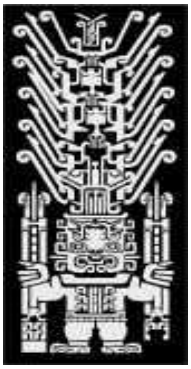
P R O Y E C T O 2018



"CIBERSEGURIDAD EN LA ACTIVIDAD ORGANIZACIONAL DE LA ERA DIGITAL"

Martin S. Gavino Ramos

Colaborador:

Juan C. Álvarez & Honorio Campo blanco, Jorge Villavicencio Meza, Iván Minaya, Ruiz Vílchez, Jean Claude

Facultad de Ingeniería Industrial y de Sistemas

Universidad Nacional Federico Villarreal

LIMA-PERÚ

2018

"TENDENCIA DE CIBER SEGURIDAD" EN LA ERA DIGITAL"

Fechas de inicio y término del proyecto:

02 de enero al 30 de diciembre del 2018

Línea de Investigación:

Línea de Investigación: Gestión empresarial y TIC´s

Código UNESCO: 3310.05

RESUMEN

El objetivo de la investigación fue determinar en qué medida la ciberseguridad mejora la actividad organizacional en la era digital. En este sentido se procedió a efectuar un análisis de la información secundaria a nivel mundial y nacional. Evidencias de análisis de expertos y evidencia estadística en la última década; esto es, en relación a la situación de la ciberseguridad y sus efectos en las organizaciones, especialmente en las empresas que manejan sistemas de información gerencial. En ese sentido tenemos los siguientes resultados;: La ciberseguridad, genera un 79% de reducción de los gastos operativo, un 85% de reducción de tiempos de operación, asimismo, facilita una disponibilidad del 99% de disponibilidad de datos ,asimismo, un 86% de reducción de problemas de infraestructura. Como conclusión tenemos: la ciberseguridad influye positivamente en la mejora de la actividad organizacional, evitando los ataques de diversos tipos del ciberespacio, especialmente en las dimensiones de planificación y cotejo de los resultados, asimismo, mejora la aplicación de la gestión institucional.

PALABRA CLAVE: Ciberseguridad, Ciberdefenza, Era Digital, Información,

ABSTRACT

The objective of the research was to determine to what extent cybersecurity improves organizational activity in the digital age. In this sense, an analysis of the secondary information at a global and national level was carried out. Evidence of expert analysis and statistical evidence in the last decade; that is, in relation to the situation of cybersecurity and its effects on organizations, especially in companies that manage management information systems. In that sense we have the following results: Cybersecurity, generates a 79% reduction in operating expenses, an 85% reduction in operating times, likewise, it facilitates 99% availability of data availability, likewise 86% % reduction of infrastructure problems. In conclusion we have: cybersecurity positively influences the improvement of organizational activity, avoiding attacks of various types of cyberspace, especially in the planning and comparison of results dimensions, also improving the application of institutional management.

KEYWORD: Cybersecurity, Cyber defense, Digital Age, Information.

2. INTRODUCCIÓN

2.1 Problema

Planteamiento del problema.

La ciberseguridad es un problema que implica a gobiernos, empresas y ciudadanos. La dependencia que todos los sectores sociales y económicos tienen de la infraestructura de información y telecomunicaciones ha crecido extraordinariamente, volviéndose compleja y difícil de gestionar.

Por eso es fundamental contar con un marco adecuado para tener una respuesta rápida, ordenada y eficaz a los incidentes en los que se ven comprometidas alguna de las dimensiones de la seguridad de la información (confidencialidad, integridad o disponibilidad).

Problema general

Es cierto que los expertos de la dinámica moderna de las organizaciones tienen en agenda la importancia de la ciberseguridad, pero muchos no están bien preparados para comenzar el proceso de gestión de estos riesgos dada la infinidad de elementos técnicos y no técnicos en esta materia, como consecuencia tenemos, las violaciones de datos están aumentando, Continúan en aumento los ataques dirigidos, Las estafas en medios sociales están aumentando, Troyanos bancarios y robos.

“Hay dos tipos de empresa: la que ha sufrido un ataque informático y la que no se ha enterado”. Así resume Diego Esteban la importancia de la ciberseguridad en el entorno de la empresa.

Problema General

¿En qué medida la ciberseguridad mejora la actividad organizacional respecto de la planificación y la aplicación en la era digital?

Problemas específicos

¿En qué medida la ciberseguridad mejora la planificación de la actividad organizacional en la era digital"

En qué medida la ciberseguridad mejora la aplicación de la actividad organizacional en la era digital"

2.2 Antecedentes

Según almomento.net, santo domingo, República Dominicana (23 agosto, 2018). – Cuando una empresa crece, se va enfrentando a nuevos retos y desafíos, entre ellos, un ciberataque.

Esto ha dado lugar a que la ciberseguridad sea un tema fundamental, en especial porque los ataques son cada vez más sofisticados, precisos y dañinos.

Un software malicioso puede ocasionar retrasos operativos de vulnerabilidad de seguridad o una violación a los datos personales, como ha ocurrido con el ransomware, que tuvo un crecimiento de más del 60% el año pasado.

El 40% de los directivos y responsables de IT entrevistados en la Encuesta Mundial sobre el Estado de la Seguridad de la Información 2018, dice no tener una estrategia general de seguridad de la información. Además, el 48% no cuenta con un programa de capacitación en concientización sobre seguridad para sus empleados, y el 54% asegura que no tiene un proceso

de respuesta a incidentes. Esto, sumado a que solo el 39% de los encuestados dice tener mucha confianza en su capacidad de manejo de ciberataques.

Esto significa que, así como los bancos necesitan seguridad física (personal de seguridad), la información alojada en la nube y en centros de datos, también requiere de protección por el valor que representa para cada organización o persona que la posee.

Entre más valores y activos almacena una empresa de forma digital, mayores serán los requerimientos de seguridad de información y lo especializados que sean, tanto para sus clientes, como para la organización misma.

Las nuevas tecnologías como el IoT (Internet de las Cosas), también repercuten en las inversiones de seguridad, con una tendencia hacia un mayor consumo de soluciones como servicio, ya que según la IDC se calcula que para el 2020 se alcancen los 600 millones de cosas conectadas.

Las empresas deben buscar un diferenciador en el mercado para brindar la certeza de que ningún dato se filtrará, esto, además, será un valor agregado que aumentará la lealtad del cliente.

“En KIO Networks, contamos con servicios de diagnóstico y solución de problemas de ciberseguridad y de seguridad electrónica para resolver las necesidades de protección. Definimos un marco de controles de cumplimiento, supervisamos su implementación y realizamos evaluaciones continuas para garantizar la seguridad”, asegura Cristian Ali, Director Regional de KIO Networks para Centroamérica y El Caribe.

Erika Lazzarin (2010), Directora Comercial de KIO Networks República Dominicana menciona que:

"Con este panorama es decisivo que, al generar su estrategia y estructura operativa, los CIO se planteen qué pasaría si se perdiera toda la información y que impacto tendría en el negocio. De esta forma se puede decidir la forma en que se invertirá para la protección de la compañía y sus activos, antes de que ocurra un incidente en la seguridad lógica".

