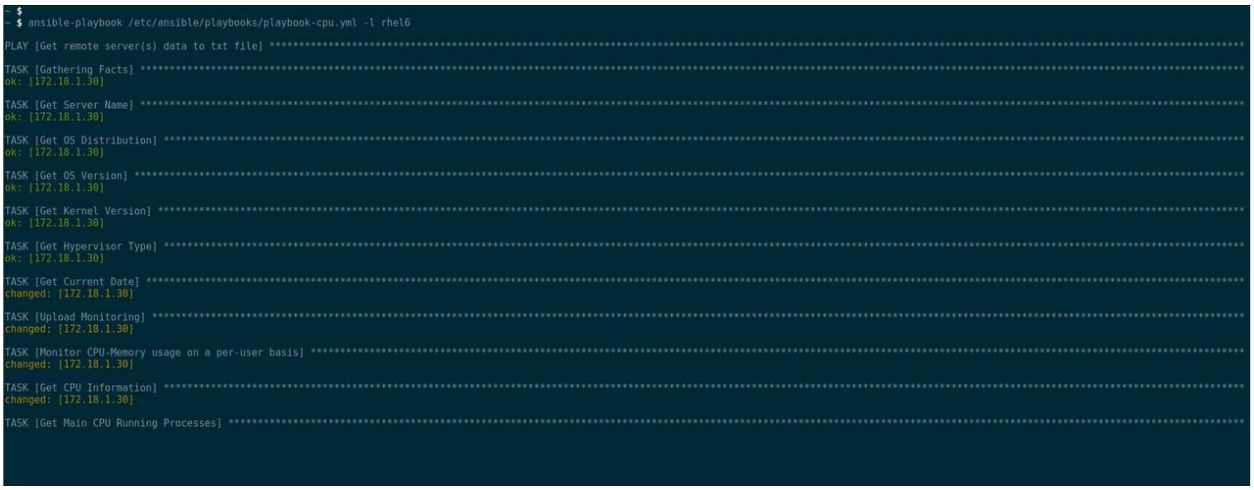
5.1.5.1 TI: es la hora de automatizar

Con la automatización, el tiempo de respuesta para revisar, implementar o ejecutar un servicio a nivel de TI es mucho mejor que la intervención manual y permite que se cumpla con los SLA. Un acuerdo de nivel de servicio se realiza entre el proveedor y el cliente sobre métricas medibles como el tiempo de actividad, la capacidad de respuesta y las responsabilidades. Por lo general, estos acuerdos los redactan entre las partes comerciales y legales de una empresa, si no se cumplen puede llegar a haber consecuencias de carácter financiero como multas. Por medio de la automatización se pueden evitar servicios lentos e ineficaces y mejorar, sin lugar a duda, la precisión con la que se realizan las labores.

5.1.5.1.1 Auditoría TI: automatizando la auditoría de activos intangibles con Ansible

Ansible es una herramienta para la automatización de TI y su propuesta es fomentar el código abierto como alternativa eficaz para la reducción de costos financieros. Aunque es una herramienta que requiere tiempo para dominarla, se debe aprender a usar de forma correcta y segura en el entorno. Los elementos que incluye no son ajenos a los que pueda entender el personal de TI, con lo cual se obtiene un mayor rendimiento del tiempo y de los costos financieros al reducir las horas laborales del recurso humano y el de error humano. Un tema a destacar es que la automatización fomenta el uso de estándares que permiten a la empresa utilizarlos junto con los marcos de seguridad para brindar mayor seguridad al informar que se trabaja según los lineamientos internacionales.

Figura 23. Auditoría de activos con Ansible en un servidor

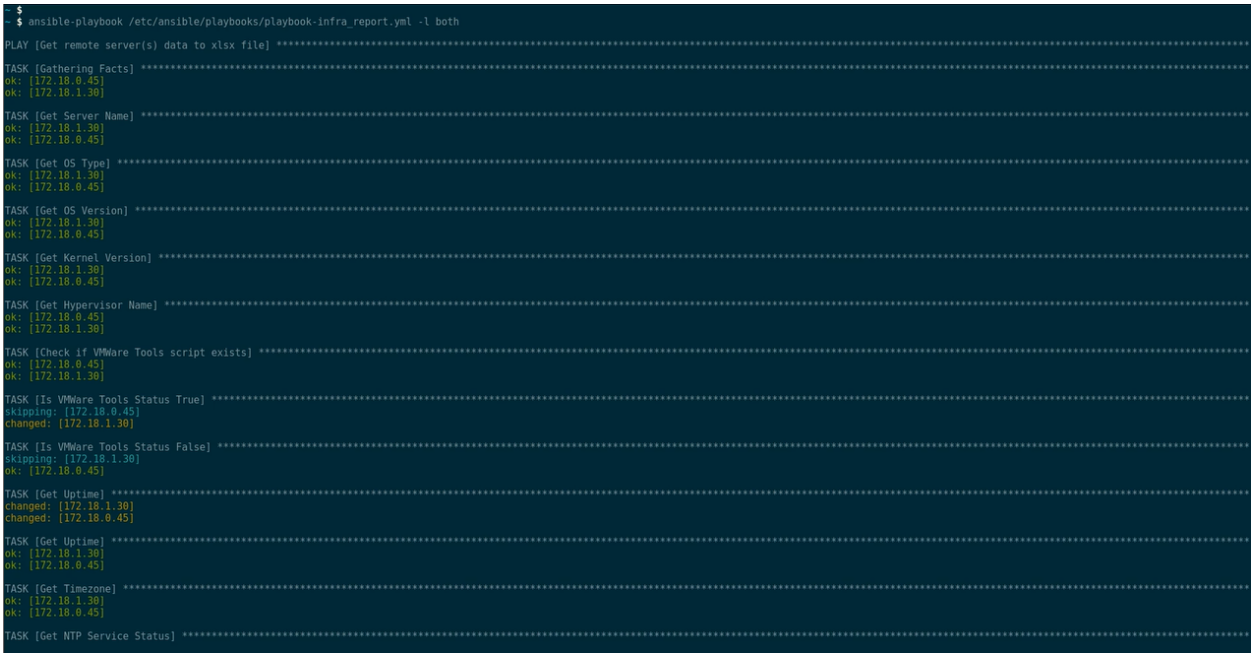


Fuente: elaboración propia.

5.1.5.1.2 Auditoría TI: automatizando la actualización de activos intangibles con Ansible

La actualización de equipo tecnológico es de suma importancia para contrarrestar los ataques cibernéticos debido a que no solo se aplican los parches que los encargados de la industria sacan para mejorar, sino también para protegerlos contra vulnerabilidades y nuevas formas de ataque que explotan los delincuentes cibernéticos. La automatización provoca que estos equipos se actualicen en paralelo; es decir que si se analizan los resultados que brinda la herramienta con el costo de inactividad, se demuestra lo importante que es realizar la actividad de actualizaciones en un momento que no afecte a la operación y que sea lo más pronto posible sin causar daños en el intento. Por tanto, la automatización por medio de Ansible permite hacer estas tareas repetitivas, pero de suma importancia, para que sean lo menos disruptivas posible, se evite los errores a causa de un descuido en la intervención del ser humano y que ayude a realizar la actividad en el menor tiempo posible. Con ello, se aumenta la eficiencia y, por supuesto, se logra tener al día los servidores en cuanto a temas de seguridad se refiere.

Figura 24. Actualizando activos con Ansible en varios servidores



Fuente: elaboración propia.

5.1.5.1.3 Auditoría TI: automatizando la seguridad de activos intangibles con Ansible

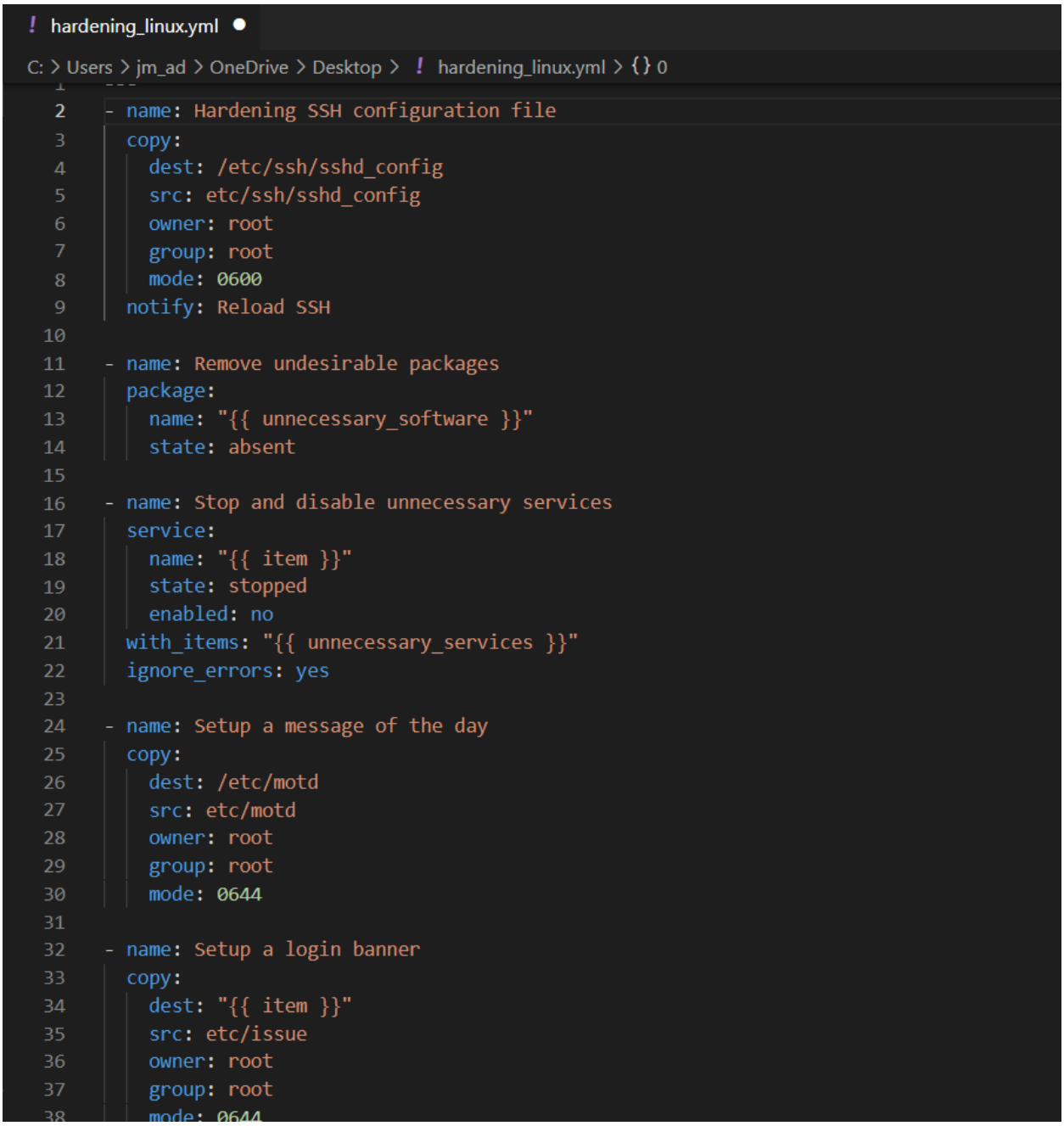
En situaciones de emergencia, si se requiere eliminar una vulnerabilidad, la automatización se puede tener como opción no solo de innovación, sino también de mejora en los métodos empleados para asegurar los activos que son bienes altamente apreciados dentro de una empresa.

Figura 25. Automatizando la seguridad de activos con Ansible

Vuln ID	Severity Type	Severity	STIG ID	Rule Title	Discussion	STIG	NIST SP 800-53 Revision 4 References	Legacy
V-230221	Cat I	High	RHEL-08-010000	RHEL 8 must be a vendor-supported release.	An operating system release is considered "supported" if	Red Hat Enter	CM-6 b	
V-230223	Cat I	High	RHEL-08-010020	RHEL 8 must implement NIST FIPS-validated cryptography fo	Use of weak or untested encryption algorithms undermir	Red Hat Enter	AC-17 (2)	
V-230234	Cat I	High	RHEL-08-010140	RHEL 8 operating systems booted with United Extensible Firm	If the system does not require valid authentication befor	Red Hat Enter	AC-3	
V-230235	Cat I	High	RHEL-08-010150	RHEL 8 operating systems booted with a BIOS must require a	If the system does not require valid authentication befor	Red Hat Enter	AC-3	
V-230264	Cat I	High	RHEL-08-010370	RHEL 8 must prevent the installation of software, patches, se	Changes to any software components can have significa	Red Hat Enter	CM-5 (3)	
V-230265	Cat I	High	RHEL-08-010371	RHEL 8 must prevent the installation of software, patches, se	Changes to any software components can have significa	Red Hat Enter	CM-5 (3)	
V-230283	Cat I	High	RHEL-08-010460	There must be no shosts.equiv files on the RHEL 8 operating	The "shosts.equiv" files are used to configure host-based	Red Hat Enter	CM-6 b	
V-230284	Cat I	High	RHEL-08-010470	There must be no .shosts files on the RHEL 8 operating syste	The ".shosts" files are used to configure host-based auth	Red Hat Enter	CM-6 b	
V-230329	Cat I	High	RHEL-08-010820	Unattended or automatic logon via the RHEL 8 graphical use	Failure to restrict system access to authenticated users r	Red Hat Enter	CM-6 b	
V-230380	Cat I	High	RHEL-08-020330	RHEL 8 must not allow accounts configured with blank or nu	If an account has an empty password, anyone could log	Red Hat Enter	CM-6 b	
V-230487	Cat I	High	RHEL-08-040000	RHEL 8 must not have the telnet-server package installed.	It is detrimental for operating systems to provide, or inst	Red Hat Enter	CM-7 a	
V-230492	Cat I	High	RHEL-08-040010	RHEL 8 must not have the rsh-server package installed.	It is detrimental for operating systems to provide, or inst	Red Hat Enter	CM-7 a	
V-230529	Cat I	High	RHEL-08-040170	The x86 Ctrl-Alt-Delete key sequence must be disabled on RH	A locally logged-on user, who presses Ctrl-Alt-Delete wh	Red Hat Enter	CM-6 b	
V-230530	Cat I	High	RHEL-08-040171	The x86 Ctrl-Alt-Delete key sequence in RHEL 8 must be disal	A locally logged-on user, who presses Ctrl-Alt-Delete, wh	Red Hat Enter	CM-6 b	
V-230531	Cat I	High	RHEL-08-040172	The systemd Ctrl-Alt-Delete burst key sequence in RHEL 8 mu	A locally logged-on user who presses Ctrl-Alt-Delete whe	Red Hat Enter	CM-6 b	
V-230533	Cat I	High	RHEL-08-040190	The Trivial File Transfer Protocol (TFTP) server package must	If TFTP is required for operational support (such as the tr	Red Hat Enter	CM-6 b	
V-230534	Cat I	High	RHEL-08-040200	The root account must be the only account having unrestrict	If an account other than root also has a User Identifier (	Red Hat Enter	CM-6 b	
V-230558	Cat I	High	RHEL-08-040360	A File Transfer Protocol (FTP) server package must not be ins	The FTP service provides an unencrypted remote access	Red Hat Enter	CM-6 b	
V-244540	Cat I	High	RHEL-08-020331	RHEL 8 must not allow blank or null passwords in the system	If an account has an empty password, anyone could log	Red Hat Enter	CM-6 b	
V-244541	Cat I	High	RHEL-08-020332	RHEL 8 must not allow blank or null passwords in the passwo	If an account has an empty password, anyone could log	Red Hat Enter	CM-6 b	
V-230222	Cat II	Medium	RHEL-08-010010	RHEL 8 vendor packaged system security patches and update	Timely patching is critical for maintaining the operationa	Red Hat Enter	CM-6 b	
V-230224	Cat II	Medium	RHEL-08-010030	All RHEL 8 local disk partitions must implement cryptographi	RHEL 8 systems handling data requiring "data at rest" pro	Red Hat Enter	SC-28	
V-230225	Cat II	Medium	RHEL-08-010040	RHEL 8 must display the Standard Mandatory DoD Notice an	Display of a standardized and approved use notification	Red Hat Enter	AC-8 a	
V-230226	Cat II	Medium	RHEL-08-010050	RHEL 8 must display the Standard Mandatory DoD Notice an	Display of a standardized and approved use notification	Red Hat Enter	AC-8 a	

Fuente: elaboración propia.

Figura 26. Código yaml o yml para automatizar la seguridad con Ansible



Fuente: Elaboración propia.

Capítulo VI. Conclusiones y recomendaciones

En el presente capítulo se detallan los resultados y el análisis respectivo de las diferentes herramientas disponibles para crear un plan de ciberseguridad acorde con las necesidades financieras de una empresa. Para el desarrollo de estos análisis, los montos utilizados están expresados en colones como porcentajes o en puntos porcentuales según corresponda.

6.1 Conclusión 1: Innovar es la estrategia empresarial necesaria

Se concluye que el país debe impulsar la innovación empresarial para poder mejorar y adaptarse a las necesidades actuales de mercado, también debe definir cuáles son los sectores de mayor productividad donde la innovación le permita a Costa Rica crecer por medio del valor que genera la difusión general de su práctica, en conjunto con las habilidades y conocimientos de el personal que tengan las empresas y el uso de la tecnología con la que se cuente, acorde con lo que requiere en la industria 4.0.

La Investigación juega un papel muy importante para poder innovar, generando una incidencia positiva en la administración general de las empresas, permitiendo que se complemente con los objetivos propuestos de cada compañía y a su vez permitiendo la transformación estructural que toda empresa necesita para un mejor desarrollo económico.

La innovación empresarial requiere de el análisis, la investigación y el desarrollo liderado por sus diferentes departamentos con el fin de buscar nuevos métodos, procesos o herramientas que les permitan mejorar su productividad, reducir costos y aumentar las ganancias.