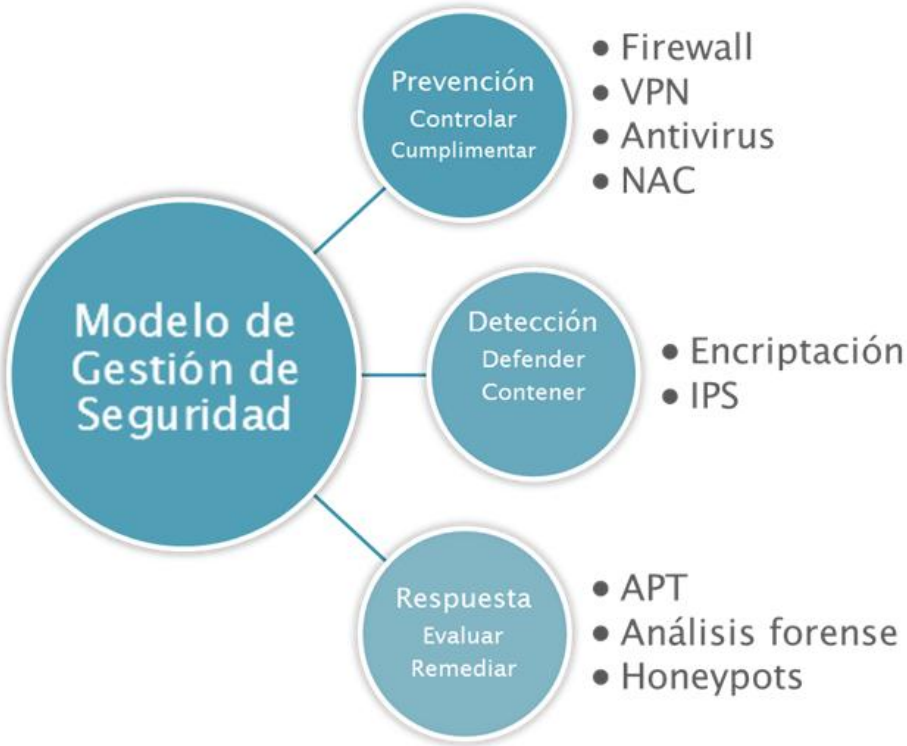
Según Altran | (Sep 5, 2018), El papel de la ciberseguridad en la transformación digital Cuando oímos hablar de Transformación Digital pensamos en la oportunidad de innovar y en la posibilidad de hacer crecer nuestra organización en un nuevo entorno, pero en este proceso la seguridad tiene un importante peso y se ha de tener en cuenta si no se quiere fracasar en el intento. Hasta hace muy poco la Ciberseguridad de las empresas se basaba en la securización y protección del perímetro mediante la integración de diversas soluciones de seguridad como Firewalls, WAFS o IDPs, pero con la introducción de este nuevo concepto, el uso cada vez más extensivo de las tecnologías de la información, el Cloud Computing, el uso de dispositivos personales para el trabajo (BYODs) y la incorporación de los Mileniums al mercado laboral, el perímetro de seguridad como lo conocimos deja de existir. Debemos analizar los nuevos riesgos asociados a la Digitalización, no solo al uso de las tecnologías que conlleva este proceso sino también desde el punto de vista del personal y de la información afectada. No bastará con analizar los riesgos derivados del uso (durante), sino también el antes y la finalización, sobre todo, si éste está basado en sistemas Cloud no dependientes de nuestro departamento TI.

Altran (Ob.cit), ha identificado y clasificado los riesgos más frecuentes derivados de este proceso de transformación, centrándose sobre todo en las posibles contramedidas que se puedan aplicar para poder mitigarlos. Estas contramedidas se han valorado desde el punto de vista predictivo, preventivo, de detección y respuesta, cubriendo así las diferentes opciones de

seguridad existentes que una organización pueda adoptar en función de su realidad y de la criticidad de los riesgos a tratar.

Antecedentes, contexto y tendencias de la transformación digital

En la actualidad más del 50 % de las empresas y organizaciones disponen de una estrategia Digital corporativa que les permitirá competir en este nuevo entorno digital. Aquellas empresas que no se adapten a esta tendencia muy probablemente desaparecerán a medio plazo. Ya existen antecedentes al respecto de empresas que no supieron adaptarse y que acabaron desapareciendo o perdiendo gran parte de su negocio; quién no recuerda casos como el de Blockbuster, donde la piratería y el P2P acabaron con su negocio, o Kodak, líder en carretes fotográficos, que la aparición de la cámara digital acabó con gran parte de su negocio. Alrededor del 50% de las compañías listadas en el fortune 500 en el año 1990 ya no aparecían diez años después. Está claro, innova o desapareces.



Las empresas, actualmente enfocadas en la creación de nuevos servicios o en inventar productos, dejan atrás las grandes inversiones en optimizar sus procesos de negocio, que ya se mejoraron en un 80% en el pasado y cuyos esfuerzos para mejorar el 20% restante superaría con creces al beneficio esperado. Dentro de este escenario, ¿qué está pasando en el ámbito de la Ciberseguridad? El aumento continuo de las vulnerabilidades, a ritmo de un 20% por año, hacen de la Ciberseguridad una de las tendencias clave en el ámbito TI. Las empresas llevan años invirtiendo en infraestructura de seguridad centrándose en la securizacion del perímetro y en el puesto de trabajo, y ahora estos pasos ya están superados y es hora de pasar a la acción.

Sólo en el 2016 se prevé un aumento en inversiones de un 60% orientadas claramente a la detección y respuesta rápida de incidentes de seguridad. La transformación digital trae de forma inherente riesgos difíciles de abordar por el CISO de una organización que contempla la introducción masiva de tecnologías "autónomas" dentro de su organización sobre las que sin embargo difícilmente podrá aplicar políticas de seguridad corporativas. La imposibilidad de conocer las diversas tecnologías implantadas y de tener técnicos especializados junto a los nuevos marcos legislativos o la posibilidad de monitorizar las nuevas soluciones, serán retos que el CISO tendrá que superar en los próximos años. Los servicios "clásicos" de consultoría y auditoria de seguridad de la información deberán ser complementados con nuevas soluciones para que éstas tengan la efectividad esperada. Sin duda, la Transformación Digital empresarial pondrá a prueba a los departamentos de seguridad corporativa, que se enfrentan no solo a un cambio tecnológico sino de filosofía empresarial.

El nuevo modelo de seguridad en la transformación digital

Hasta ahora las organizaciones centraban su estrategia de seguridad en la prevención, instalando dispositivos o software que evitaran una posible infección o ataque, dedicándole un 90% del total de sus inversiones, mientras que el 10 % restante quedaba para la respuesta en caso de incidente. Este modelo deja de ser válido en el momento en que nuestra organización se ve inmersa en un proceso de Transformación Digital. Los datos (Redes sociales, BIG DATA y Analítica), las aplicaciones (CLOUD) incluso los dispositivos (BYOD o IoT) ya no están bajo el perímetro de la empresa y por tanto la estrategia de seguridad actual será ineficiente tal y como estaba enfocada. El responsable de seguridad deberá poner foco en la detección y respuesta de incidentes de seguridad, centrándose sobre todo en la protección del dato y empezar a olvidarse de la securizacion de las infraestructuras ya que éstas, en cierto modo, ya no dependen directamente del departamento TI de la organización y por tanto su capacidad de acción se reduce notablemente. Con este nuevo enfoque, lejos de securizar la infraestructura, nos preparamos para responder de forma eficaz a un posible incidente de seguridad.

Pero ¿cómo centrarse en los datos? ¿Por dónde empezar?

Aceptando el reto, los riesgos de seguridad en la transformación digital

Considerando, como se ha mencionado anteriormente, que la Ciberseguridad debe ser uno de los pilares a tener en cuenta si queremos tener éxito, Altran (Ob. Cit) ha clasificado los 5 riesgos de seguridad más importantes y frecuentes en esta nueva era digital.

Sin duda, uno de los retos iniciales será identificar dónde y qué información existe, ya que la mayoría de datos será información informal y desconocida por la organización. Además,

la constante aparición de nuevos players y soluciones dificultará sin duda obtener esta información.

Para poder definir correctamente el modelo de seguridad y asegurar la información de forma correcta, debemos crear un mapa de la información teniendo en cuenta:

- Dónde está y cómo se accede a la información de la empresa, (sistemas clouds, redes sociales, herramientas colaborativas, etc.)
- Requerimientos de seguridad de los datos como podrían ser los requerimientos de acceso (público, restringido, etc.)

Toda esta información nos permitirá analizar las posibles amenazas derivadas del uso de estas "nuevas" tecnologías y por tanto seleccionar los controles de seguridad requeridos y adecuados, siempre que esto sea posible.

Cumplimiento

El cumplimiento legal será uno de los riesgos a tener en cuenta en el uso de servicios e Infraestructura Cloud. En concreto deberían tenerse en cuenta leyes de protección de datos, leyes de privacidad o incluso leyes por violaciones de seguridad por divulgación. Desde el punto de vista de la Ley orgánica de protección de datos(LOPD) se ha de tener en cuenta que la contratación de este tipo de servicio no excluye de responsabilidades legales a la empresa contratante que será siempre responsable del tratamiento.

En general, para asegurar el cumplimiento legal hay tres aspectos comunes a tener en cuenta para la contratación de estos servicios:

- *La localización* (país) de los datos, ya que se ha de asegurar unas garantías exigibles de protección de los datos.
- *La portabilidad* de los datos. El servicio contratado debe garantizar poderse llevar los datos en un momento determinado y el proveedor estará obligado a entregar toda la información y a destruirla en sus sistemas si así lo pide el cliente.

La dificultad de poder ejercer los derechos (ARCO) o tener información de quién, cuándo o dónde han accedido a unos datos es uno de los riesgos a tratar. Por tanto, tener un contrato donde nos reservemos el derecho a auditoria puede ser una buena práctica a tener en cuenta.

2.3 Objetivos.

Objetivo General

Determinar en qué medida la ciberseguridad mejora la actividad organizacional en la era digital

Objetivos específicos

- Determinar en qué medida la ciberseguridad mejora la planificación de la actividad organizacional en la era digital”
- Determinar en qué medida la ciberseguridad mejora la aplicación de la actividad organizacional en la era digital”

2.4. Justificación e Importancia.

El interés principal de realizar la investigación es que la universidad tiene una doble misión, la de educar al estudiante y hacer investigación sobre los problemas actuales y proyectarse a la sociedad del futuro para rediseñar sus programas de enseñanza e investigación.