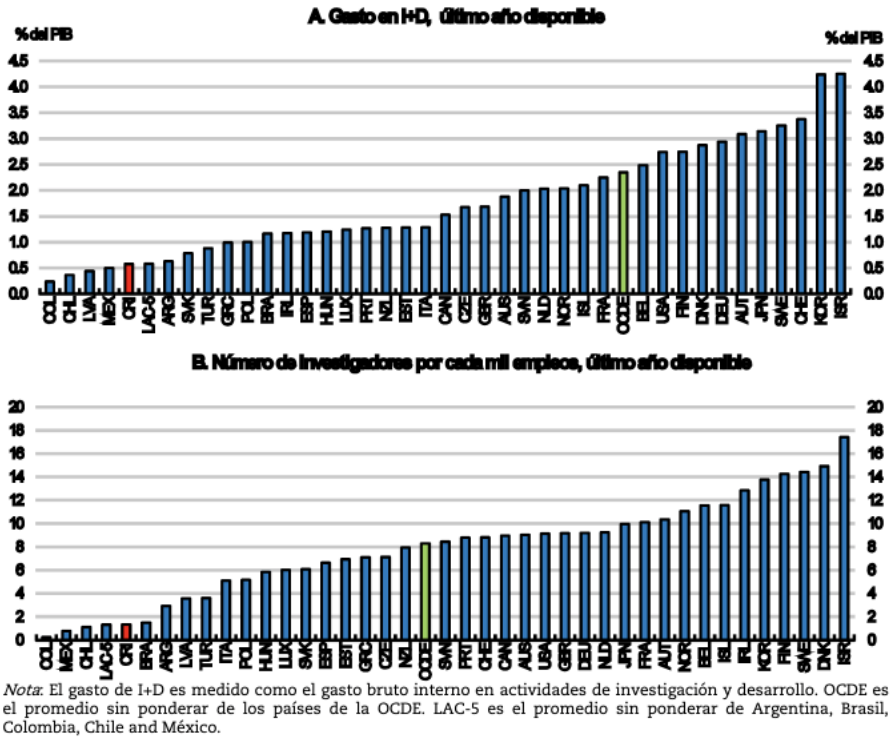
6.1.1 Situación Actual: El país debe incrementar la investigación y la innovación

Costa Rica a nivel general necesita mejorar mucho en el campo de la investigación y la innovación no solo para poder afrontar los retos que trajo esta década sino también para

continuar las relaciones comerciales de acuerdo con las exigencias y necesidades de otros países con los que se hacen negocios.

De acuerdo con la Organización para la Cooperación y el Desarrollo Económicos (OCDE), Costa Rica esta en clara desventaja en comparación con otros países en materia de investigación y desarrollo, así mismo en el número de investigadores por cada mil empleos.

Figura 27: Gasto en I+D y número de investigadores



Nota: El gasto de I+D es medido como el gasto bruto interno en actividades de investigación y desarrollo. OCDE es el promedio sin ponderar de los países de la OCDE. LAC-5 es el promedio sin ponderar de Argentina, Brasil, Colombia, Chile and México.

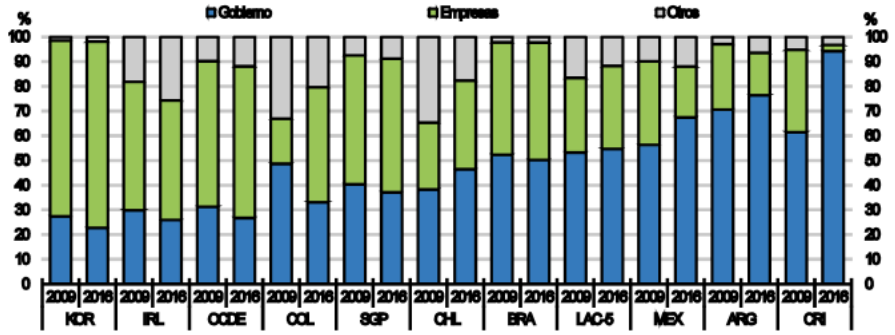
Fuente: OCDE, base de datos de Indicadores Principales de Ciencia y Tecnología; UNESCO Institute for Statistics.

Por otro lado, se debe reconocer el trabajo que el gobierno de Costa Rica viene haciendo para mejorar en investigación e innovación utilizando entidades gubernamentales como el MICITT para poder identificar las necesidades y requerimientos del país.

El Instituto Tecnológico de Costa Rica es uno de los pioneros en el país en materia de investigación, desarrollo e innovación que apoya al país en mejorar en esas áreas, reafirmando que a nivel público el país busca crecer en investigación y desarrollo, esto lo reafirma la

Organización para la Cooperación y el Desarrollo Económico (OCDE), donde muestra que Costa Rica a nivel gubernamental busca la mejora de el país.

Figura 28: Una gran y creciente proporción de I+D es financiada por el gobierno



Nota: El gasto de I+D es medido como el gasto bruto interno en actividades de investigación y desarrollo. OCDE es el promedio sin ponderar de los países de la OCDE. LAC-5 es el promedio sin ponderar de Argentina, Brasil, Colombia, Chile and México.

Fuente: OCDE, base de datos de Indicadores Principales de Ciencia y Tecnología; UNESCO Institute for Statistics.

6.2 Conclusión 2: Las empresas requieren proteger los datos

Se concluye que la protección de datos se divide en dos tipos que son los datos empresariales y los datos personales, ambos son un derecho que hoy más que nunca es necesario especialmente por la gran cantidad de medios en los que se puede divulgar e inclusive darle un mal uso a la información.

Los datos empresariales son de gran importancia, especialmente porque muchos países están adoptando leyes que exigen poner en práctica la protección de datos y requiere que sus socios comerciales lo hagan también.

La protección de datos es un tema complejo especialmente porque en la actualidad varían de acuerdo con el país, pero en el caso del GDPR representa un desafío importante para todo tipo de empresas ya que abarca aspectos nunca tomados anteriormente como es el tema de las sanciones a las compañías que no cumplan con la norma. GDPR presenta una serie de medidas innovadoras que expone a los países y empresas que no tienen ningún tipo de reglamento o medida para proteger datos, al mismo tiempo hace que se reflejen los riesgos y debilidades en que se incurre a causa de no utilizar ni diseñar algún modelo de protección.

La protección de datos empresariales de carácter extraterritorial busca demostrar que las naciones pueden hacer valer los derechos de sus ciudadanos por medio de el principio de jurisdicción universal y es por lo que las compañías deben prepararse mejor.

6.2.1 Situación Actual: El país debe mejorar en ciberseguridad

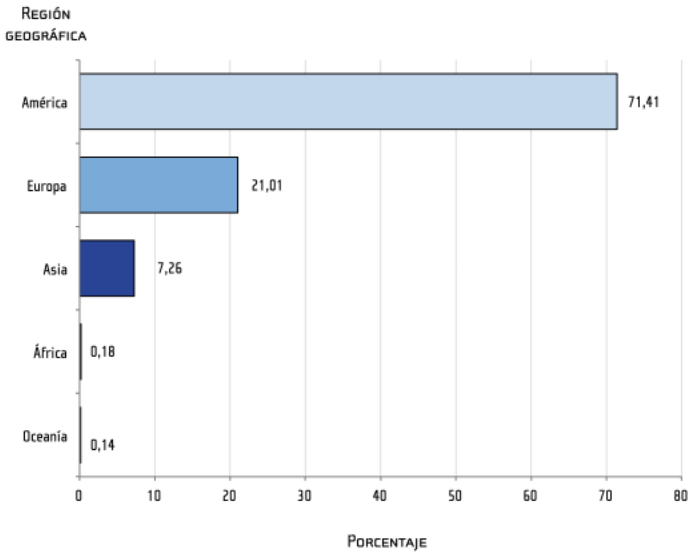
Costa Rica debe trabajar fuertemente en la protección de datos y eso conlleva a mejorar en ciberseguridad. Actualmente nuestro mercado depende comercialmente de Norte América especialmente de los Estados Unidos.

Es por ellos que la industria costarricense debe buscar ampliar sus horizontes y mejorar sus relaciones comerciales en otras latitudes que pueden sin duda alguna crecer y desarrollar la economía del país, pero para ellos deberá entender, incorporar y cumplir ciertas reglas como la de GDPR por parte de la Unión Europea.

Si se cumple con dicha norma que es la más robusta a nivel mundial en materia de protección de datos, existirá una gran oportunidad de poder expandir las relaciones comerciales con la Unión Europea.

Como lo indica la INEC (2020), en su informe de exportaciones la segunda área geográfica más grande con la que se cuentan relaciones comerciales para que el país pueda exportar es Europa.

Figura 29: Costa Rica. Distribución porcentual del valor de las exportaciones, según región geográfica, 2020



Fuente: INEC-Costa Rica. Estadísticas comercio exterior, 2020

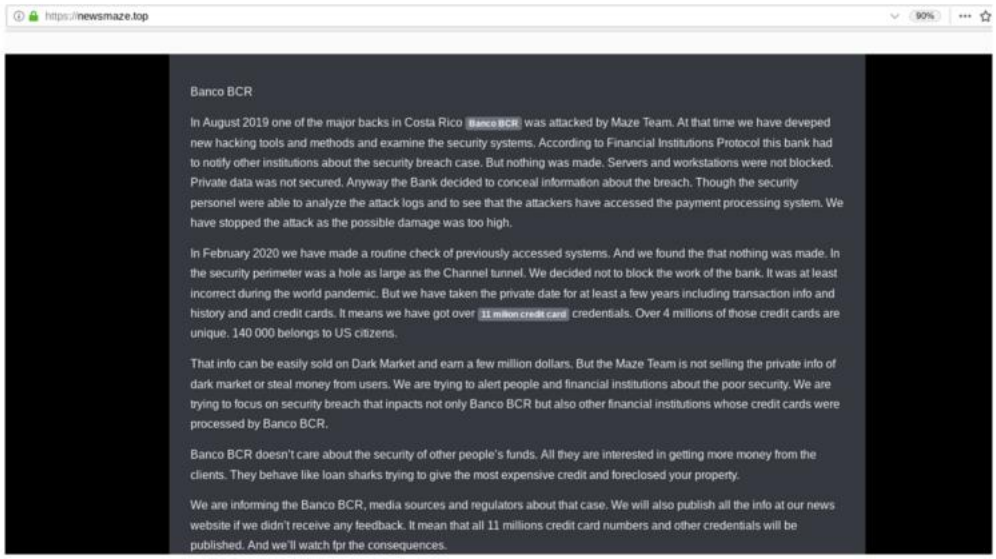
Actualmente existe la oportunidad de que las empresas nacionales puedan cumplir con la norma GDPR y al mismo tiempo llegar virtualmente a cumplir con la de naciones como Canadá, Brasil y otras de Asia que, manejan sus propias versiones sobre políticas de protección de datos al igual que su contraparte europea y que pueden llegar a solicitar cumplir sus normas si se desea continuar o tener relaciones comerciales.

Uno de los problemas en que se puede incurrir al no cumplir con esta norma es no tener implementado o no utilizar los mecanismos necesarios de ciberseguridad y este tema es de suma importancia en las empresas actuales para evitar riesgos y problemas.

En el año 2020 un grupo llamado Maze alegó haber atacado al Banco de Costa Rica (BCR) por medio de un programa malicioso llamado Maze ransomware, el cual consiste en un nuevo y sofisticado ransomware que ataca el Sistema Operativo Windows en empresas y organizaciones de todo el mundo.

El grupo llamado Maze exige un pago en criptomonedas a cambio de la recuperación segura de los datos cifrados, pero en caso de que las víctimas se niegan a pagar, los delincuentes amenazan con filtrar los datos confidenciales de las víctimas y aparentemente eso fue lo que hicieron con la información del BCR.

Figura 30: Información dada por el grupo llamado Maze



Fuente: A Life of Hacking (2021)

La protección de datos es vital, la publicación de información que se considera confidencial puede afectar grandemente a los usuarios, las empresas y el comercio en general.

Figura 31: Supuesta lista de sistemas ATM vulnerados

RESPONSE	TERMINALTRACE	REVERSED	UPDATEBALANCE	BACKOFFICEHOST	MERCHANTID	DATESTAMP	SYNCSTAMP	AUTHORIZER	CARDACQNA
50 Approved 012366 (00)	108006672	0	0 BCR		437	11:54.5	NULL	5	ATM MUNICI
50 Approved 050589 (00)	38001569	0	0 BCR		945	11:55.7	NULL	5	ATM MORAV
50 Approved 883459 (00)	250009557	0	0 BCR		401	12:09.9	NULL	5	ATM AG. BA
50 Approved 805492 (00)	198000155	0	0 BCR		939	11:49.8	NULL	5	ATM VASCO
50 Approved 000000 (00)	94009607	0	0 BCR		342	11:52.5	NULL	5	ATM SANTA
23 Approved 231157 (00)	395008013	0	0	0	241	11:57.5	NULL	2 2	ATM MAL PA
50 Approved 000000 (00)	381008478	0	0 BCR		359	12:10.2	NULL	5	ATM PASEO
50 Approved 000000 (00)	244004791	0	0 BCR		326	12:11.0	NULL	5	ATM COOPE
50 Approved 123462 (00)	382003551	0	0 BCR		235	12:15.6	NULL	5	ATM SUC NIC
50 Approved 000000 (00)	225007135	0	0 BCR		179	20:30.8	NULL	5	ATM CASA C
0 Unable to Dispense Cassettes D	150002941	0	0	0	0	20:31.0	NULL	5	
50 Approved 000000 (00)	61009558	0	0 BCR		954	20:37.1	NULL	5	ATM PLAZA
50 Approved 889986 (00)	275002932	0	0 BCR		218	00:34.9	NULL	5	ATM MUELLE
50 Approved 563936 (00)	44003553	0	0 BCR		541	00:35.2	NULL	5	ATM GOLFIT
50 Approved 000000 (00)	384005588	0	0 BCR		304	00:37.2	NULL	5	ATM AG EL R
50 Approved 000000 (00)	202004735	0	0 BCR		493	40:29.0	NULL	5	ATM PLAZOL
50 Approved 518418 (00)	198000502	0	0 BCR		939	40:38.1	NULL	5	ATM VASCO
50 Not Sufficient Funds (51)	202004736	0	0 BCR		493	40:51.7	NULL	5	ATM PLAZOL
50 Approved 000000 (00)	184004850	0	0 BCR		323	40:52.0	NULL	5	ATM BAGAC
23 Approved 720358 (00)	387004515	0	0	0	326	40:53.3	NULL	2	ATM MERCA
50 Approved 000000 (00)	99000044	0	0 BCR		196	41:00.1	NULL	5	ATM MONTE
50 Approved 559171 (00)	44008388	0	0 BCR		541	11:58.0	NULL	5	ATM GOLFIT
0 > Maximum Cash / BIN	37002450	0	0	0	953	11:58.3	NULL	5	ATM JACO 03
50 Approved 000000 (00)	237000904	0	0 BCR		347	11:59.0	NULL	5	ATM RIO CU
50 Approved 000000 (00)	184002777	0	0 BCR		323	43:34.5	NULL	5	ATM BAGAC
50 Approved 821662 (00)	165006969	0	0 BCR		327	43:35.5	NULL	5	ATM AGEN.
50 Approved 000000 (00)	153003848	0	0 BCR		479	43:35.8	NULL	5	ATM SARCHI
50 Approved 379353 (00)	343001413	0	0 BCR		964	23:48.0	NULL	5	ATM PLAZA
0 Unable to Dispense	3004383	0	0	0	0	23:48.3	NULL	5	
50 Approved 420963 (00)	219006731	0	0 BCR		437	23:49.5	NULL	5	ATM CIUDAD
50 Approved 765269 (00)	640003061	0	0 BCR		437	23:56.6	NULL	5	ATM C.C. PU
50 Approved 999081 (00)	9008622	0	0 BCR		921	24:04.0	NULL	5	ATM SN RAF
50 Approved 932399 (00)	451007845	0	0 BCR		437	24:05.1	NULL	5	ATM MULTI

Fuente: A Life of Hacking (2021)

Si no se toman las medidas necesarias ni se considera con seriedad el tema de la ciberseguridad no solo la empresa costarricense se expone a perder credibilidad y reputación, sino que también se puede exponer a no llegar a tener o mantener relaciones comerciales en otros mercados de gran importancia como lo es el europeo.

GDPR decidió multar a las empresas u organizaciones que no cumplen sus estatutos, a continuación, se muestran dos ejemplos de empresas cuyas industrias son la turística y la de banca y finanzas cuyas actividades también se dan en nuestro país y las misma localmente pueden tener usuarios o clientes europeos como la de los ejemplos que se citan no se pueden permitir caer en este tipo de multas que significarían perdidas económicas sin precedentes.

Las distintas empresas nacionales deben de implementar la ciberseguridad necesaria para evitar este tipo de situaciones y estar preparadas para eventualmente ser aceptadas en el mercado europeo o mantenerse en el mismo y así no depender nuestra economía únicamente de la Norte Americana.

Figura 32: Multa por incumplir con la protección de datos I

Fuente: El País, Julio 10, 2021

Figura 33: Multa por incumplir con la protección de datos II

Fuente: El País, enero 14, 2021

6.3 Conclusión 3: Las empresas requieren beneficiarse de la ciencia de datos

Se concluye que en la actualidad se genera una gran cantidad de información que nos permite conocer más a fondo a las empresas a nivel general.

El fracaso o éxito de las empresas será en base a la toma de decisiones y esas decisiones a su vez permitirá a las empresas ser más competitivas y sobre todo más eficientes, especialmente si se usaron herramientas tecnológicas en el proceso de la toma de decisiones.

El beneficio de la ciencia de datos y su máximo potencial aun no se conoce, las empresas tienen en sus manos una gran oportunidad para desarrollar la investigación por media de esta.

También hay que recordar que se requiere de un entrenamiento adecuado para obtener los resultados esperados y la situación se presta para que tanto las empresas públicas como las privadas integren en su uso cotidiano esta disciplina del saber que integra a su vez a otras ciencias, desarrollando resultados increíbles según la necesidad de la empresa.

6.3.1 Situación Actual: El país debe incursionar en la sociedad 4.0

Según la publicación del BID (2019) “Costa Rica Según un estudio encargado por Microsoft y realizado por el Centro para la Implementación de Políticas Públicas para la Equidad y el Crecimiento (CIPPEC), Costa Rica tiene un potencial significativo para el desarrollo de la Inteligencia Artificial (AI) por sus siglas en inglés.

El estudio sugiere que, si aumenta la tasa de adopción de tecnologías relacionadas con la Inteligencia Artificial, el crecimiento económico podría aumentará en 1 punto porcentual adicional del PIB por año en la próxima década, alcanzando el 5,7 por ciento. Para superar los desafíos y aprovechar esta oportunidad, el rol del gobierno es clave para promover y facilitar el proceso de adopción de tecnología (Albrieu et al.2019)".

Esto nos indica que el país debe poner su mirada en el uso de nueva y mejor herramientas tecnológicas que les permitan a los gerentes ser mas precisos y acertados en sus análisis y toma de decisiones para el beneficio de la empresa.

El uso de estas herramientas se puede extender según la necesidad al personal de los diversos departamentos que constituyen a la empresa.