La Universidad tiene un rol social, en el caso particular en especial la ingeniería está relacionada con la producción, desarrollo, ecología, ecosistemas, tecnología y dentro de la prospectiva de enfoque sistémico tiene mayor relevancia, parte de una reflexión personal por la situación actual imperante del uso de la ciberseguridad en las organizaciones productivas en la era digital.

La incorporación de la tecnología digital, al ámbito académico puede hacer de la educación un fenómeno masivo de grandes dimensiones atendiendo necesidades individualmente requeridas.

La universidad es el espacio más propicio y poderoso para socializar y generar nuevo conocimiento. Al masificarse la difusión de las tecnologías digitales, surgen innovaciones en aplicaciones y servicios en todos los sectores económicos.

3. MARCO TEÓRICO

Era digital

De acuerdo a Carmona, Luis(2014) , La norma ISO 27001 ofrece los requisitos necesarios para establecer un **Sistema de Gestión de Seguridad de la Información** en las organizaciones

En la actualidad el término "ciberseguridad" se encuentra asociados a ciberespacio, ciberamenazas, etc.

Definición de ciberseguridad

Según ISACA (*Information Systems Audit and Control Association – Asociación de Auditoría y Control sobre los Sistemas de Información),* se define la Ciberseguridad como "Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados".

Dentro de la Norma ISO 27001, se define el **Activo de la Información** como los conocimientos o datos que tienen valor para una organización, mientras que, en la misma norma, los **Sistemas de Información** comprenden a las aplicaciones, servicios, activos de tecnologías de información u otros componentes que permiten el manejo de la misma.

Por tanto, es fácil deducir que la Ciberseguridad, tiene como foco la **protección de la información digital** que "vive" en los sistemas interconectados. En consecuencia, está comprendida dentro de la seguridad de la información.

El estándar **ISO 27001** establece que la definición de **activo de información** pueden ser los conocimientos que tienen un valor añadido para la empresa, mientras que los **Sistemas de Información** establecen las aplicaciones, los servicios, los activos ,etc. y utiliza otros compuestos que faciliten el manejo de la información.

La ciberseguridad ofrece un foco de protección para la información digital que se encuentra entre sistemas interconectados. Como consecuencia, se encuentra en la **seguridad de la información.**

Seguridad de la Información

Para poder establecer la diferencia con la **seguridad de la información**, debemos revisar varios conceptos más que nos permiten tener el contexto general. Según la Real Academia Española (RAE), la seguridad se puede definir como: "Libre o exento de todo peligro, daño o riesgos"

Sin embargo, es una condición ideal, ya que en la realidad no es posible tener la certeza de que se puedan evitar todos los peligros.

El principal propósito de seguridad en todos los ámbitos de aplicación es el de reducir riegos hasta un nivel que se pueda aceptar y que los interesados puedan mitigar las amenazas latentes. Es decir, la seguridad también entiende que las actividades se encuentran destinadas a proteger del peligro a los activos sensibles de la organización.

La información se puede encontrar en diferentes formatos, por ejemplo, en formato digital (utilizando los diferentes medios electrónicos que existen hoy en día), de forma física (bien sea escrita o impresa), además de manera no representada, esto pueden ser ideas o conocimiento de personas que pertenecen a la organización. Los **activos de información** se pueden encontrar en diferentes formatos

En un **Sistema de Gestión de Seguridad de la Información ISO 27001** la información se puede almacenar, procesar o trasmitir de diferentes maneras:

- Formato electrónico
- Forma verbal
- Mediante mensajes escritos
- Impresos

Esto quiere decir que será posible encontrarlos en diferentes formatos.

No importa la forma o el estado, la información requiere que se cumpla una serie de medidas de protección que sean adecuadas según la importancia y la criticidad de la información, esto es especialmente importante en el ámbito de la **seguridad de la información**.

Debemos recordar que la seguridad en cómputo se limita a la protección de los sistemas y equipos que permiten procesar toda la información, mientras que la seguridad informática se involucra en todos los métodos, procesos o técnicas para tratar de forma automática la información que se encuentra en formato digital, teniendo un mayor alcance, ya que se incluye la protección de las redes e infraestructuras tecnológicas.

Cuando lo que se busca es poder proteger el software, el hardware, las redes, las infraestructuras o los servicios, nos topamos con el ámbito de la seguridad informática o la ciberseguridad. Se incluyen muchas actividades de seguridad que se encuentran relacionadas con la información que manejan todas las personas, el cumplimiento o la concienciación cuando nos estamos refiriendo a la **seguridad de la información**.

Principales diferencias entre ciberseguridad y seguridad de la información

Una vez hemos revisado los conceptos, es posible que se identifiquen todas las diferencias y por lo tanto conocer en el momento en el que se debe aplicar un concepto u otro. En primer lugar, podemos resaltar que la **seguridad de la información** presenta un mayor alcance que la ciberseguridad, ya que la primera quiere proteger la información en cuanto a los diferentes tipos de riesgos a los que se enfrentan, en los distintos estados y formas.

En caso contrario, la ciberseguridad se encuentra enfocada, de forma principal, en la información que se encuentra en formato digital y los sistemas interconectados que la procesan, transmiten o almacena, por lo que tienen una mayor cercanía a la seguridad informática.

La **seguridad de la información** se encuentra sustentada por diferentes metodologías, normas, herramientas, estructuras, técnicas, tecnología y otros elementos, que soportan la idea de proteger las diferentes áreas de la información, además se involucra durante la aplicación y la gestión de las medidas de seguridad apropiadas, mediante un enfoque holístico.

Por lo general, los límites no importan para cada concepto, el principal objetivo es **proteger la información**, de forma independiente de que ésta pertenezca a una empresa tratándose de información personal, ya que nadie se encuentra exento de padecer algún riesgo en seguridad.

Una vez que ya conocemos la definición de cada uno de los términos y el alcance que tienen, podemos utilizarlos en diferentes momentos ya que seguramente podemos seguir aplicando el concepto. Con los avances tecnológicos que se incorporan cada vez más a nuestras vidas cotidianas, la **dependencia de la tecnología** se incrementa, y como consecuencia se genera la necesidad de aplicar la ciberseguridad

Diferencias en las definiciones

- Ciberguerra: Conflicto en el Ciberespacio.
- Ciberdefensa: Conjunto de acciones de defensa activas pasivas, proactivas, preventivas y reactivas para asegurar el uso propio del ciberespacio y negarlo al enemigo o a otras inteligencias en oposición.
- Ciberseguridad: Conjunto de acciones de carácter preventivo que tienen por objeto el asegurar el uso de las redes propia y negarlo a terceros.
- Cibercrimen: Acción criminal en el ciberespacio.
- Ciberterrorismo: Acción terrorista en el ciberespacio.

Definición de Ciberdefensa Ciberdefensa es el conjunto de acciones y/u operaciones activas o pasivas desarrolladas en el ámbito de las redes, sistemas, equipos, enlaces y personal de los recursos informáticos y teleinformáticas de la defensa a fin de asegurar el cumplimiento de las misiones o servicios para los que fueran concebidos a la vez que se impide que fuerzas enemigas los utilicen para cumplir los suyos.

Ciber espacio, definición.

- **Ciberespacio**, es la dimensión generada durante el tiempo de interconexión e interoperabilidad de redes, sistemas, equipos y personal relacionados con los sistemas informáticos cualesquiera sean estos y las telecomunicaciones que los vinculan.

La Inteligencia y la Ciberdefensa.

- Se ha planteado iniciar el proceso de la Ciberdefensa por la Inteligencia Informática con el Ciberespacio como ambiente, para poder obtener los elementos descriptores, que conformen la identificación de los escenarios y a la vez parametrizar las amenazas, para poder dimensionar los riesgos y así posibilitar el diseño de los instrumentos de defensa.

Vigilancia Global

- Todos los países hacen inteligencia.
- Brasil conoce perfectamente los riesgos de su conectividad.
- Todos los sorprendidos son cómplices y conocen de las capacidades que denuncian.
- Costo de los procesos de obtención de información.
- By Pass de redes nacionales
- Planificación de acceso a Big data.
- La Ingeniería Social y las redes sociales.

Caracterización de las Amenazas por el origen El hecho de conectar una red a un entorno externo nos da la posibilidad de que algún atacante pueda entrar en ella, con esto, se puede hacer robo de información o alterar el funcionamiento de la red. Sin embargo el hecho de que la red no esté conectada un entorno externo, como Internet, no nos garantiza la seguridad de la misma. De acuerdo con el Computer Security Institute(CSI) de San Francisco aproximadamente entre el 60 y 80 por ciento de los incidentes de red son causados desde dentro

de la misma. Basado en el origen del ataque podemos decir que existen dos tipos de amenazas:

. Amenazas externas

. Amenazas Internas.