6.4 Conclusión 4: Las empresas deben mejorar sus costos y ganancias

Se concluye que se debe visualizar un mejor uso de los recursos con que cuenta la empresa, a nivel gerencial se debe poner mucha atención al UAIIDA o Utilidades antes de intereses pagados, impuestos, depreciación y amortización (EBITDA, por sus siglas en inglés) ya que este juega un papel muy importante como indicador financiero en la determinación del valor de cualquier compañía porque no solo describe las ganancias operativas, sino también que se utiliza como criterio para establecer el precio que un potencial inversor estaría dispuesto a pagar por la misma.

EBITDA se puede utilizar como una medida de rentabilidad, los dos componentes principales de las ganancias son los ingresos y los costos, por tanto, cualquier actividad que aumente los ingresos o reduzca los costos tendrá un impacto directo en el EBITDA.

Por medio de la implementación de la automatización por ejemplo se puede llegar a disminuir diferentes tipos de gastos que van a variar según las circunstancias y verse reflejados sin duda alguna.

Así mismo si se implementan mecanismos de seguridad para proteger datos se pueden aumentar los ingresos al ser eventualmente aceptado en el mercado europeo por cumplir entre muchas cosas con la ley GDPR y todo esto a su vez se traduciría en más ventas, más ganancias y una disminución de costos.

6.4.1 Situación Actual: El país debe mejorar económicamente

Costa Rica debe sin duda alguna apoyarse en los recursos tecnológicos que están a su alcance, especialmente para insertar en el país una cultura administrativa que sin importar el tamaño de la empresa se comprenda como buscar otras alternativas de análisis que le permitan a las compañías disminuir costos al acelerar los tiempos de ejecución de las tareas, la disminución de mano de obra en una misma tarea y la utilización más eficiente del recurso humano para utilizarlos en otras tareas que pueden de igual forma traer nuevos beneficios.

Existen muchas oportunidades para que el país crezca económicamente, pero deberá cambiar en muchos aspectos y uno de ellos es la mentalidad de que la investigación y desarrollo, así como también la innovación son temas exclusivos de entidades gubernamentales y que este tipo de prácticas pueden posicionar al país en nuevos campos.

Las empresas pueden ayudar a que Costa Rica en el corto tiempo aumente su capacidad económica pero la cultura administrativa debe cambiar y será esencial que se incursione en nuevos campos que nos permitirá tener las puertas abiertas de nuevos mercados que requieran nuestros productos, mano de obra y servicios.

6.5 Recomendación 1: Usar la automatización como estrategia de innovación

Costa Rica debe desarrollar una nueva estrategia de innovación y la automatización puede jugar un papel muy importante en el desarrollo económico de el país ya que cada vez mas emprendimientos basan su empresa en el comercio electrónico donde es fundamental el uso de servidores, computadoras y tecnología en general.

Otras industrias como el sector salud brindan servicios del tipo 24 x 7 los 365 días del año como es el caso de los hospitales o clínicas privadas por lo que cada vez es más difícil detener el uso de sus equipos tecnológicos para mantenimiento.

Debido a que no solo las empresas nacionales y multinacionales que se encuentran en territorio nacional están basando su economía en el uso de la tecnología sino también a nivel internacional la automatización es necesaria para ser disruptivos de la menor manera posible.

Se recomienda utilizar la plataforma de automatización de equipo tecnológico perteneciente a IBM y administrado por RedHat que se llama Ansible Core que es gratuito.

TECNOLOGÍA	COSTO	USO
Ansible Core	Gratis	Automatizar tareas tecnológicas

Por medio de la automatización se disminuyen diferentes tipos de gastos que van a variar según las circunstancias por ejemplo si buscamos proteger a nivel de ciberseguridad los servidores de un banco y se agenda una ventana de tiempo determinada para actualizarlos los gastos que genera dicha actividad se podrán disminuir drásticamente al evitar contratar más personal para realizar la actividad, evitar el pago de horas extra, utilizar menos personal, evitar errores humanos que generan más gasto de tiempo y dinero.

A continuación, podemos observar el desglose de las actividades que conlleva actualizar cien servidores, práctica que se recomienda para no solo tener el equipo actualizado y protegido de amenazas cibernéticas sino también para asegurarnos que cumplimos con una de las medidas necesarias que debe cumplir toda empresa para protegerse de ataques cibernéticos.

Para calcular el costo manual de actualizar un servidor aplicamos:

(((T * S) /60) /I) * (I * C)

T	Duración
S	Núm. Servidores
I	Núm. Ingenieros
C	Costo x Hora del Ingeniero

Figura 34: Actualización manual vs automatizada

TAREA	Ejecutor	Duración (minutos)	Núm. Servidores	Núm. de Ing	Costo Hra Ing	Costo Manual
Auditar el Servidor 1	Administrador de Sistema Operativo	5	100	4	₡30.000,00	₡250.000,00
Detener BD/APPS	Administrador de Base de Datos o Apps	10	100	4	₡30.000,00	₡500.000,00
Actualizar el Servidor	Administrador de Sistema Operativo	20	100	4	₡30.000,00	₡1.000.000,00
Iniciar BD/APPS	Administrador de Base de Datos o Apps	10	100	4	₡30.000,00	₡500.000,00
Auditar el Servidor 2	Administrador de Sistema Operativo	5	100	4	₡30.000,00	₡250.000,00
Total						**₡2.500.000,00**

TAREA	Ejecutor	Duración * Servidor (min)	Núm. Servidores	Núm. de Ing	Costo Hra Ing	Costo Automatizado
Auditar el Servidor 1	Ansible	0,5	100	0	₡0,00	₡0,00
Detener BD/APPS	Ansible	0,5	100	0	₡0,00	₡0,00
Actualizar un Servidor	Ansible	8	100	0	₡0,00	₡0,00
Iniciar BD/APPS	Ansible	0,5	100	0	₡0,00	₡0,00
Auditar el Servidor 2	Ansible	0,5	100	0	₡0,00	₡0,00
Auditar el Servidor 3	Administrador de Sistema Operativo	1,5	100	1	₡30.000,00	₡75.000,00
Total						**₡75.000,00**

TAREA	Actualización Manual	Actualización Automatizada
	₡2.500.000,00	₡75.000,00
Total de Ahorro con Automatización		₡2.425.000,00

Fuente: Elaboración propia

Para realizar la actividad se requiere un total de cuatro ingenieros, que deberán de auditar los activos intangibles de cada servidor en este caso es el software o programas informáticos que están instalados en cada uno de ellos, ya que se requiere sabe el nombre de cada programa, su versión y sus dependencias antes de actualizarlos en caso de que si por alguna razón se deba devolver a su estado original se tenga el registro de como se encontraba antes de la actividad.

Posteriormente se requieren cuatro encargados de bases de datos o aplicaciones para que las detengan y que puedan asegurar que la operación no dañará los datos o información sensitiva del banco. La siguiente actividad la ejecutan cuatro administradores de sistemas que inician el parcheo o actualización de cada uno de los servidores. Cuando se termina esta actividad los administradores de las bases de datos o aplicaciones deberán reiniciarlas y asegurarse de que se recolectará y asegurará la información bancaria de nuevo.

El siguiente paso es que de nuevo los cuatro administradores de sistemas vuelven a ejecutar una auditoría de activos intangibles como se dijo anteriormente es para tener un registro de el nombre, cantidad y versión de cada programa o software que se encuentre instalado. Finalmente, proceden a revisar cada servidor para asegurarse que funcionan como se espera.

EBITDA se utiliza especialmente para analizar el desempeño operativo de una compañía o proyecto, ya que indica la dimensión de la cantidad que genera el negocio en sí mismo de la empresa o proyecto, en este caso se mejora sin duda el desempeño de esta actividad tan importante al utilizar la automatización debido a que su implementación es gratuita por ser Ansible código abierto, además de disminuir drásticamente el tiempo que toma actualizar los servidores por lo que el tiempo de disrupción es mínimo así mismo se denota la drástica disminución del costo de la actividad de ₡2,500,000.00 a ₡75,000.00 llegando a ser el total de ahorro ₡2,425,000.00.

Usemos como referencia el siguiente caso: La empresa llamada “Hospital Privado” donde podemos estimar la reducción de los gastos de administración por concepto de automatización de ₡3,500,000.00 a ₡1,075,000.00

Figura 35: Estado de Resultado con ahorro por automatización

Hospital Privado ESTADO DE RESULTADOS Periodo 2021		
	2021	2021
PERIODOS	**real**	**estimado**
ventas netas	18.020.300	18.020.300
costo de ventas	10.821.200	10.821.200
UTILIDAD BRUTA	**7.199.100**	**7.199.100**
gastos de ventas	1.485.700	1.485.700
gastos de administracion	3.500.000	1.075.000
total gastos de operacion	**4.985.700**	**2.560.700**
UTILIDAD DE OPERACION	**2.213.400**	**4.638.400**
gastos financieros	1.990.700	1.990.700
otros gastos	98.700	98.700
otros ingresos	81.900	81.900
utilidad antes de impuesto	**205.900**	**2.630.900**
impuesto de renta	61.770	789.270
UTILIDAD NETA	**144.130**	**1.841.630**
detalle		
gastos de administracion		
salarios	2.500.000	75.000
depreciacion	1.000.000	1.000.000
	3.500.000	**1.075.000**
	-	-
gastos financieros		
intereses en deudas	1.615.700	1.615.700
comisiones bancarias	375.000	375.000
	1.990.700	**1.990.700**

Fuente: Elaboración propia

En este caso la empresa “Hospital Privado” debe mantener su equipo actualizado ya que cuenta con sucursales tanto fuera como adentro del país, mantiene un registro muy estricto de la información de sus clientes que en este caso son los pacientes, los cuales hay muchos procedentes de Europa que son atraídos por la calidad de su servicio y que cuenta con mejores precios que en Europa por lo que incurrieron en el turismo médico y esto les obliga a cumplir con la norma GDPR.

Al aplicar la automatización de todos sus equipos se obtiene el siguiente resultado:

- Se estima que para el periodo 2021 la utilidad bruta no presentaría cambios por cuanto este margen solo utiliza ventas netas y costo de ventas netas, los cuales no tiene incidencia por el cambio que presento el uso de la automatización.
- Disminuye en forma significativa en un 31,75% lo gastos administrativos

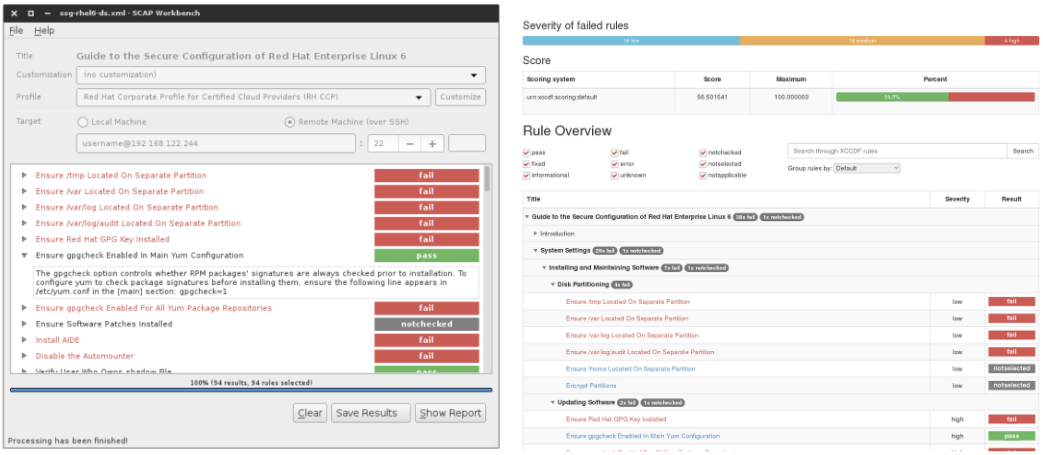
6.6 Recomendación 2: Usar la Automatización y la Ciberseguridad para proteger los datos

En base al ejemplo anterior para la empresa “Hospital Privado” por medio de Ansible se pueden aplicar recomendaciones de ciberseguridad dadas por el Centro para la seguridad de la

internet (CIS) por sus siglas en inglés y visualizar los resultados por medio de una herramienta llamada OpenScap sin incurrir en ningún gasto ni tampoco en pagos de licencia por ser herramientas de código abierto.

Se puede aplicar tanto en computadoras personales como en servidores, dando como resultado una mayor seguridad cibernética de los equipos, esto a la vez implica asegurar la información que contengan cumpliendo con la norma GDPR.

Figura 36: Resultados del escáner de OpenScap



Fuente: OpenScap (2021)

Si cumple con la ley de la Unión Europea en este caso la norma GDPR la empresa puede continuar perfectamente relaciones comerciales con ciudadanos europeos o asegurarse de que será aceptado por los mismos al velar y asegurar por la información privada y confidencial de los pacientes.

También puede obtener nuevos pacientes que soliciten información sobre temas concernientes a la protección de datos como lo son personas provenientes de Canadá donde se cuenta con la Ley de Protección de Información Personal y Documentos Electrónicos (PIPEDA) por sus siglas en inglés, similar en muchos aspectos a la ley GDPR.

Esto les permite a las empresas costarricense poder tener presencia en otros mercados y países donde contemplan utilizar leyes similares aplicables a todo tipo de industria.

6.7 Recomendación 3: Usar la ciencia de datos como estrategia de innovación

Gracias a las herramientas de la ciencia de datos a nivel gerencial se puede mejorar a la hora de tomar decisiones debido a la obtención de resultados más precisos que los que teníamos en el pasado.

Una de las actuales controversias a nivel empresarial es entender y saber como se cuantifica el riesgo cibernético para justificar la compra de equipo de ciberseguridad y que sea aprobado por el departamento de finanzas.

En el pasado se utilizaba el uso exclusivo de las llamadas matrices de riesgo, que si bien es cierto se rescata de ellas que es un intento de modelar los riesgos cibernéticos, como base inicial es una buena iniciativa, pero produce muchos sesgos.

Hipotéticamente hablando digamos que gerencia general convoca al gerente de TI y le consulta lo siguiente:

¿Cuánto se debe invertir por empleado en entrenamiento de *phishing*?

La matriz de riesgo puede califica usualmente al *phishing* como una amenaza de "Alto Riesgo", entonces se deduce que el cuadro rojo o el mensaje de "Alto Riesgo" indica que sí deberíamos proveer el entrenamiento pero no nos dice el monto que se debería invertir.

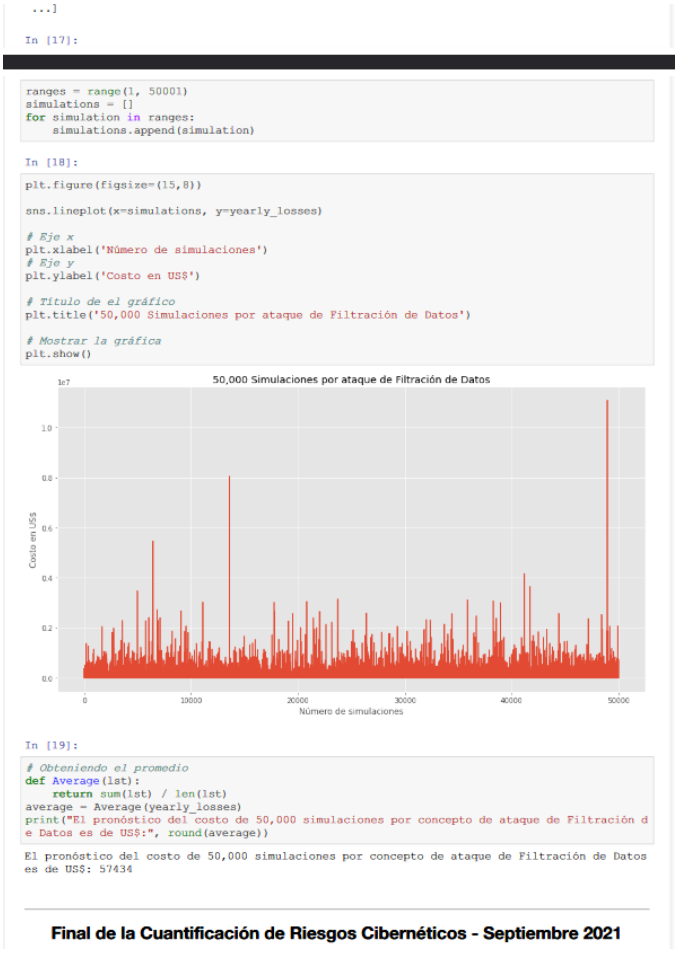
Otro tipo de preguntas que pueden surgir son:

¿Cuál es el valor económico que un firewall le retornaría a la empresa? En caso de que el presupuesto elaborado por gerencia de TI incluya la compra de un *firewall* por valor de ₡586,500.00.

¿Qué posibilidades hay de que la empresa pierda dinero ante un potencial ciberataque durante el año 2022? ¿Puede mostrar un listado de riesgos y el potencial valor económico en perdidas que generaría cada uno de esos riesgos?, etc.

Ante este tipo de cuestionamientos, se entiende que la matriz de riesgo no es suficiente para entender la situación o entorno como se requiere, pero por medio de modelos estadísticos aplicados y el uso del lenguaje de programación PYTHON si se puede realizar una mejor cuantificación como se demuestra en el anexo 9.

Figura 37: $57,434.00 el costo por concepto de filtración de datos



Fuente: Elaboración propia

En este caso gracias a PYTHON y la Estadística se puede comprender el costo económico de un eventual ataque cibernético, también permite que las empresas comprendan la necesidad de estar seguras proteger no solo su equipo sino también los datos.

Por ello se recomienda que las empresas establezcan una cultura de gestión de riesgos para que pueda generarse el efecto conocido como apetito al riesgo, el cual consiste en desarrollar el control de el manejo de los riesgos que se considera que pueden afectar a la empresa con base en la industria en la que se encuentra y en las actividades que realiza, de esta forma se sabe el desempeño deseado y el desempeño real.

Esto permite también entender como se La mejora del proceso de gestión de riesgos se desarrolla con la identificación de riesgos basada en el análisis y la opinión de los expertos para obtener datos, cruzar esas recomendaciones con lo que dicen los estudios internacionales y públicos para los temas de ciberseguridad. Una vez que se tengan los datos que corresponden a las mayores amenazas a las que la empresa se puede enfrentar se procede a aplicar las estimaciones cuantitativas de probabilidad e impacto para generar una "curva de pérdida-excedencia" utilizando simulaciones de Monte Carlo.

Las simulaciones de Monte Carlo permiten combinar múltiples estimaciones de rangos de valores simulando miles de ensayos aleatorios; en los que, por ejemplo, el resultado de 1000 simulaciones puede dar una idea del valor o costo económico del riesgo, pero en busca de una estimación real podemos utilizar 50 000 estimaciones. Los resultados de las simulaciones se combinan y se grafican para su análisis administrativo. Gracias a los modelos estadísticos y de PYTHON, esto se puede hacer sin incursionar en gastos.

También, se recomienda utilizar y explorar modelos de automatización que aceleren el tiempo de ejecución de tareas. Este procedimiento no elimina la mano de obra como se cree, al contrario, mejora el rendimiento del equipo, ahorra dinero y no genera errores que provocarían que se incursione en más gastos o, peor aun, que se pierdan clientes. Como recomendación final, se debe dar al personal entrenamiento en el área de seguridad, explicarle la importancia que tienen sin importar que tareas realizan dentro de la organización para reducir el riesgo de un ataque, pues solo siendo responsables, se disminuye la carga que puede tener el departamento de TI.

6.8 Recomendación 4: La nueva estrategia empresarial en la mejora de costos e ingresos

A nivel empresarial tanto los costos como los ingresos van a variar de acuerdo con la industria y el manejo administrativo que experimente la empresa. Debido a la disminución de ingresos que sufrieron muchas compañías durante los años 2020 y 2021 cada vez es mas recurrente escuchar que se solicite una disminución de los costos y un aumento en las ganancias.

La nueva estrategia empresarial incluye la mejora de costos e ingresos mediante diferentes métodos uno de ellos es disminuir el error humano por medio de la automatización.

En el ámbito gerencial, cuando se comete un error se pide un análisis de causa raíz (RCA) por sus siglas en inglés para obtener respuestas sobre lo ocurrido, pero muchas veces no eliminan la causa real debido a no poder encontrar el motivo y en tecnología ese hecho es recurrente.

La automatización no solo elimina el error humano sino también que potencializa su trabajo al llegar a ejecutarse exitosamente eliminado la posibilidad de incurrir en gastos extra, otra forma de evitar gastos es hacer cumplir lo que se llama en tecnología de la Información como contrato de nivel de servicio (SLA) por sus siglas en inglés, donde se especifica los tiempos de duración de un servicio determinado, donde si estos no se cumplen las empresas deberán pagar una multa. Este tipo de sanciones ocurren mucho en las empresas de tecnología.

La posible eliminación, o no, de un error en términos financieros es un lujo que no se puede permitir, por lo que se deben implementar controles que se encarguen de eliminar ese tipo de errores, los cuales provocan que todos, en algún momento, estemos expuestos a eso.

Los controles deben ser periódicos para que, constantemente, se busquen las posibles vulnerabilidades.

Por ejemplo, como se expuso las contraseñas son un caso típico que genera una gran vulnerabilidad, llegando a crear grandes perdidas económicas por lo que se tiene que prevenir a toda costa por medio de la utilización de herramientas como PYTHON tal y como se demuestra en los anexos 4 y 5.

Gracias a el análisis de datos podrá comprender tanto los factores externos como internos de una empresa con mayor precisión.

Por ejemplo se puede llegar a entender lo que los clientes están comprando y sus preferencias, como también ser capaz de medir y comprender la situación del clima laboral interno como se demuestra en el anexo 10 donde la intención es poder identificar las personas que potencialmente vayan a renunciar mediante el uso del entrenamiento de máquinas o Machine Learning y así evitar perder mano de obra calificada que cuesta tiempo y dinero entrenar y formar en muchas empresas según el puesto que desempeñen.

También identificar aquellas personas que trabajan desde la casa y que requieran recibir primero un entrenamiento de seguridad porque trabajan desde la casa y potencialmente están más vulnerables a nivel de ciberseguridad.

Como se sabe el objetivo de un análisis de datos eficaz es ayudar a identificar oportunidades clave, desafíos y la generación de mayores ingresos.

Sin duda alguna la automatización permite ahorrar en costos e incrementar las ganancias, volviendo a retomar el ejemplo inicial llamado “Hospital privado” podemos utilizar indicadores financieros para conocer a fondo la situación de la empresa.

Figura 38: Estado de Resultado con ahorro por automatización con indicadores financieros

Hospital Privado ESTADO DE RESULTADOS Periodo 2021		
	2021	2021
PERIODOS	**real**	**estimado**
ventas netas	18.020.300	18.020.300
costo de ventas	10.821.200	10.821.200
UTILIDAD BRUTA	**7.199.100**	**7.199.100**
gastos de ventas	1.485.700	1.485.700
gastos de administracion	3.500.000	1.075.000
total gastos de operacion	**4.985.700**	**2.560.700**
UTILIDAD DE OPERACION	**2.213.400**	**4.638.400**
gastos financieros	1.990.700	1.990.700
otros gastos	98.700	98.700
otros ingresos	81.900	81.900
utilidad antes de impuesto	**205.900**	**2.630.900**
impuesto de renta	61.770	789.270
UTILIDAD NETA	**144.130**	**1.841.630**
detalle		
gastos de administracion		
salarios	2.500.000	75.000
depreciacion	1.000.000	1.000.000
	3.500.000	**1.075.000**
	-	-
gastos financieros		
intereses en deudas	1.615.700	1.615.700
comisiones bancarias	375.000	375.000
	1.990.700	**1.990.700**

	2021	2021
INDICADORES	**real current**	**estimated**
Margen de Utilidad Bruta	40%	40%
Margen de Utilidad Operacional	12%	26%
Margen de Utilidad Neta	1%	10%
Margen EBITDA	16%	29%

	2021	2021
EBITDA	**real current**	**estimated**
utilidad neta	144.130	1.841.630
intereses	1.615.700	1.615.700
impuestos	61.770	789.270
amort (depreciación)	1.000.000	1.000.000
	2.821.600	**5.246.600**

Fuente: Elaboración propia

- Se estima que para el periodo 2021 la utilidad bruta no presentaría cambios por cuanto este margen solo utiliza ventas netas y costo de ventas netas, los cuales no tiene incidencia por el cambio que presento el uso de la automatización.
- La empresa en el año 2021 estima que por medio de la automatización poseería un margen de utilidad operacional con un comportamiento de alta mejoría que pasaría de 12% a un 26%. Es decir, por cada 100 colones de ventas la empresa produciría 26 colones de ganancia estimada, lo cual esta relacionado directamente con una baja en los gastos de la empresa.

- La empresa en el año 2021 estima que por medio de la automatización llegaría a poseer un margen de utilidad neta con un comportamiento de alta mejoría pasando de 1% a un 10%. Mostrando una mayor eficiencia en la empresa.
- La empresa en el año 2021 presenta un margen de utilidad operacional con un incremento que va de 21% a un 40%. Se presenta en el mismo periodo una disminución de los gastos generales y de administración beneficiando con respecto al periodo anterior.
- El margen ebitda proporciona información sobre la rentabilidad de una empresa en términos de sus procesos operativos. Para el período 2021 se presentaría un margen EBITDA de un 29%.

6.10 Conclusión y Recomendación Final

Se concluye que actualmente el país esta en una etapa prematura de la inserción a la sociedad 4.0, lo que abre las puertas a la innovación donde la empresa privada tiene que impulsar más su adopción.

La innovación debe ser basada en las finanzas es decir en nuevas fuentes de ingresos que le permitan a la empresa costarricense no solo diferenciarse de su competidor sino también poder ingresar a nuevos mercados y poder generar mayores ganancias.

Se expuso como ejemplo la utilización de Ansible, en empresas que se dediquen al servicio de ciberseguridad o de tecnología de la información en general sin duda alguna este tipo de servicio es innovador y llega a generar grandes ganancias porque no se gasta por su adquisición, pero si disminuye el tiempo de trabajo y por lo tanto de costos, igualmente logra generar más servicios que al final se traducen en más dinero por la velocidad en que se ejecutan.

La automatización al ser uno de los componentes que permiten innovar no solo genera mejores ganancias sino también como ya se explicó disminuye los costos, agiliza procesos y tiempos de respuesta que es lo que se busca hoy en día en un mercado cada vez más exigente.

Las empresas deben comprender que la ciberseguridad no es solo para el personal de cómputo, en realidad es para cada integrante de la empresa. Los problemas cibernéticos crecen desproporcionalmente y se tienen que tomar medidas efectivas que contrarresten esta problemática. Para ello, se debe entender a la perfección qué es, cómo ocurre y cómo se puede

colaborar para evitarlos sin importar la función que se desempeñe dentro de la empresa esto evitará tener problemas económicos, llegar a sufrir extorsiones por parte de personas.

La toma de decisiones debe ser también alineada con la innovación que requieran las empresas y esta a su vez a nivel de las finanzas para que se considere en todo momento como obtener mejores ganancias y menores costos, mostrando en todo momento unas finanzas sanas.

Referencias

Accenture. (2021). *Noveno estudio anual del Coste del Cibercrimen*. Recuperado de: https://www.accenture.com/es-es/insights/security/cost-cybercrime-study

Akula Madhu. (2017). *Security Automation with Ansible 2.* (1ª ed). Packt Publishing Ltd.

A Life of Hacking. (2021). Maze Group: Y la fuga de 11 Millones de registros financieros de clientes del banco de Costa Rica. Recuperado de: https://www.estebanjimenez.com/post/maze-group-fuga-de-11-millones-de-registros-financieros-de-clientes-del-banco-de-costa-rica

Ansible. (2021). RedHat Ansible. Recuperado de: https://www.ansible.com/

Aurélien Géron. (2019). *Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems* (2da edición). O'Reilly Media, Inc.

Azofeifa-Z., C. E. (2004). Aplicación de la Simulación Monte Carlo en el cálculo del riesgo usando Excel. Revista Tecnología En Marcha, 17(1), pág. 97–109. Recuperado a partir de https://revistas.tec.ac.cr/index.php/tec_marcha/article/view/1438

Banco Interamericano de Desarrollo. (2019). Artificial Intelligence for social good in Latin America and the Caribbean. Recuperado de: https://publications.iadb.org/es/publications/english/document/Artificial-Intelligence-for-Social-Good-in-Latin-America-and-the-Caribbean-The-Regional-Landscape-and-12-Country-Snapshots.pdf

Barrantes, Echavarría. (2013). La investigación: un camino al conocimiento (2da. edición). Ágora: Serie Estudios.

Calder Alan. (2020). The *Security Handbook – Prepare for, respond to and recover from cyber-attacks.* (1ª ed). IT Governance Publishing.

Carnegie Endowment for International Peace. (2020). How to Protect the Global Financial System from Cyber Threats [Video]. Disponible en: https://carnegieendowment.org/specialprojects/fincyber/about/

Castro, Johnny. (15 de mayo de 2020). Costa Rica registró casi 32 millones de intentos de ciberataques en primeros tres meses. *La Republica*. https://www.larepublica.net/noticia/costa-rica-registro-casi-32-millones-de-intentos-de-ciberataques-en-primeros-tres-meses

Check Point. (2021). Live Cyber Threat Map. Recuperado de: https://threatmap.checkpoint.com/

Cinde. (2021). Empresas de zonas francas generan 72% de las exportaciones de servicios de alto valor agregado del país. Recuperado de: https://www.cinde.org/es/noticias/empresas-de-zonas-francas-generan-72-de-las-exportaciones-de-servicios-de-alto-valor-agregado-del-pais

Comex. (2021). CP-2565 Multinacionales aportan la mayoría de empleos en Costa Rica durante la pandemia. Recuperado de: https://www.comex.go.cr/sala-de-prensa/comunicados/2020/diciembre/cp-2565-multinacionales-aportan-la-mayor%C3%ADa-de-empleos-en-costa-rica-durante-la-pandemia/

CSO Computerworld España. (2020). El dinero supera al espionaje como principal motivo de los ciberataques. Recuperado de: https://cso.computerworld.es/cibercrimen/el-dinero-supera-al-espionaje-como-principal-motivo-de-los-ciberataques

Deep Instinct. (2021). Cyber Threat: Report on 2020 Shows Triple-Digit Increases across all Malware Types. Recuperado de: https://www.deepinstinct.com/news/cyber-threat-report-on-2020-shows-triple-digit-increases-across-all-malware-types

EC-Council. (2021). *What is Ethical Hacking?*. Recuperado de: https://www.eccouncil.org/ethical-hacking/

FireEye. (2021). FireEye Cyber Threat Map. Recuperado de: https://www.fireeye.com/cyber-map/threat-map.html

Fisa Group. (2021). *Ciberseguridad │Retos para el sector bancario este 2021*. Recuperado de: https://www.fisagrp.com/blogs/ciberseguridad-reto-sector-bancario-2021.html

Glogowski, Artur. (2021). Red Hat Ansible Engine 2.8 DO447 Advanced Automation: Red Hat Ansible Best Practices. (2da edición). Red Hat, Inc.

Gitman, Lawrence J.; Zutter, Chad J.. *Principios de Administración Financiera*. (12da edición). Pearson Educación.

Gitman, Lawrence J.; Joehnk, Michael. *Fundamentos de Inversiones*. (10ma edición). Pearson Educación.

Hernández Sampieri, R, Fernández, C & Baptista, P. (2014). Metodología de la Investigación. (6a. edición). México D.F, México: Mc Graw Hill/Interamericana Editores, S.A. de C.V.

Hsiang-Chih Hsu, Tony (2019). *Practical Security Automation and Testing*. (1ª ed). Packt Publishing Ltd.

IBM. (2021). *How much does a data breach cost?*. Recuperado de: https://www.ibm.com/security/data-breach

INEC. (2020). Estadística de Comercio Exterior 2020: Datos preliminares. Recuperado de: https://www.inec.go.cr/sites/default/files/documetos-biblioteca-virtual/recomex-preli2020.pdf

Isaca. (2017). *The CISM Review Manual* (15th Edition). Isaca.

ITU. (2021). Global Cybersecurity Index 2020. Recuperado de: https://www.itu.int/epublications/publication/global-cybersecurity-index-2020/en/

ISACA. (2021). COBIT® An ISACA Framework. Recuperado de: https://www.isaca.org/resources/cobit

ISO 9001-2015. (2021). *ISO 9000 ¿Qué diferencia hay entre proceso y procedimiento?*. Recuperado de: https://www.nueva-iso-9001-2015.com/2016/01/iso-9001-2015-diferencia-proceso-procedimiento/

Jeff Geerling. (2020). *Ansible for DevOps: Server and configuration management for humans.* (2da edición). Lean Publishing.

Kevin, L. Jackson, Scott Goeeslin (2018). United States Healthcare Cybersecurity Market Report 2020: Top 5 Threats are Phishing Attacks, Credential Harvesting, Ransomware, Social Engineering Attacks, and Information Theft or Loss Architecting Cloud Computing Solutions: Build cloud strategies that align technology and economics while effectively managing risk. (1st edición). Packt Publishing Ltd.

Leiva, B. Juan Carlos. (2021). *Empresas Innovadoras. Como empezar a innovar en su empresa sin gastar una fortuna y con poco riesgo*. (1Era edición).

Llamas, Jonathan. (03 de octubre, 2020). *Presupuesto base cero. Economipedia.com*. Recuperado de: https://economipedia.com/definiciones/presupuesto-base-cero.html

Martinez, H. Jose. (18 de setiembre de 2020). *Random Forest (Bosque Aleatorio): combinando árboles*. Recuperado de https://www.iartificial.net/random-forest-bosque-aleatorio/

MICITT. (2021). Costa Rica e Israel trabajarán juntos en temas de Ciberseguridad. Recuperado de: https://www.micit.go.cr/noticias/costa-rica-e-israel-trabajaran-juntos-temas-ciberseguridad

MICITT. (2021). *Costa Rica y Estonia firman convenios de cooperación en temas de Gobierno Digital y La Cuarta Revolución Industrial*. Recuperado de: https://www.micit.go.cr/noticias/costa-rica-y-estonia-firman-convenios-cooperacion-temas-gobierno-digital-y-la-cuarta

MITRE ATT&CK®. (2021). ATT&CK Matrix for Enterprise. Recuperado de: https://attack.mitre.org/

NCSI. (2021). 55th National Cyber Security Index Costa Rica. Recuperado de: https://ncsi.ega.ee/country/cr/

NICSS. (2021). Cyber Security *Glossary*. Recuperado de: https://niccs.cisa.gov/about-niccs/cybersecurity-glossary#C

NIST. (2021). NIST Special Publication 800-63B. Digital Identity Guidelines Authentication and Lifecycle Management. Recuperado de: https://pages.nist.gov/800-63-3/sp800-63b.html

NIST. (2021). Cybersecurity. Recuperado de: https://www.nist.gov/cybersecurity

NIST. (2018). NIST Releases Version 1.1 of its Popular Cybersecurity Framework. Recuperado de: https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework

OCDE. (2018). Estudios Económicos de la OCDE: Costa Rica. Recuperado de: https://www.comex.go.cr/media/6036/finalspanish-survey-cr-2018.pdf

Organismo de Investigación Judicial. (2021). *Sección especializada contra el cibercrimen*. Recuperado de https://sitiooij.poder-judicial.go.cr/index.php/oficinas/departamento-de-investigaciones-criminales/delitos-informaticos

Osterwalder, Alexander & Pigneur, Yves. (2011). *Generación de modelos de negocio.* (1Era edición). Editorial Deusto.

Phillips, Patricia., Phillips, Jack. (2021). *ROI Basics*. (2d edition). ATD Press Editorial.

PCI Security Standards Council. (2021). Why Security Matters. Recuperado de: https://www.pcisecuritystandards.org/pci_security/why_security_matters

RISKIQ. (2019). *The Evil Internet Minute 2019*. Recuperado de: https://www.riskiq.com/resources/infographic/evil-internet-minute-2019/

SANS. (2021). CIS Controls v8. Recuperado de: https://www.sans.org/blog/cis-controls-v8/

SCIJ Sistema Costarricense de Información jurídica. (2001). Adición de los artículos 196 BIS, 217 BIS y 229 BIS al Código Penal, Ley N° 4573 para reprimir y sancionar los delitos informáticos 8148. Recuperado de: https://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=47430&nValor3=50318&strTipM=TC

SCIJ - Sistema Costarricense de Informacion Juridica. (2012). Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal N° 9048. Recuperado de: https://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=73583&nValor3=90354&strTipM=TC

SCIJ - Sistema Costarricense de Informacion Juridica. (2013). Reforma de los artículos 196, 196 bis, 230, 293 y 295 y adición del artículo 167 bis al Código Penal N° 9135. Recuperado de: https://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=74706&nValor3=92348&strTipM=TC

Secplicity. (2021). 2021 World Password Day: How Many Will Be Stolen This Year?. Recuperado de: https://www.secplicity.org/2021/05/04/2021-world-password-day-how-many-will-be-stolen-this-year/

United Nations. (2021). 'Explosive' Growth of Digital Technologies Creating New Potential for Conflict, Disarmament Chief Tells Security Council in First-Ever Debate on Cyberthreats. Recuperado de: https://www.un.org/press/en/2021/sc14563.doc.htm

USA Today print edition. (7 de mayo de 2010). The machines took over. Kiosko.NET. https://es.kiosko.net/us/2010-05-07/np/usa_today.html

Van Horne, J.C., & Wachowicz, J.M. (2010). *Fundamentos de Administración Financiera*. Pearson Education.