Amenazas internas: Generalmente estas amenazas pueden ser más serias que las externas Los usuarios o personal técnico, conocen la red y saben cómo es su funcionamiento, ubicación de la información, datos de interés, etc. Además, tienen algún nivel de acceso a la red por las mismas necesidades de su trabajo, lo que les permite unos mínimos de movimientos. Los sistemas de prevención de intrusos o IPS, y firewalls son mecanismos no efectivos en amenazas internas por, habitualmente, no estar orientados al tráfico interno.

Amenazas Externas

• Se originan fuera de la red local.

• Al no tener información certera de la red, un atacante tiene que realizar ciertos pasos para poder conocer qué es lo que hay en ella y buscar la manera de atacarla.

• La ventaja que se tiene en este caso es que el administrador de la red puede prevenir una buena parte de los ataques externos.

• Para clasificarlo como externo debe ser exclusivamente por personas ajenas a la red, podría ser por vulnerabilidades que permiten acceder a la red: rosetas, switches o Hubs accesibles, redes inalámbricas desprotegidas, equipos sin vigilancia, etc.

SISTEMA DE INFORMACIÓN Y CLASIFICACIÓN

Según La propuesta por Andreu, Ricart y Valor (1991), en la cual un sistema de información queda definido como: "conjunto formal de procesos que, operando sobre una colección de datos estructurada de acuerdo a las necesidades de la empresa, recopila, elabora y distribuyen selectivamente la información necesaria para la operación de dicha empresa y para las actividades de dirección y control correspondientes, apoyando, al menos en parte, los procesos de toma de decisiones necesarios para desempeñar funciones de negocio de la empresa de acuerdo con su estrategia".

Durante los últimos años los sistemas de información constituyen uno de los principales ámbitos de estudio en el área de organización de empresas. El entorno donde las compañías desarrollan sus actividades se vuelve cada vez más complejo. La creciente globalización, el proceso de internacionalización de la empresa, el incremento de la competencia en los mercados de bienes y servicios, la rapidez en el desarrollo de las tecnologías de información, el aumento de la incertidumbre en el entorno y la reducción de los ciclos de vida de los productos originan que la información se convierta en un elemento clave para la gestión, así como para la supervivencia y crecimiento de la organización empresarial. Si los recursos básicos analizados hasta ahora eran tierra, trabajo y capital, ahora la información aparece como otro insumo fundamental a valorar en las empresas. A la hora de definir un sistema de información existe un amplio abanico de definiciones.

Todo sistema de información va a poseer unos objetivos principales, los cuales se resumen a continuación: apoyar los objetivos y estrategias de la empresa: el sistema de información ha de suministrar a la organización toda la información necesaria para su correcto funcionamiento. La información manejada abarcará desde la actividad rutinaria de la empresa hasta aquella necesaria para el proceso de planificación a largo plazo de la empresa.

- proporcionar información para el control de la totalidad de actividades de la empresa, pudiendo comprobar el cumplimiento de las metas establecidas por la organización. Los sistemas de información abarcan a todos los departamentos de la empresa y a la gestión global de la organización.
- adaptar las necesidades de información a la evolución de la empresa: conforme la empresa va creciendo y desarrollándose, surgen nuevas necesidades de información que han de ser satisfechas por el sistema de información, evolucionando este último adecuándose a las nuevas circunstancias del entorno.
- interactuar con los diferentes agentes de la organización, permitiendo que estos empleen el sistema de información para satisfacer sus necesidades de un modo rápido y eficaz. La interactividad y flexibilidad de los sistemas de información constituyen un punto clave en el éxito o fracaso.

Para la consecución de dichos objetivos, un buen sistema de información ha de ser capaz recibir y procesar los datos del modo más eficaz y sin errores, suministrar los datos en el momento preciso, evaluar la calidad de los datos de entrada, eliminar la información poco útil evitando redundancias, almacenar los datos de modo que estén disponibles cuando el usuario lo crea conveniente, proporcionar seguridad evitando la perdida de información o la intrusión de personal no autorizado o agentes externo a la compañía y generar información de salida útil para los usuarios de sistemas de información, ayudando en el proceso de toma de decisiones.

Tipos de Sistema de Informacion	Tipos
Grado de Confiabilidad	Formales
	Informales
Automatizacion	Manuales
	Informaticos
Relacion con la Toma de decisiones	Estrategicos(Alta Direccion)
	Gerencial(Nivel Intermedio)
	Operativos(Control Operativo)
Funcionalidad	Gestion Comercial
	Gestion Contable
	Gestion Financiera
	Gestion de Recursos Humanos
	Gestion de la Produccion
Grado de Especializacion	Especificos
	Generales
Tabla 1.Tipologia de Sistemas de Informacion(Basado en Garcia Bravo,2000 y Edwars,Ward y Bythesway, 1998)	

Sin embargo, la clasificación más útil es la propuesta por K y J Laudon (1996), en ella los sistemas de Información se agrupan según su utilidad en los diferentes niveles de la organización empresarial. La organización consta de 4 niveles básicos: un nivel operativo referido a las operaciones diarias de la organización, un nivel del conocimiento que afecta a los empleados encargados del manejo de la información (generalmente el departamento de informática), un nivel administrativo (abarcaría a los gerentes intermedios de la organización) y un nivel estratégico (la alta dirección de la empresa).

Según estos niveles, K y J Laudon establecen la siguiente clasificación de sistemas de información:

a) **Sistema de Procesamiento de Operaciones (SPO):** sistemas informáticos encargados de la administración de aquellas operaciones diarias de rutina necesarias en la gestión empresarial (aplicaciones de nóminas, seguimiento de pedidos, auditoría, registro y datos de empleados). Estos sistemas generan información que será utilizada

por el resto de sistemas de información de la compañía siendo empleados por el personal de los niveles inferiores de la organización (Nivel Operativo)

b) **Sistemas de Trabajo del Conocimiento (STC):** aquellos sistemas de información encargados de apoyar a los agentes que manejan información en la creación e integración de nuevos conocimientos para la empresa (estaciones de trabajo para la administración); forman parte del nivel de conocimiento

c) **Sistemas de automatización en la oficina (SAO):** sistemas informáticos empleados para incrementar la productividad de los empleados que manejan la información en los niveles inferiores de la organización (procesador de textos, agendas electrónicas, hojas de cálculo, correo electrónico,); se encuentran encuadrados en el nivel de conocimiento al igual que los Sistemas de Trabajo del Conocimiento

d) **Sistemas de información para la administración (SIA):** sistemas de información a nivel administrativo empleados en el proceso de planificación, control y toma de decisiones proporcionando informes sobre las actividades ordinarias (control de inventarios, presupuestación anua l, análisis de las decisiones de inversión y financiación). Son empleados por la gerencia y directivos de los niveles intermedios de la organización.

e) **Sistemas para el soporte de decisiones (SSD):** sistemas informáticos interactivos que ayudan e los distintos usuarios en el proceso de toma de decisiones, a la hora de utilizar diferentes datos y modelos para la resolución de problemas no estructurados (análisis de costes, análisis de precios y beneficios, análisis de ventas por zona geográfica). Son empleados por la gerencia intermedia de la organización.

f) **Sistemas de Soporte Gerencial (SSG):** sistemas de información a nivel estratégico de la organización diseñados para tomar decisiones estratégicas mediante el empleo de gráficos y comunicaciones avanzadas. Son utilizados por la alta dirección de la

organización con el fin de elaborar la estrategia general de la empresa (planificación de ventas para 4 años, plan de operaciones, planificación de la mano de obra).

Todos esto sistemas de información a su vez podrían analizarse según las diferentes áreas de la empresa: ventas y mercadotecnia, manufactura y producción, finanzas, contabilidad y recursos humanos. Para cada una de estas áreas existe un conjunto especifico de aplicaciones informáticas y equipos, los cuales han de estar coordinados entre sí. Si ello no se realizara, una empresa tendrá problemas de intercambio de datos entre las diferentes áreas, aparecerá la existencia de redundancia de datos y la existencia de ineficiencias e incrementos de costes de comunicación. Por ello resulta clave la correcta planificación y desarrollo de los sistemas de información.

Según Alonso de la Rosa Moreno & Víctor Daniel Rodríguez Viana, (2014), *Estrategia de la Información y Seguridad en el Ciber- espacio,* se afronta, unas veces de forma conjunta y otras describiendo las particularidades específicas en cada país, un repaso en profundidad a algunos temas clave que se pueden articular en:

1. ciberespacio: concepto y ámbito de aplicación en seguridad y defensa,
2. estrategia de seguridad de la información en el ciberespacio.