World Economic Forum (2005). Davos 2021 - Averting a Cyber Pandemic [Vídeo]. Disponible en: https://www.weforum.org/videos/davos-2021-averting-a-cyber-pandemic-option-1-english

Yahoo! Finance. (2021). United States Healthcare Cybersecurity Market Report 2020: Top 5 Threats are Phishing Attacks, Credential Harvesting, Ransomware, Social Engineering Attacks, and Information Theft or Loss. Recuperado de: https://finance.yahoo.com/news/united-states-healthcare-cybersecurity-market-112800054.html

Your Europe. (2021). Reglamento general de protección de datos. Recuperado de: https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_es.htm

2010 flash crash. (2010, 6 de mayo). Wikipedia, The Free Encyclopedia. Fecha de consulta: 18:25, setiembre 16, 2021 desde https://en.wikipedia.org/wiki/2010_flash_crash

Anexos

ORGANISMO DE INVESTIGACIÓN JUDICIAL
OFICINA DE PLANES Y OPERACIONES
UNIDAD DE ANÁLISIS CRIMINAL

SOLICITUD DE INFORMACIÓN 1504-OPO/UAC/S-2021

ORGANISMO DE INVESTIGACIÓN JUDICIAL
OIJ,investigación y ciencia a su servicio

CONSULTA SOBRE INCIDENCIA DELITO INFORMATICO 2018 A 2021 ID-50349

Vº Bº Orlando Corrales Ugalde Jefe; Unidad de Análisis Criminal

Confeccionado por: Lic. Victor Fernandez V

Setiembre, 2021

Tabla#1

1. **Delitos Informáticos según año y mes 2018 a 2021**

AÑO	ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC	Total general
2018	71	84	91	86	80	112	106	89	94	84	97	81	**1075**
2019	96	95	103	96	126	110	120	102	101	81	92	86	**1208**
2020	94	92	77	91	126	102	104	89	101	81	79	76	**1112**
2021	109	106	112	96	96	109	165	134					**927**
Total general	**370**	**377**	**383**	**369**	**428**	**433**	**495**	**414**	**296**	**246**	**268**	**243**	**4322**

Tabla#2

2. **Delitos Informáticos según año y provincia 2018 a 2021**

PROVINCIA	2018	2019	2020	2021	Total general
SAN JOSE	638	676	588	405	**2307**
CARTAGO	125	186	132	162	**605**
ALAJUELA	103	109	170	116	**498**
PUNTARENAS	114	124	78	59	**375**
HEREDIA	27	51	44	76	**198**
LIMON	42	40	51	59	**192**
GUANACASTE	26	22	49	50	**147**
Total general	**1075**	**1208**	**1112**	**927**	**4322**

Tabla#3

3. **Delitos Informáticos según año y tipos de delito 2018 a 2021**

DELITOS INFORMATICOS	2018	2019	2020	2021	Total general
SUPLANTACION DE IDENTIDAD	385	608	762	647	**2402**
OTRO O INDETERMINADO	520	487	138	146	**1291**
SEDUCCION O ENCUENTRO CON MENORES POR MEDIOS ELECTRONICOS	53	53	52	46	**204**
SUPLANTACION DE PAGINAS ELECTRONICAS	88	33	36	27	**184**
INSTALACION O PROPAGACION DE PROGRAMAS INFORMATICOS MALICIOSOS	5	7	90	42	**144**
SABOTAJE INFORMATICO	24	20	34	19	**97**
Total general	**1075**	**1208**	**1112**	**927**	**4322**

Tabla#4

4. Delitos Informáticos según año y tipo de víctima 2018 a 2021

TIPO DE VICTIMA	2018	2019	2020	2021	Total general
OTRO O INDETERMINADO	700	832	810	628	**2970**
CLIENTE BANCARIO	115	95	38	86	**334**
MENOR DE EDAD	79	100	83	69	**331**
PEATON	67	59	54	44	**224**
USUARIO SERVICIO PUBLICO/PRIVADO	12	26	35	36	**109**
NO DEFINIDO	17	34	24	14	**89**
EMPRESARIO/COMERCIANTE	19	19	17	11	**66**
ESTUDIANTE	11	15	11	9	**46**
CLIENTE LOCAL COMERCIAL	14	8	3	8	**33**
OFICINAS/EMPRESA	7	4	10	6	**27**
EL ESTADO	12	3	5	2	**22**
ENTIDADES COMERCIALES Y FINANCIERAS	10	2	3		**15**
SIN CLASIFICAR		2	3	6	**11**
CENTRO EDUCATIVO		2	4		**6**
ENTIDADES PUBLICAS NO FINANCIERAS	5		1		**6**
TAXISTA		1	2	2	**5**
NO APLICA	1	2	1		**4**
GUARDA	1		2		**3**
BODEGA/DEPOSITO/ALMACEN		2		1	**3**
PASAJERO DE TRANSPORTE PUBLICO	1	1	1		**3**
USUARIO CAJERO AUTOMATICO	1			1	**2**
HOTEL/MOTEL/PENSION	1	1			**2**
COBRADOR/MENSAJERO/PAGADOR			2		**2**
CLIENTE HOTEL/MOTEL/PENSION				1	**1**
TURISTA/NACIONAL			1		**1**
SERVICIOS SOCIALES				1	**1**
CAJERO AUTOMATICO	1				**1**
SERVICIO PUBLICO	1				**1**
SUPER MERCADO			1		**1**
VENDEDOR DE LOTERIA			1		**1**
PRIVADO DE LIBERTAD				1	**1**
TURISTA/EXTRANJERO				1	**1**
Total general	**1075**	**1208**	**1112**	**927**	**4322**

Nota: Para interponer una denuncia de cualquier tipo, la persona denunciante u ofendida, debe de presentarse ante una de las oficinas del Organismo de Investigación Judicial, dispuestas a lo largo del país, en el enlace a continuación se puede observar un video oficial sobre el proceso de recepción de denuncias:

https://sitiooij.poder-judicial.go.cr/index.php/ayuda/video-respuestas/item/10715que-se-debe-hacer-para-presentar-una-denuncia

5. Auditoría de contraseñas con PYTHON

De: El Departamento de la Gestión del Talento Humano

Para: El Departamento de Tecnología de la Información

Solicitud: Realizar la Auditoría de Contraseñas para el Último Trimestre del Año 2021

Objetivo: TI - Identificar vulnerabilidades / GTH - Identificar quién necesita entrenamiento en ciberseguridad

Inicio de la Auditoría - Septiembre 2021

In [3]:

```
# Importamos la biblioteca de código abierto llamada Pandas
import pandas as pd
import warnings
warnings.simplefilter(action='ignore', category=FutureWarning)
# Cargamos el archivo llamado "usuarios.csv"
usuarios = pd.read_csv("C:\\Users\\jm_ad\\OneDrive\\Desktop\\usuarios.csv",encoding='latin1'
)
```

In [4]:

```
# Se muestra el total de usuarios que tiene el archivo (representa el número de colaboradore
s de la empresa)
print(len(usuarios))
```

```
1010
```

In [5]:

```
# Se muestran los primeros 5 usuarios y sus contraseñas
usuarios.head()
```

Out[5]:

	Número_Usuario	Nombre_Usuario	Contraseña
0	1	jessica.vega	c0kta1l
1	2	milton.velazquez	V3la5k35
2	3	joao.villalta	hpotter2019
3	4	raul.cabrera	t1c0s0y
4	5	gustavo.talavera	acme 2020

In [6]:

```
# Se muestran los últimos 5 usuarios y sus contraseñas
usuarios.tail()
```

Out[6]:

	Número_Usuario	Nombre_Usuario	Contraseña
1005	1006	hernan.rodriguez	grengo5mrt
1006	1007	mariela.ugalde	tuanis
1007	1008	valeria.chacon	3ltr3n
1008	1009	carlos.bonilla	br3dunla0s
1009	1010	michael.delgado	pwkm1os

Las contraseñas no deben ser demasiado cortas

Toda contraseña debe tener al menos 8 caracteres de longitud.

In [7]:

```
# Calculamos la longitud de cada contraseña
usuarios['Longitud'] = usuarios['Contraseña'].str.len()
# Identificamos cada usuario que utilize una contraseña corta o menor a 8 caracteres
usuarios['Corto'] = usuarios['Longitud'] < 8
```

In [8]:

```
# Información de los resultados:
total = (usuarios.Corto.sum())
print("El Total de colaboradores con contraseñas menores a 8 caracteres son:", (total))
#
porcentaje = (total/(len(usuarios))*100)
print("El porcentaje de colaboradores con contraseñas menores a 8 caracteres representan el:
", round(porcentaje),("%"))
```

```
El Total de colaboradores con contraseñas menores a 8 caracteres son: 387
El porcentaje de colaboradores con contraseñas menores a 8 caracteres representan el: 38 %
```

Las contraseñas no deben ser contraseñas comunes

Podemos comparar la lista de contraseñas utilizadas por nuestos usuarios con una lista de contraseñas comunes.

In [9]:

```
# Cargamos un archivo que contiene 10011 contraseñas de las más comunes
Contraseña_Comun = pd.read_csv("C:\\Users\\jm_ad\\OneDrive\\Desktop\\10010_passwords.txt",
header=None, squeeze=True)
```

In [10]:

```
# Estas son las últimas 5 contraseñas de la lista
Contraseña_Comun.tail()
```

Out[10]:

```
10008       u5au5a
10009         kiss
10010        4ever
10011    c05tarlca
10012      bltc01n
Name: 0, dtype: object
```

In [11]:

```
# Identificamos los usuarios que usan contraseñas comunes
```

```
usuarios['Contraseña_Comun'] = usuarios.Contraseña.isin(Contraseña_Comun)
```

In [13]:

```
# Información de los resultados:
total2 = (usuarios[usuarios['Contraseña_Comun']].shape[0])
print("El Total de colaboradores que usan contraseñas comunes son:", (total2))
#
porcentaje2 = (total2/(len(usuarios))*100)
print("El porcentaje de colaboradores que usan contraseñas comunes representan el:", round(p
orcentaje2),("%"))
```

```
El Total de colaboradores que usan contraseñas comunes son: 130
El porcentaje de colaboradores que usan contraseñas comunes representan el: 13 %
```

Las contraseñas no deben ser palabras comunes

Podemos comparar la lista de contraseñas utilizadas por nuestos usuarios con una lista de palabras comunes.

In [14]:

```
# Cargamos un archivo que contiene 20020 palabras comunes de los idiomas Español e Inglés
# Debido a que en nuestro país es común el uso de ciertas palabras en ese otro idioma
palabras = pd.read_csv("C:\\Users\\jm_ad\\OneDrive\\Desktop\\20020_palabras.txt", header=No
ne, squeeze=True)

# Revisamos las primeras 5 palabras de nuestra lista
palabras.head()
```

Out[14]:

```
0     arbol
1      arar
2      nube
3     cielo
4    oceano
Name: 0, dtype: object
```

In [15]:

```
# Identificamos los usuarios con contraseñas que usan palabras comunes
usuarios['Palabra_Comun'] = usuarios.Contraseña.str.lower().isin(palabras)
```

In [16]:

```
# Información de los resultados:
total3 = (usuarios[usuarios['Palabra_Comun']].shape[0])
print("El Total de colaboradores que usan contraseñas comunes son:", (total3))
#
porcentaje3 = (total3/(len(usuarios))*100)
print("El porcentaje de colaboradores que usan contraseñas comunes representan el:", round(p
orcentaje3),("%"))
```

```
El Total de colaboradores que usan contraseñas comunes son: 142
El porcentaje de colaboradores que usan contraseñas comunes representan el: 14 %
```

Las contraseñas no deben ser repetitivas

In [17]:

```
import warnings
warnings.simplefilter(action='ignore', category=UserWarning)
# Identificamos los usuarios con contraseñas igual o mayor a cuatro repeticiones
```

```
usuarios['repetidos'] = usuarios['Contraseña'].str.contains(r'(.)\1\1\1')

# Veamos los usuarios con contraseñas que sean igual o mayor a cuatro repeticiones
usuarios[usuarios['repetidos']]
```

Out[17]:

	Número_Usuario	Nombre_Usuario	Contraseña	Longitud	Corto	Contraseña_Comun	Palabra_Comun	repetidos
146	147	valeria.cortez	555555	6	True	True	False	True
572	573	damaris.bustamante	555555	6	True	True	False	True
644	645	roberto.lopez	11111	5	True	True	False	True
798	799	ana.delgado	888888	6	True	True	False	True
807	808	felipe.barco	rinnnng0	8	False	False	False	True
941	942	ericka.muñoz	aaaaaa	6	True	True	False	True
1001	1002	bernal.rios	calebbbb01	10	False	False	False	True

Usemos todas las recomendaciones

In [18]:

```
# Identificamos las contraseñas incorrectas
usuarios['contraseña_incorrecta'] = usuarios['Corto'] | usuarios['Contraseña_Comun'] | usuar
ios['Palabra_Comun'] | usuarios['repetidos']
```

In [19]:

```
# Estas son las primeras 25 contraseñas incorrectas
usuarios[usuarios['contraseña_incorrecta']].head(25)
```

Out[19]:

	Número_Usuario	Nombre_Usuario	Contraseña	Longitud	Corto	Contraseña_Comun	Palabra_Comun	repetidos	contrasei
0	1	jessica.vega	c0kta1l	7	True	False	False	False	
3	4	raul.cabrera	t1c0s0y	7	True	False	False	False	
5	6	brenda.naranjo	kiss	4	True	True	True	False	
7	8	jeffrey.amador	mipirulo	8	False	True	False	False	
9	10	laura.alpizar	T1cT0c	6	True	False	False	False	
11	12	tania.villegas	hubbard	7	True	False	False	False	
13	14	randall.coto	310356	6	True	False	False	False	
15	16	gerardo.corrado	oZ4k0QE	7	True	False	False	False	
16	17	andres.carmona	chelsea	7	True	True	True	False	
17	18	martin.pacheco	zvc1939	7	True	False	False	False	
18	19	jenifer.sandoval	nickgd	6	True	False	False	False	
21	22	leticia.perez	cocacola	8	False	True	False	False	
22	23	jenny.cabrera	woodard	7	True	False	False	False	
25	26	dianna.munoz	AJ9Da	5	True	False	False	False	
26	27	julia.savage	ewokzs	6	True	False	False	False	
28	29	joaquin.walters	YyGjz8E	7	True	False	False	False	
30	31	jorge.azofeifa	reid	4	True	False	True	False	
34	35	daniela.lara	jOYZBs8	7	True	False	False	False	

	Número_Usuario	Nombre_Usuario	Contraseña	Longitud	Certo	Contraseña_Comun	Palabra_Comun	repetidos	contrasei
38	39	mario.chavez	wwewwrt	7	True	False	False	False	
43	44	alvaro.vargas	225377	6	True	False	False	False	
45	46	kenneth.navas	NdZ7E6	6	True	False	False	False	
47	48	eduardo.garita	CQB3Z	5	True	False	False	False	
48	49	pedro.morales	diffo	5	True	False	False	False	
51	52	tito.rosales	123456789	9	False	True	False	False	
52	53	auxiliadora.mendoza	y8uM7D6	7	True	False	False	False	

In [20]:

```
# Información de los resultados:
total_final = (usuarios[usuarios['contraseña_incorrecta']].shape[0])
tot_usuarios = (len(usuarios))
print("El Total de colaboradores que usan contraseñas incorrectas son:", (total_final))
#
porcentaje_total = (total_final/tot_usuarios*100)
print("El porcentaje de colaboradores que usan contraseñas incorrectas representan el:", rou
nd(porcentaje_total),("%"))
```

```
El Total de colaboradores que usan contraseñas incorrectas son: 435
El porcentaje de colaboradores que usan contraseñas incorrectas representan el: 43 %
```

Final de la Auditoría - Septiembre 2021

Resultado de la Auditoría:

Se envía al Dpto. de Gestión del Talento Humano la lista de los 435 colaboradores que no pasaron la auditoría.

Representan un 43% de el total de empleados.

Queda a su criterio administrativo el curso que deberán llevar en un plazo no mayor a 5 días.

6. Generador de contraseñas con PYTHON

De: El Departamento de la Gestión del Talento Humano

Para: El Departamento de Tecnología de la Información

Solicitud: Crear para todos los colaboradores un generador de Contraseñas para este Trimestre del Año 2021

Objetivo: TI - Eliminar vulnerabilidades / GTH - Mejorar los resultados en la Auditoría de Contraseñas

Inicio de la Creación de un Generador de Contraseñas - Septiembre 2021

In [1]:

```
# Importamos los modulos requeridos
import secrets
import string

def password_gen(password_length):

    characters = string.ascii_letters + string.digits + string.punctuation

    secure_password = ''.join(secrets.choice(characters) for i in range(password_length))

    return secure_password

def main():

    user_password_length = int(input("Digite en números la longitud de la contraseña: "))

    print("Contraseña Generada: ", password_gen(user_password_length))

main()
```

```
Digite en números la longitud de la contraseña: 9
Contraseña Generada:  okIJtGj-C
```

Final de la Generación de Contraseñas - Septiembre 2021

Resultado de la Herramienta para la Generación de Contraseñas:

Esta Herramienta ya está a disposición de los colaboradores en la intranet de la empresa

La herramienta genera Contraseñas que cumplen con lo solicitado en la auditoria.

7. Control de verificación de ingreso

Control de verificación de ingreso

Fecha de Ingreso ___/___/___

Encargado _____ Firma

_____

Entrega de activos tangibles

- ❑ Laptop/Computadora/Monitor
- ❑ Celular/Tableta
- ❑ Llave USB/Disco Duro
- ❑ Manuales/Libros/Archivos
- ❑ Tarjetas de Identificación
- ❑ Llaves/Tarjetas de Acceso
- ❑ Tarjeta Corporativa
- ❑ Permiso de Estacionamiento
- ❑ Identificación de Seguro medico empresarial/Uso de Soda/Otros

Entrega de activos intangibles

- ❑ Licencias de uso de Software
- ❑ Datos sensibles
- ❑ Patentes
- ❑ Información confidencial
- ❑ Diseños/herramientas digitales
- ❑ Repositorios digitales

Solicitud de actualizaciones

- ❑ Remover usuario de empleado
- ❑ Remover el empleado de planilla
- ❑ Actualizar el directorio empresarial
- ❑ Remover el correo del empleado
- ❑ Remover todo acceso físico
- ❑ Remover todo acceso digital
- ❑ Remover de boletín interno/intranet
- ❑ Remover fotos de página web o redes sociales si existiese
- ❑ Remover tokens/llaves/claves

Serial de Laptop _____
Serial de Monitor _____
Licencia Sistema Operativo _____
Numero de Placa _____

Serial de Computadora _____
Serial de Celular _____
Licencia de Software _____
Numero de permiso Estacionar _____

8. Control de verificación de salida de la empresa

Control de verificación de salida

Fecha de Salida ___/___/___

Encargado _____

Firma _____

Entrega de activos tangibles

- ❑ Laptop/Computadora/Monitor
- ❑ Llave USB/Disco Duro
- ❑ Tarjetas de Identificación
- ❑ Celular/Tableta
- ❑ Manuales/Libros/Archivos

Entrega de activos intangibles

- ❑ Licencias de uso de Software
- ❑ Patentes
- ❑ Diseños/herramientas digitales
- ❑ Datos sensibles
- ❑ Información confidencial
- ❑ Repositorios digitales

Requisito de Actualizaciones

- ❑ Tarjeta de Crédito Corporativa
- ❑ Identificación de Seguro medico empresarial/Uso de Soda/Otros
- ❑ Serial de Laptop_____
- ❑ Serial de PC_____
- ❑ Serial de Monitor_____
- ❑ Serial de Celular_____
- ❑ Lic. de Software_____
- ❑ Actualizar el directorio empresarial
- ❑ Remover todo acceso digital
- ❑ Llaves/Tarjetas de Acceso
- ❑ Permiso de Estacionamiento
- ❑ Remover todo acceso físico
- ❑ Remover de boletín interno/intranet
- ❑ Remover tokens/llaves/claves/VPN
- ❑ Remover el empleado de planilla
- ❑ Remover el correo del empleado
- ❑ Remover todo acceso digital
- ❑ Remover fotos de página web o redes sociales si existiese

9. Cuantificación de riesgos cibernéticos con PYTHON

De: El Departamento de Finanzas

Para: El Departamento de Tecnología de la Información

Solicitud: Realizar la cuantificación de Riesgo Cibernético para el Último Trimestre del Año 2021

Objetivo: TI - Identificar vulnerabilidades / Finanzas - Cuantificar riesgos de ciberseguridad

---

Inicio de la Cuantificación de Riesgos Cibernéticos - Septiembre 2021

In [3]:

```
# Se importan las librerias y módulos requeridos
import pandas as pd
import matplotlib.pyplot as plt
plt.style.use('ggplot')
import seaborn as sns
```

In [4]:

```
# Cargamos el archivo llamado riesgo_cibernetico.xlsx que contiene una lista de eventos de r
iesgo
cyber_risks = pd.read_excel('C:\\Users\\jm_ad\\OneDrive\\Desktop\\riesgo_cibernético.xlsx')
print(cyber_risks)
```

```
           Cyber event  Probability  Lower   Upper
0  Filtracion de Datos          0.4  10000  500000
```

Inicio de la simulación de Riesgos

In [5]:

```
# se importa la librería Numpy la cual proporcionara una potentes estructuras de datos para
implementar
# una matriz multidimensional []

import numpy as np
probability = []
def attack_occurs(attack_probability):

    prob = np.random.rand() # Devuelve una matriz aleatoria con valores aleatorios
     #Si el número esta por debajo de 0.4 (40% probabilidad) Ocurre el evento (ataque de Fil
tración de Datos).
    if prob <= 0.4:
        probability.append(prob)
    return prob < attack_probability
```

Usamos NumPy, para obtener una cantidad simulada de riesgo usando la Distribución Log-Normal

In [6]:

```
def attack_loss_amount(lower, upper):
    mean = (np.log(lower) + np.log(upper))/2.0     # Calcula la media de los datos de una m
uestra o población
    std_dv = (np.log(upper) - np.log(lower))/3.29  # Calcula la desviación estándar de una
lista de valores

    return np.random.lognormal(mean, std_dv)
```

In [7]:

```
i=0
loss = []
while i < 1000:
    if attack_occurs(0.4):
        attack_loss = attack_loss_amount(10000, 500000)
        loss.append(attack_loss)
        print('Un ataque de Filtración de Datos con 1,000 simulaciones muestra una pérdida d
e US ${:,.2f}'.format(attack_loss))
    else:
        print('El ataque de Filtración de Datos simulado no se efectuó')
    i+=1
```

```
El ataque de Filtración de Datos simulado no se efectuó
Un ataque de Filtración de Datos con 1,000 simulaciones muestra una pérdida de US $120,894.1
2
El ataque de Filtración de Datos simulado no se efectuó
El ataque de Filtración de Datos simulado no se efectuó
Un ataque de Filtración de Datos con 1,000 simulaciones muestra una pérdida de US $49,037.06
El ataque de Filtración de Datos simulado no se efectuó
Un ataque de Filtración de Datos con 1,000 simulaciones muestra una pérdida de US $6,049.02
El ataque de Filtración de Datos simulado no se efectuó
El ataque de Filtración de Datos simulado no se efectuó
El ataque de Filtración de Datos simulado no se efectuó
Un ataque de Filtración de Datos con 1,000 simulaciones muestra una pérdida de US $72,564.57
Un ataque de Filtración de Datos con 1,000 simulaciones muestra una pérdida de US $52,004.74
El ataque de Filtración de Datos simulado no se efectuó
El ataque de Filtración de Datos simulado no se efectuó
Un ataque de Filtración de Datos con 1,000 simulaciones muestra una pérdida de US $253,893.7
9
Un ataque de Filtración de Datos con 1,000 simulaciones muestra una pérdida de US $33,079.25
El ataque de Filtración de Datos simulado no se efectuó
Un ataque de Filtración de Datos con 1,000 simulaciones muestra una pérdida de US $106,198.2
8
Un ataque de Filtración de Datos con 1,000 simulaciones muestra una pérdida de US $579,555.5
0
El ataque de Filtración de Datos simulado no se efectuó
Un ataque de Filtración de Datos con 1,000 simulaciones muestra una pérdida de US $115,957.9
1
El ataque de Filtración de Datos simulado no se efectuó
El ataque de Filtración de Datos simulado no se efectuó
Un ataque de Filtración de Datos con 1,000 simulaciones muestra una pérdida de US $257,847.5
2
Un ataque de Filtración de Datos con 1,000 simulaciones muestra una pérdida de US $50,476.53
Un ataque de Filtración de Datos con 1,000 simulaciones muestra una pérdida de US $11,837.54
Un ataque de Filtración de Datos con 1,000 simulaciones muestra una pérdida de US $23,379.62
El ataque de Filtración de Datos simulado no se efectuó
El ataque de Filtración de Datos simulado no se efectuó
Un ataque de Filtración de Datos con 1,000 simulaciones muestra una pérdida de US $23,034.72
El ataque de Filtración de Datos simulado no se efectuó
Un ataque de Filtración de Datos con 1,000 simulaciones muestra una pérdida de US $184,147.0
3
El ataque de Filtración de Datos simulado no se efectuó
```

```
El ataque de Filtración de Datos simulado no se efectuó
El ataque de Filtración de Datos simulado no se efectuó
Un ataque de Filtración de Datos con 1,000 simulaciones muestra una pérdida de US $32,472.23
Un ataque de Filtración de Datos con 1,000 simulaciones muestra una pérdida de US $5,145.98
El ataque de Filtración de Datos simulado no se efectuó
El ataque de Filtración de Datos simulado no se efectuó
Un ataque de Filtración de Datos con 1,000 simulaciones muestra una pérdida de US $36,157.29
El ataque de Filtración de Datos simulado no se efectuó
Un ataque de Filtración de Datos con 1,000 simulaciones muestra una pérdida de US $27,986.36
Un ataque de Filtración de Datos con 1,000 simulaciones muestra una pérdida de US $12,646.23
Un ataque de Filtración de Datos con 1,000 simulaciones muestra una pérdida de US $618,890.4
7
El ataque de Filtración de Datos simulado no se efectuó
El ataque de Filtración de Datos simulado no se efectuó
El ataque de Filtración de Datos simulado no se efectuó
Un ataque de Filtración de Datos con 1,000 simulaciones muestra una pérdida de US $241,136.8
0
El ataque de Filtración de Datos simulado no se efectuó
El ataque de Filtración de Datos simulado no se efectuó
El ataque de Filtración de Datos simulado no se efectuó
El ataque de Filtración de Datos simulado no se efectuó
El ataque de Filtración de Datos simulado no se efectuó
Un ataque de Filtración de Datos con 1,000 simulaciones muestra una pérdida de US $31,956.61
El ataque de Filtración de Datos simulado no se efectuó
El ataque de Filtración de Datos simulado no se efectuó
El ataque de Filtración de Datos simulado no se efectuó
El ataque de Filtración de Datos simulado no se efectuó
Un ataque de Filtración de Datos con 1,000 simulaciones muestra una pérdida de US $1,207,213
.28
El ataque de Filtración de Datos simulado no se efectuó
Un ataque de Filtración de Datos con 1,000 simulaciones muestra una pérdida de US $149,543.9
3
El ataque de Filtración de Datos simulado no se efectuó
El ataque de Filtración de Datos simulado no se efectuó
Un ataque de Filtración de Datos con 1,000 simulaciones muestra una pérdida de US $210,009.3
5
Un ataque de Filtración de Datos con 1,000 simulaciones muestra una pérdida de US $7,700.67
El ataque de Filtración de Datos simulado no se efectuó
El ataque de Filtración de Datos simulado no se efectuó
El ataque de Filtración de Datos simulado no se efectuó
Un ataque de Filtración de Datos con 1,000 simulaciones muestra una pérdida de US $44,059.22
Un ataque de Filtración de Datos con 1,000 simulaciones muestra una pérdida de US $49,197.39
Un ataque de Filtración de Datos con 1,000 simulaciones muestra una pérdida de US $570,609.8
2
Un ataque de Filtración de Datos con 1,000 simulaciones muestra una pérdida de US $7,436.36
Un ataque de Filtración de Datos con 1,000 simulaciones muestra una pérdida de US $55,402.69
El ataque de Filtración de Datos simulado no se efectuó
El ataque de Filtración de Datos simulado no se efectuó
El ataque de Filtración de Datos simulado no se efectuó
El ataque de Filtración de Datos simulado no se efectuó
Un ataque de Filtración de Datos con 1,000 simulaciones muestra una pérdida de US $45,115.54
Un ataque de Filtración de Datos con 1,000 simulaciones muestra una pérdida de US $61,539.40
El ataque de Filtración de Datos simulado no se efectuó
Un ataque de Filtración de Datos con 1,000 simulaciones muestra una pérdida de US $36,262.59
El ataque de Filtración de Datos simulado no se efectuó
El ataque de Filtración de Datos simulado no se efectuó
Un ataque de Filtración de Datos con 1,000 simulaciones muestra una pérdida de US $130,477.4
7
El ataque de Filtración de Datos simulado no se efectuó
El ataque de Filtración de Datos simulado no se efectuó
El ataque de Filtración de Datos simulado no se efectuó
Un ataque de Filtración de Datos con 1,000 simulaciones muestra una pérdida de US $11,866.87
El ataque de Filtración de Datos simulado no se efectuó
```

In [9]:

```
# Creando una lista de simulaciones
```

```
ranges1 = range(1, len(loss)+1)
simulations1 = []
for simulation1 in ranges1:
    simulations1.append(simulation1)
```

Generar la lista de pérdidas y sus probabilidades

In [10]:

```
df = pd.DataFrame(simulations1 , columns = ['Simulation Number'])
df['Loss']  = loss
df['Probability'] = probability
df.head(10)
```

Out[10]:

	Simulation Number	Loss	Probability
0	1	120894.124867	0.209565
1	2	49037.064497	0.149461
2	3	6049.017267	0.134638
3	4	72564.574613	0.096833
4	5	52004.742843	0.181384
5	6	253893.787658	0.335677
6	7	33079.248914	0.208974
7	8	106198.277005	0.376308
8	9	579555.495113	0.045283
9	10	115957.910951	0.165470

In [11]:

```
# Python program to get average of a list
def Average(lst):  # Función para encontrar el promedio de números dados en una lista
    return sum(lst) / len(lst)
average = Average(loss)
print("El pronóstico del costo de 1,000 simulaciones por concepto de Filtración de Datos es
de US$:", round(average))
```

```
El pronóstico del costo de 1,000 simulaciones por concepto de Filtración de Datos es de US$:
159225
```

In [12]:

```
P = []
def simulate_risk_portfolio(cyber_risks):
    total_loss_amount = 0
    for risk in cyber_risks.itertuples():  #Interactuar con filas de la matriz de calculo de
secuencia inmutable
        if attack_occurs(risk.Probability):
            P.append(risk.Probability)
            total_loss_amount += attack_loss_amount(risk.Lower, risk.Upper)
    return total_loss_amount

def monte_carlo_simulation(cyber_risks, iterations):
    yearly_losses = []
    for i in range(iterations):
        loss_amount = simulate_risk_portfolio(cyber_risks)
        yearly_losses.append(loss_amount)
    return yearly_losses
```

```
yearly_losses = monte_carlo_simulation(cyber_risks, iterations = 10000)
yearly_losses
```

Out[12]:

```
[0,
 0,
 109643.85192453179,
 190246.3911370999,
 0,
 0,
 0,
 77154.04791593013,
 155056.10521033723,
 0,
 0,
 12231.667614566008,
 0,
 0,
 0,
 0,
 0,
 0,
 0,
 9132.841253762905,
 105092.981488855,
 0,
 0,
 651209.95494891,
 0,
 0,
 0,
 0,
 49567.48795989202,
 0,
 0,
 21837.024114265365,
 28750.794052723617,
 0,
 0,
 0,
 0,
 79335.958152201,
 0,
 0,
 0,
 0,
 0,
 0,
 0,
 32354.775981369243,
 0,
 0,
 2948.8588306786683,
 1576253.311903763,
 43807.49289589247,
 148608.38914112467,
 0,
 0,
 0,
 0,
 80303.79444832503,
 0,
 0,
 0,
 0,
 0,
 0,
```

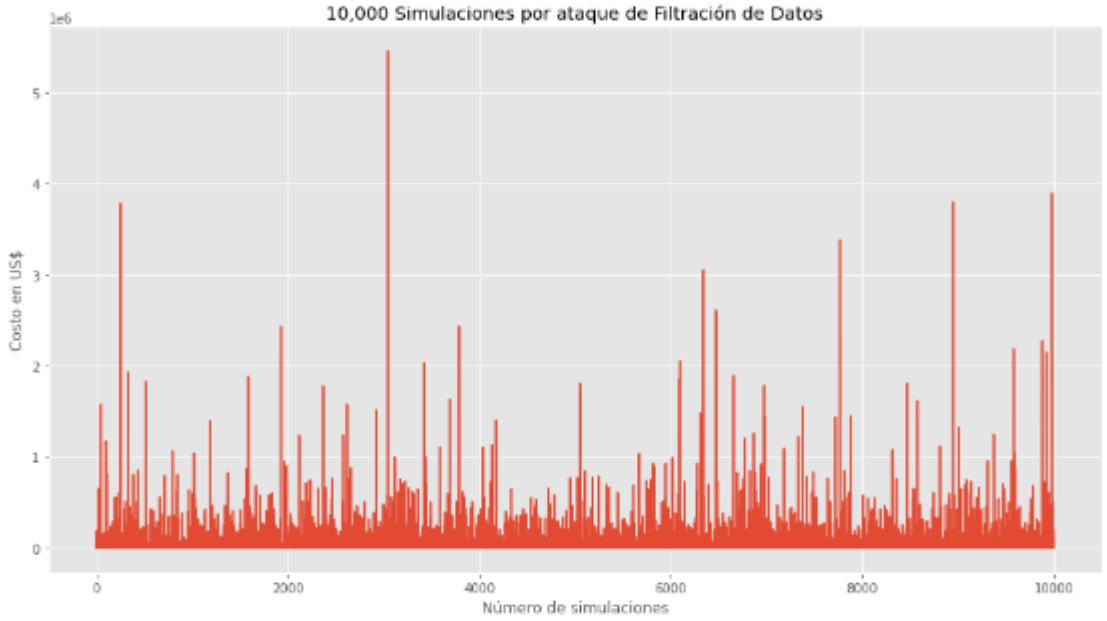
```
0,
0,
0,
0,
88095.18770294906,
0,
0,
0,
0,
0,
0,
64457.0638313214,
0,
0,
0,
403859.77242879895,
96824.95983048709,
0,
103113.7008775283,
51925.17182848631,
0,
60204.99000311134,
0,
0,
214946.51819164015,
0,
15864.790647613165,
639507.303379446,
0,
0,
0,
0,
0,
0,
0,
0,
0,
0,
69268.39142522958,
14519.23573077132,
0,
0,
0,
0,
100603.42420013106,
180673.90490143278,
0,
84278.69083652356,
59272.94982017353,
219653.65548327295,
0,
0,
237293.15794783458,
0,
0,
0,
...]
```

In [13]:

```
ranges = range(1, 10001)
simulations = []
for simulation in ranges:
    simulations.append(simulation)
```

In [14]:

```
plt.figure(figsize=(15,8))

sns.lineplot(x=simulations, y=yearly_losses)

# Eje x
plt.xlabel('Número de simulaciones')
# Eje y
plt.ylabel('Costo en US$')

# Titulo de el gráfico
plt.title('10,000 Simulaciones por ataque de Filtración de Datos')

# Mostrar la gráfica
plt.show()
```



In [15]:

```
# Obtener el promedio de una lista
def Average(lst):
    return sum(lst) / len(lst)
average = Average(yearly_losses)
print("El pronóstico del costo de 10,000 simulaciones por concepto de ataque de Filtración d
e Datos es deUS$:", round(average))
```

```
El pronóstico del costo de 10,000 simulaciones por concepto de ataque de Filtración de Datos
es deUS$: 59158
```