En lo relacionado con la seguridad en el ciberespacio, se desarrollan en profundidad:

- El análisis y la gestión del riesgo social;
- La gestión de riesgos: infraestructuras críticas, amenazas, vulnerabilidades y las buenas prácticas para el análisis y la gestión de riesgos;
- La seguridad de la información en el ciberespacio y la capacidad de respuesta ante incidentes informáticos;
- Ciberdefensa: capacidades de ciberdefensa, ciber ejército.

Era de la Información

De acuerdo al sociólogo Manuel Castells (1090) el concepto la era de la información es el nombre que se le ha dado el referido autor al período que, aproximadamente, sucede a la era espacial y antecede a la economía del conocimiento y va ligada a las tecnologías de la información y la comunicación. La era de la información es un término aplicado al período en el cual el movimiento de información se volvió más rápido que el movimiento físico.

La dirección de nuestro futuro está marcada en parte por la tecnología y junto a ella por la comunicación. Por ello no es raro ver un monje en el Himalaya con TV LED, o con un IPhone, tampoco ver que en una vereda de un país africano están viendo la última película que estrenó Hollywood, o que un ejecutivo esté dirigiendo una gran multinacional desde la comodidad de su casa de playa, o leyendo las ultimas noticias a la hora que desee, mientras disfruta del confort de su cama, esto solo puede catalogarse como el inicio de la nueva revolución informativa, la cual comienza a dar sus primeros pasos hace 40 años y que cada día camina con mayor rapidez. ¿Podrá el hombre vivir al ritmo de la información?

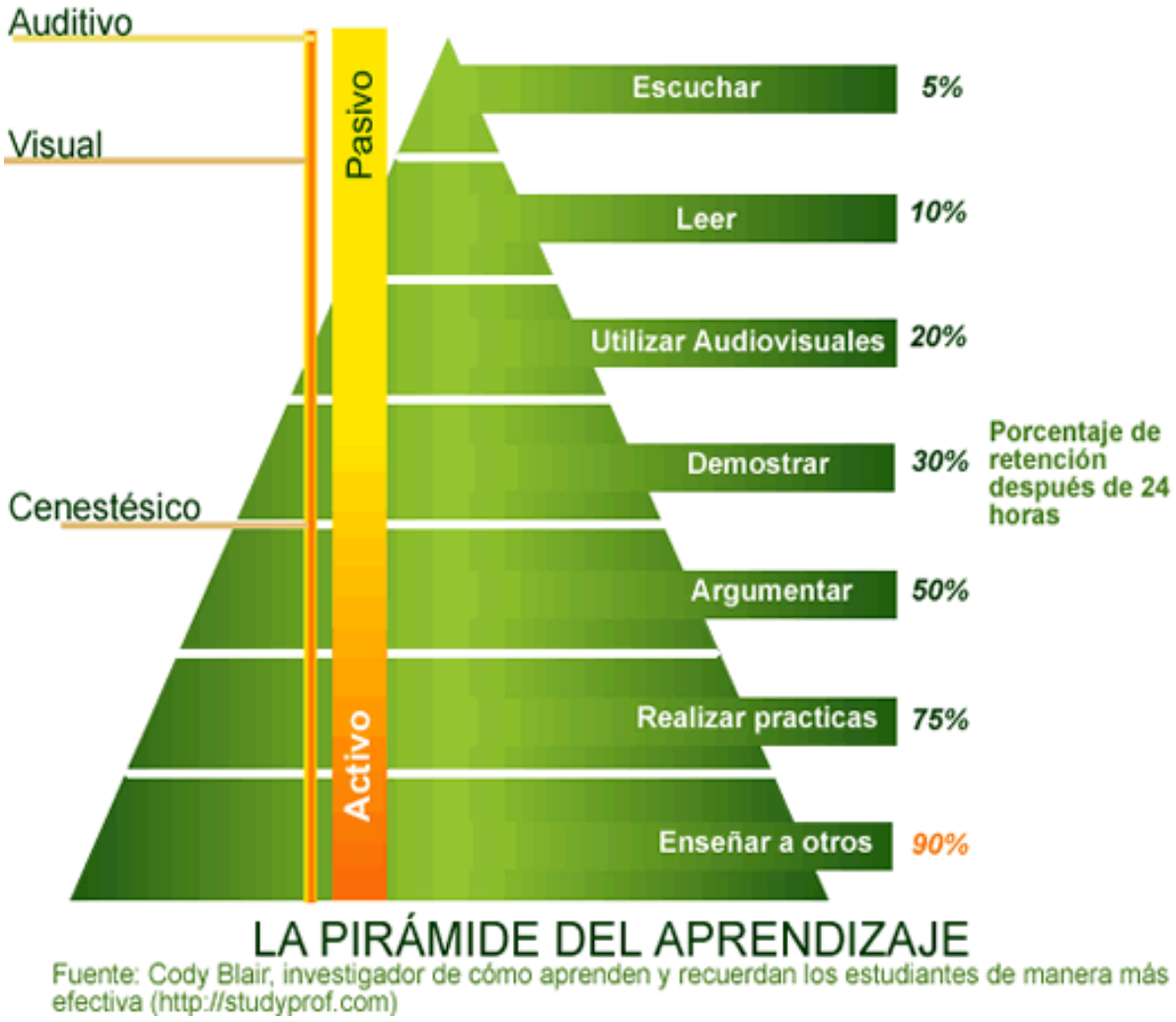


Figura Nº 1. Taxonomía de Bloom era digital

4. MÉTODO

Dimensión espacial y temporal

-Mundo y Perú 2018

Tipo de investigación

La presente investigación es de tipo exploratoria - básico, tecnológica y Humanística **de** aporte teórico cuyo nivel es descriptivo, tendrá una duración de un año (2018) y se realizará en el Perú, la Investigación será Analítica, que nos permitirá descomponer y reconocer todos los elementos concurrentes en esta materia.

Nivel de investigación

a. Investigación descriptiva, por este tipo de investigación se estableció los atributos, características; propiedad o rasgos importantes, de la ciberseguridad de las organizaciones
b. Investigación documental; se utilizó análisis de la información escrita y estadística sobre su naturaleza y funcionalidad.

Materiales

Las fuentes de información que se emplearon fueron libros obtenidos de las bibliotecas de la FIIS, UNI UNMS, Instituciones nacionales autorizada relacionadas con la ciberseguridad. con la finalidad de obtener información de primera mano, las especificaciones se detallan en las referencias bibliográficas. Consideramos también las publicaciones de artículos relacionados con el tema.

Procedimiento

Se acopio información de las fuentes secundarias por cuanto existe familiaridad con la materia en estudio.

Se recogerá datos desde las áreas productivas, que serán para estudio de laboratorio y su debido análisis que estarán cargo a cargo nuestro equipo de apoyo en sus respectivos laboratorios de Universidad. útiles empleando fichas, libretas o cuadernos, grabaciones y filmaciones; extraeremos ideas y comentarios, resumiendo algunas referencias, reproduciendo otras textualmente y sintetizando las que son necesarias. Luego de obtenidos los datos codificados, serán transferidos a una matriz y guardados en un archivo, procederemos a realizar el análisis empleando computadora en los casos necesarios.

De las fuentes complementarias o terciarias haremos el análisis documental de acuerdo a las necesidades del problema y los objetivos planteados. Los materiales y procedimientos elegidos son apropiados inicialmente para investigar los problemas planteados, por su simplicidad y accesibilidad a ellos y poder obtener los resultados acordes con los objetivos propuestos.

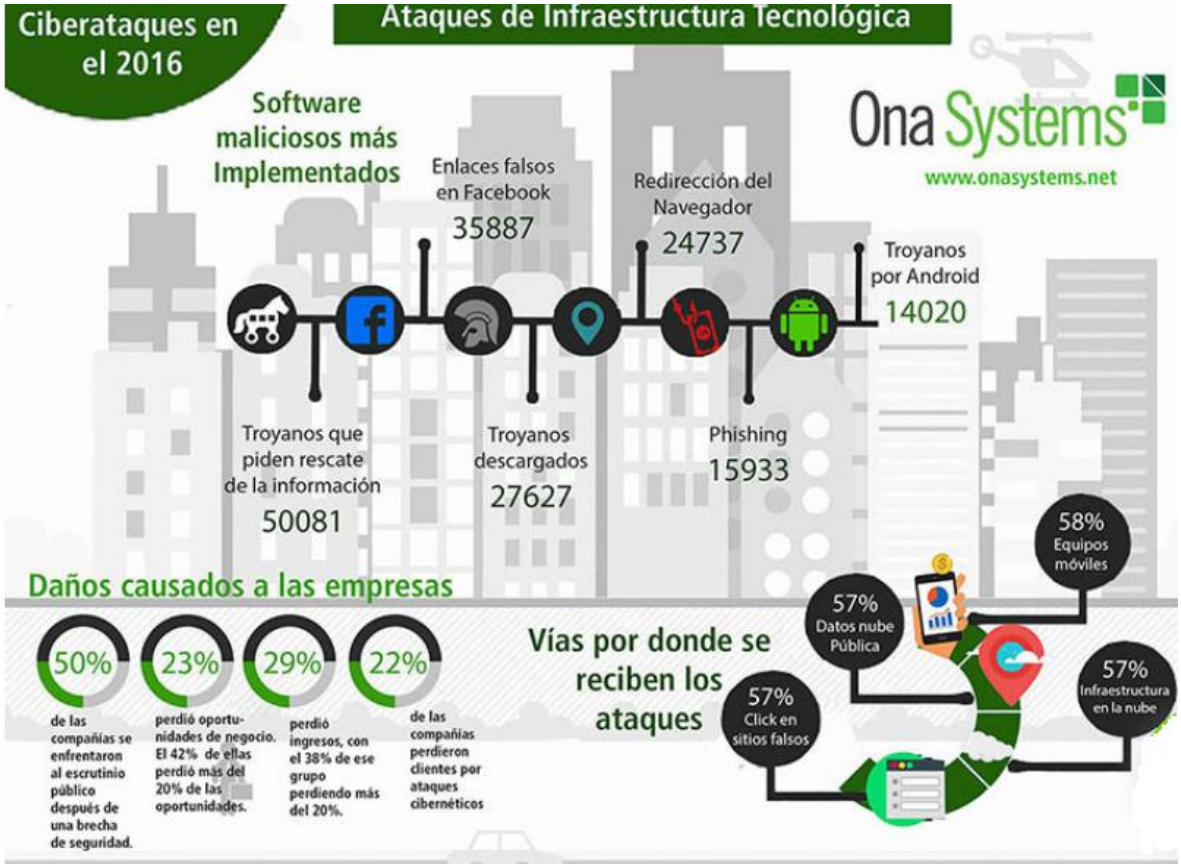
De esta manera podremos llevar a cabo la contribución original del proyecto consistente reducción de la brecha digital.

5. RESULTADOS

De acuerdo al análisis en los diferentes escenarios a nivel interno y externo teórico :

Ciberseguridad

Grafico N° 01: Evidencias de ataque cibernéticos a las Empresas



FUENTE:ONA SYSTEMS https://www.onasystems.net/estadisticas-ciberataques-empresas/

Los ataques a las empresas ya no sólo están relacionados con la perdida de dinero, pueden de cierta manera afectar el prestigio y la reputación de la compañía. (Cisco presentó el reporte anual).

Las empresas están perdiendo oportunidades de ingreso de más del 20%. Muchos Hackers están encontrando la forma más fácil para enviar amenazas. Las ganancias también se vieron comprometidas ya que se registraron pérdidas.

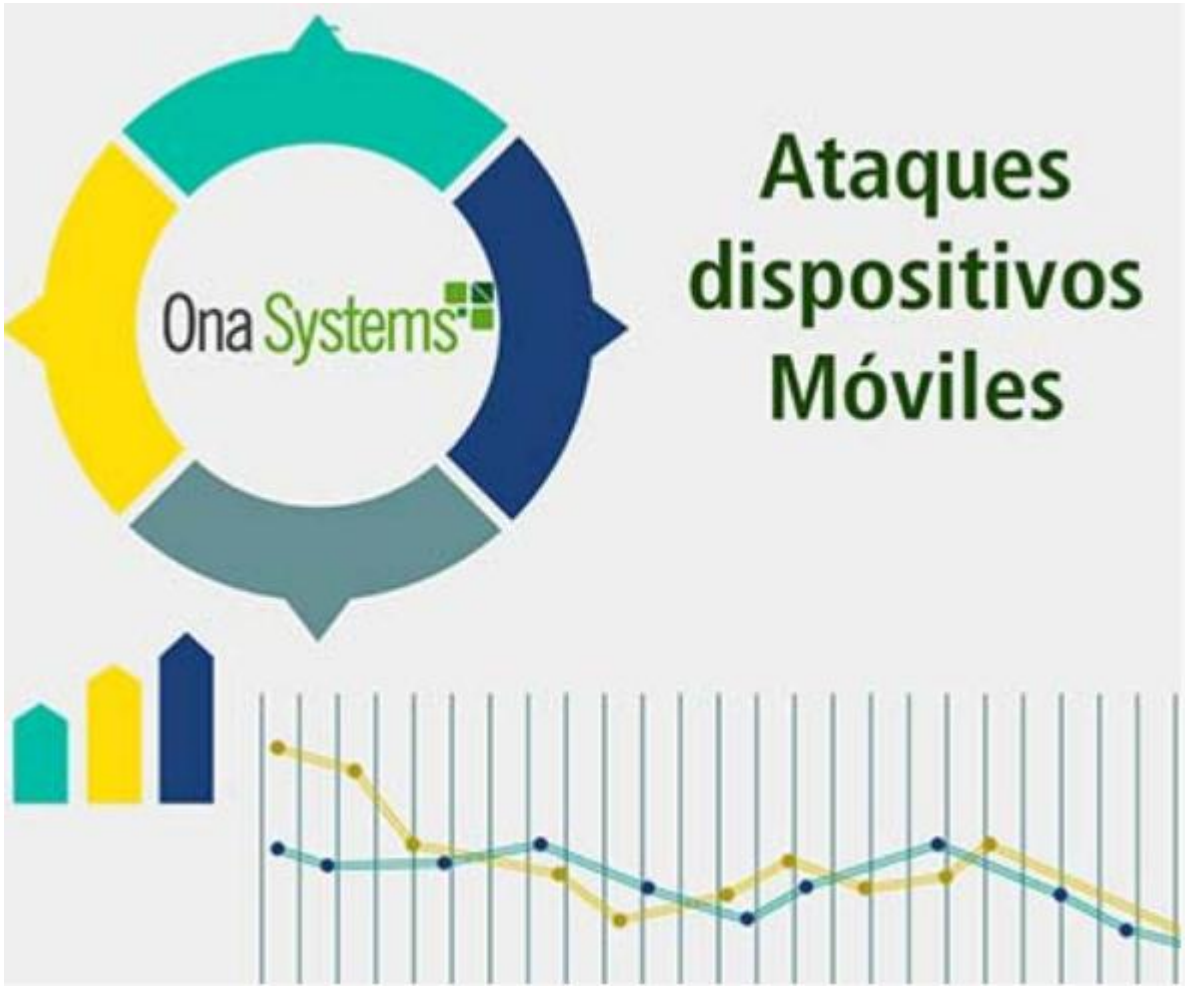
Es muy probable que no se puedan reducir los ataques, pero si se pueden reducir, haciendo un análisis minucioso de todo el sistema informático de una organización.

Dentro del estudio se encontró que el 27% de las aplicaciones en nube de terceros fueron clasificadas como de alto riesgo y crearon problemas de seguridad. Las apps que funcionan en la nube que tienen mayor riesgo de ser infectadas son las que pertenecen al sector financiero, gobierno, educativo (Universidades), manufactura, medios de comunicación y empresas de tecnología.

ATAQUES DISPOSITIVOS MÓVILES

La mitad de los dispositivos móviles en el mundo están en riesgo contra posibles ataques y malware. Muy pocas empresas intentan proteger sus dispositivos móviles. En los últimos años el uso de smartphones ha aumentado un 39% y el de tabletas un 17%. A la luz de estos datos, no es extrañar que los ataques a terminales móviles sigan creciendo.

Gráfico N° 02: Ataques a dispositivos Móviles



FUENTE:ONA SYSTEMS https://www.onasystems.net/estadisticas-ciberataques-empresas/

Internet de las cosas

Los ataques a dispositivos conectados a internet son cada vez más importantes. El peligro es tan grande que pueden dejar desconectado a millones de dispositivos. El gran problema de muchos fabricantes es que no tiene la seguridad entre sus prioridades.

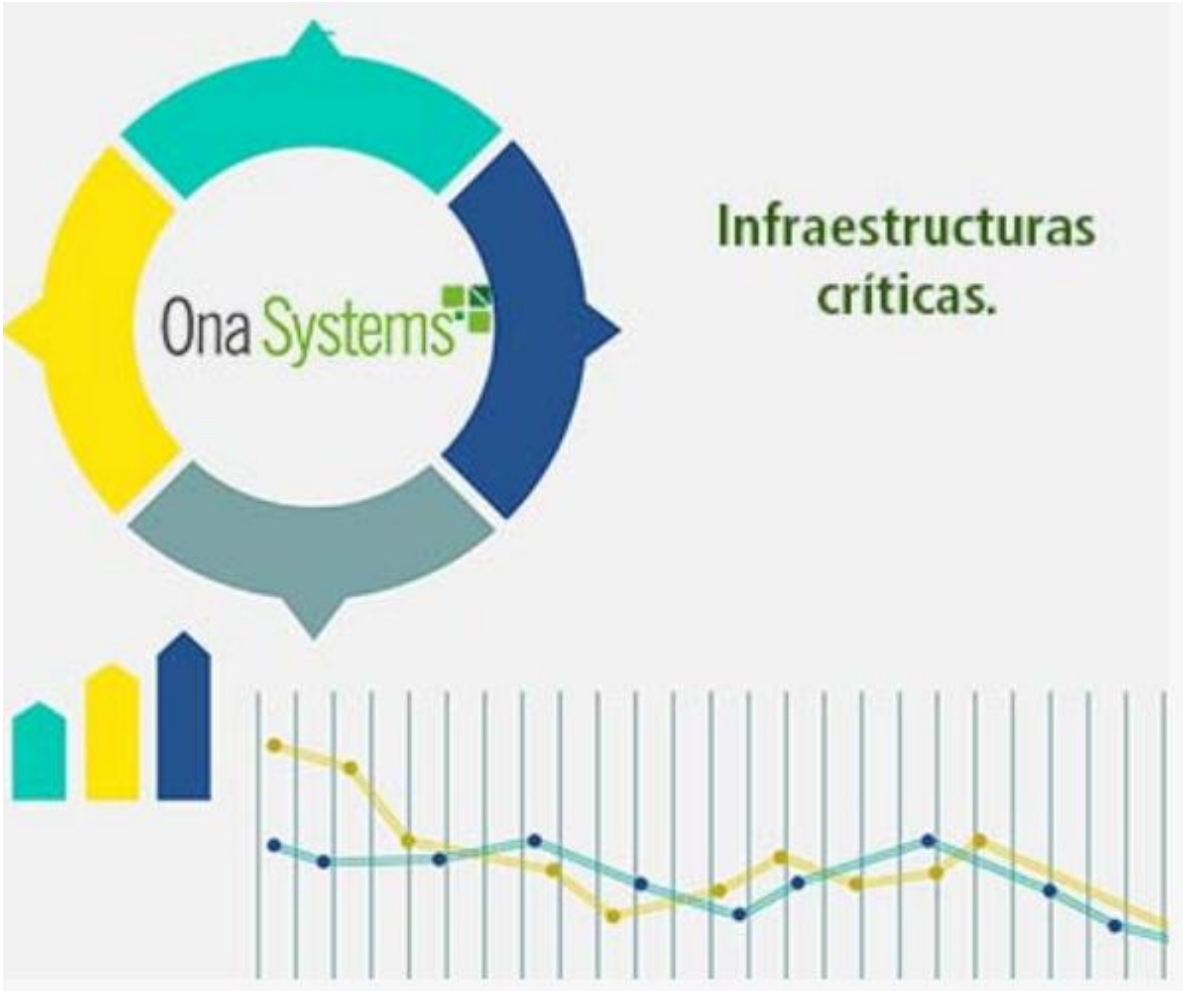
Gráfico N°03: Internet de las cosas

FUENTE:ONA SYSTEMS https://www.onasystems.net/estadisticas-ciberataques-empresas/

Infraestructuras Críticas

Los ataques se dirigirán a sectores como energía, el agua, el sistema financiero o la alimentación. Sectores que al poder fallar generan caos. A comienzos de 2016, de hecho, se desveló el primer apagón causado por ciberdelincuentes.

Gráfico N° 05: Infraestructuras Críticas



FUENTE:ONA SYSTEMS https://www.onasystems.net/estadisticas-ciberataques-empresas/

Vulnerabilidad e n la Nube

Muchas de las empresas están manejando a través de la nube, al hacer eso utilizan arquitecturas hibridas que pueden crear puertas traseras con lo que los hackers tienen acceso a los sistemas de la empresa. Garthner predice en muy pocos años el 71% de las de los servicios virtuales estarán en la nube.

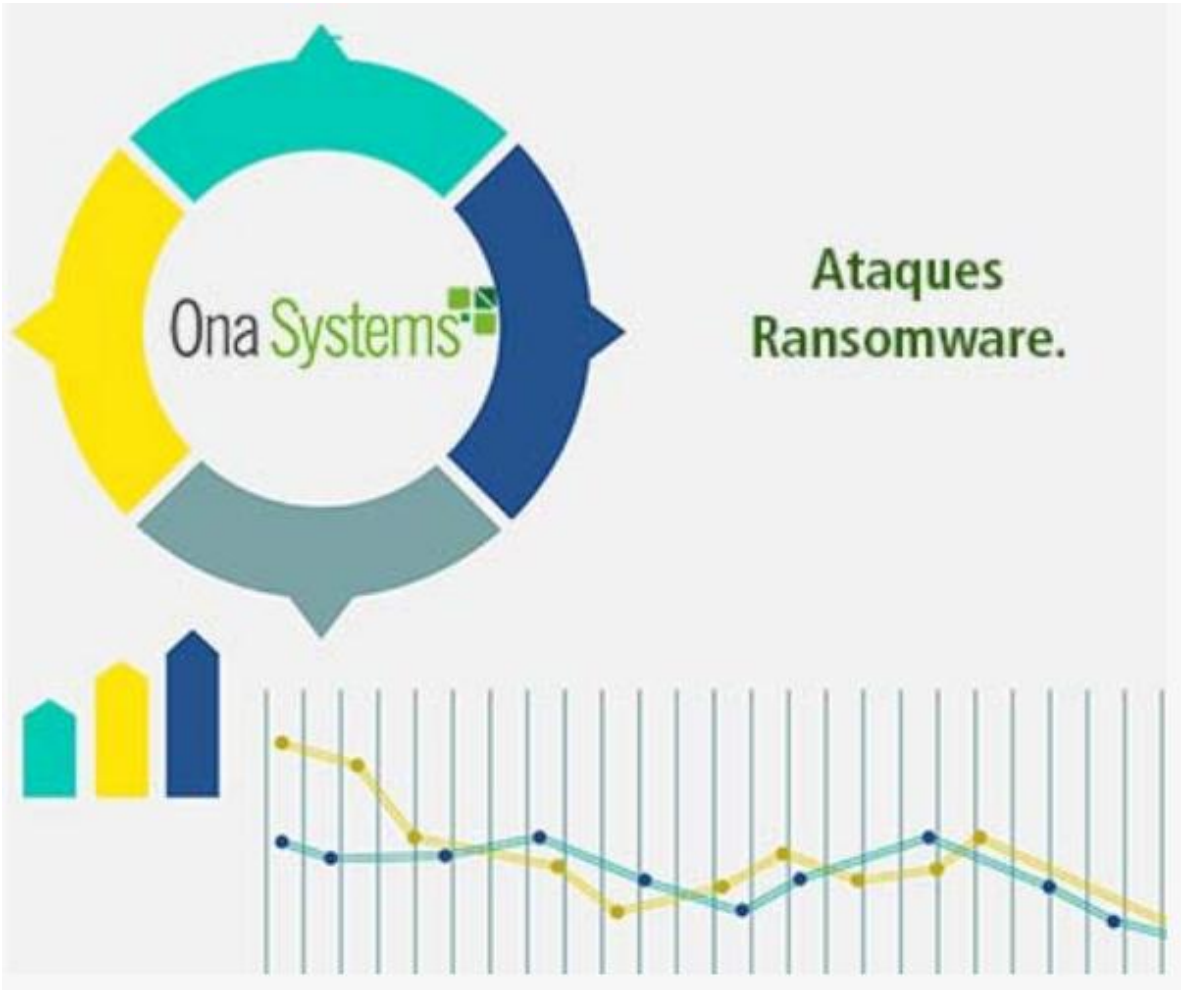
Gráfico N° 06

FUENTE:ONA SYSTEMS https://www.onasystems.net/estadisticas-ciberataques-empresas/

Ransomware

Cuantas mas empresas se pasen a cloud más ataques se dirigirán a sus infraestructuras emergentes.

El ransomware es uno de los métodos de ataque mas comunes y efectivos de hoy en día y esta tendencia según las presiones no va a cambiar.



FUENTE:ONA SYSTEMS https://www.onasystems.net/estadisticas-ciberataques-empresas/

Era digital

Según Ponte Geek(jueves 15 ,2018), la ciberseguridad, indispensable en la era digital

La conversión digital o digitalización en transacciones, datos e información de las empresas, ha generado una nueva modalidad en la operación diaria: la Seguridad Cibernética o ciberseguridad.

Cuando una empresa crece, se va enfrentando a nuevos retos y desafíos, entre ellos, un ciberataque. Esto ha dado lugar a que la ciberseguridad sea un tema fundamental, en especial

porque los ataques son cada vez más sofisticados, precisos y dañinos. Un software malicioso puede ocasionar retrasos operativos de vulnerabilidad de seguridad o una violación a los datos personales, como ha ocurrido **con el ransomware, que tuvo un crecimiento de más del 60% el año pasado.**

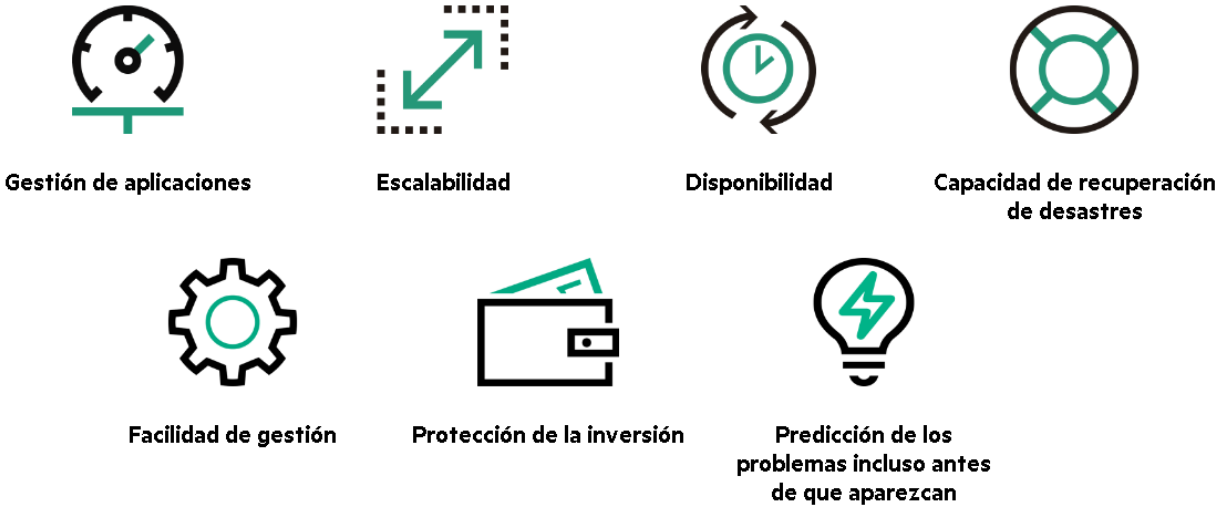
El 40% de los directivos y responsables de IT entrevistados en la Encuesta Mundial sobre el Estado de la Seguridad de la Información 2018, dice no tener una estrategia general de seguridad de la información. Además, el 48% no cuenta con un programa de capacitación en concientización sobre seguridad para sus empleados, y el 54% asegura que no tiene un proceso de respuesta a incidentes. Esto, sumado a que solo el 39% de los encuestados dice tener mucha confianza en su capacidad de manejo de ciberataques.

Esto significa que, así como los bancos necesitan seguridad física (personal de seguridad), la información alojada en la nube y en centros de datos, también requiere de protección por el valor que representa para cada organización o persona que la posee. Entre más valores y activos almacena una empresa de forma digital, mayores serán los requerimientos de seguridad de información y lo especializados que sean, tanto para sus clientes, como para la organización misma. Las nuevas tecnologías como el IoT (Internet de las Cosas), también repercuten en las inversiones de seguridad, con una tendencia hacia un mayor consumo de soluciones como servicio, ya que según la IDC se calcula que para el 2020 se alcancen los 600 millones de cosas conectadas

Inteligencia artificial para el almacenamiento empresarial

La tecnología flash ha evolucionado de forma imparable y ha logrado que empresas de todos los tamaños aprovechen de una manera más eficaz la tecnología disponible acelerando el acceso al dato de forma inmediata y reduciendo el tiempo de gestión.

En HPE e Intel® apostamos por la Inteligencia Artificial y hemos creado una hoja de ruta en la que te ayudamos a enfrentarte a los principales retos.



La IA y el análisis predictivo se ponen a tu servicio yendo un paso más allá. A través de la tecnología InfoSight y gracias a su aprendizaje automático, HPE Nimble Storage y 3PAR optimizados para discos flash y con procesadores escalables Intel® Xeon® ayudan a predecir y evitar los problemas en toda la infraestructura y garantiza la disponibilidad y un uso eficiente de los recursos permitiendo tener una infraestructura o data center prácticamente autónomo.


79% de reducción
en los gastos operativos de TI
85% de reducción
de tiempos de gestión
86% de reducción
de problemas de la
infraestructura
99.9999% de
disponibilidad
de los datos

6. DISCUSIÓN

Según almomento.net, santo domingo, República Dominicana (23 agosto, 2018). – Cuando una empresa crece, se va enfrentando a nuevos retos y desafíos, entre ellos, un ciberataque. Un software malicioso puede ocasionar retrasos operativos de vulnerabilidad de seguridad o una violación a los datos personales, como ha ocurrido con el ransomware, que tuvo un crecimiento de más del 60% el año pasado.

Cuando más empresas se pasen a cloud, más ataques se dirigirán a sus infraestructuras emergentes. El ransomware es uno de los métodos de ataque más comunes y efectivos de hoy en día y esta tendencia según las previsiones no va a cambiar.

De acuerdo a los resultados de ONA SYSTEMS los ataques a las empresas ya no solo están relacionados con la pérdida de dinero, pueden de cierta manera afectar el prestigio y la reputación de la compañía. (Cisco presento el reporte anual). Ataques a dispositivos móviles. La mitad de los dispositivos móviles en el mundo están en riesgo contra posibles ataques y malware. Muy pocas empresas intentan proteger sus dispositivos móviles. En los últimos años el uso smartphones ha aumentado un 39% y el de tableta un 17%. A la luz de estos hechos datos no de extrañar que los ataques a terminales móviles sigan creciendo.

Las empresas están perdiendo oportunidades de ingreso de más del 20%. Muchos Hackers están encontrando la forma más fácil para enviar amenazas. Las ganancias también se vieron comprometidas ya que se registraron pérdidas.

Según Altran | (Sep 5, 2018), El papel de la ciberseguridad en la transformación digital Cuando oímos hablar de Transformación Digital pensamos en la oportunidad de innovar y en la posibilidad de hacer crecer nuestra organización en un nuevo entorno, pero en este proceso la seguridad tiene un importante peso y se ha de tener en cuenta si no se quiere fracasar en el intento**.**

7. CONCLUSIONES

1. La ciberseguridad tiene un efecto positivo en la mejora la actividad organizacional respecto de la planificación y la aplicación en la era digital. De acuerdo a los resultados se puede ver que genera un 79% de reducción de los gastos operativos.

2. la ciberseguridad mejora la planificación de la actividad organizacional en la era digital, con un 85% de reducción de tiempos de operación, asimismo, con una disponibilidad del 99% de disponibilidad de datos.
3. La Ciberseguridad mejora la aplicación de la actividad organizacional en la era digital. Con 86% de reducción de problemas de infraestructura.

8. RECOMENDACIONES

1. Mantenimiento y mejora del sistema de ciberseguridad, pare evitar y minimizar los niveles de riesgo que se traducen en costos operativos.

2. Mantener la planificación del sistema de ciberseguridad, para lograr los objetivos de eficiencia d y efectividad del uso del tiempo; asimismo, las bases de datos necesarias para la organización.

3. En la era digital, para el control del software y hardware no se necesita una alta inversión en infraestructura, dado que se puede administrar vía remota y arquitectura virtual.

4. Implementación de sistemas de ciberseguridad en las organizaciones y en especial en la Universidad, creando un área específica para dar soporte y brindar el servicio en línea de tiempo.

9. REFERENCIAS BIBLIOGRÁFICAS

- *Isaca (*Information Systems Audit and Control Association – Asociación de Auditoría y Control sobre los Sistemas de Información),
- *Salas, A. Los hombres que susurran a las maquinas, Madrid, Espasa Libros, 2015. ISBN: 9788467046212.*
- *Castells,M. (1997).* La era de la información. Economía, sociedad y cultura. *Vol. I:* La sociedad red. *Traducción de Carmen Martínez Gimeno y Jesús Alborés. Madrid: Alianza.*
- *Castells, M. (2002).* La era de la información. Economía, sociedad y cultura. *Vol. II:* El poder de la identidad. *Traducción de Carmen Martínez Gimeno y Jesús Alborés. Madrid: Alianza.*
- *Castells, M. (2005).* La era de la información. Economía, sociedad y cultura. *Vol. III:* Fin de milenio. *Traducción de Carmen Martínez Gimeno y Jesús Alborés. Madrid: Alianza.*
- *Castells, M. (ed.) (2006).* La sociedad red: una visión global. *Madrid: Alianza.*
- *Celaya, Javier (2010).* Sociedad digital. *Madrid: Aguilar.*
- *Cordón, J. (2003).* La edición electrónica en el contexto de los estudios sobre edición contemporánea en España.

http://www.eoi.es/blogs/ciberseguridad/
http://nae.es/la-seguridad-digital-amenazas-y-soluciones/

https://pontegeekpty.com/la-ciberseguridad/