In [16]:

```
P = []
def simulate_risk_portfolio(cyber_risks):
    total_loss_amount = 0
    for risk in cyber_risks.itertuples():
        if attack_occurs(risk.Probability):
            P.append(risk.Probability)
            total_loss_amount += attack_loss_amount(risk.Lower, risk.Upper)
    return total_loss_amount
```

```
def monte_carlo_simulation(cyber_risks, iterations):
    yearly_losses = []
    for i in range(iterations):
        loss_amount = simulate_risk_portfolio(cyber_risks)
        yearly_losses.append(loss_amount)
    return yearly_losses

yearly_losses = monte_carlo_simulation(cyber_risks, iterations = 50000)
yearly_losses
```

Out[16]:

```
[0,
 0,
 0,
 0,
 18536.487416322143,
 121382.05872174562,
 0,
 273075.01584889926,
 0,
 0,
 0,
 382650.0686319467,
 0,
 36993.518043916985,
 0,
 0,
 27072.057929949377,
 52218.00570643567,
 92731.40522111529,
 90801.13928006939,
 0,
 399853.0365575311,
 0,
 0,
 91140.24490053508,
 0,
 63275.783039191825,
 0,
 216012.11756716165,
 0,
 136725.99405026948,
 0,
 0,
 39029.97553674082,
 11848.18535650196,
 0,
 0,
 41393.7947772181,
 230027.66704175255,
 0,
 284078.8915131241,
 0,
 0,
 95382.58703414735,
 0,
 169921.99506361084,
 193940.68272601708,
 0,
 0,
 0,
 0,
 0,
 0,
 0,
 0,
 0,
 0,
```

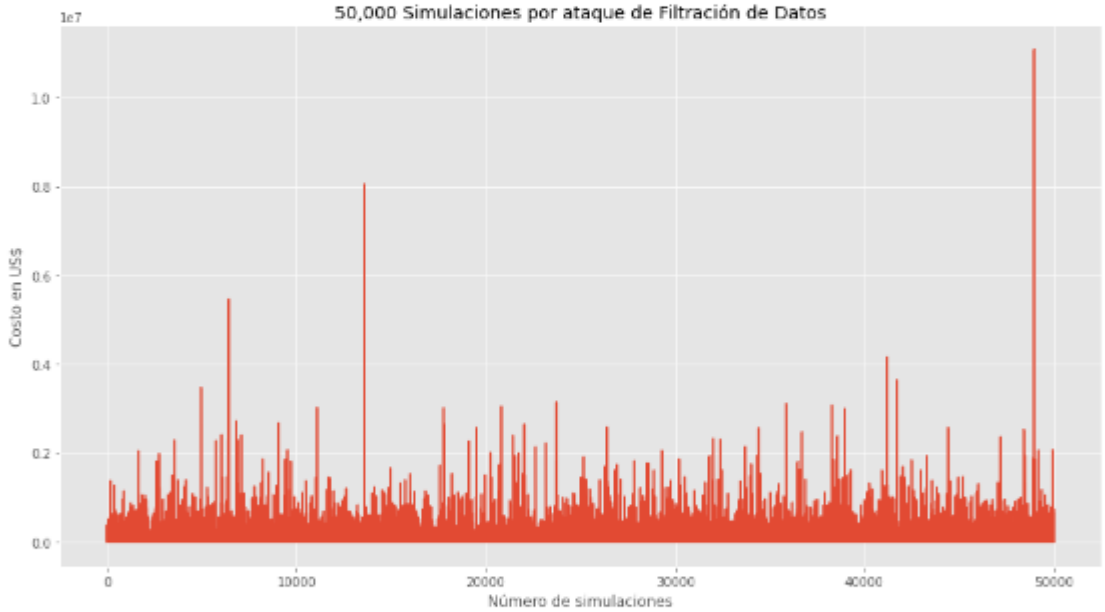
...]

In [17]:

```
ranges = range(1, 50001)
simulations = []
for simulation in ranges:
    simulations.append(simulation)
```

In [18]:

```
plt.figure(figsize=(15,8))

sns.lineplot(x=simulations, y=yearly_losses)

# Eje x
plt.xlabel('Número de simulaciones')
# Eje y
plt.ylabel('Costo en US$')

# Título de el gráfico
plt.title('50,000 Simulaciones por ataque de Filtración de Datos')

# Mostrar la gráfica
plt.show()
```



In [19]:

```
# Obteniendo el promedio
def Average(lst):
    return sum(lst) / len(lst)
average = Average(yearly_losses)
print("El pronóstico del costo de 50,000 simulaciones por concepto de ataque de Filtración d
e Datos es de US$:", round(average))
```

```
El pronóstico del costo de 50,000 simulaciones por concepto de ataque de Filtración de Datos
es de US$: 57434
```

Final de la Cuantificación de Riesgos Cibernéticos - Septiembre 2021

Resultado de la Cuantificación:

Se envía al Dpto. de Finanzas la lista de la Cuantificación de los Riesgos.

Se muestra que a 1,000 simulaciones el modelo no es consistente a 10,000 muy bueno pero a 50,000 es preciso.

Los montos económicos que genera se pueden utilizar perfectamente para realizar un presupuesto.

In [ ]:

10. Identificando posibles Renuncias y necesidad de Entrenamiento con Machine Learning

---

De: El Departamento de la Gestión del Talento Humano

Para: El Departamento de Tecnología de la Información

Solicitud: Realizar la Auditoría/Análisis de Entrenamiento para el Último Trimestre del Año 2021

Objetivo: TI - Vulnerabilidades / GTH - Identificar necesidad de entrenamiento y mejora para que no renuncie

---

Inicio de la Auditoría/Análisis de Entrenamiento - Septiembre 2021

In [34]:

```
#Se importan las librerias y modulos requeridos
import pandas as pd
import numpy as np
import seaborn as sns
import matplotlib.pyplot as plt
import warnings
warnings.simplefilter(action='ignore', category=FutureWarning)
```

Cargamos el archivo llamado "datos.csv" brindado por el Departamento de GTH para su análisis

In [93]:

```
datos=pd.read_csv("C:\\Users\\jm ad\\OneDrive\\Desktop\\datos.csv",encoding='latin1')
```

Se procede a revisar la cantidad de colaboradores que trabajan desde la casa

In [94]:

```
datos['Trabajo Remoto'].value_counts()
```

Out[94]:

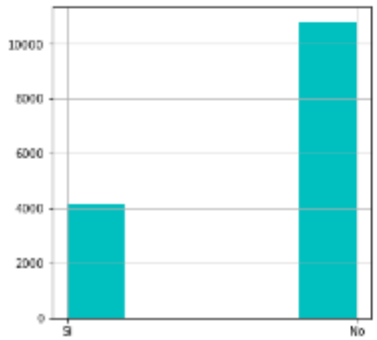
```
No    10812
Si     4188
Name: Trabajo Remoto, dtype: int64
```

De acuerdo al resultado 4188 colaboradores trabajan desde la casa

Este grupo debe ser el primero en tener entrenamiento de ciberseguridad y revisión de condiciones

In [36]:

```
datos['Trabajo Remoto'].hist(bins = 5, figsize = (5,5), color = 'c');
```



Cargamos el archivo llamado "datos_actualizados.csv" brindado por el Departamento de GTH para su análisis

In [95]:

```
# Se mostran los primeros 5 resultados
datos=pd.read_csv("C:\\Users\\jm_ad\\OneDrive\\Desktop\\datos_actualizados.csv",encoding='latin1')
datos.head()
```

Out[95]:

	Núm_Empleado	Núm_Proyectos	Núm_hrs_Mensuales	Tiempo_Laborado_Años	Accidente_Laboral	Renuncia	Promoción_Últ_5años	Departamento	Salario
0	100	6	130	5	0	1	0	Ventas	Alto
1	101	5	233	4	0	1	0	Ventas	Medio
2	102	7	256	3	0	1	1	Ventas	Medio
3	103	5	257	4	0	1	1	Ventas	Alto
4	104	6	160	3	0	1	1	Ventas	Alto

In [39]:

```
# Se muestra el tipo de datos
datos.info()
```

```
<class 'pandas.core.frame.DataFrame'>
RangeIndex: 15000 entries, 0 to 14999
Data columns (total 9 columns):
 #   Column                Non-Null Count  Dtype 
---  ------                --------------  ----- 
 0   Núm_Empleado          15000 non-null  int64 
 1   Núm_Proyectos         15000 non-null  int64 
 2   Núm_hrs_Mensuales     15000 non-null  int64 
 3   Tiempo_Laborado_Años  15000 non-null  int64 
 4   Accidente_Laboral     15000 non-null  int64 
 5   Renuncia              15000 non-null  int64 
 6   Promoción_Últ_5años   15000 non-null  int64 
 7   Departamento          15000 non-null  object
 8   Salario               15000 non-null  object
dtypes: int64(7), object(2)
memory usage: 1.0+ MB
```

In [40]:

```
datos.select_dtypes(exclude=['int', 'float']).columns
```

Out[40]:

```
Index(['Departamento', 'Salario'], dtype='object')
```

In [41]:

```
# Se muestran los valores según columna
print(datos['Departamento'].unique())
print(datos['Salario'].unique())
```

```
['Ventas' 'Contabilidad' 'GTH' 'Ciberseguridad' 'Finanzas'
 'Administrativo' 'TI' 'Mantenimiento' 'Mercadeo' 'Auditoria']
['Alto' 'Medio' 'Bajo']
```

In [42]:

```
# Se muestran el número de filas y columnas
datos.shape
```

Out[42]:

```
(15000, 9)
```

Cargamos el archivo llamado "Evaluación_Satisfacción_Empleados.xlsx" brindado por el Departamento de GTH para su análisis

In [43]:

```
empleados=pd.read_excel("C:\\Users\\jm_ad\\OneDrive\\Desktop\\Evaluación_Satisfacción_Empleados.xlsx")
empleados.head()
```

Out[43]:

	Empleado #	Nivel_Satisfacción	Última_Evaluación
0	100	0.38	0.53
1	101	0.80	0.86
2	102	0.11	0.88

	Empleado	Nivel_Satisfacción	Última_Evaluación
4	104	0.37	0.52

In [44]:

```
resultado = datos.set_index('Núm_Empleado').join(empleados.set_index('Empleado #'))
resultado = resultado.reset_index()
resultado.head()
```

Out[44]:

	Núm_Empleado	Núm_Proyectos	Núm_hrs_Mensuales	Tiempo_Laborado_Años	Accidente_Laboral	Renuncia	Promoción_Últ_5años	Departamento	Salario	Nivel_Satisfacción	Últi
0	100	6	130	5	0	1	0	Ventas	Alto	0.38	
1	101	5	233	4	0	1	0	Ventas	Medio	0.80	
2	102	7	256	3	0	1	1	Ventas	Medio	0.11	
3	103	5	257	4	0	1	1	Ventas	Alto	0.72	
4	104	6	160	3	0	1	1	Ventas	Alto	0.37	

In [46]:

```
resultado[resultado.isnull().any(axis=1)]
```

Out[46]:

	Núm_Empleado	Núm_Proyectos	Núm_hrs_Mensuales	Tiempo_Laborado_Años	Accidente_Laboral	Renuncia	Promoción_Últ_5años	Departamento	Salario	Nivel_Satisfacción
18	118	3	127	3	1	1	1	Ventas	Bajo	Nal
19	119	5	297	5	0	1	0	Ventas	Bajo	Nal
33	133	2	140	3	0	1	0	GTH	Bajo	Nal
53	153	2	132	3	0	1	0	Finanzas	Bajo	Nal
72	172	2	149	3	0	1	0	Mantenimiento	Alto	Nal
92	192	2	143	3	0	1	0	Ventas	Bajo	Nal
107	207	2	148	3	0	1	0	Contabilidad	Medio	Nal
120	220	4	158	4	1	1	0	Ciberseguridad	Bajo	Nal
137	237	2	129	3	0	1	0	Administrativo	Bajo	Nal
175	275	4	164	2	0	1	0	Ventas	Bajo	Nal
191	291	4	226	6	1	1	0	Ciberseguridad	Medio	0.92
352	452	4	262	6	0	1	0	Finanzas	Bajo	Nal
376	476	4	296	2	0	1	0	TI	Medio	0.58
402	502	5	275	5	0	1	0	Ventas	Bajo	Nal
427	527	3	180	4	0	1	0	Ciberseguridad	Medio	Nal
442	542	5	229	5	0	1	0	Administrativo	Bajo	0.77
468	568	5	245	5	0	1	0	Ventas	Bajo	Nal
543	643	5	237	5	0	1	0	Ventas	Medio	0.86
882	982	4	276	5	0	1	0	Finanzas	Bajo	0.74
1588	1688	5	264	5	0	1	0	TI	Medio	Nal
1934	2034	4	225	5	0	1	0	Ventas	Medio	0.78
2343	2443	3	115	2	1	0	0	Finanzas	Bajo	Nal
2743	2843	5	149	2	0	0	0	Auditoria	Bajo	0.63
3170	3270	5	188	2	0	0	0	Ciberseguridad	Medio	Nal
3609	3709	3	263	2	1	0	0	Ventas	Medio	0.98
3776	3876	4	214	3	0	0	0	Ciberseguridad	Medio	Nal
4122	4222	3	192	3	0	0	0	Mercadeo	Alto	0.88
4740	4840	3	253	3	0	0	0	Mercadeo	Medio	Nal
5028	5128	4	180	4	0	0	0	Mantenimiento	Medio	0.64
6453	6553	5	166	2	0	0	0	Ciberseguridad	Alto	Nal
7005	7105	4	150	3	0	0	0	Ciberseguridad	Bajo	0.83
7516	7616	4	264	3	0	0	0	Ciberseguridad	Bajo	Nal
8630	8730	4	167	3	1	0	0	Ciberseguridad	Bajo	0.90
9455	9555	4	270	3	0	0	0	Mantenimiento	Bajo	Nal
9901	10001	5	252	3	0	0	0	Finanzas	Medio	0.93
10647	10747	4	165	3	0	0	0	Ciberseguridad	Bajo	Nal
10962	11062	5	233	3	0	0	0	Finanzas	Bajo	0.66

	Núm_Empleado	Núm_Proyectos	Núm_hrs_Mensuales	Tiempo_Laborado_Años	Accidente_Laboral	Renuncia	Promoción_Últ_5años	Departamento	Salario	Nivel_Satisfacción
11967	12067	3	148	3	0	0	0	TI	Bajo	0.83
12422	12522	5	257	5	0	1	0	Ciberseguridad	Medio	NaN
12853	12953	3	136	2	0	0	0	GTH	Alto	NaN
13482	13582	3	207	7	0	0	1	Administrativo	Medio	0.58
13925	14025	3	133	3	0	0	0	Ventas	Medio	NaN

In [47]:

```
resultado.describe()
```

Out[47]:

	Núm_Empleado	Núm_Proyectos	Núm_hrs_Mensuales	Tiempo_Laborado_Años	Accidente_Laboral	Renuncia	Promoción_Últ_5años	Nivel_Satisfacción	Última_Evaluación
count	15000.000000	15000.000000	15000.000000	15000.000000	15000.000000	15000.000000	15000.000000	14973.000000	14973.000000
mean	7599.500000	3.805667	201.042667	3.498133	0.144600	0.238133	0.021467	0.612814	0.716130
std	4330.271354	1.231748	49.934823	1.460184	0.351709	0.425955	0.144939	0.248713	0.171134
min	100.000000	2.000000	96.000000	2.000000	0.000000	0.000000	0.000000	0.090000	0.360000
25%	3849.750000	3.000000	156.000000	3.000000	0.000000	0.000000	0.000000	0.440000	0.560000
50%	7599.500000	4.000000	200.000000	3.000000	0.000000	0.000000	0.000000	0.640000	0.720000
75%	11349.250000	5.000000	245.000000	4.000000	0.000000	0.000000	0.000000	0.820000	0.870000
max	15099.000000	7.000000	310.000000	10.000000	1.000000	1.000000	1.000000	1.000000	1.000000

In [48]:

```
# Se muestra el valor de la media de los primeros colaboradores

resultado.fillna(resultado.mean(), inplace=True)
resultado.head()
```

Out[48]:

	Núm_Empleado	Núm_Proyectos	Núm_hrs_Mensuales	Tiempo_Laborado_Años	Accidente_Laboral	Renuncia	Promoción_Últ_5años	Departamento	Salario	Nivel_Satisfacción	Últi
0	100	6	130	5	0	1	0	Ventas	Alto	0.38	
1	101	5	233	4	0	1	0	Ventas	Medio	0.80	
2	102	7	256	3	0	1	1	Ventas	Medio	0.11	
3	103	5	257	4	0	1	1	Ventas	Alto	0.72	
4	104	6	160	3	0	1	1	Ventas	Alto	0.37	

In [49]:

```
#resultado

resultado.loc[resultado['Núm Empleado'] == 14025]
```

Out[49]:

	Núm_Empleado	Núm_Proyectos	Núm_hrs_Mensuales	Tiempo_Laborado_Años	Accidente_Laboral	Renuncia	Promoción_Últ_5años	Departamento	Salario	Nivel_Satisfacción
13925	14025	3	133	3	0	0	0	Ventas	Medio	0.612814

In [50]:

```
# Se muestran los primeros 5 resultados

resultado.head()
```

Out[50]:

	Núm_Empleado	Núm_Proyectos	Núm_hrs_Mensuales	Tiempo_Laborado_Años	Accidente_Laboral	Renuncia	Promoción_Últ_5años	Departamento	Salario	Nivel_Satisfacción	Últi
0	100	6	130	5	0	1	0	Ventas	Alto	0.38	
1	101	5	233	4	0	1	0	Ventas	Medio	0.80	
2	102	7	256	3	0	1	1	Ventas	Medio	0.11	
3	103	5	257	4	0	1	1	Ventas	Alto	0.72	
4	104	6	160	3	0	1	1	Ventas	Alto	0.37	

In [51]:

```
# Removemos la columna llamada "Núm_Empleado"
```

```
resultado_final = resultado.drop(columns='Núm_Empleado')
resultado_final.head()
```

Out[51]:

	Núm_Proyectos	Núm_hrs_Mensuales	Tiempo_Laborado_Años	Accidente_Laboral	Renuncia	Promoción_Últ_5años	Departamento	Salario	Nivel_Satisfacción	Última_Evaluación
0	6	130	5	0	1	0	Ventas	Alto	0.38	0.53
1	5	233	4	0	1	0	Ventas	Medio	0.80	0.86
2	7	256	3	0	1	1	Ventas	Medio	0.11	0.88
3	5	257	4	0	1	1	Ventas	Alto	0.72	0.87
4	6	160	3	0	1	1	Ventas	Alto	0.37	0.52

In [52]:

```
resultado_final.groupby('Departamento').sum()
```

Out[52]:

Departamento	Núm_Proyectos	Núm_hrs_Mensuales	Tiempo_Laborado_Años	Accidente_Laboral	Renuncia	Promoción_Últ_5años	Nivel_Satisfacción	Última_Evaluación
Administrativo	2432	126787	2711	103	91	69	391.785629	456.234519
Auditoria	3033	158030	2650	134	121	27	487.800000	560.446130
Ciberseguridad	10459	546014	9191	378	682	28	1640.072515	1944.020649
Contabilidad	2935	154324	2702	96	204	14	446.682814	550.706130
Finanzas	8558	450508	7624	347	567	20	1386.268443	1623.544519
GTH	2736	148538	2511	90	219	15	447.365629	530.696130
Mantenimiento	3434	180369	3135	132	198	0	559.185629	644.662259
Mercadeo	3164	171073	3063	138	203	43	530.622814	613.946130
TI	4683	248119	4256	164	273	3	758.172814	879.452259
Ventas	15651	831878	14629	587	1014	103	2543.779701	2938.236778

In [53]:

```
resultado_final.groupby('Departamento').mean()
```

Out[53]:

Departamento	Núm_Proyectos	Núm_hrs_Mensuales	Tiempo_Laborado_Años	Accidente_Laboral	Renuncia	Promoción_Últ_5años	Nivel_Satisfacción	Última_Evaluación
Administrativo	3.860317	201.249206	4.303175	0.163492	0.144444	0.109524	0.621850	0.724182
Auditoria	3.853875	200.800508	3.367217	0.170267	0.153748	0.034307	0.619822	0.712130
Ciberseguridad	3.879451	202.527448	3.409125	0.140208	0.252967	0.010386	0.608336	0.721076
Contabilidad	3.826597	201.204694	3.522816	0.125163	0.265971	0.018253	0.582377	0.718000
Finanzas	3.812027	200.671715	3.395991	0.154566	0.252561	0.008909	0.617492	0.723182
GTH	3.657754	198.580214	3.356952	0.120321	0.292781	0.020053	0.598737	0.709487
Mantenimiento	3.807095	199.965632	3.475610	0.146341	0.219512	0.000000	0.619951	0.714703
Mercadeo	3.687646	199.385781	3.569930	0.160839	0.236597	0.050117	0.618442	0.715555
TI	3.816626	202.215974	3.468623	0.133659	0.222494	0.002445	0.617908	0.716750
Ventas	3.780435	200.936715	3.533575	0.141787	0.244928	0.024879	0.614440	0.709719

In [54]:

```
# La función ".value_counts()" devuelve un objeto que contiene recuentos de valores únicos.
# El objeto resultante estará en orden descendente, el primero posee mayor frecuencia.
# Excluye los valores NA por defecto.

resultado_final['Departamento'].value_counts()
```

Out[54]:

```
Ventas            4140
Ciberseguridad    2696
Finanzas          2245
TI                1227
Mantenimiento      902
Mercadeo           858
Auditoria          787
Contabilidad       767
GTH                748
Administrativo     630
Name: Departamento, dtype: int64
```

Se procede a revisar la cantidad de colaboradores que Renunciaron

In [55]:

```
resultado_final['Renuncia'].value_counts()
```

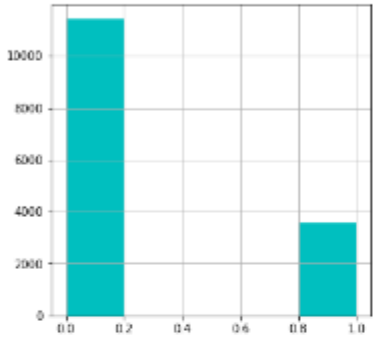
Out[55]:

```
0    11428
1     3572
Name: Renuncia, dtype: int64
```

De acuerdo al resultado 3572 colaboradores renunciaron

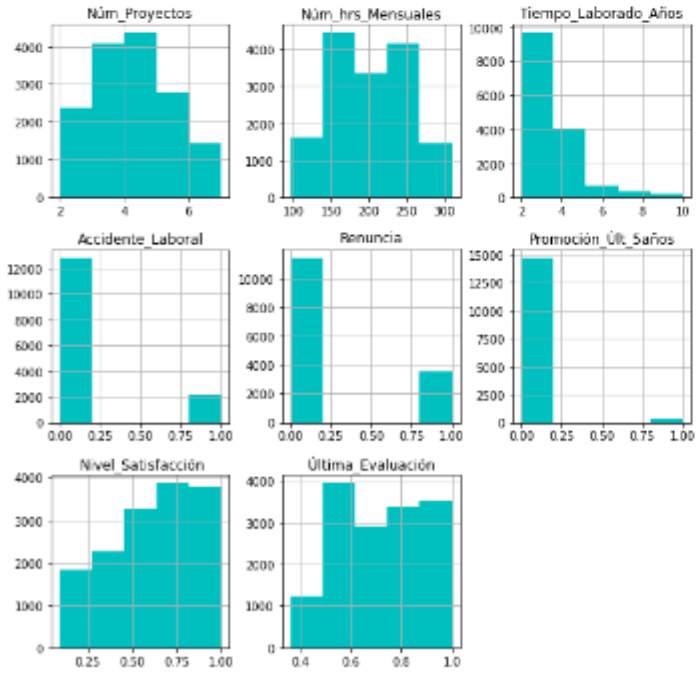
In [56]:

```
resultado_final['Renuncia'].hist(bins = 5, figsize = (5,5), color = 'c');
```



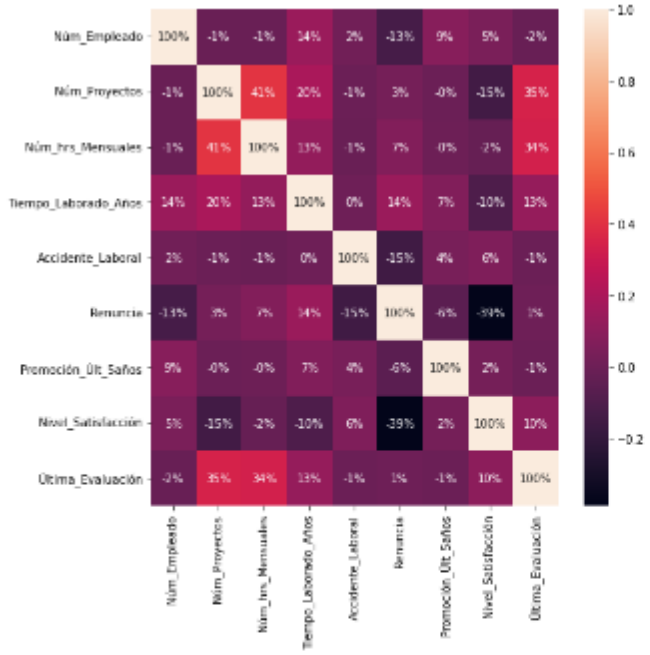
In [57]:

```
resultado_final.hist(bins = 5, figsize = (10,10), color = 'c');
```



In [58]:

```
# Se procede a analizar las correlaciones en forma gráfica
plt.figure(figsize=(8,8))  #14in by 14in
sns.heatmap(resultado.corr(), annot=True, fmt='.0%')
plt.show()
```



Preparación del conjunto de datos para usar Machine Learning

In [60]:

```
# Se realiza una codificación en caliente de los datos categóricos
categorial = ['Departamento','Salario']
resultado_final = pd.get_dummies(resultado_final, columns=categorial, drop_first=True)
resultado_final.head()
```

Out[60]:

	Núm_Proyectos	Núm_hrs_Mensuales	Tiempo_Laborado_Años	Accidente_Laboral	Renuncia	Promoción_Últ_5años	Nivel_Satisfacción	Última_Evaluación	Departamento_Auditoria
0	6	130	5	0	1	0	0.38	0.53	0
1	5	233	4	0	1	0	0.80	0.86	0
2	7	256	3	0	1	1	0.11	0.88	0
3	5	257	4	0	1	1	0.72	0.87	0
4	6	160	3	0	1	1	0.37	0.52	0

In [61]:

```
resultado_final.info()
```

```
<class 'pandas.core.frame.DataFrame'>
RangeIndex: 15000 entries, 0 to 14999
Data columns (total 19 columns):
 #   Column                      Non-Null Count  Dtype  
---  ------                      --------------  -----  
 0   Núm_Proyectos               15000 non-null  int64  
 1   Núm_hrs_Mensuales           15000 non-null  int64  
 2   Tiempo_Laborado_Años        15000 non-null  int64  
 3   Accidente_Laboral           15000 non-null  int64  
 4   Renuncia                    15000 non-null  int64  
 5   Promoción_Últ_5años         15000 non-null  int64  
 6    Nivel_Satisfacción         15000 non-null  float64
 7   Última_Evaluación           15000 non-null  float64
 8   Departamento_Auditoria      15000 non-null  uint8  
 9   Departamento_Ciberseguridad 15000 non-null  uint8  
 10  Departamento_Contabilidad   15000 non-null  uint8  
 11  Departamento_Finanzas       15000 non-null  uint8  
 12  Departamento_GTH            15000 non-null  uint8  
 13  Departamento_Mantenimiento  15000 non-null  uint8  
 14  Departamento_Mercadeo       15000 non-null  uint8  
 15  Departamento_TI             15000 non-null  uint8  
 16  Departamento_Ventas         15000 non-null  uint8  
 17  Salario_Bajo                15000 non-null  uint8  
 18  Salario_Medio               15000 non-null  uint8  
dtypes: float64(2), int64(6), uint8(11)
memory usage: 1.1 MB
```

Preparando nuestro conjunto de datos para el aprendizaje automático

In [62]:

```
from sklearn.model_selection import train_test_split

# We remove the label values from our training data
X = resultado_final.drop(['Renuncia'],axis=1).values

# We assigned those label values to our Y dataset
y = resultado_final['Renuncia'].values
```

In [63]:

```
# Split it to a 70:30 Ratio Train:Test

X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.3)
```

In [64]:

```
# Normalize the data
from sklearn.preprocessing import StandardScaler

sc = StandardScaler()
X_train = sc.fit_transform(X_train)
X_test = sc.transform(X_test)

# fit(raw_documents[, y]): Learn a vocabulary dictionary of all tokens in the raw documents.
# fit_transform(raw_documents[, y]): Learn the vocabulary dictionary and return term-document matrix. This is equivalent t
o fit followed by the transform, but more efficiently implemented.
```

In [65]:

```
df_train = pd.DataFrame(X_train)
df_train.head()
```

Out[65]:

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	1
0	0.148714	0.703022	-1.032510	-0.412209	-0.147979	0.351108	0.491724	4.257427	-0.468824	-0.234884	-0.418200	-0.230334	-0.251577	-0.250076	-0.297167	-0.613896	-0.966835	1.1484
1	2.588547	1.744722	0.344782	-0.412209	-0.147979	-2.093736	1.488480	-0.234884	-0.468824	-0.234884	2.391203	-0.230334	-0.251577	-0.250076	-0.297167	-0.613896	-0.966835	1.1484
2	0.961992	0.743087	1.722074	-0.412209	-0.147979	0.791981	1.371215	-0.234884	2.132999	-0.234884	-0.418200	-0.230334	-0.251577	-0.250076	-0.297167	-0.613896	1.034302	0.8707
3	0.961992	0.983479	-0.343864	-0.412209	-0.147979	1.313014	-0.739563	-0.234884	-0.468824	-0.234884	-0.418200	4.341517	-0.251577	-0.250076	-0.297167	-0.613896	1.034302	0.8707
4	0.148714	0.462629	1.033428	-0.412209	-0.147979	1.032458	1.664378	-0.234884	2.132999	-0.234884	-0.418200	-0.230334	-0.251577	-0.250076	-0.297167	-0.613896	-0.966835	1.1484

In [66]:

```
df_train.describe()
```

Out[66]:

	0	1	2	3	4	5	6	7	8	9	10	1
count	1.050000e+04	1.050000e+04	1.050000e+04	1.050000e+04	1.050000e+04	1.050000e+04	1.050000e+04	1.050000e+04	1.050000e+04	1.050000e+04	1.050000e+04	1.050000e+0
mean	-2.578678e-16	2.473894e-16	1.001125e-15	-1.515719e-15	5.875882e-16	3.052136e-14	2.178403e-14	6.879629e-16	-6.083441e-16	3.724481e-16	-6.327743e-16	-1.869346 1
std	1.000048e+00	1.000048e+00	1.000048e+00	1.000048e+00	1.000048e+00	1.000048e+00	1.000048e+00	1.000048e+00	1.000048e+00	1.000048e+00	1.000048e+00	1.000048e+0
min	-1.477842e+00	-2.101556e+00	-1.032510e+00	-4.122092e-01	-1.479791e-01	-2.093736e+00	-2.088116e+00	-2.348837e-01	-4.688236e-01	-2.348837e-01	-4.181996e-01	-2.303342 0
25%	-6.645642e-01	-8.995939e-01	-3.438639e-01	-4.122092e-01	-1.479791e-01	-6.909567e-01	-9.154613e-01	-2.348837e-01	-4.688236e-01	-2.348837e-01	-4.181996e-01	-2.303342 0
50%	1.487137e-01	-1.815534e-02	-3.438639e-01	-4.122092e-01	-1.479791e-01	1.105314e-01	2.266212e-02	-2.348837e-01	-4.688236e-01	-2.348837e-01	-4.181996e-01	-2.303342 0
75%	9.619915e-01	8.833158e-01	3.447821e-01	-4.122092e-01	-1.479791e-01	8.320608e-01	9.021528e-01	-2.348837e-01	-4.688236e-01	-2.348837e-01	-4.181996e-01	-2.303342 0
max	2.588547e+00	2.185441e+00	4.476659e+00	2.425953e+00	6.757712e+00	1.553490e+00	1.664378e+00	4.257427e+00	2.132999e+00	4.257427e+00	2.391203e+00	4.341517e+0

Se procede a entrenar un modelo de regresión logística

In [67]:

```
from sklearn.linear_model import LogisticRegression
```

```
from sklearn.metrics import confusion_matrix
from sklearn.metrics import classification_report
from sklearn.metrics import accuracy_score

model = LogisticRegression(solver='lbfgs')
model.fit(X_train, y_train)

predictions = model.predict(X_test)

print("Accuracy {0:.2f}%".format(100*accuracy_score(predictions, y_test)))
print(confusion_matrix(y_test, predictions))
print(classification_report(y_test, predictions))
```

```
Accuracy 79.18%
[[3198  232]
 [ 705  365]]
              precision    recall  f1-score   support

           0       0.82      0.93      0.87      3430
           1       0.61      0.34      0.44      1070

    accuracy                           0.79      4500
   macro avg       0.72      0.64      0.66      4500
weighted avg       0.77      0.79      0.77      4500
```

Se prueba el modelo en una sola fila nueva de datos

In [68]:

```
# Create Test Input
# Enter your values here

input_data = {'Núm_Proyectos': [3],
              'Núm_hrs_Mensuales': [160],
              'Tiempo_Laborado_Años': [5],
              'Accidente_Laboral': [0],
              'Promoción_Últ_5años': [1],
              'Última_Evaluación': [0.5],
              'Nivel_Satisfacción': [0.5],
              'Departamento_Auditoria': [0],
              'Departamento_Contabilidad': [0],
              'Departamento_GTH': [0],
              'Departamento_Finanzas': [0],
              'Departamento_Mercadeo': [1],
              'Departamento_Mantenimiento': [0],
              'Departamento_Ventas': [0],
              'Departamento_Ciberseguridad': [0],
              'Departamento_TI': [0],
              'Salario_Bajo': [0],
              'Salario_Medio': [1]}

# Convert to pandas dataframe
input_data = pd.DataFrame(input_data)

# Transform data using sc.transform
input_data = sc.transform(input_data)

# Reshape data for input into our model predict function
input_data = input_data.reshape(1, -1)

# Run prediction for our test sameple, 0 means employee will not leave, 1 means they are likely to leave/resign
model.predict(input_data)

# print probabilities of belonging to either class
model.predict_proba(input_data)
```

Out[68]:

```
array([[0.83662317, 0.16337683]])
```

Probamos un clasificador de bosque aleatorio

In [69]:

```
from sklearn.ensemble import RandomForestClassifier
from sklearn.metrics import confusion_matrix
from sklearn.metrics import classification_report
from sklearn.metrics import accuracy_score

model = RandomForestClassifier()
model.fit(X_train, y_train)

predictions = model.predict(X_test)
score = model.score(X_test, y_test)

print("Accuracy {0:.2f}%".format(100*accuracy_score(predictions, y_test)))
print(confusion_matrix(y_test, predictions))
print(classification_report(y_test, predictions))
```

```
Accuracy 99.02%
[[3424    6]
 [  38 1032]]
              precision    recall  f1-score   support

           0       0.99      1.00      0.99      3430
           1       0.99      0.96      0.98      1070

    accuracy                           0.99      4500
   macro avg       0.99      0.98      0.99      4500
weighted avg       0.99      0.99      0.99      4500
```

In [72]:

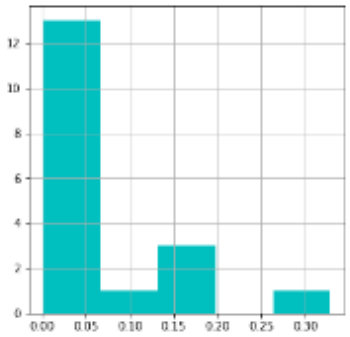
```
import pandas as pd
feature_importances = pd.DataFrame(model.feature_importances_,
                                   index = pd.DataFrame(X_train).columns,
                                    columns=['importance']).sort_values('importance',ascending=False)

feature_importances
```

Out[72]:

	importance
5	0.328552
2	0.182720
0	0.164936
1	0.159168
6	0.120880
3	0.009427
16	0.006913
17	0.004388
8	0.003825
15	0.003814
10	0.003383
4	0.002116
14	0.001966
11	0.001845
9	0.001816
7	0.001765
12	0.001299
13	0.001186

In [73]:

```
feature_importances['importance'].hist(bins = 5, figsize = (5,5), color = 'c');
```



Final de la Auditoría/Análisis de Entrenamientoy Posibles Renuncias - Septiembre 2021

--

Resultado de la Auditoría:

Se envía al Dpto. de Gestión del Talento Humano el siguiente informe:

De acuerdo al resultado 4188 colaboradores trabajan desde la casa, este grupo debe ser el primero en tener entrenamiento de ciberseguridad y revisión de condiciones

De acuerdo al segundo resultado un total de 3572 colaboradores renunciaron

Se propone un modelo de RandomForestClassifier o bosque aleatorio para identificar a todos aquellos colaboradores que se consideran candidatos a renunciar para que se incremente la seguridad con respecto a sus actividades.

In [ ]: