Decanato de Ingenierías e Informática

Escuela de Informática

Curso Monográfico

Trabajo de grado para optar por el título de:

INGENIERO(A) DE SOFTWARE

TEMA:

Controles de Ciberseguridad del servicio de Internet en centros comerciales de un aeropuerto.

Estudiantes:

César Vidal González Ferreras	**2015-1627**
Josue Reyes Matos	**2015-1523**
Ronald Antonio Rodriguez Asencio	**2013-2636**

Asesor:

Willy Alfredo Padua Ruiz

Santo Domingo, D. N.

2020

Controles de Ciberseguridad del servicio de Internet en centros comerciales de un aeropuerto

Dedicatoria

Dedico este trabajo principalmente a mi padre, Dr. César Gonzalez, por haberme apoyado en cada uno de mis pasos. Le agradezco por todo el esfuerzo y trabajo que pasó para criarnos a mi, mis hermanas, aun después de la pérdida de nuestra madre, Juana Ferrera. Sé que él está orgulloso de nosotros y ella también lo estaría.

-César Vidal González F.

Dedicatoria

Le dedico este trabajo a toda mi familia, ya que gracias a su apoyo incondicional durante toda mi vida, he podido obtener el impulso necesario para lograr superar cualquier barrera u obstáculo presente en mi camino, en especial a mi madre por estar presente en todos mis logros. También a todos mis amigos y colegas de Universidad que tuve el placer de conocer a lo largo de este gran reto formativo hacia el profesionalismo.

-Josue Reyes

Dedicatoria

Dedico este trabajo a mi padre y a mi madre, que con su apoyo incondicional me motivan siempre a alcanzar mis metas y desarrollarme tanto en el ámbito profesional como personal. A mis compañeros y maestros que han aportado a mi crecimiento durante este trayecto.

-Ronald Rodriguez

Agradecimiento

Quiero dar gracias a toda mi familia por todo el amor incondicional y compañía que me han dado. A mi hermana Katherine González, por estar siempre ahí conmigo aunque no siempre nos llevemos de lo mejor. A mi hermana Mariel González, por ser un gran modelo a seguir y siempre estar disponible para ayudarme y aconsejarme junto con mi cuñado Julian Henao. A mi hermanastro y mi madrastra Enmanuel y Jaquelin Lee que siempre me han apoyado.Y a mi tío Felipe Guerrero, que se esforzó muchísimo, y pasó por muchos dolores de cabeza ayudándonos a conseguir la información que necesitábamos para este trabajo.

Quiero también agradecer a mis compañeros Carlo Cespedes, Pedro Lebron y Marielena Valdez que me acompañaron en este camino aunque no todos terminamos en la misma salida. Y principalmente quiero agradecer a Josue Reyes, mi compañero y camarada en tantas de nuestras materias, incluyendo este trabajo, se que sin su compañía, liderazgo, y dirección este hubiera sido un camino mucho más difícil.

-César González

Agradecimiento

En primer lugar quiero agradecer a mis abuelos maternos, Aristóteles Matos Herasme y Guarina Morillo Ortega, quienes siempre me orientaron a nivel profesional y estuvieron dispuestos a ayudarme ante cualquier necesidad a lo largo de mi formación profesional. De igual manera, agradezco a mi padrino, Salvador Ramirez, quien con sus conocimientos y apoyo me guió a través de mi formación educativa, incentivando en mi el hábito de la curiosidad y de la lectura.

También quiero agradecer a la universidad APEC por brindarme todos los recursos y herramientas que fueron necesarios para llevar a cabo el proceso de investigación. No hubiésemos podido conseguir estos resultados de no haber sido por su incondicional ayuda.

Por último, quiero agradecer a todos mis compañeros y a mi familia, por apoyarme aún en momentos de incertidumbre. En especial, quiero hacer mención de mi madre, Loyda Matos Morillo, que siempre estuvo presente para darme palabras de apoyo y un abrazo reconfortante para renovar energías.

-Josue Reyes

Agradecimiento

Quiero agradecer a mi madre, Maria Asencio y a mi padre Ramon Antonio Rodriguez, quienes son siempre mi principal fuente de motivación en todo propósito que tengo en la vida, gracias a su orientación siempre me facilitan el camino, y este es uno más de ellos.

De igual forma agradecer a todos los maestros que a lo largo de mi carrera me han apoyado y han aportado a mi crecimiento personal agregando sus conocimientos.

También a la universidad Apec por brindar siempre su ayuda en todos los procesos académicos que tuve, como también esta investigación.

-Ronald Rodriguez

Índice de contenido

Índice de figuras

Índice de tablas

Introducción

En la sociedad moderna, el internet tiene un papel predominante en la ejecución de un sinnúmero de procesos cotidianos que van desde las localidades domésticas hasta las grandes corporaciones multinacionales. El uso de este ha traído numerosas ventajas que van desde el simple acceso a la información en línea hasta la adquisición de cualquier tipo de bien sean materiales o intelectuales. Dichas ventajas y nivel de presencia han hecho de esta herramienta un elemento vital en el día a día de los ciudadanos de República Dominicana y un ejemplo notable de esto son los centros comerciales, los cuales han evolucionado para brindar la mejor experiencia de usuario posible gracias a esta tecnología.

A pesar de todas estas ventajas y facilidades que brinda el internet a los centros comerciales y demás áreas públicas, también se tiene que tomar en cuenta que esto trae consigo sus factores de riesgo. según Juanes (2016):

> *Este tipo de instalaciones destinadas a reunir a un gran número de personas debe tener en cuenta los aspectos relacionados con la seguridad, desde el mismo momento en el que se proyecta el edificio junto a todos los aspectos relacionados con los planes de emergencia y*

evacuación, el aforo, las facilidades en los accesos, etc. Criterios iniciales que deben complementarse posteriormente con otra serie de elementos de seguridad imprescindibles para garantizar una completa protección, tanto de los usuarios como de los propios comercios. (p.1)

Esto hace evidente que el enfoque de seguridad para este tipo de espacios públicos tiene que tener una integración uniforme entre los aspectos físicos y virtuales para salvaguardar de manera efectiva las propiedades de no solo de los clientes de la plaza sino que también de los mismos comercios dentro de sus locales. Es por esta misma razón por la cual a la hora de hablar de ciberseguridad para este tipo de espacios se habla de soluciones *VSaaS*[1] , las cuales son respuestas fundamentales ante este tipo de necesidades, pero que han presentado inconvenientes de seguridad en los últimos años.

Otro aspecto de seguridad que se toma en cuenta de parte de los clientes, es su vulnerabilidad al conectarse a puntos de acceso de red inalámbrica (wi-fi) que pueden aparecer como públicos, pero que pueden ser generados por personas o entidades con intenciones maliciosas.

"....el Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (Dicat) ha plasmado que durante los últimos cinco años estos casos han aumentado. 'Por lo que, podemos decir, que la mayoría de los espacios públicos carecen de controles de seguridad tecnológica y se deben tomar medidas para contrarrestar dicha situación'."
(Rivas,2018, p.1)

[1] ***VSaaS**: inglés para "video vigilancia como servicio" (video surveillance as a service). no es más que la gestión remota de sistemas de videovigilancia a través de la nube.*

1

En evidencia de todos los puntos anteriores, se tiene la siguiente hipótesis:

Para la creación de un ambiente de seguridad cibernética estable y confiable para los clientes tanto comerciales como empresariales de espacios públicos de República Dominicana, se ve necesaria **la creación de un marco de ciberseguridad** que contenga los controles necesarios para manejar, contener y/o disipar los ataques o posibles inconvenientes relacionados a la protección de datos en las áreas de acceso público (dígase plazas,centros comerciales y aeropuertos) dentro de todo el territorio del distrito nacional.

Capítulo 1

Elementos preambulares de la investigación

1.1 - Elección del título de la investigación

Controles de Ciberseguridad del servicio de Internet en centros comerciales de un aeropuerto

- **OBJETO DE ESTUDIO**: La ciberseguridad en el ámbito civil o público
- **MODELO O INSTRUMENTO**: Controles de Ciberseguridad del servicio de Internet en centros comerciales de un aeropuerto.
- **CAMPO DE ACCIÓN:** Plazas, centros comerciales y aeropuertos

1.2 - Planteamiento del problema o foco de la investigación

El internet tiene un papel importante en la vida de las personas, sean esta de cualquier edad o grupo social. Un ejemplo notable de esto son los centros comerciales, los cuales han evolucionado para brindar la mejor experiencia de usuario posible gracias a esta tecnología. A pesar de todas estas ventajas y facilidades, también se tiene que tomar en cuenta que esto trae consigo riesgo de ciberseguridad. El enfoque de seguridad para este tipo de espacios públicos tiene que tener una integración uniforme entre los aspectos físicos y virtuales para salvaguardar de manera efectiva las propiedades de no solo de los clientes de la plaza sino que también de los mismos comercios dentro de sus locales.

Otro aspecto de seguridad que se toma en cuenta de parte de los clientes de estas localidades, es su vulnerabilidad al conectarse a puntos de acceso de red inalámbrica (wi-fi) que pueden aprovecharse para ataques maliciosos a gran escala. Por tanto para la creación de un ambiente de seguridad cibernética estable y confiable para los clientes tanto comerciales como empresariales de espacios públicos de República Dominicana, se ve necesaria la creación de un

marco de ciberseguridad que contenga los controles necesarios para manejar, contener y/o disipar los ataques o posibles inconvenientes relacionados a la protección de datos en las áreas de acceso público (dígase plazas,centros comerciales y aeropuertos) dentro de todo el territorio del distrito nacional.

1.3 - Objetivos de la investigación.

1.3.1 - Objetivo General

Diseñar un marco de controles para la ciberseguridad de las plazas y aeropuertos de República Dominicana, que permita mitigar los incidentes y/o fraudes cibernéticos mediante el uso de los servicios de Internet público.

1.3.2 - Objetivos específicos

1. **Analizar** la situación actual derivada de los incidentes y fraudes cibernéticos recurrentes en las plazas, centro comerciales y aeropuertos de la República Dominicana.
2. **Proponer** el diseño de un marco o guía de controles para mejorar la ciberseguridad de las plazas, centros comerciales y aeropuertos de República Dominicana.
3. **Evaluar** el impacto de las implementaciones del marco de controles de Ciberseguridad en las plazas, centros comerciales y aeropuertos de República Dominicana.

1.4 - Justificaciones

1.4.1 - Justificación Teórica

Mediante este trabajo de investigación se propone analizar y medir la cantidad de ataques cibernéticos que ocurren dentro del territorio de República Dominicana , especialmente enfocado en las localidades de acceso público más concurridas (centros comerciales, plazas y aeropuertos). Esto tomando en cuenta la proliferación de las redes WIFI en espacios públicos y el uso masivo que se le da a estas por parte de los ciudadanos dominicanos.También se toma en cuenta el crecimiento exponencial que posee este elemento a nivel global, ya que según según estudios realizados por cisco (2019):

“El papel y la cobertura de WiFi continuarán expandiéndose, y el tráfico de WiFi representará el 50% del tráfico IP total para 2022. Mientras tanto, el número de puntos de acceso WiFi públicos se multiplicará por cuatro a nivel mundial, de 124 millones (2017) a 549 millones. (2022) en un lapso de cinco años”.(p.3)

Se entiende que dentro de este proceso de crecimiento acelerado de las redes públicas, también se ascienden los focos de riesgo que presentan sus usuarios en relación a hurto de información privada, fraudes monetarios cibernéticos, suplantación de identidad, etc.

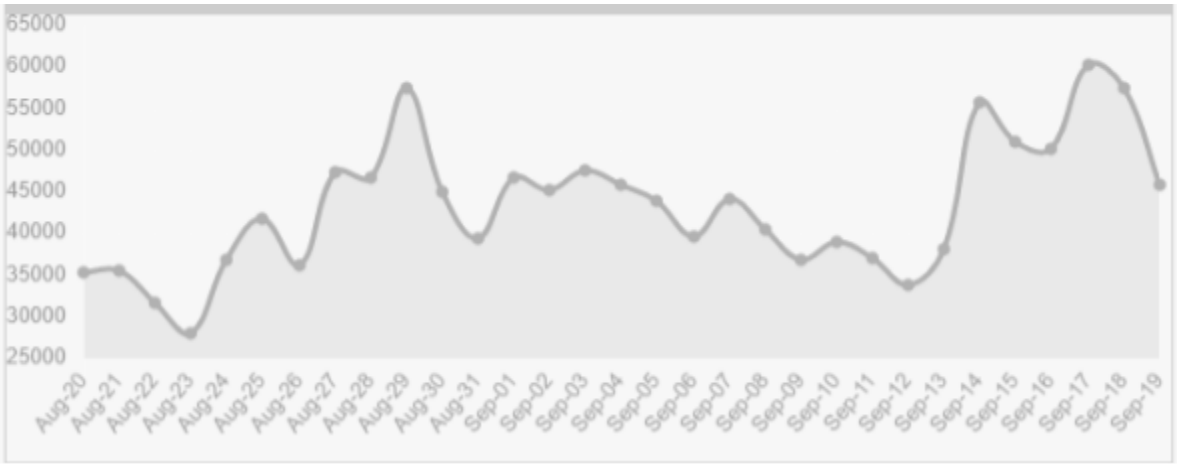


Figura 1.1: Gráfico de ciberataques en República Dominicana.
Fuente: (Kaspersky, 2020)

Según las estadísticas levantadas por el mapa de ciberamenazas de Kaspersky[2], tan solo en el transcurso de tiempo entre el 20 de agosto al 19 de septiembre se registraron de 30,000 a 60,000 amenazas por dia solo en cuestion de ataques de red en República Dominicana.

Esto clarifica que las amenazas cibernéticas tienen alta presencia en el país y se pueden categorizar como un problema en aumento que puede afectar a gran cantidad de personas dentro de la sociedad dominicana. Por esta misma razón se entiende que las zonas donde estos ataques pueden darse a lugar son las zonas más concurridas para los dominicanos: las zonas de centros comerciales y aeropuertos.

"No existen leyes o normas que atiendan la problemática de manera integral. Cabe destacar que la Ley No. 53-07 ha sido un paso de avance respecto al anterior estado de cosas existente en República Dominicana en la materia y también lo ha sido la Estrategia Nacional de Ciberseguridad. Sin embargo,

[2] ***Kaspersky****: es una compañía dedicada a la seguridad informática con reputación a nivel global. (tiene presencia en aproximadamente 195 países del mundo).*

conforme avanza la tecnología, se presentan nuevas maneras de delinquir en el ciberespacio." (Gonzalez, 2019)

La protección de las leyes dominicanas en si no se consideran suficientes como para abarcar la gran variedad de tipos de ataque existentes en internet en la actualidad, ya que estos se encuentran en constante evolución y resulta de gran complicación para predecir.

1.4.2 - Justificación metodológica

Este trabajo tiene como finalidad realizar un proceso de evaluación y análisis de las amenazas, vulnerabilidades y riesgos que se presentan en redes wi-fi públicas en Centro comerciales y aeropuertos para presentar nuestras recomendaciones en forma de un marco de guis para tratar apropiadamente estos elementos.

"Los programas de ciberseguridad más exitosos son aquellos que no se basan simplemente en la aplicación de controles técnicos, sino que definen una estrategia, un marco, para abordar cada una de las funciones esenciales de ciberseguridad." (Almagro, 2019)

1.4.3 - Justificación práctica

Este trabajo de investigación propone la mejora de procesos de ciberseguridad utilizados actualmente en centros comerciales y aeropuertos de la República Dominicana. Dado el gran incremento de usuarios que se conectan a redes públicas en estos espacios, la cantidad de datos que están siendo usados representa un problema cuando el acceso a estos no están debidamente protegidos.

Al ser explotadas las vulnerabilidades en estas redes se puede presentar robo de información personal y clasificada, tanto para usuarios como para compañías que ofrezcan este servicio en las plazas, presentando así una pérdida económica.

En España, para mitigar esta pérdida se ha implantado la GDPR, Que es la General Data Protection Regulation de la unión europea, donde se plantea en primer lugar identificar e inventariar toda la información manejada por la empresa que se encuentra afectada por la ley, esto es, información de carácter personal y que pueda identificar al propietario de la misma.

En segundo lugar, se tiene que identificar a qué nos obliga la ley respecto a esta información, utilizando servicios como el eIDAS(electronic identification, Authentication and trust Services), estas medidas están siendo auditadas para su complumiento.

“Los ciberdelincuentes robaron 1.750 millones en España en 2017, el informe mundial norton cyber security insights, Cada afectado español perdió una media de 65,53 euros y 22 horas de trabajo a consecuencia de los ciberataques. Cerca de un 30% de estos en redes públicas de plazas comerciales”.

-Informe mundial norton cyber security insights 2017

1.5 - Aspectos Metodológicos

1.5.1 - Tipo de investigación

La investigación será de tipo **descriptiva** ya que consta con un análisis de las dr en detalle, los eventos físicos y lógicos encontrados en el área de estudio. Esto, con el propósito de medir las vulnerabilidades, riesgos y amenazas de una infraestructura tecnológica y describir una solución en forma de marco o guías relacionados que responda dichos elementos.

1.5.2 - Métodos

La investigación utilizara el **método Inductivo**, basado en la conclusión a partir de de hechos. Debido a que la técnica principal de recopilación será la observación mediante la cual se realizará las conclusiones y recomendaciones relacionadas a la seguridad de las redes de internet carácter público.

También se tendrá como apoyo el método de análisis, que permitirá descomponer la problemática que se está investigando lográndose identificar cada elemento que esta contiene y la relación causal de los mismo y así de esta forma lograr plantear una solución que cumpla con los requisitos presentados sobre problema propuesto.

1.5.3 - Fuentes y Técnicas

Las fuentes de información son principalmente secundarias y externas. Entre estas se encuentran libros y artículos que describen conceptual y prácticamente normas, la utilización de métricas, mejores prácticas de seguridad; estadísticas recopiladas y presentadas por terceros y trabajos de investigación relevantes al área de estudio. También se utilizan algunas fuentes primarias como son las normativas ISO e IEEE relacionadas a la seguridad de redes y seguridad de la información.

Capítulo 2

La tecnología WIFI y sus factores de ciberseguridad en plazas, centros comerciales y aeropuertos.

2.1 - Funcionamiento del internet en los espacios públicos.

2.1.1 - Estructuración de las redes inalámbricas públicas

Se le denomina red inalámbrica a toda conexión inter computacional de carácter nodal que se realice por medio de ondas electromagnéticas y en la cual no se emplea el uso de cableado. Este tipo de conexiones puede dividirse de dos formas:

- **Según el alcance:**
  - WPAN*(Wireless Personal Area Network*).Se traduce al español como red inalámbrica de área personal y como su nombre lo indica, esta se usa con fines de uso individual y como máximo se tienen solo dos usuarios . Este tipo de conexiones tiene un rango de 10 metros.

  - WLAN(*Wireless Area Network*).se traduce como red inalámbrica de área local y se caracteriza por tener mucho mayor alcance que la WPAN, esto gracias a su capacidad de repetición de señal a base de ondas radiales. Este tipo de red se comprende como la base de la tecnología wifi.

  - WMAN(*Wireless Metropolitan Area Network*). Se traduce como red inalambrica de area metropolitana. Esta conexión supera las WLAN por mucho, llegando a un rango de cobertura de hasta 20 kilómetros.

  - WWAN(Wireless Wide Area Network). Su traducción es Red inalámbrica de área amplia y se utilizan para la comunicación entre zonas con un gran grado de distanciación, para dicha función se utilizan torres de comunicaciones (celular,microondas,etc.). Dentro

de este tipo de red se encuentran el 3G, 4G, 5G entre otras tecnologías para telecomunicaciones.

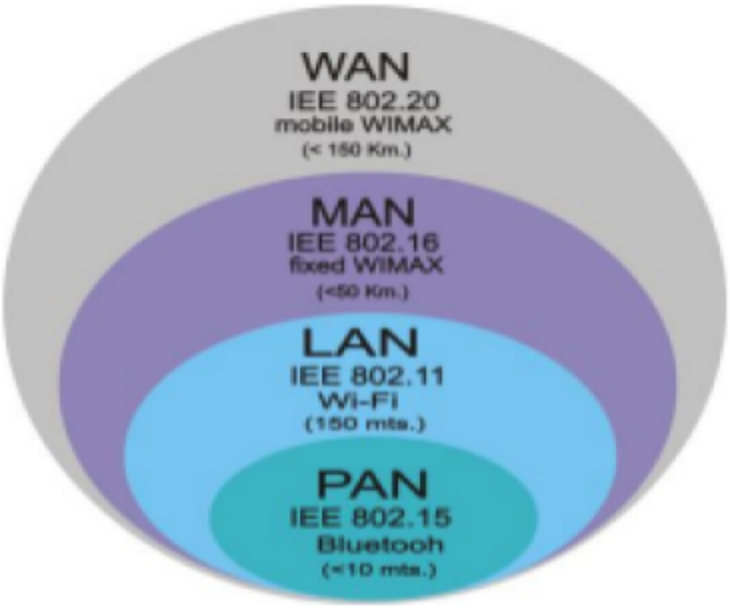


Figura 2.1: Tipos de redes inalámbricas según alcance.
Fuente: (UOC, 2019)

➢ **Según el rango de frecuencia:**

- Infrarrojo. Utiliza la comunicación y traspaso de datos a través de la luz infrarroja. Este medio requiere que tanto el emisor como el receptor cuenten con medios para alinear los infrarrojos, ya que se requiere una alineación del rayo de luz.

- Ondas radiales. Emplea diferentes frecuencias de radio (AM,FM,HF,etc.) para el envío y recepción de información . Mientras más cerca esté el medio receptor del emisor, más alta será la velocidad de transmisión.

- Microondas. Estas pueden subdividirse de dos formas:

- Microondas terrestres, las cuales utilizan las antenas parabólicas como medio de difusión, alcanzando como máximo los 300 GHz.
- Microondas Satelitales, que dependen de la interconexión entre satélites que orbitan en la atmósfera de la tierra, produciendo mucho mayor alcance y velocidad que por medios terrestres.

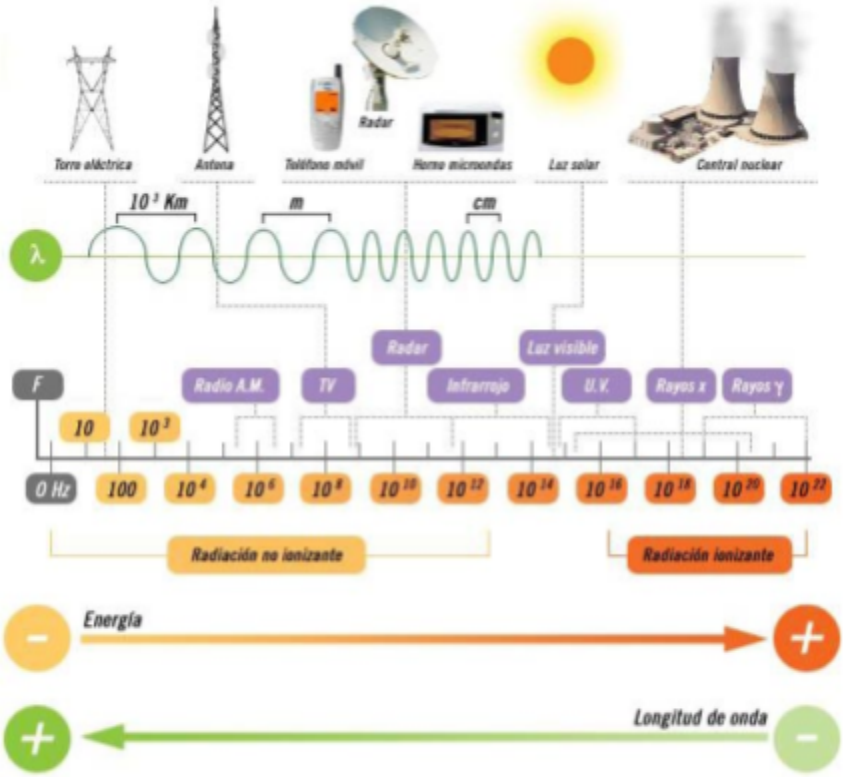


Figura 2.2: Tipos de redes inalámbricas según frecuencia. Fuente: (UOC, 2019)

2.1.2 - Funcionamiento de la tecnología Wifi

Como fue señalado previamente, la tecnología wifi utiliza la emisión de ondas radiales como vehículo de la información. Las frecuencias utilizadas por esta herramienta son los 2,4 GHz y los 5 GHz. Ambos rangos de señal se encuentra regulado bajo los estándares internacionales *IEEE*[2] *802.11b, IEEE 802.11g e IEEE 802.11n* (de los cuales se hablará en detalle más adelante) que se encargan de establecer que a estas frecuencias se les permite ir a velocidades

de 11 Mbit/s, 54 Mbit/s y 300 Mbit/s respectivamente. En el caso del rango 5GHz, es una configuración de frecuencia relativamente nueva y se le conoce también como WIFI 5. Este tiene la particularidad de ser más rápido que la frecuencia 2,4 GHz, pero a su vez tener menor alcance que esta.

A nivel operativo, la tecnología wifi tiene tradicionalmente el siguiente flujo: Primero se obtiene la conexión a internet por vía de cableado de ethernet[3] o de fibra óptica[4] el cual se conecta a un modem que decodifica la información para luego proceder a transmitirla a través de las ondas radiales. Se tiene que tener en cuenta que este tipo de flujo estructural puede variar según diversos factores como lugar, distancia, protocolos de seguridad nacionales y el avance de la tecnología en sí misma.

2.1.3 - Topologia de redes WIFI

La topología de una red no es más que la estructuración (a nivel físico o lógico) de una red y como sus distintos elementos se conectan entre sí a través de un medio, que en este caso serían las ondas de radio. Específicamente para las conexiones de wifi, se habla de dos tipologías principales: Primero se encuentra **la topología de infraestructura**, en la cual se define el requerimiento de uno o varios núcleos base(puntos de acceso) donde poder conectarse a la red a través de de un sistema de cableado y así coordinar entre procesos de transmisión y recepción de datos. Por otro lado, también existe **la topología Ad-Hoc**, en la cual se crea una red LAN a partir de un ecosistema de dispositivos con capacidad e interacción inalámbrica, sin tener que utilizar un

[3] ***Ethernet**: Consiste en un estándar de redes de área local. permite que dispositivo se puedan comunicar entre sí por medio de un protocolo (el lenguaje de red común).*

[4] ***Fibra óptica**: es un medio físico de transmisión de información. Funciona como guía de ondas dieléctricas que trabaja con frecuencias ópticas.*

punto de acceso. Esta última tipología aplica para grupos de dispositivos pequeños dentro de comunidades específicas (Pequeños negocios, reuniones corporativas, etc.). La tecnología wifi también cuenta con otros tipos de topologías menos populares o que atacan necesidades muy específicas. Algunas que vale la pena mencionar son:

- Las conexiones a localidades remotas a través de ***wireless bridges*** (esp. Puentes inalámbricos), Dispositivos que pueden acceder a distintas configuraciones de conexión (punto-a-punto y Punto multipunto) utilizando antenas direccionales para lograr alcanzar distancias de alto kilometraje.
- Las redes ***Mess***, que no es más que una variante del modo Ad-Hoc que maneja el transporte de datos de diferentes formas, utilizando cada dispositivo integrante de la red como un nodo para distribuir paquetes de información.

2.1.4 - Implementación de wifi en centros comerciales y/o aeropuertos

Para localidades públicas como los centros comerciales, tiendas departamentales y aeropuertos se tienda a utilizar una implementación de modo infraestructura BSS[5], que no es más que el nombre particular que le da la norma IEEE 802.11 al uso de la topografía de infraestructura mencionado anteriormente en el punto *1.1.3* lo que da como conclusión el uso de puntos de acceso(*AP* por sus siglas en inglés) como los ejes principales de la red.

Según la WI-FI ALLIANCE (2019), El flujo de conexión a la red tiene la siguiente secuencia de pasos:

1. El dispositivo detecta la indicación Hotspot 2.0 en el marco de la señal AP.

[5] ***BSS**: Basic service set o conjunto de servicios básicos en español*

2. El dispositivo consulta al servidor *ANQP*[6] para los dominios del identificador de acceso a la red (NAI, por sus siglas en inglés) y los *OI*[7] del consorcio de itinerancia.
3. El dispositivo compara los reinos y los *OI* recibidos con su lista de credenciales y redes preferidas.
4. El dispositivo se asocia automáticamente con *Passpoint* AP.
5. El dispositivo realiza la autenticación *IEEE 802.1X* en el servidor AAA doméstico utilizando *EAP-Transport Layer Security* (EAP-TLS) o *EAP-Tunneled TLS (EAP-TTLS)* con *MS-CHAPv2.*

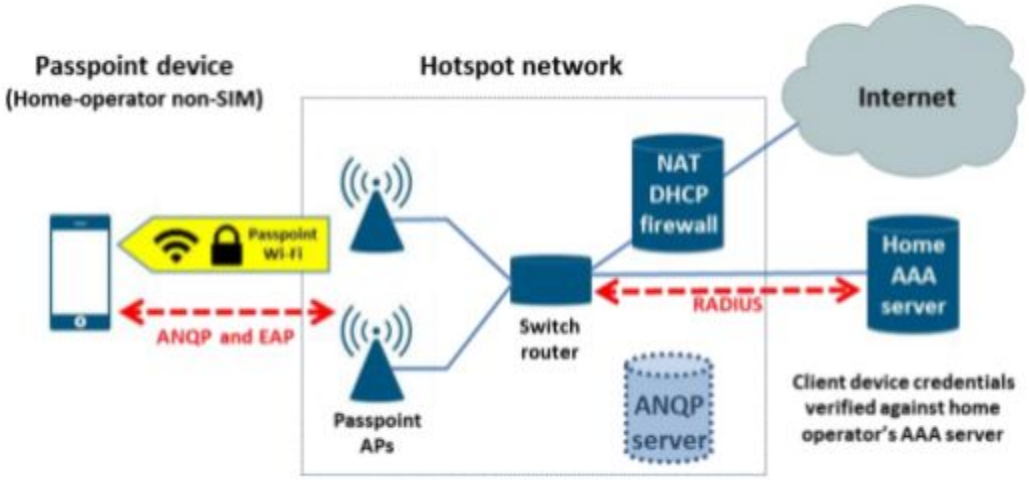


Figura 2.3: Representación gráfica del flujo de conexión a red inalambrica.
Fuente: WI-FI alliance (2019)

[6] **Servidor *ANQP*:** *El Access Network Query Protocol (ANQP) es un protocolo para consulta y respuesta de datos que se encarga de definir los servicios ofrecidos por un acceso.*
[7] ***OI****(Organizational Identifier)*: *Identificadores de organización.*

2.2 - Riesgos de ciberseguridad en redes inalámbricas públicas.

2.2.1 - ¿Qué es la ciberseguridad?

La ciberseguridad consiste en la protección de activos de información mediante el manejo de los riesgos y amenazas a los datos que son procesados, almacenados y transportada en sistemas de información que se encuentran conectados con redes, tanto locales como el Internet . Busca proteger, mantener y asegurar la Confidencialidad, Integridad y Disponibilidad de los datos. Esto se realiza mediante: la Identificación de posibles amenazas posibles que peligren los activos, la búsqueda y corrección de Vulnerabilidades, y la implementación y ejecución de controles para para mitigar, transferir, evitar o asumir los riesgos que peligren la seguridad de la información.

> *"La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciber entorno."* ***(UIT, 2010)***

Objetivos de la Seguridad de la Información

- ➔ **Confidencialidad**. La propiedad de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados. En el contexto de esta investigación mantener la confidencialidad no es solo evitar que hackers puedan obtener información transmitida a través, también se debe asegurar que, si se mantiene información de los dispositivos que se conectan a la red, estos no deben caer en mano de personas no autorizadas. Las técnicas como el sniffing, análisis de tráfico y el esparcimiento de malware como los *keyloggers* son amenazas para la confidencialidad en una red Wi-Fi.
- ➔ **Integridad**. Se trata de la Protección de los datos ante las modificaciones no autorizadas. *"La integridad de los datos se refiere a la certeza de que los datos no se manipulan ni degradan durante o después del envío. Es la certeza de que los datos no han sido objeto de modificación no autorizada, ya sea intencionada o no. Hay dos puntos durante el proceso de transmisión durante los cuales la integridad podría verse comprometida: durante la carga o transmisión de datos o durante el almacenamiento del documento en la base de datos o colección*." (Ng, 2020)
- ➔ **Disponibilidad**. Se trata de asegurar que los dispositivos y las personas puedan acceder a una red y sus recursos cuando sea necesario. Asegurarse que sus clientes y usuarios tengan acceso al internet mediante su red de wifi tiene valor en sí mismo, pero la carencia de este puede llevar a que los usuarios intenten conectarse a puntos de acceso wifi menos confiables pero más rápidamente accesibles, incluyendo aquellos creados por actores con intenciones maliciosas.

Conceptos de Seguridad

Vulnerabilidad

Una vulnerabilidad es una debilidad en el diseño, implementación, operación o en el control de un proceso que podría exponer el sistema a las amenazas adversas de los eventos. Se podría decir que una característica de un activo que permite que una Amenaza tome lugar dando una oportunidad a un atacante a comprometer la seguridad.

Amenaza

Es toda acción es capaz de actuar en contra un activo de manera que pueda resultar en daño. “Una amenaza es cualquier entidad o circunstancia que atente contra el buen funcionamiento de un sistema informático. Aunque hay amenazas que afectan a los sistemas de forma involuntaria, como, por ejemplo, un desastre natural, en la mayoría de casos es necesaria una intención de producir daño.” (Escrivá, 2013). Se pueden dividir en amenazas pasivas, como el análisis de tráfico de datos en una red, y amenazas activas, como un ataque de denegación de servicio (DoS).

Riesgo

El riesgo es la probabilidad de un evento y sus consecuencias, aunque existe el riesgo positivo, en la seguridad solo se enfoca en el riesgo negativo. *“El riesgo es la probabilidad de que se produzca un incidente de seguridad, materializandose una amenaza y causando pérdidas o daños. Se mide asumiendo que existe una cierta vulnerabilidad frente a una determinada amenaza, como puede ser un hacker, un ataque de denegación de servicios, un virus…”* (INCIBE, 2017). El riesgo depende de la existencia de una vulnerabilidad que pueda ser explotada y una amenaza que se aproveche de esta.

Activos

Un activo es algo de valor ya sea tangible o intangible que vale la pena proteger. En el contexto de una red pública los activos son "*los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciber entorno*". **(UIT, 2010)**

Controles

Los controles de seguridad son métodos, parámetros o medidas implementados para mitigar, transferir, evitar o asumir los riesgos a un activo. Pueden ser controles físicos, como puertas, candados y cámaras, o digitales como son la encriptación, contraseñas, firewalls y antivirus.

2.2.2 - Malware

Malware, o "software malicioso", es un término general que describe cualquier programa o código malicioso que sea dañino para los sistemas.

> *“El malware, hostil, intrusivo e intencionalmente desagradable, busca invadir, dañar o inhabilitar computadoras, sistemas informáticos, redes y dispositivos móviles, a menudo tomando un control parcial sobre las operaciones de un dispositivo que interfieren con el funcionamiento normal.*
>
> *Aunque el malware no puede dañar el hardware, puede robar, cifrar o eliminar datos, alterar o secuestrar funciones básicas de la computadora y espiar la actividad de los usuarios sin su permiso.” **(Malwarebytes, 2018)***

El malware se puede categorizar en diferentes tipos de acuerdo a ciertas características como su impacto potencial, método de propagación, o las acciones que realiza. Este último tipo se puede subdividir en dañinos o no dañinos, pero a pesar del uso de este término cabe recalcar que, por definición, todo malware tiene un impacto negativo en el usuario.

Virus

Según Escrivá (2013): “Un virus informático es un software malicioso que tiene por finalidad alterar el funcionamiento de un equipo informático sin el conocimiento o consentimiento de su usuario, corrompiendo o destruyendo archivos”. La característica principal y diferenciadora de los virus es, como su contraparte en el mundo real, su capacidad de “infectar” otros archivos. Los virus son autoreplicables, cuando un virus se ejecuta este se instala en la RAM del dispositivo, donde procede a infectar archivos en el sistema. Los efectos de un virus tienen un amplio rango de impacto, desde molestias inofensivas; cómo reemplazar las carpetas con acceso directo, a amenazas graves, como modificar los registros del sistema operativos para deshabilitar controles y abrir la puerta a otros ataques.

Gusano

Un gusano o *Worm* es un malware que es capaz de duplicarse a sí mismo automáticamente y esparcirse a otras computadoras, sin la necesidad de infectar archivos como los virus. Normalmente viaja a través de una red, explotando fallas de seguridad en sus blancos y utilizando un dispositivo específico como Host para escanear e infectar otros puntos en la red que pueda utilizar como nuevos Hosts y repetir el ciclo. Aunque, comparado con el virus, los gusanos no tienden a causar mucho daño directo por sí mismos, más allá del consumo excesivo de recursos, pueden utilizarse para crear *Backdoors* que permitan controlar los dispositivos remotamente, creando así un *Botnet.*

Troyano

“Un troyano o caballo de Troya es un software malicioso que se introduce en un ordenador y se instala en él, aparentando ser un programa inofensivo, pero su finalidad es permitir a un usuario no autorizado tomar el control de la máquina infectada. A diferencia de los virus, los troyanos no infectan ni corrompen archivos o programas y, a diferencia de los gusanos, no tienen capacidad de propagarse automáticamente, únicamente buscan permitir la administración remota del equipo a usuarios ilegítimos.” **Escrivá (2013)**

Para lograr su infección, los troyanos se disfrazan o forman parte de un programa legítimo. Estos programas suelen aparentar o realmente realizar sus funciones, creando confianza y despistando al usuario. En segundo plano, mientras se utiliza el programa, infectan el dispositivo del usuario y realizan varias acciones, típicamente con la meta de tomar control del sistema.

Spyware

El Spyware es un tipo de software que trata de conseguir información del usuario. Este tipo de malware es prominente en el ecosistema móvil. Varios desarrolladores móviles, notoriamente compañías como Facebook, utilizan sus aplicaciones móviles con estos fines, espían conversaciones de sus usuarios por mensajería instantánea y en audio a través del micrófono presente en sus dispositivos, crean listas de los contactos presentes en los dispositivos y las aplicaciones que tienen instaladas, y monitorean las acciones y hábitos de uso de sus usuarios fuera de sus aplicaciones. La información obtenida por estos métodos suelen ser utilizadas en campañas publicitarias o son vendidas a terceros con el mismo fin.

Keylogger

Los *Keyloggers* son un tipo de software o un dispositivo hardware específico que se encarga de registrar todo lo que se digita en en el teclado del dispositivo comprometido, para posteriormente memorizarlas en un fichero o enviarlas, a través de internet, al responsable original. Los *Keyloggers* suelen tener fines maliciosos, buscando obtener información confidencial como contraseñas y cuentas de usuario, o registrar los hábitos de uso de los usuarios afectados para ser utilizados por el perpetrador o vendidos a un tercero.

Adware

> “El adware es probablemente el tipo de malware (software malicioso) que todo el mundo reconoce cuando lo ve. Es difícil no hacerlo cuando las ventanas emergentes ocupan la mayor parte de la pantalla. El adware, que significa "malware publicitario", presenta anuncios no deseados mediante métodos intrusivos y potencialmente peligrosos.” **Lemonnier & Latto (2020)**

Una forma común de esparcir adware, es a través de aplicaciones gratis que contienen software adicional diseñado para presentar anuncios al usuario. Algunos sitios web emplean tácticas para convencer al usuario que ellos mismos activen las notificaciones push, para luego enviar con una cantidad excesiva de mensajes no deseados y potencialmente dañinos. La finalidad de este software es ganar dinero, cada *clic o Impresión* con un anuncio genera dinero para el desarrollador.

El *Adware* tiende a utilizarse en conjunto con el *Spyware,* explotando la información obtenida del usuario para servir *ads* más relevantes y así generar más clics. En un estudio realizado por Malwarebytes (2020) el Adware fue la categoría de software con mayor número de detecciones en 2019 y el Spyware tomó séptimo lugar.

Ransomware

El ransomware es un tipo de malware que encripta archivos de la víctima, prohibiendo totalmente su acceso. Su nombre de *Ransom,* secuestro en inglés, proviene del hecho de que el software está acompañado de un mensaje que exige un pago de rescate a cambio de la desencriptación de sus archivos. El dinero de rescate suele ser pagado a través de criptomonedas como el Bitcoin.

La severidad del ataque puede variar, algunas víctimas sólo tienen algunos de sus archivos encriptados, mientras que otros no pueden acceder en ninguna forma a sus sistemas hasta que paguen al secuestrador. La infección puede ocurrir a través de Phishing, explotaciones activas de fallos de seguridad como NotPretya o pueden viajar automáticamente entre computadoras como el gusano *Wanna Cry.*

2.2.3 - Ataques de Ciberseguridad comunes relevantes a redes Wi-Fi

Ataque de intermediario (Man-in-the-Middle)

Un ataque de intermediario, también conocido por el inglés *Man-in-the-Middle* (Hombre en el medio), es un ataque en el cual el atacante adquiere la capacidad de leer, insertar y modificar datos a voluntad. Estos ataques se logran cuando se intercepta las comunicaciones de datos entre dos partes las cuales desconocen que no se están comunicando directamente. Estas conexión pueden pueden ser entre partes de diferentes tipos como son Usuario-Usuario, Usuario-Servidor y, la más relevante, entre un Usuario y un Punto de Acceso Wi-Fi.

“Los ataques MitM consisten en colocarse entre la conexión de dos partes y observar o manipular el tráfico. Esto podría realizarse a través de la interferencia con redes legítimas o la creación de redes falsas que controle el atacante. Luego, el tráfico comprometido se despoja de cualquier cifrado para robar, cambiar o redirigir ese tráfico al destino elegido por el atacante. Debido a que los atacantes pueden estar observando en silencio o volviendo a cifrar el tráfico [...], puede ser un ataque difícil de detectar.” (Swinhoe, 2019)

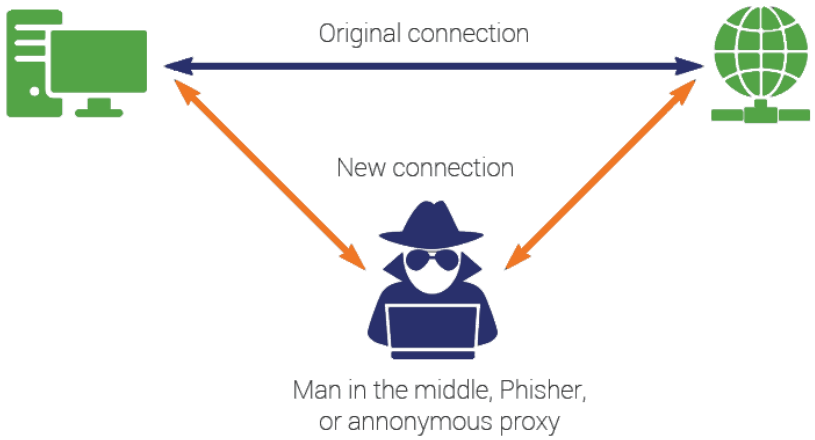


Figura 2.4: Diagrama de un ataque Man-in-the-Middle.

Fuente: The SSL Store, 2018

Una cantidad significativa de ataques cibernéticos, en especial esos relevantes a un área de internet local, tienen como objetivo lograr una posición de Man-in-the-middle o requieren de esta para poder efectuarse. Estos ataques representan una violacion total de los objetivos de la seguridad de la información. El atacantes tienen acceso a toda la información que se transmite entre los puntos, pueden interceptar y modificar los datos como deezer y también pueden terminar la conexión a su discreción.

Packet Sniffing: Rastreo de paquetes

El rastreo de paquetes consiste en la interceptación de cada paquete de información a medida que este es transmitido a través de una red. Es una técnica en la que un usuario rastrea datos pertenecientes a otros usuarios de la red. Esto se logra mediante la utilización de herramientas y software, llamados *Sniffers*, que monitorean la información que está siendo compartida, y luego la analizan en busca de su meta principal, las credenciales de acceso, como cuentas de sitios web y sus contraseñas, información bancaria, o simplemente cualquier dato que les permita identificar a un usuario específico para utilizarlo como medio al realizar otros crímenes y estafas.

> *"Un analizador de red, o un atrapador de información de la red, permite supervisar toda la información que pasa a través de una tarjeta de red, sobre todo si esta tarjeta es inalámbrica, En un inicio, el analizador se desarrolló para que los administradores de redes supervisarán el flujo de información que viaja por una red y pudieran detectar cualquier problema relacionado, Pero si un atacante pudiera tener acceso físico a la red, también sería capaz de analizar la información que viaja por la red y tomar la que necesite para sus intenciones"* **Baca Urbina (2016)**

Una de las vulnerabilidades, de las cuales el rastreo de paquetes toma ventaja, son de redes abiertas, que no están protegidas por contraseñas o que cuyas contraseñas son de conocimiento público. Además, son más efectivas en redes de alto tráfico, donde es más fácil esconder sus actividades a plena vista. Siendo estas características que describen nuestro objeto de investigación. Esto puede evitarse mediante la utilización de contraseñas y la autorización individual de los usuarios o a través de la utilización del WPS para autenticar sin contraseña, pero estas opciones no son factibles en el contexto de la investigación debido al alto flujo de usuarios que se presenta.

Este tipo de ataque también se aprovecha de los usuarios que se conectan a sitios web mediante el protocolo HTTP en lugar del HTTPS . El Protocolo HTTPS es una extensión del HTTP, este provee una encriptación bidireccional de las comunicaciones entre un cliente y un servidor, previniendo que los datos sean interceptados u modificados. Es recomendable configurar los puntos de acceso de manera que solo se puedan acceder a sitios web que utilicen Https y así evitar amenazas como el sniffing.

Denegación de Servicios (DoS)

La denegación de servicios consiste en un ataque que atenta contra la Disponibilidad de los Datos mediante la sobrecarga de algún sistema de información para impedir que sus usuarios tengan acceso a esta.

> *“Cualquiera que esté familiarizado con la seguridad de la red conoce el concepto de denegación de servicio (DoS). Es uno de los ataques de red más simples de llevar a cabo porque sólo requiere limitar el acceso a los servicios. Esto se puede hacer simplemente enviando una gran cantidad de tráfico a un objetivo específico. Por supuesto, la cantidad de tráfico necesaria para afectar a un dispositivo de destino puede ser mucho mayor que las capacidades de una sola máquina. Sin embargo, la inundación del tráfico no es la única forma de limitar el acceso a los servicios; para las redes inalámbricas, puede ser mucho más fácil, ya que la señal se puede interferir con varias técnicas diferentes."* **(Wilkins, 2011)**

Estos ataques pueden prevenirse mediante una gestión adecuada del consumo de ancho de banda en la red, la implementación de límites de ancho de banda para usuarios individuales a través de la configuración de la red, y el monitoreo de consumos excesivos o sospechosos en la red.

Aunque los ataques DoS interrumpen la Disponibilidad del servicio, estos por sí solos no comprometen directamente la confidencialidad de la información de los usuarios. A pesar de esto, estos ataques se pueden utilizar en conjunto con otros tipos de ataques, al no tener acceso a internet mediante un punto específicos, los dispositivos (automáticamente) o los usuarios (conscientemente) pueden tratar de conectarse a otro punto de acceso. Este punto de acceso puede ser un **Punto de Acceso no-autorizado**, configurado por un atacante previamente, que se hace pasar como una red abierta oficial del establecimiento.

Puntos de Acceso No Autorizados

Un punto de acceso no autorizado es cualquier punto de acceso inalámbrico que se ha instalado en una red sin el consentimiento del administrador o propietario de la red, proporcionando así acceso inalámbrico no autorizado a la infraestructura cableada de la red. Esto puede ser creado tanto como por un actor malicioso como por un empleado que quiere tener acceso a Wi-Fi en algún área que no exista, pero este segundo ejemplo aún presenta riesgos.

Para establecer un ejemplo, visualice un restaurante llamado, *Italianos. Italianos* le da acceso a sus clientes a su red wi-fi, protegida con contraseña y llamada '*WIFI ITALIANOS'.* La clave de esta red es entregada a clientes que la soliciten, si ya han realizado alguna compra. Un atacante puede aprovecharse de este sistema mediante la ingeniería social. Este entra a la tienda con su propio *Wi-Fi Hotspot* ya configurando con el nombre '*Italianos Invitados*' y sin protección por contraseña, haciéndose pasar como un punto legítimo proveído por el restaurante. Algunos de los clientes ya sea por la conveniencia de no tener que solicitar una clave o simplemente por descuido terminan conectándose al punto malicioso, cayendo en la trampa del atacante y comprometiendo sus datos y dispositivos.

“Gemelos Malvados”

Este tipo de ataque es una versión más sofisticada del Punto de Acceso no Autorizado ya que el atacante utiliza la SSID y dirección MAC de los puntos legítimos para lograr que su “Gemelo Malvado” sea prácticamente indistinguible, tanto para los dispositivos como para los usuarios, del legítimo.

“El atacante falsifica los Identificadores (la dirección MAC y el SSID) de un punto de acceso genuino para configurar el gemelo malvado. Cuando un cliente ve la lista de puntos de acceso Wi-Fi disponibles, solo ve un punto de acceso en lugar de dos puntos de acceso, ya que el gemelo malvado falsifica tanto la identificación del punto de acceso genuino. ” **(Agarwal, 2019)**

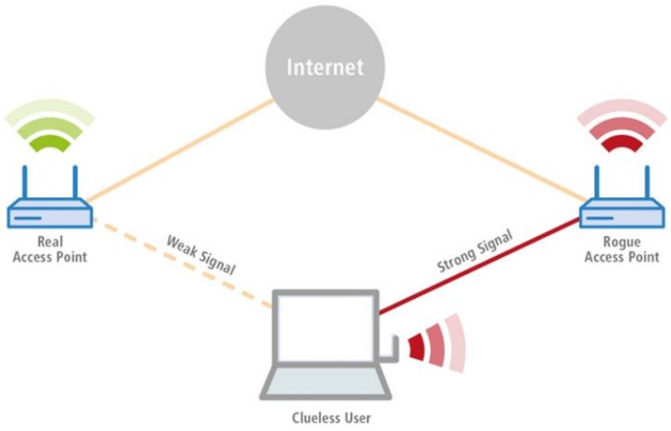


Figura 2.5: Ataque mediante el uso de Puntos de Acceso no Autorizados
Fuente: ISCF, 2019

La mayoría de los sistemas operativos están configurados para conectarse al punto con mayor intensidad de señal, en caso de que haya varios puntos asociados al mismo SSID. En presencia de un gemelo malvado, si la fuerza de la señal del gemelo excede la señal del punto genuino, los clientes se asocian con el gemelo automáticamente.

Una forma de evitar los ataques más sofisticados es a través de la concientización de los usuarios. Se pueden utilizar letreros o posters que

informen a los usuarios del nombre de los puntos de accesos legítimos, les informe si tienen que ingresar a una página o solicitar la contraseña y también les advierta de posibles puntos de acceso impostores.

> *"Estos ataques son posibles porque los usuarios no pueden autenticar las redes Wi-Fi públicas. La mayoría de estos ataques también se basan en el descuido del usuario. Simplemente verificar si las redes disponibles deberían estar*
> *disponibles, podría evitar algunos de estos ataques."* **(Gehring, 2016)**

Para prevenir estos ataques también se pueden utilizar dispositivos que detecten estos puntos y desactivarlos. *"Una entidad podría usar adaptadores USB Wi-Fi y computadoras terminales para crear escáneres AP no autorizados (baratos). Estos escáneres pueden enviar un mensaje de advertencia a seguridad o al administrador del sistema de que se ha detectado un AP no autorizado."* **(Gehring, 2016)**

Phishing

> "*En el phishing, una forma automatizada de ingeniería social, los delincuentes utilizan Internet para extraer de forma fraudulenta información confidencial de empresas e individuos, a menudo haciéndose pasar por sitios web legítimos. Mediante este existe la posibilidad de obtener grandes recompensas por ejemplo, a través del acceso a cuentas bancarias y números de tarjetas de crédito."* **(Parno, 2006)**

Aunque los ataques de Phishing se realizan más comúnmente a través de la imitación de sitios web o campañas de correos electrónicos spam, podríamos considerar los puntos de acceso autorizados, que imitan los legítimos, como un tipo de *Phishing,* pero también hay que tener en cuenta que una vez un actor fraudulento llega a conseguir que un usuario esté haya obtenido un vector muy eficaz para efectuar mas *Phishing.* Sería sencillo a través de filtros de red configurar redirecciones automáticas de las páginas web más populares a versiones fraudulentas y así conseguir una gran cantidad de credenciales eficazmente. En redes publicidad abiertas es común redireccionar a los usuarios nuevos a una página de registro cuando estos acceden por primera vez en una situación Man-in-the-Middles se puede redireccionar al usuario a una página que imite este formulario y robar su información de esta manera.

Secuestro de Sesión

> *"El secuestro de sesiones es un ataque en el que un atacante toma control de la sesión de un usuario. Una sesión comienza cuando se inicia sesión en un servicio, por ejemplo, su aplicación bancaria, y finaliza cuando se cierra la sesión. El ataque depende del conocimiento que tiene el atacante de su cookie de sesión, por lo que también se denomina secuestro de cookies o secuestro lateral de cookies. Aunque cualquier sesión de computadora puede ser secuestrada, el secuestro de sesiones se aplica más comúnmente a las sesiones del navegador y las aplicaciones web."* **(Banach, 2019)**

Para lograr un secuestro de sesión se necesita obtener la *Session ID* (clave de sesión) de la víctima. Un atacante puede obtener dicha clave a través de diferentes métodos, incluidos algunos discutidos previamente. Mediante el *phishing* el atacante puede convencer a un usuario a ingresar a un enlace malicioso que tiene una *Session ID* preparada previamente y luego utilizar esta misma para sus fines. Y con el Rastreo de Paquetes un atacante puede analizar los datos que están siendo transmitidos a través de la red para identificar e interceptar la *Session ID* de un usuario en específico.

Una vez se haya conseguido secuestrar la sección el perpetrador tiene la misma autorización que el usuario original y puede realizar todas las mismas acciones que este tiene permitido realizar durante sus sesiones normales. Puede realizar transacciones bancarias, comprar items al nombre de la víctima en tiendas virtuales, acceder a información personal y hasta comunicarse, a través de redes sociales y mensajería instantánea, a los conocidos de la víctima para estafarlos.

Emotet, Malware atraves de Wi-FI

Aunque no sea ligera la cantidad malware que son transmitidos por el internet, los malware capaces de propagarse directamente a través de redes inalámbricas son un fenómeno relativamente reciente. Uno de estos en cuestión, es el Botnet Emotet. Emotet fue descubierto por primera vez en 2014, en ese entonces era un troyano bancario dedicado a robar información sensitiva de las computadores personales, pero desde su creacion Emotet a evolucionado convirtiéndose en una Botnet que se esparce mediante las conexiones inalámbricas para expandir su red de dispositivos infectados. En un informe publicado por Malwarebytes (2020), la entidad informó que la actividad de Emotet aumentó un 375% solo en 2019.

> *“Primero, Emotet infecta un dispositivo host, luego descarga y ejecuta el módulo esparcidor de Wi-Fi. Este módulo enumera todos los dispositivos Wi-Fi habilitados en el host y presenta la lista de redes Wi-Fi accesibles. Posteriormente, el módulo lanza ataques de fuerza bruta en cada una de las redes enumeradas; para ello, utiliza sus listas internas de contraseñas fáciles de adivinar. No se indicó de dónde procedían estas listas. Si este ataque tiene éxito, lanza un segundo ataque de fuerza bruta para adivinar las credenciales de las computadoras y servidores conectados a la red Wi-Fi comprometida y, si el segundo ataque tiene éxito, el ciclo se repite para más rondas de infección.”* ***(TrendMicro, 2020)***

2.3 - Impacto económico de ataques a redes públicas.

2.3.1 - Efectos de los ciberataques en la economía

La actividad cibernética maliciosa, o ciberataques dirigidos al sector público o a redes públicas se manifiestan como negación de servicios, destrucción de propiedad y datos, ruptura en la operación de los negocios, algunas veces para recolectar ransoms o rescates, y robo de datos privados, propiedad intelectual e información financiera y estratégica

Los daños causados por estos ataques pueden pasar del objetivo inicial, por ejemplo, el usuario de una red pública, hasta entidades en la misma red, magnificando el daño económico, ya que comparten vulnerabilidades, que causan estas amenazas en común. El desconocimiento o conocimiento limitado de estas vulnerabilidades en común en una red pública impide el desarrollo o fortalecimiento de la ciberseguridad en general.

En la actualidad, los ciberataques son considerados como uno, si no el mayor de los riesgos para la estabilidad de las empresas y organizaciones, según lo afirma el informe The Global Risks Report 2018-2019 del World Economic Forum, donde un riesgo global es entendido como un evento o condición incierta que, en caso de ocurrir, puede causar un impacto negativo significativo en varias industrias (y países), en un lapso de diez años.

Los costos financieros de los ciberataques fueron de un incremento del 27.4% del 2017 al 2018, en un estudio realizado a 254 compañías anónimas de 7 países diferentes, con un costo de 11 millones de Euros por compañía. Se espera que el costo a principio de la década del 2020 sea de un estimado de 8 trillones de dólares.

2.3.2 - Ataques cibernéticos con más impacto económico

Ransomware

Los tipos de ataque que más pérdida económica han causado son relacionados al ransomware, un tipo de malware que impide a los usuarios acceder a su sistema o archivos y exige un tipo de pago para poder rescatar los datos. Los ataques de ransomware suponen el 64% de los emails maliciosos enviados desde el 2018 al 2020, afectando el doble de negocios comparados al 2016.

Algunos ejemplos notables son el Wanna Cry, Petya y No Petya, el cual causó pérdidas grandes en compañías como Merck y FedEx, reportando pérdidas en el último trimestre del año de 300 millones de dólares.

Estos ataques no solo suponen un costo financiero, sino que también afectaron estrategias de infraestructura alrededor del mundo, no solo en redes públicas, con pérdidas gubernamentales, de proveedores de telecomunicaciones, compañías energéticas y centros de comercio.

2.3.3 - Costo de ataques cibernéticos

Las cifras de pérdida por ciberataques ya no son hipotéticas, estos tienen un costo real para las empresas u organizaciones, que pueden tardar meses o años en reponerse, Según un estudio de cisco, Estudio de Referencia de las Capacidades de Seguridad de Cisco 2018, el 53% de todos los ataques cibernéticos a nivel general resultaron en daños financieros por más de 500,000 dólares, entre estos están incluidos ingresos, clientes, oportunidades y costos de bolsillo.

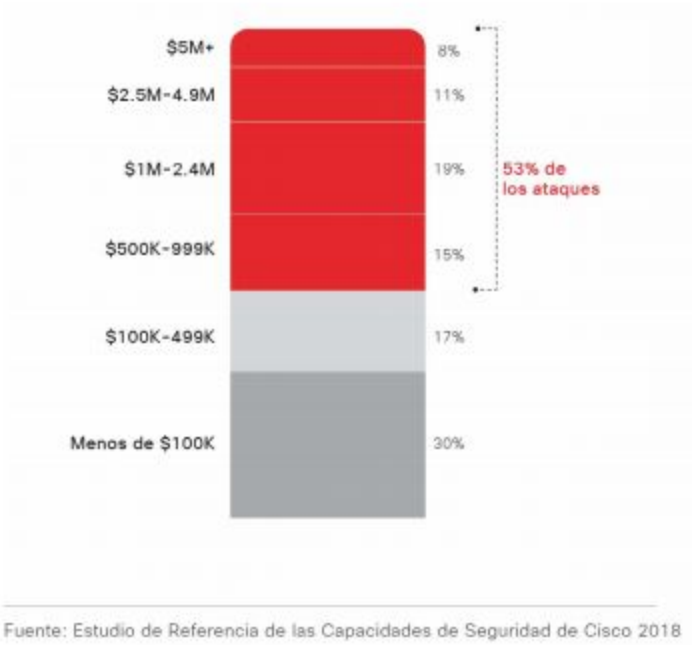


Figura 2.6: Costos de Ataques Cibernéticos en 2018
Fuente: Cisco (2018)

Las redes públicas son las más vulnerables a ataques cibernéticos por su falta de medidas rigurosas en la seguridad, haciendo que los atacantes se enfoquen más en esta para robo de datos personales con fin de robar recursos económicos. En gran medida esto se da porque, en redes públicas son más comunes los dispositivos móviles y datos que estos contienen en la nube, haciendo estas áreas más difíciles de defender, también teniendo en cuenta el comportamiento del usuario al desconocer cómo funcionan los ataques cibernéticos.

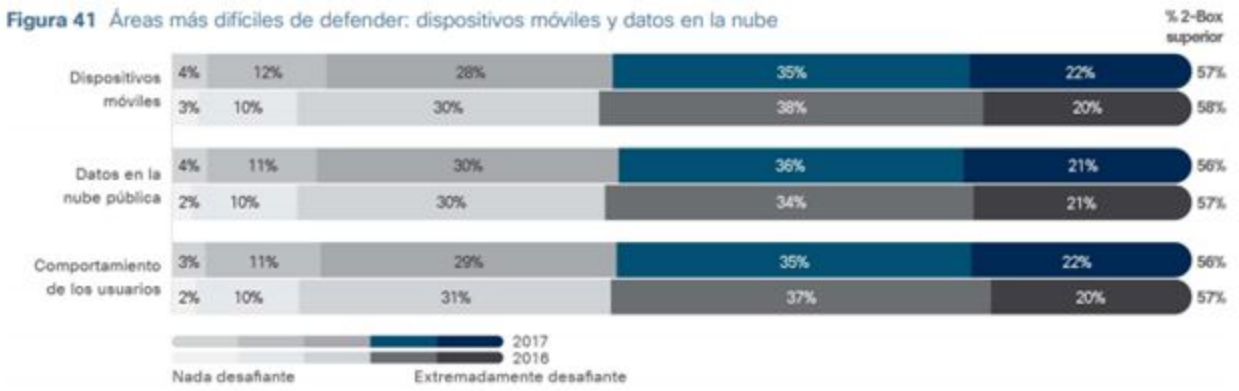


Figura 2.7: *Áreas de ciberseguridad más difíciles de defender*

Fuente: Cisco (2018)

Capítulo 3

Controles de Ciberseguridad en localidades públicas Dominicanas.

3.1 - Marco legal dominicano con relación a los delitos cibernéticos.

3.1.1 - Ley No. 53-07: sobre Crímenes y Delitos de Alta Tecnología.

El 23 de abril de 2007 se promulgó en República Dominicana la **ley 53-07** sobre crímenes y delitos de alta tecnología. Esta ley tiene como finalidad:

- Proteger la información que es procesada o manejada por sistemas tecnológicos
- Resguardar los acuerdos y transacciones monetarias que se realicen a través de medios digitales
- Penalizar los delitos de origen tecnológico que atenten a la integridad de la información de las personas.

Esta ley se estructura a partir de 2 principios generales, el primero habla sobre la territorialidad, que delimita los aspectos tratados por la ley con referente a las sanciones están limitados a cubrir el territorio nacional a excepción de que el delito sea realizado desde territorio dominicano al extranjero o viceversa. El segundo principio se orienta a la Razonabilidad y Proporcionalidad, que declara todo lo restringido o prohibido por esta ley a tener que cumplir con la proporciones y expectativas establecidas por la propia ley debido a la consideración de sus consecuencias sociales.

En cuestión de penalizaciones, esta ley abarca varios tipos de crímenes tecnológicos entre los cuales están:

- CRÍMENES Y DELITO CONTRA LA CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD DE DATOS Y SISTEMAS DE INFORMACIÓN
  - manipulación/divulgación de contraseñas.
  - clonación de dispositivos.
  - acceso y manipulación de datos no autorizada.

- ➢ daño o borrado de datos.
- ➢ intercepción/intervención de datos.
- ➢ beneficios de estos delitos por parte de terceros.

❖ DELITOS DE CONTENIDO

- ➢ Atentado contra la Vida de la Persona.
- ➢ Robo mediante la utilización de alta tecnología.
- ➢ Obtención Ilícita de Fondos.
- ➢ Transferencias Electrónicas de Fondos.
- ➢ Estafa.
- ➢ Chantaje.
- ➢ Robo de Identidad.
- ➢ atentado sexual/pornografia infantil.

❖ DELITOS DE PROPIEDAD INTELECTUAL Y AFINES

- ➢ De violarse las siguientes leyes a través de medios tecnológicos y/o de telecomunicaciones, se procederá con sus respectivos procesos penales
  - ■ la Ley No.20-00(sobre Propiedad Industrial).
  - ■ la Ley No.65-00 (sobre Derecho de Autor).

❖ DELITOS CONTRA LAS TELECOMUNICACIONES

- ➢ Llamada de Retorno de Tipo Fraudulento.
- ➢ Redireccionamiento de llamadas de larga distancia.
- ➢ Robo de Línea.
- ➢ Manipulación Ilícita de equipos de telecomunicaciones.
- ➢ Intervención de centrales privadas.
- ➢ Desvío de tráfico.

- ❖ CRÍMENES, DELITOS CONTRA LA NACIÓN Y ACTOS DE TERRORISMO
  - ➢ Crímenes y actos delictivos que atenten contra la nación Dominicana.
  - ➢ Actos de Terrorismo o alteracion del orden a mayor escala en territorio Dominicano.

La ley No.53-07 es una norma que para su tiempo, fue un paso importante en cuestión de seguridad de la información, sin embargo, se debe tomar en cuenta que su criterio a nivel de protección ante amenazas está desactualizado y es necesario que se actualice a las necesidades de ciberseguridad que se viven actualmente y al avance de las nuevas tecnologías. en cuestiones de implementación de esta ley, Tanto las autoridades como los habitantes de República Dominicana no han presentado mucho interés. Muchos crímenes quedan impunes o sin reportar por el poco conocimiento y/o difusión de esta ley.

3.1.2 - Ley No. 172-13: Sobre protección integral de los datos personales.

Esta orden del estado surge el 15 de diciembre de 2013 bajo el gobierno del presidente Danilo medina y tiene como función principal "la protección integral de los datos personales presentes en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes sean estos públicos o privados" . Dicha ley deroga la *Ley No. 288-05*, del 18 de agosto del año 2005, sobre las Sociedades de Información Crediticia y de Protección al Titular de la Información.

Esta ordenanza caracteriza los privilegios de las personas en cuanto a la información y los datos que se guardan sobre ellos, así como los sistemas para su actividad, que según la misma constitución, son "actualización, oposición al

tratamiento, rectificación o destrucción” de cualquier dato que los influya erróneamente.

Como garantía de la actividad de este derecho, se gestiona un sistema que parte del caso del titular de los datos realizado ante el responsable del banco de información, ya sea para la actualización, resistencia, corrección o aniquilación de los datos, la última reacción dentro de diez días hábiles. En el caso de que no obtenga una reacción o no esté satisfecho con lo que se transmitió, el propietario de los datos está calificado para realizar un movimiento legal. Esta actividad legítima viable es venerada como *"Habeas Data"*, que según el artículo 70 de la Constitución, permite al ofendido "conocer de la presencia y acceder a la información contenida en ella a través de registros abiertos o privados o bancos de información y, en caso de tergiversación o segregación, solicitar la suspensión, corrección, actualización y clasificación " de los datos.

3.1.3 - Decreto No.230-18: Establecimiento y Regulación de la Estrategia Nacional de Ciberseguridad 2018-2021.

El decreto no. 230-18 es un edicto manifestado por el presidente Danilo Medina el 2 de julio del 2018, en el cual se definen mecanismos y estrategias coordinadas por el estado Dominicano con finalidad de fortalecer la ciberseguridad a nivel nacional a través de organismos estatales afines y alianzas con entidades privadas. Como objetivo final de este mandato la integración de un marco de ciberseguridad óptimo para todos los ciudadanos de República Dominicana a la llegada del año 2021.

Cabe destacar que esta ordenanza hace girar sus estrategias entorno a 4 pilares fundamentales:

I. Marco legal y fortalecimiento Institucional.

Esta estrategia toma importancia del ámbito legal y establece como eje fundamental el fortalecimiento del marco legal a través de la incorporación de conceptos de ciberseguridad actualizados al marco legal Dominicano.

II. Protección de infraestructuras críticas nacionales e infraestructuras TI del estado.

Este enfoque se relaciona con la protección de información y medios de almacenamiento que se encuentran bajo las infraestructuras del estado dominicano mediante el análisis, catalogación y mejoramiento del manejo de estos elementos de TI para la creación de una estrategia nacional que sea homogénea y robusta.

III. Educación y cultura nacional de ciberseguridad.

Se toma la inclusión de la ciberseguridad en la formación educativa (Desde todos sus niveles) como un foco estratégico importante que permite la inclusión del pueblo Dominicano a esta estrategia desde cualquier rango de edad en los que se encuentren, creando así una cultura de protección cibernética que tendrá impacto tanto en la sociedad actual como en generaciones futuras.

IV. Alianzas nacionales e internacionales.

Como último pero no menos importante, se toma en consideración la creación de alianzas entre el sector público y privado, así como también del estado con entidades internacionales para la fomentación de planes de acción que contengan cooperación de entidades con presencia local y/o en el extranjero con experiencia en el ámbito de la seguridad informática.

3.2 - Manejo de ciberataques desde el punto de vista gubernamental.

3.2.1 - Equipo de respuesta a incidentes de cibernéticos de República Dominicana (CSIRT-RD)

El CSIRT-RD surge gracias al previamente mencionado Decreto No.230-18, como un organismo focalizador de los distintos planes de ciberseguridad planteados por dicha declaración. Dentro de los múltiples servicios que este organismo ofrece se encuentran:

- ➔ SERVICIOS PROACTIVOS

  El CSIRT-RD posee servicios que tienen la finalidad de brindar asistencia orientada a la protección de procesos de infraestructura y seguridad para prevenir la ocurrencia o reducir el impacto de un incidente cibernético a través de la concientización, información y prevención.

- ➔ BOLETINES

  Boletines que ofrecen consejos e información de los diferentes objetivos de seguridad que se planean para el país y sobre conceptos básicos y tendencias actuales relacionados con la ciberseguridad.

- ➔ MONITOREO Y DETECCIÓN DE VULNERABILIDADES

  Comprende el monitoreo y observación del surgimiento de nuevos mecanismos de “intrusión, campañas de ataque, amenazas políticas, daños ambientales, tendencias tecnológicas, entre otros”.

- ➔ SERVICIOS REACTIVOS

  Estos se encuentran enfocados al análisis de incidentes y la confección de medidas correctivas en función a demandas que se prestan luego de presentarse un evento de seguridad.

➔ ALERTAS

Hacer llamados de seguridad y alertas en respecto a las tecnologías más usadas en la actualidad y sus posibles implicaciones en relación a los sistemas de las comunidades atendidas.

➔ GESTIÓN DE INCIDENTES

Abarca tareas asociadas a la gestión de eventos e incidentes incluyendo detección y reporte, triaje, análisis y respuesta.

➔ GESTIÓN DE VULNERABILIDADES

La recepción de información y reportes acerca de productos de hardware/software vulnerable, y los posibles efectos de dichas vulnerabilidades, así como también la creación de estrategias para la respuesta, detección y corrección de estas anomalías.

➔ VALORES AGREGADOS

Estos Servicios buscan desarrollar de manera positiva el estado general de la ciberseguridad mediante el uso de retroalimentación y lecciones aprendidas con el conocimiento adquirido respondiendo a incidentes cibernéticos a través de formación especializada en ciberseguridad y la promoción de eventos de sensibilización.

3.2.2 - Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (DICAT)

El Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (DICAT) es un organismo que surge en noviembre del 2005 a motivo del incremento de los delitos electrónicos en República Dominicana, a su vez por

las nuevas formas y métodos de ejecución de los delitos tradicionales utilizando medios informáticos. tras la promulgación de la ley 57-07, se define como una extensión de la policía nacional Dominicana y su labor principal es velar por la seguridad de la información de los ciudadanos Dominicanos presentes en los distintos medios digitales. El DICAT se segmenta en los siguientes departamentos:

- Sección de Investigaciones.
- Sección de Inteligencia Electrónica.
- Sección de Fraude a Empresas.
- Sección de Fraudes Bancarios.
- Sección de Evidencia Electrónica.
- Sección de Análisis Forense Equipos Electrónicos.
- Sección de Análisis Forense Imágenes / Videos
- Sección de Llamadas Molestosas y/o Amenazantes.

3.2.3 - División de Investigaciones de Delitos Informáticos

La División de Investigaciones de Delitos Informáticos es una subdivisión de la dirección nacional de investigaciones (DNI) y su función es proteger de manera exhaustiva el cumplimiento de la previamente mencionada ley no. 53-07. Sus labores se integran constantemente con organismos con el DICAT, el Ministerio de Defensa y la Dirección nacional de control de drogas (DNCD) pero también se le puede ver colaborando con entidades como el Instituto Dominicano de Telecomunicaciones (INDOTEL) con fines de promulgación de políticas de ciberseguridad a nivel nacional o con el Instituto Tecnológico de Santo Domingo (INTEC) con fines de certificacion y capacitacion de personal en base a seguridad informática.

3.2.4 - Instituto Dominicano de Telecomunicaciones (INDOTEL)

Esta institución surge tras la puesta en marcha de la ley 153-98 (mejor conocida como la ley general de telecomunicaciones) en respuesta a las necesidades de cumplimientos de dicho mandamiento. En conjunto con la procuraduría general de la República Dominicana, se encarga de presentar acciones de control contra el crimen cibernético y la vez promover políticas de ciberseguridad que cubran las necesidades de anticipar, resistir o recuperar cualquier ataque preservando así la integridad de los servicios críticos como los de salud, energía, transporte, suministro de agua potable, o acceso a servicios financieros.

3.3 - Modelos de protección de datos eficaces.

3.3.1 - Datos personales

La información de carácter personal es toda aquella que puede vincular a un individuo identificable. Ya que es posible identificar a una persona juntando/reuniendo diversos datos, incluso sin estar asociados a un nombre, lo que constituye un dato personal puede ser muy amplio. Un número de calzado, una afición o una imagen, son ejemplos de datos identificativos de una persona, si es posible establecer una asociación entre aquellos y esa persona. Nótese, además, que los responsables del tratamiento, que son las compañías y/u organizaciones que procesan los datos no son necesariamente capaces de realizar una identificación.

3.3.3 - Respuesta a fuga de datos

En general, un modelo de protección de datos a nivel nacional debe informar de cualquier fallo de seguridad a la Autoridad para la Protección de Datos en un plazo de 72 horas desde que se conozca. También, debe informar a aquellas personas cuyos datos personales su empresa u organización haya procesado cuando sea probable que el fallo de seguridad haya afectado negativamente a esas personas, por ejemplo: en caso de fuga de datos financieros o si personas no autorizadas han conseguido acceso a sus historiales médicos.

3.3.3 - Entrevista a un Profesional de Redes Públicas

La siguiente tabla de resumen presenta las respuestas obtenidas de una entrevista realizada al Ing. Luis Arias, especialista en diseño, instalación y administración de redes. (Detalles adicionales de la entrevista, al igual que la transcripción completa de la misma, se encuentran disponibles en los anexos de este trabajo)

Temas	Preguntas y Respuestas
Control de la red	➔ **¿Considera las redes públicas del país vulnerable a ciberataques?** ◆ **Son muy vulnerables a ataques, debido a la falta de cultura de seguridad preventiva en en el país.** ➔ **¿Cuáles ataques considera pueden ser más posibles a este tipo de redes?** ◆ **Ransomware, debido a que es muy rentable (aun si no todos las víctimas paguen el rescate).** ◆ **Phishing, debido a que debe mitigarse mediante la**

	educación del usuario no con medidas de software. ➔ **¿Los establecimientos con los que ha trabajado poseen alguna regla, reglamento o política sobre redes inalámbricas que deba seguirse?** ◆ Depende, en el país se encuentran muchos casos. ◆ Existen muchas empresas del país que toman su seguridad en serio, pero también empresas de gran tamaño que poseen estructuras inadecuadas ◆ Las empresas internacionales suelen traer sus políticas de seguridad e infraestructura de red ◆ Los centros comerciales, generalmente, no invierten en la seguridad de sus redes. ➔ **Con qué frecuencia son auditados los sistemas de red inalámbrica?** ◆ Las empresas que se responsabilizan y toman en serio su seguridad hacen auditorías externas de seguridad y calidad con frecuencia.
Estandares	• **¿Con cuáles estándares(IEEE/ISO) están trabajando?** ○ 9001, 9126, 27001 • **¿Cuál es el estándar con mayor importancia en su estructura de red?** ○ IEEE 802.11n y IEEE 802.11ac son los más relevantes para las redes públicas de alta tráfico. ○ Segmentación de Redes (VLAN) es un fundamento esencial para la seguridad de redes de acceso

	público.

Mitigación de ataques	• **Se han presentado ataques en las redes que ha trabajado?**
	  ○ **Si, entre estos se encuentran: Escaneos de puertos, Rogue Access Points, Ataques de fuerza bruta, y Phishing mediante correo, entre otros.**
	• **¿Posee dicha red un plan de respuesta contra ataques de red inalámbrica?**
	  ○ **Los appliances y firewalls de alta gama son capaces de realizar respuestas a ataques automáticamente si son configurados**
	  ○ **A nivel medio es necesario tener y mantener un plan de respuesta manual**
	  ○ **Es de gran importancia educar y controlar al usuario**
	  ■ **Bloquear permisos de usuario en la red**
	• **Cómo manejan el surgimiento de algún rogue ap (Puntos de Acceso no Autorizados)?**
	  ○ **Bloquear todos los puertos (físicos y lógicos) que no se estén utilizando**
	  ○ **Alertar y responder cualquier actividad sospechosa relacionadas a los puertos**
	• **¿Cuál cree que es su mayor reto a nivel de seguridad ahora mismo?**
	  ○ **Falta de inversión monetaria en la seguridad de las redes, tanto en los equipos de red y seguridad, como en el diseño y la implementación de la red.**

Contacto gubernamental	• **¿Su marco de seguridad está regulado por alguna institución del país?**
	  ○ **Indotel, Aunque los estándares que exigen son muy generales y básicos.**
	• **¿Cree necesaria la incorporación, reforzamiento o refinamiento del contacto gubernamental con este establecimiento a nivel de ciberseguridad?**
	  • **Dirección e Integración. El gobierno debe dar dirección y liderazgo en el área de ciberseguridad, a *través de una misma entidad*, para mejorar la ciberseguridad en el país**.

Tabla 3.3.3: Entrevista a un Profesional de Redes Públicas

3.4 - Estadísticas de ataques en República Dominicana

Con el fin de recolectar los datos estadísticos más precisos sobre ataques cibernéticos a redes públicas del país, se trató de contactar al DICAT y al CSIRT-RD con el fin de recolectar todas las estadísticas de ataques en redes públicas reportados en los últimos 3 años (2018-19), En el caso del DICAT, se presentó un permiso para obtener datos estadísticos a través de la policía nacional dominicana el cual fue autorizado el 27 de noviembre del 2020.

3.4.1 - Reportes de ataques a través del DICAT (2018-2020)

NO.	TIPOS DE DELITOS	TOTAL GENERAL 2018		
		TOTAL DENUNCIAS RECIBIDAS	TOTAL CASOS RESUELTOS	TOTAL PENDIENTES
1	DIFAMACION Y / O AMENAZA VIA PAGINA WEB	52	68	-16
2	EXTORSION VIA PAGINA WEB	28	24	4
3	ESTAFA VIA PAGINA WEB	502	85	417
4	HACKING	12	0	12
6	DIFAMACION Y/O AMENAZA VIA E-MAIL	4	3	1
8	SUSTRACCION DE EQUIPOS ELECTRONICOS	6	8	-2
9	FRAUDES ELECTRONICOS A PERSONAS E EMPRESAS	8	7	1
10	CERTIFICACION DE CORREO ELECTRONICO	0	40	-40
11	LLAMADAS MOLESTOSAS Y/O AMENAZANTES	44	5	39
12	ROBO DE E-MAIL	0	0	0
13	PHISHING	179	76	103
14	ROBO DE IDENTIDAD	51	21	30
15	ACCESO ILICITO Y SABOTAJE	23	8	15
16	PORNOGRAFIA INFANTIL	0	7	-7
17	CLONACION DE TARJETAS (SKIMMING)	100	75	25
18	ESTAFA VIA TELEFONICA	29	4	25
	TOTAL DE LOS AÑOS 2017, 2018, 2019 Y 2020	1038	431	607

Reportes de ataques recibidos en el 2018. Fuente: DICAT(2020)

Durante el 2018, el DICAT recibió un total de 1028 reportes de ataques, de los cuales se pueden destacar a las estafas vía página web (502 casos) como el tipo de ataque más común en dicho año. Esta forma de intrusión en los espacios públicos se asocia con la utilización de puntos de acceso no autorizados, sabotaje de redes y con el uso de ingeniería social.

NO.	TIPOS DE DELITOS	TOTAL GENERAL 2019		
		TOTAL DENUNCIAS RECIBIDAS	TOTAL CASOS RESUELTOS	TOTAL PENDIENTES
1	DIFAMACION Y / O AMENAZA VIA PAGINA WEB	19	4	17
2	EXTORSION VIA PAGINA WEB	3	1	3
3	ESTAFA VIA PAGINA WEB	137	25	118
4	HACKING	0	1	0
6	DIFAMACION Y/O AMENAZA VIA E-MAIL	0	0	0
8	SUSTRACCION DE EQUIPOS ELECTRONICOS	0	0	0
9	FRAUDES ELECTRONICOS A PERSONAS E EMPRESAS	0	0	0
10	CERTIFICACION DE CORREO ELECTRONICO	0	5	0
11	LLAMADAS MOLESTOSAS Y/O AMENAZANTES	6	6	4
12	ROBO DE E-MAIL	0	0	0
13	PHISHING	57	7	50
14	ROBO DE IDENTIDAD	3	1	2
15	ACCESO ILICITO Y SABOTAJE	4	3	4
16	PORNOGRAFIA INFANTIL	0	0	0
17	CLONACION DE TARJETAS (SKIMMING)	1	8	1
18	ESTAFA VIA TELEFONICA	14	4	10
	TOTAL DE LOS AÑOS 2017, 2018, 2019 Y 2020	244	65	209

Reportes de ataques recibidos en el 2019. Fuente: DICAT(2020)

En el 2019, el DICAT recibió un total de 244 reportes de ciberataques, de los cuales 137 fueron por estafa vía página web(365 casos menos que el año anterior), siendo el ataque más común por segunda vez consecutiva.

NO.	TIPOS DE DELITOS	TOTAL GENERAL 2020		
		TOTAL DENUNCIAS RECIBIDAS	TOTAL CASOS RESUELTOS	TOTAL PENDIENTES
1	DIFAMACION Y / O AMENAZA VIA PAGINA WEB	0	20	-20
2	EXTORSION VIA PAGINA WEB	119	29	90
3	ESTAFA VIA PAGINA WEB	596	86	510
4	HACKING	0	1	-1
6	DIFAMACION Y/O AMENAZA VIA E-MAIL	0	3	-3
8	SUSTRACCION DE EQUIPOS ELECTRONICOS	0	0	0
9	FRAUDES ELECTRONICOS A PERSONAS E EMPRESAS	0	3	-3
10	CERTIFICACION DE CORREO ELECTRONICO	0	3	-3
11	LLAMADAS MOLESTOSAS Y/O AMENAZANTES	21	4	17
12	ROBO DE E-MAIL	0	0	0
13	PHISHING	174	15	159
14	ROBO DE IDENTIDAD	27	3	24
15	ACCESO ILICITO Y SABOTAJE	79	6	73
16	PORNOGRAFIA INFANTIL	0	0	0
17	CLONACION DE TARJETAS (SKIMMING)	16	6	10
18	ESTAFA VIA TELEFONICA	7	2	5
	TOTAL DE LOS AÑOS 2017, 2018, 2019 Y 2020	1039	183	856

Reportes de ataques recibidos en el 2020. Fuente: DICAT(2020)

En el 2020, el DICAT recibió un total de 1039 reportes de ciberataques, de los cuales 597 fueron por estafa vía página web(460 reportes más que el año anterior), siendo este el ataque más común por tercera vez consecutiva.

NO.	TIPOS DE DELITOS	TOTAL GENERAL		
		TOTAL DENUNCIAS RECIBIDAS	TOTAL CASOS RESUELTOS	TOTAL PENDIENTES
1	DIFAMACION Y / O AMENAZA VIA PAGINA WEB	71	92	-21
2	EXTORSION VIA PAGINA WEB	150	54	96
3	ESTAFA VIA PAGINA WEB	1235	196	103
4	HACKING	12	2	10
6	DIFAMACION Y/O AMENAZA VIA E-MAIL	4	6	-2
8	SUSTRACCION DE EQUIPOS ELECTRONICOS	6	8	-2
9	FRAUDES ELECTRONICOS A PERSONAS E EMPRESAS	8	10	-2
10	CERTIFICACION DE CORREO ELECTRONICO	0	48	-48
11	LLAMADAS MOLESTOSAS Y/O AMENAZANTES	71	15	56
12	ROBO DE E-MAIL	0	0	0
13	PHISHING	410	98	312
14	ROBO DE IDENTIDAD	81	25	56
15	ACCESO ILICITO Y SABOTAJE	106	17	89
16	PORNOGRAFIA INFANTIL	0	7	-7
17	CLONACION DE TARJETAS (SKIMMING)	117	89	28
18	ESTAFA VIA TELEFONICA	50	10	40
	TOTAL DE LOS AÑOS 2017, 2018, 2019 Y 2020	2221	677	164

Total general de ataques recibidos del 2018 al 2020. Fuente: DICAT(2020)

Reportes dicat 2017-2020

Del año 2017 hasta el 2020, DICAT recibió un total de 2221 reportes de ciberataques, de los cuales 1235 fueron por estafa vía página web. Esta forma de cibercrimen queda evidentemente comprobada como el principal medio de ataque a través de medios electrónicos en la actualidad.

En relación al CSIRT-RD, al tratar de contactarlos para la recolección de datos, notificaron que este tipo de informaciones son “de carácter sensible” y que no podían ser procesadas. En vista de estas condiciones, se optó por utilizar los gráficos estadísticos levantados por la compañía *Kaspersky* con relación a los ciberataques realizados en República Dominicana durante todo el mes de octubre del 2020.

3.4.2 - Amenazas de red

Figura 3.1: Gráfico de amenazas de red en República Dominicana.
Fuente: (Kaspersky,2020)

Troyanos

- Representan el **94.62%** de las amenazas web más comunes en la República Dominicana según *Kaspersky*, ocupando 9 de los 10 Puestos en esta categoría.
- Un Troyano es un malware que aparenta ser un programa inofensivo, pero busca perjudicar el dispositivo infectado.
- Los troyanos más comunes detectados son:

1. **Trojan.Script.Generic** (69.39%). Clasificación genérica de malware que contiene scripts Troyanos.

2. **Trojan-Downloader.Win32.Upatre.sfs** (13.3%). Caracterizados por su compacto tamaño menor a 3.5KB. Se limitan a descargar otros Malware, principalmente troyanos bancarios.
3. **Trojan.Script.Miner.gen** (3.41%). Utilizan scripts para minar criptomonedas sin el conocimiento ni consentimiento del usuario.
4. **Trojan.Multi.Preq.gen** (2.66%). Consisten de POST request a sitios web maliciosos.
5. **Backdoor.HTTP.TeviRat.gen** (2.08%). Consisten de GET request hechas por la familia de malware Backdoor.Win32.TeviRat. Buscan obtener acceso remoto.
6. **Trojan-PSW.Script.Generic** (1.87%). Roban cookies y credenciales de sitios web.
7. **Trojan.PDF.Badur.gen** (1.57%). Documento PDF que contiene enlaces a sitios de contenido cuestionable.
8. **Trojan-Clicker.HTML.Iframe.dg** (1.31%). Abre paginas web en el navegador sin el permiso del usuario. Estas páginas pueden contener malware adicional.
9. **Trojan.Script.Redirector.gen** (0.69%). Contiene scripts que redirigen al usuario a sitios maliciosos con la meta de realizar ataques de phishing.
10. **Trojan-Downloader.JS.Inor.a** (0.42%). Son scripts maliciosos de JavaScript, utilizados para descargar o incrustar malware JavaScript en páginas HTML.

3.4.3 - Ataques de Redes

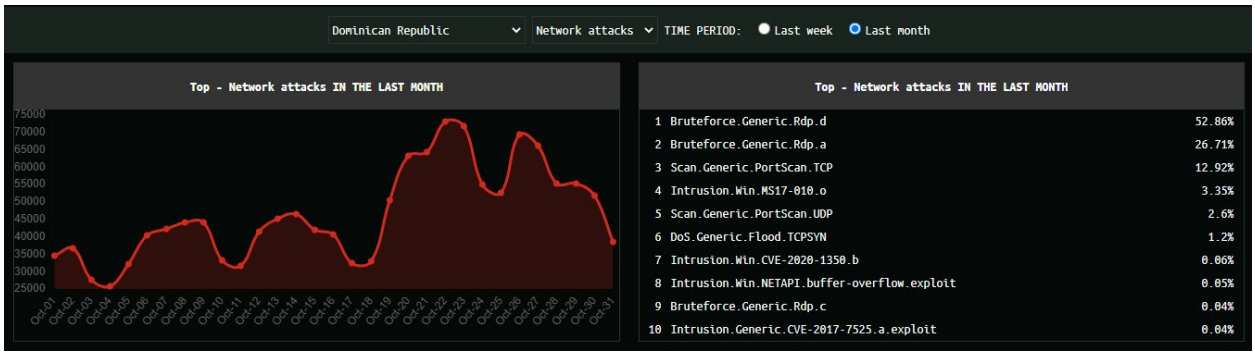


Figura 3.2: Gráfico de Ataques a redes en República Dominicana.
Fuente: (Kaspersky,2020)

- **Bruteforce.Generic.RDP**
    - Corresponden al **79.61%** de los ataques de redes más comunes en la República Dominicana según Kaspersky.
    - Bruteforce: Son ataques que tratan de adivinar las contraseñas utilizando un programa que intenta todas las combinaciones de caracteres posibles
    - RDP: Remote desktop protocol: es el protocolo de microsoft para conectarse a una pc de forma remota
    - Utilizan estos fuerza bruta para tratar de acceder remotamente a computadoras.
    - Estos ataques aumentaron en popularidad significativamente, después de la pandemia del COVID-19
- **SCAN.GENERIC.PORTSCAN (.TCP y .UDP)**
    - Corresponden al **15.52%** de los ataques de redes más comunes en la República Dominicana según kaspersky
    - Port Scanning. Es un proceso donde la mandan diferentes request a una computadora para ver cuáles puertos están abiertos.
    - Los ataques de Escaneo de Puertos no son dañinos por sí mismos pero suelen ser utilizados como parte de otros ataques.

- **Intrusiones**
    - Una intrusión trata de explotar sistemas, vulnerables o mal configurados, a través de una red para ejecutar código y otras actividades de redes no autorizadas
    - INTRUSION.WIN.MS17-010
        - Corresponden al **3.35%** de los ataques de redes más comunes en la República Dominicana según Kaspersky
        - Es un ataque que explota la vulnerabilidad llamada **Eternal Blue** de Windows y permite que se ejecute código arbitrario con el nivel más alto de permisos.
        - Eternalblue fue la principal vulnerabilidad que permitió la ejecución de los ataques *Ransomware 'WannaCry'* en 2017.
        - La vulnerabilidad fue parcheada, pero todavía hay muchos dispositivos expuestos
    - INTRUSION.Win.NETAPI.buffer-overflow.exploit
        - Corresponden al **0.05%** de los ataques de redes más comunes en la República Dominicana según Kaspersky
        - Explota la vulnerabilidad 'NetAPI buffer overflow' de Windows para cargar malware y transmitirlo a otros dispositivos *host* vulnerables a través de una red
        - El malware Net-Worm.Win32.Kido se aprovechó de este tipo de ataque para esparcirse a través de una red.
- **DOS.GENERIC.FLOOD.TCPSYN**
    - Corresponden al **1.2%** de los ataques de redes más comunes en la República Dominicana según Kaspersky
    - Es un ataque de denegación de servcio (DoS) dirigido a servidores.
    - Realiza varias solicitudes SYN (*initial connection request*), para sobrecargar los puertos del servidor blanco, alentando o previniendo totalmente las respuestas de este al tráfico legítimo.

3.4.4 - Vulnerabilidades más explotadas

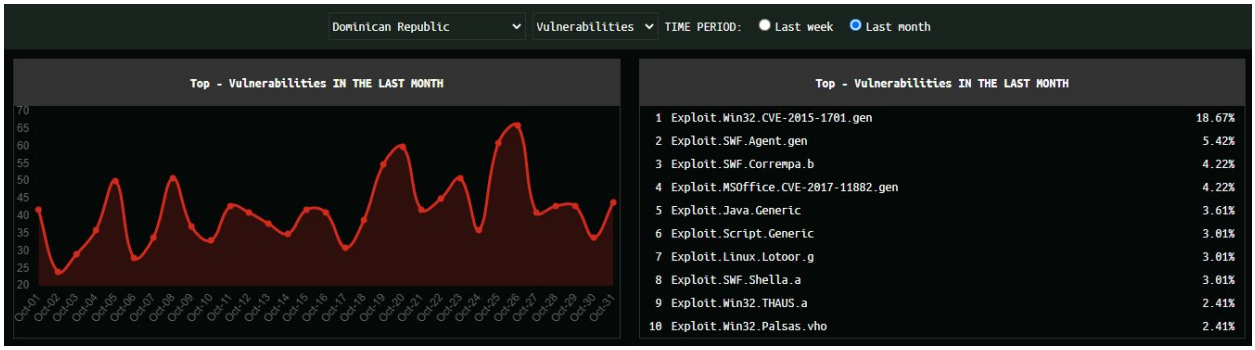


Figura 3.3: Gráfico de vulnerabilidades en República Dominicana.
Fuente: (Kaspersky,2020)

Exploits

- El nombre proviene del verbo inglés explotar, que significa “usar algo en beneficio propio”.
- Son fragmentos de software / secuencia de comandos que se aprovecha de un error o vulnerabilidad en una aplicación o un sistema para provocar un comportamiento no intencionado o no anticipado.
- Las personas con intenciones maliciosas emplean este tipo de métodos para penetrar en el equipo de la víctima con el fin de instalar posteriormente código malintencionado (por ejemplo, para infectar a todos los visitantes de un sitio web comprometido con un programa malintencionado).

1. **Exploit.WIN32.CVE-2015-1701**
    a. Corresponde a **18.67%** de las vulnerabilidades más comunes en la República Dominicana según Kaspersky.
    b. Este malware tiene como objetivo penetrar en los dispositivos de su posible víctima y **robar datos o inyectar publicidad no autorizados**.

c. También se conoce como *Win32/Trojan.Exploit.470* o *Generic Trojan.ir*
d. Es común entre personas que no tienen un antivirus en tiempo real

2. Exploit.SWF.Agent.gen (Blue termite)

a. Corresponde a **5.32%** de las vulnerabilidades más comunes en la República Dominicana según Kaspersky.
b. Consiste en una campaña de ciberespionaje con creciente popularidad en Asia.
c. Los atacantes buscan información confidencial de la víctima y utilizan un exploit de Flash Player de día cero y una puerta trasera (*Backdoor*) sofisticada, que se personaliza para cada víctima.
d. Es común en lugares públicos con dependencias gubernamentales o un gran número de instituciones financiera

3. Exploit.SWF.Corrempa.b

a. Corresponde a **4.22%** de las vulnerabilidades más comunes en la República Dominicana según Kaspersky.
b. Utiliza una vulnerabilidad de *Adobe* para descargar y ejecutar archivos en los dispositivos de sus víctimas, incluido el malware.
c. Esta amenaza está asociada con un kit de explotación llamado *SweetOrange.*

4. Exploit.MSOffice.CVE-2017-11882.gen

a. Corresponde a **4.22%** de las vulnerabilidades más comunes en la República Dominicana según Kaspersky.
b. Esta vulnerabilidad explota el *Microsoft Equation Editor*, que es un componente de *Microsoft Office*, contiene una vulnerabilidad de

desbordamiento del búfer de pila que permite la ejecución remota de código en un sistema vulnerable.

c. Común en personas que no poseen versiones actualizadas del paquete de *Microsoft office*.

5. **Exploit.Java.Generic**
    a. Corresponde a **3.61%** de las vulnerabilidades más comunes en la República Dominicana según Kaspersky.
    b. identifica los archivos de explotación que se utilizan para apuntar y explotar vulnerabilidades en Java Runtime Environment (JRE).
    c. Si se utilizan con éxito, los exploits pueden proporcionar al atacante una amplia gama de posibles acciones, desde ver datos en una base de datos de usuarios restringidos hasta un control casi completo de un sistema comprometido.
    d. Los archivos de explotación pueden ser entregados por otros malwares populares mencionados anteriormente en el documento.

6. **Exploit.Script.Generic**
    a. Corresponde a **3.01%** de las vulnerabilidades más comunes en la República Dominicana según Kaspersky.
    b. Las aplicaciones de este tipo son *scripts* maliciosos que intentan aprovechar las vulnerabilidades del software del sistema.
    c. Se distribuye al mundo con la ayuda de la red.
    d. Los ciberdelincuentes implantan esta amenaza en algunos sitios web de phishing, que parecen muy similares a las páginas web legítimas reales.

7. **Exploit.Linux.Lotoor.g**
    a. Corresponde a **3.01%** de las vulnerabilidades más comunes en la República Dominicana según Kaspersky.
    b. Es un software condicionalmente malicioso que otorga privilegios de superusuario al usuario en dispositivos que ejecutan el sistema

operativo *Android* mediante la explotación de una vulnerabilidad en el sistema de seguridad (CVE-2009-1185).

8. **Exploit.SWF.Shella**
    a. Corresponde a **3.01%** de las vulnerabilidades más comunes en la República Dominicana según Kaspersky.
    b. Está diseñado para crear nuevos virus, gusanos y troyanos utilizando el dispositivo infectado de la víctima.

9. **Exploit.Win32.THAUS**
    a. Corresponde a **2.41%** de las vulnerabilidades más comunes en la República Dominicana según Kaspersky.
    b. Está conformado por objetos maliciosos que aprovechan una vulnerabilidad en el protocolo SMB implementado en Windows.
    c. Si un ataque tiene éxito, el atacante obtiene la capacidad de ejecutar algún código como usuario del "sistema".

10. **Exploit.Win32.Palsas.vho**
    a. Corresponde a **2.41%** de las vulnerabilidades más comunes en la República Dominicana según Kaspersky.
    b. Funciona de manera similar al Exploit.Win32.THAUS, con diferencias mínimas en las puertas traseras que utiliza.

Capítulo 4

Implementación de controles de ciberseguridad para las redes públicas

4.1 - Marco de control de ciberseguridad sugerido para las redes públicas de internet para plazas comerciales y aeropuertos.

4.1.2 - Cuadro de vulnerabilidades

En este primer cuadro se menciona todas las vulnerabilidades que se consideran relevantes en las conecciones de red inalámbricas de carácter público

ID	Vulnerabilidad	Descripción
V-01	Configuraciones por defecto no cambiadas	Las contraseñas por defecto de routers wi-fi son muy conocidas y fáciles de encontrar en repositorios web. Utilizar dichas credenciales aumenta la probabilidad de éxito de ataques de fuerza bruta entre otros.
V-02	Utilización de rangos de señal altos	El uso de puntos de acceso con rangos de señal elevados puede facilitar que los atacantes puedan realizar acciones maliciosas desde fuera de la localidad.
V-03	Falta de comunicación con lo usuarios en respecto a amenazas	Tanto los usuarios corporativos como los comerciales tienen que ser informados de los peligros a los que se exponen al no conectarse a la red principal del lugar o al presentarse una falla dentro del sistema de red. Esto teniendo en cuenta el grado de exposición de información de la red
V-04	Diversificación de puntos de acceso ajenos a la red principal	La presencia de puntos de acceso pertenecientes a empresas afiliadas dentro del espacio público puede afectar fundamentalmente la fuerza de la señal de la red principal del lugar y a su vez facilitar la aparición de rogue AP.
		Las redes abiertas se refiere a redes wi-fi que no requieren autenticación para que los usuarios tengan acceso a esta. Aunque este tipo de red tradicionalmente son una

V-05	Red abierta	necesidad para un servicio de Wi-Fi público a gran escala, presentan una vulnerabilidad debido a que ataques como el Man-in-the-middle son más fácil de realizar en este tipo de redes comparado con redes cerradas y protegidas por contraseña. Existen alternativas a este tipo de redes, como Passpoint (**AC-05**).
V-06	Conexión automática a puntos de acceso	La mayoría de los sistemas operativos están configurados para conectarse al punto con mayor intensidad de señal, en caso de que haya varios puntos asociados al mismo SSID. En presencia de un gemelo malvado, si la fuerza de la señal del gemelo excede la señal del punto genuino, los clientes se asocian con el gemelo automáticamente
V-07	Utilización de HTTP	El Protocolo HTTPS es una extensión del HTTP, este provee una encriptación bidireccional de las comunicaciones entre un cliente y un servidor, previniendo que los datos sean interceptados u modificados. Aunque la mayoría de los sitios web utilicen HTTPS, no todos lo hacen por defecto y otros son susceptibles a ataques de degradación.
V-08	Puntos de acceso en ubicaciones vulnerables	Dispositivos de Punto de acceso en lugares de fácil alcance físico, donde pueden ser manipulados por empleados no autorizados o actores maliciosos externos. Un puerto expuesto puede ser robado o destruido,

		reiniciado totalmente, o utilizado para instalar Rogue APs (**ATK-05**) en sus puertos abiertos.
V-09	Cobertura de Señal Insuficiente	Si existen sitios en en local donde no la señal de l a red inalámbrica es insuficiente, podría llevar a la creación de Puntos de Acceso no autorizados tanto por empleados que deseen tener acceso en esas áreas como actores maliciosos que buscan tomar ventaja de la situación.
V-10	Protocolos no actualizados	Los protocolos antiguos como el WEP, WPA y WPA2, son muy poco seguros, debido a que a través de los años se han descubiertos numerosos problemas de seguridad en estos estándares, las cuales son conocidas y explotadas por atacantes.

Tabla 4.1: Cuadro de vulnerabilidades

4.1.2 - Cuadro de riesgo de ataques

El siguiente cuadro expresa el nivel de probabilidad de que un ataque se produzca dentro de un espacio público. A su vez, se expresan el nivel de impacto dentro de la estructura de red y su nivel de riesgo (Probabilidad + impacto). Esto se realiza tomando en cuenta lo siguiente:

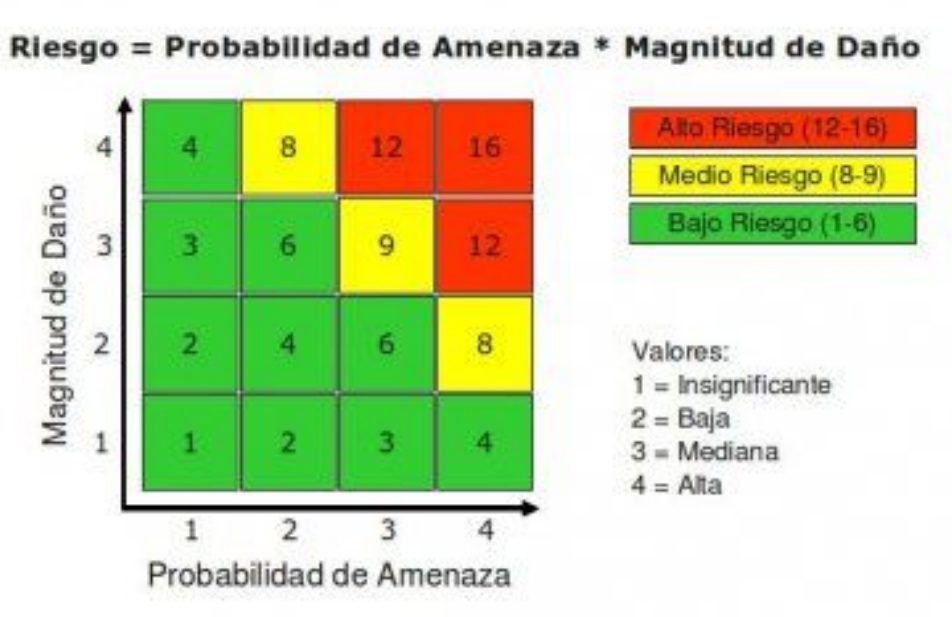


Figura 4.1: Matriz de riesgo.

Fuente: (Velazquez, 2011)

Id	Ataques	Probabilidad	Magnitud de daño	Riesgo
ATK-01	Man-in-the-Middle	**Media (3)**	**Alto (4)**	**Alto (12)**
ATK-02	Ataque de Fuerza Bruta	**Baja (2)**	**Alto (4)**	**Medio (8)**
ATK-03	Espionaje (Packet-Sniffing)	**Baja (2)**	**Medio (2)**	**Bajo (4)**
ATK-04	Denegacion de Servicio	**Baja (2)**	**Alto (4)**	**Medio (8)**
ATK-05	Puntos de Acceso no Autorizados	**Media (3)**	**Alto (4)**	**Alto (12)**

ATK-06	Gemelos malvados	**Baja (2)**	**Alto (4)**	**Medio (8)**
ATK-07	Session Hijacking (ARP Spoofing)	**Baja (2)**	**Medio (3)**	**Bajo (6)**
ATK-08	Manipulación Física de puntos de acceso	**Media (3)**	**Medio (3)**	**Medio (9)**
ATK-09	Ingenieria Social	**Media (3)**	**Bajo (2)**	**Bajo (6)**
ATK-10	Malware	**Baja (2)**	**Medio (3)**	**Bajo (6)**
ATK-11	Ataque KRACK	**Media (3)**	**Medio (3)**	**Medio (9)**

Tabla 4.2: Cuadro de riesgo de ataques

4.1.3 - Cuadro de descripción de controles

En el siguiente cuadro se presentan los controles de seguridad sugeridos que, al momento de la realización de este trabajo de investigación, se consideran los más adecuados a integrar a una localización pública (Plazas y/o aeropuertos).

ID	Control	Tipo de acción	Descripción
			Los puntos de acceso no deben

CS-01	Cambio de configuración por defecto	Preventiva	tener credenciales por defecto, debido a que estas ya son ampliamente conocidas por atacantes. Antes de ser desplegados, los puntos de acceso deben ser configurados con usuarios no genéricos, SSID y contraseñas adecuadas (véase **AC-18**). Además los puntos de acceso no deben compartir credenciales unos con otros.
CS-02	Autenticación 802.1x	Preventiva	Es un método utilizado mundialmente para la autenticación de dispositivos debido a sus sólidas medidas de seguridad. 802.1x incluye el uso de un servidor RADIUS[8] para autenticar y autorizar los dispositivos que pidan acceso a la conexión. Los servidores RADIUS están integrados con los servicios de directorio de la red para que sepa a quién aprobar y rechazar.
			El sistema inalámbrico de prevención de intrusiones (o WIPS por sus siglas en inglés), es un sistema que está

[8] ***Servidor RADIUS**: es un protocolo que ofrece un mecanismo de autenticación de usuarios para acceder a un recurso compartido. Pasado este proceso, permite autorizar a un usuario a dicho recurso.*

CS-03	Implementación de WIPS	Preventiva	diseñado con fin de prevenir ataques de Man-in-the-Middle porque el sistema analiza todos los puntos de acceso a la red y alerta a la red cuando encuentra un punto de acceso no autorizado. Básicamente, si WIPS detecta un *Rogue AP*[9] en la red, evitará que se difunda el SSID, evitando que ocurran ataques MITM en su campus.
CS-04	Reemplazo de credenciales con certificados digitales	Preventiva	Los certificados digitales eliminan el factor de riesgo humano que se asocia a las contraseñas. El uso de un certificado hace que este permanezca equipado en un dispositivo y no se puede compartir.
CS-05	Implementación de *Passpoint*	Preventiva	Es una tecnología Wi-Fi que permite a los usuarios conectarse de forma segura y automática a puntos de acceso Wi-Fi. Para que este sea implementado correctamente, los dispositivos deben

[9] ***Rogue AP**: Es un punto de acceso no autorizado que se instala en una red segura sin la autorización explícita de un administrador de red local, este puede ser agregado por un empleado de manera inofensiva o por un atacante malintencionado.*

			configurarse con la ID única del SSID, y el propietario de los puntos de acceso necesita un servidor de registro en línea (OSU por sus siglas en inglés).
CS-06	Verificación de las configuraciones de TLS / SSL	Reactiva	Deshabilitar los algoritmos más antiguos dentro del sistema o el cifrado y la autenticación que sean considerados débiles en referencia a los estándares más actuales, como **NULL, RC4, 3DES, MD5 y SHA1,** junto con las versiones anteriores de los protocolos, como las versiones **SSL y TLS anteriores a la v1.2**.
CS-07	*HTTP Strict Transport Security (HSTS)* [Seguridad de transporte estricto]	Reactiva	Mitiga los ataques a los servidores al permitir que los sitios web sean accesibles sólo a través de HTTPS mediante la utilización de filtros.
CS-08	Agregar entradas ARP[10] estáticas a la caché	Reactiva	Este método evita que los atacantes puedan efectuar solicitudes y respuestas ARP, ya que los dispositivos de la red dependen de la caché local.
			Bloquear cuentas después de un

[10] ***ARP(Address Resolution Protocol)****: es un protocolo de comunicaciones utilizado para resolver direcciones de red (como IPV4 e IPV6) y físicas (como una dirección MAC) a través de la capa de enlace de datos.*

CS-09	Bloqueo de cuentas	Reactiva	número definido de intentos de contraseña incorrectos. Se recomienda una duración específica de **una hora como máximo**. las cuentas pueden permanecer bloqueadas hasta que un administrador las desbloquee manualmente. Esta acción también se puede llevar a cabo en un esquema de delay progresivo en el cual se incrementa el tiempo de bloqueo con cada intento fallido.
CS-10	Uso de CAPTCHAS	Preventiva	CAPTCHA, es un programa que permite distinguir entre humanos y máquinas. son particularmente efectivos para detener cualquier tipo de abuso automatizado, incluidos los ataques de fuerza bruta.
CS-11	Aislamiento de Clientes Inalámbricos	Preventiva	El aislamiento de clientes inalámbricos es una función de seguridad que evita que los clientes, los dispositivos de los usuarios conectados a la red, se comuniquen entre sí. Esta función es útil para limitar los ataques y las amenazas entre los dispositivos conectados a

			redes inalámbricas
CS-12	Uso de Autenticación de dos factores (2FA)	Preventiva	2FA agrega otra capa de seguridad al formulario de inicio de sesión a la red. Una vez que se inicie sesión con las credenciales correctas, se debe ingresar un código al que solo el solicitante pueda acceder, como un correo electrónico o un código único generado por una herramienta de autenticación.
CS-13	Uso de *Anti Sniffers*	Preventiva	Software y hardware diseñados para detectar el uso de rastreadores (*Sniffers*) en una red. Dicho software y hardware no elimina por completo la amenaza, pero como muchas herramientas de seguridad de red, son parte del sistema general. Se encargan de detectar cambios en el tiempo de respuesta de los hosts para determinar si los hosts están procesando más tráfico que el de la misma herramienta.
CS-14	Educar sobre los riesgos	Preventiva	Consiste en la creación de banners, tanto físicos como virtuales que alerten a los usuarios corporativos y

	de seguridad a usuarios		comerciales sobre los peligros asociados a potenciales amenazas asociadas a ingeniería civil, puntos de acceso sospechosos y/o alteraciones dentro de la red.
CS-15	Limitación de la intensidad de la señal de los enrutadores Wi-Fi	Preventiva	Los dispositivos móviles y las computadoras portátiles no tienen antenas de alta ganancia, por tanto, no es necesario utilizar señales de largo alcance. En este caso, si un usuario está fuera de la plaza o aeropuerto, la red wifi se vuelve prácticamente inaccesible.
CS-16	Posicionamiento de puntos de acceso en zonas estratégicas.	Preventiva	Con esta medida se sugiere la colocación de los enrutadores y puntos de acceso de la red en lugares donde la señal se distribuya de manera uniforme y que a su vez se encuentre aparentemente inaccesible para los usuarios de la localidad o personal no autorizado, como paredes o techos.
			Esta acción permite configurar los tiempos disponibles para cada SSID dentro de la red. Los puntos de acceso habilitarán o

CS-17	Planificación de actividad para la red wifi	Preventiva	deshabilitarán el SSID durante el proceso de registro. El SSID se habilita o deshabilita durante el primer registro después del tiempo especificado, generalmente dentro de cinco o diez minutos. Para esta acción se puede tomar en cuenta los protocolos **IEEE 802.11k-2008 (sobre la medición de recursos de radio)** y **IEEE 802.11r-2008 (sobre conectividad continua entre puntos de acceso)**
CS-18	Utilización de contraseñas robustas	Preventiva	Se debe asegurar que las contraseñas sean lo suficientemente complejas para que los atacantes no puedan adivinarlas fácilmente. La NIST recomienda utilizar contraseñas de por lo menos caracteres, utilización de puntuación/caracteres especiales, alternar entre letras mayúsculas y minúsculas. Se deben evitar contraseñas default, palabras comunes, fechas y secuencias sencillas. Mientras que una contraseña compleja reduce el riesgo de

			ataques, también dificulta la memorización por parte de los usuarios. Es recomendable la utilización de un gestor de contraseñas para facilitar el uso de contraseñas complejas y diferentes entre dispositivos.
CS-19	Monitoreo de registros de acceso	Detectora	Consiste en mantener y monitorear un registro de acceso a las configuraciones de los APs para identificar accesos autorizados y realizar revisiones a la configuración.
CS-20	Monitoreo del tráfico de la red	Detectora	Consiste en la utilización y la implementación *sniffers y* analizadores de tráfico dentro del periferico de la red, al igual que el tipo y origen de este, para detectar tráfico sospechoso potencialmente malicioso que esté siendo transmitido en la red.
CS-21	Actualización de firmware	Correctiva	Mantener una política de actualización para actualizar el firmware de los dispositivos de red de manera oportuna según actualizaciones de seguridad sean lanzadas cuando se descubran nuevos fallos o

			vulnerabilidades o se implementen nuevos protocolos de seguridad.
CS-22	Seguridad Física de los Puntos de Acceso	Preventiva	En adición a la ubicación estratégica de los puntos de acceso (AC-16) estos deben tener algún encerramento físico, que oculte el punto, y prevenga la manipulación física (Apagado, reiniciado), y proteja sus puertos abiertos de actores no autorizados.
CS-23	Utilizar protocolo WPA3	Preventiva	WPA3 es el estándar de seguridad Wi-Fi más reciente, diseñado para corregir las faltas del protocolo anterior, WPA3. Incluye medidas de protección contra ataques de fuerza bruta y los ataques intermediarios más comunes, ya que permite encriptar la conexión entre usuarios y Puntos de Acceso aún en redes abiertas sin contraseña. Se recomienda la adquisición de dispositivos que soporten este estándar al igual que la actualización del firmware los dispositivos presentes si existen dichas actualizaciones.

CS-24	Segmentación de Redes	Preventiva	Las redes de negocios deben separar, ya sea física o lógicamente, sus redes de negocio de sus redes de acceso público.
CS-25	Límites de Banda Ancha	Preventiva	Consiste en limitar la cantidad bandwith que cada dispositivo individual en la red puede consumir, para asegurar una velocidad constante a todos los otros conectados a la red y mitigar la posibilidad de ataques DoS.

Tabla 4.3: Cuadro de descripción de controles

4.1.4 - Cuadro de control de Ataques

Dentro del siguiente cuadro se enlistan los controles necesarios para prevenir y/o mitigar los ataques de red más relevantes para las redes públicas acorde a los controles sugeridos gracias a nuestras investigaciones.

Id	Ataques	Controles sugeridos mas relevantes	Vulnerabilidades aprovechadas
AC-01	Man-in-the-Middle	CS-01, CS-03, CS-06, CS-07, CS-11, CS-14, CS-16, CS-20, CS-23, CS-26	V-01, V-03, V-05, V-06, V-07, V-10
AC-02	Ataque de Fuerza Bruta	CS-01, CS-10, CS-12, CS-18, CS-19, CS-23	V-01, V-02, V-10
AC-03	Espionaje (Packet Sniffing)	CS-03, CS-06, CS-07, CS-11, CS-13, CS-20, CS-23	V-02, V-03, V-05, V-07, V-10
AC-04	Denegacion de Servicio	CS-08, CS-09, CS-20, CS-23, CS-25	V-02, V-05, V-06, V-08, V-10
AC-05	Puntos de Acceso no Autorizados	CS-03, CS-05, CS-14, CS-16, CS-22	V-01, V-03, V-04, V-05, V-08, V-10
AC-06	Gemelos malvados	CS-01, CS-03, CS-05, CS-12, CS-16, CS-22	V-01, V-04, V-05, V-06, V-08
AC-07	Session Hijacking (ARP Spoofing)	CS-03, CS-07, CS-08, CS-11, CS-20, CS-23	V-03, V-05, V-10
AC-08	Manipulación física de puntos de acceso	CS-16, CS-22	V-04, V-08

AC-09	Ingenieria Social, Phishing	CS-14	V-03, V-04, V-07
AC-10	Malware	CS-03, CS-11, CS-14, CS-20, CS-24	V-03, V-05, V-10
AC-11	Ataque KRACK	CS-01, CS-06, CS-07, CS-11, CS-21, CS-23	V-01, V-02, V-05, V-07, V-10

Tabla 4.4: Cuadro de control de ataques

4.2 - Integración orgánica de controles de ciberseguridad en Puntos de acceso público existentes

4.2.1 - Marco de retroalimentación de controles de ciberseguridad

Para que se tomen en cuenta los controles de seguridad previamente mencionados y se puedan implementar como un estándar para redes públicas pertenecientes a centros comerciales y aeropuertos a nivel de distrito, se plantea que partir desde una distribución a base de una institución gubernamental como el **CSIRT-RD**, es la mejor opción posible, ya que a diferencia de las demás instituciones mencionadas en este documento, esta no forma parte de ningún organismo particular, y no tiene connotaciones distintas o divariantes de lo que es su principal enfoque: la ciberseguridad a nivel nacional.

En relación a dicha premisa, se entiende que la información recaudada luego de que se implemente el marco de controles de ciberseguridad puede almacenarse en dicha institución con fines de balanceo y refinamiento de medidas en concordancia con las necesidades y amenazas que surjan gracias a nuevas tecnologías emergentes. Tomando ventaja de esto, se plantea el siguiente diagrama de retroalimentación:

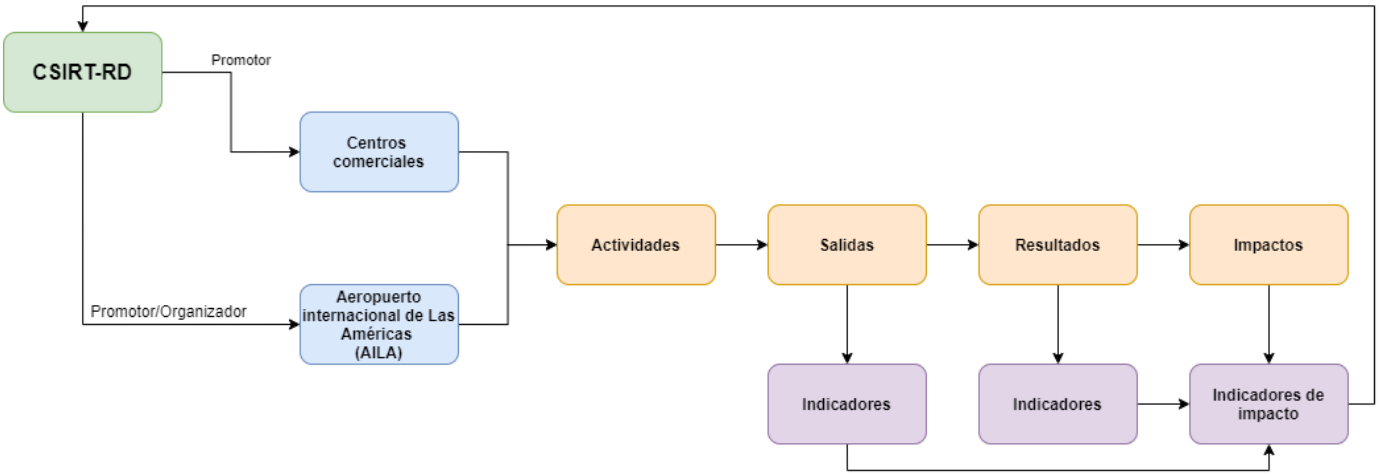


Figura 4.2: Diagrama de Retroalimentación de distribución.

Fuente: Elaboración Propia

Se estima que bajo este esquema la CSIRT-RD pueda obtener datos de retroalimentación en un periodo **mensual**. Cada localidad tendrá la responsabilidad de asignar un equipo de reporte y recolección de datos que se contacte directamente con la institución cuando ésta los requiera.

4.2.2 - Marco de Distribución de controles de ciberseguridad

Dentro de lo que se comprende como el área distrital de Santo Domingo se reconocen como espacios públicos de carácter comercial a **16 lugares en el gran Santo domingo** y 10 en Santo Domingo Este, mientras que a nivel de aeropuertos con espacios comerciales, se reconoce solo al AILA[11]

[11] ***AILA***: Acrónimo para el Aeropuerto Internacional de Las Américas, una de las principales terminales aéreas de la República Dominicana. Ocupa el segundo lugar en cuestión de flujo de pasajeros regulares a nivel del país.

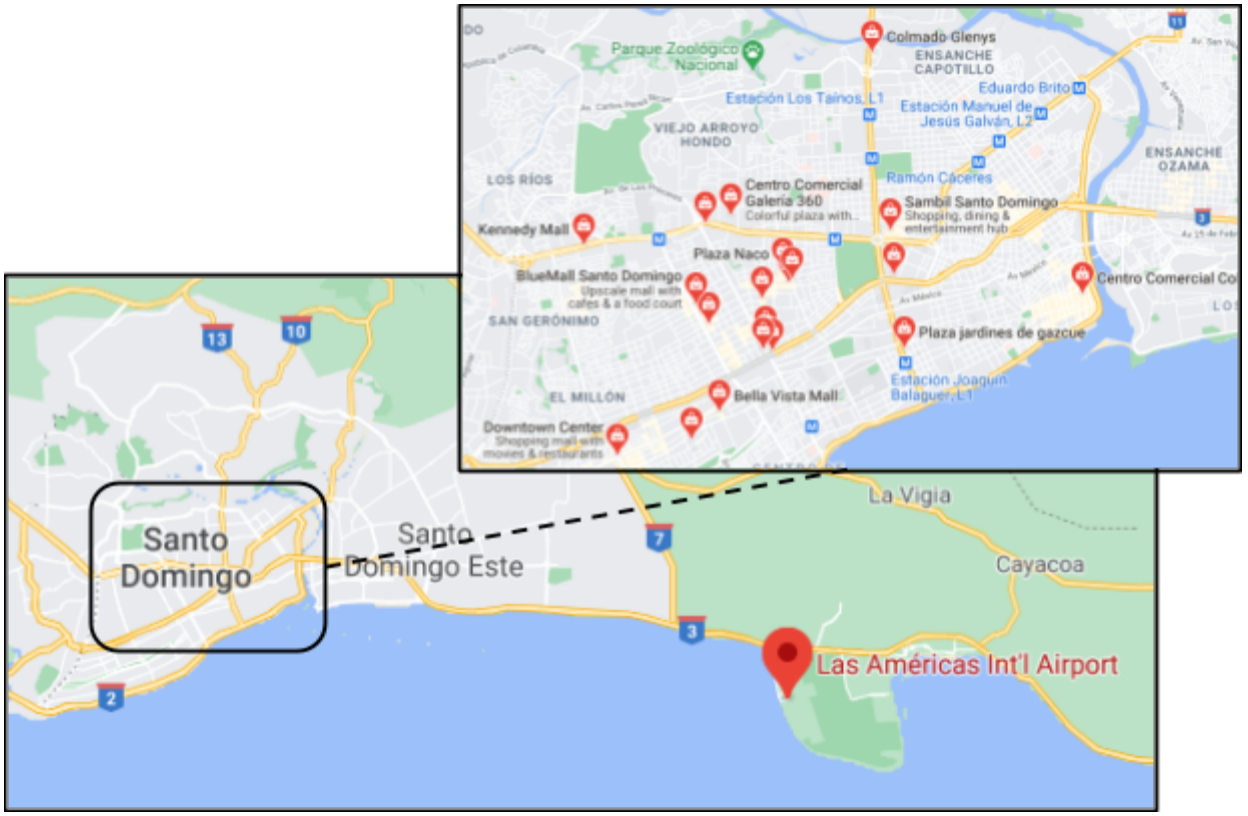


Figura 4.3: Mapa de centros comerciales y aeropuertos correspondientes al área del gran Santo Domingo.
Fuente:(Google maps, 2020).

Correspondiente al área del gran Santo Domingo, se encuentran los siguientes centros comerciales autorizados:

- Sambil
- Agora Mall
- Galeria 360
- BlueMall
- Acrópolis Center
- Centro Comercial Colón
- Kennedy Mall
- Novo Centro

- Unicentro Plaza
- Commercial Plaza 2000
- Plaza jardines de gazcue
- Downtown Center
- Plaza Alexandra
- Bella Vista Mall
- Plaza Naco
- Silver Sun Gallery

Dentro de esta zona, se consideran como puntos vitales estratégicos las plazas: **Ágora Mall**, **Sambil** y **BlueMall** por su alto nivel de concurrencia y popularidad, según Google maps (2020). Tomando esto como referencia, se recomienda que la fase de pruebas para la implementación de estos controles de ciberseguridad se empiece con estos lugares.

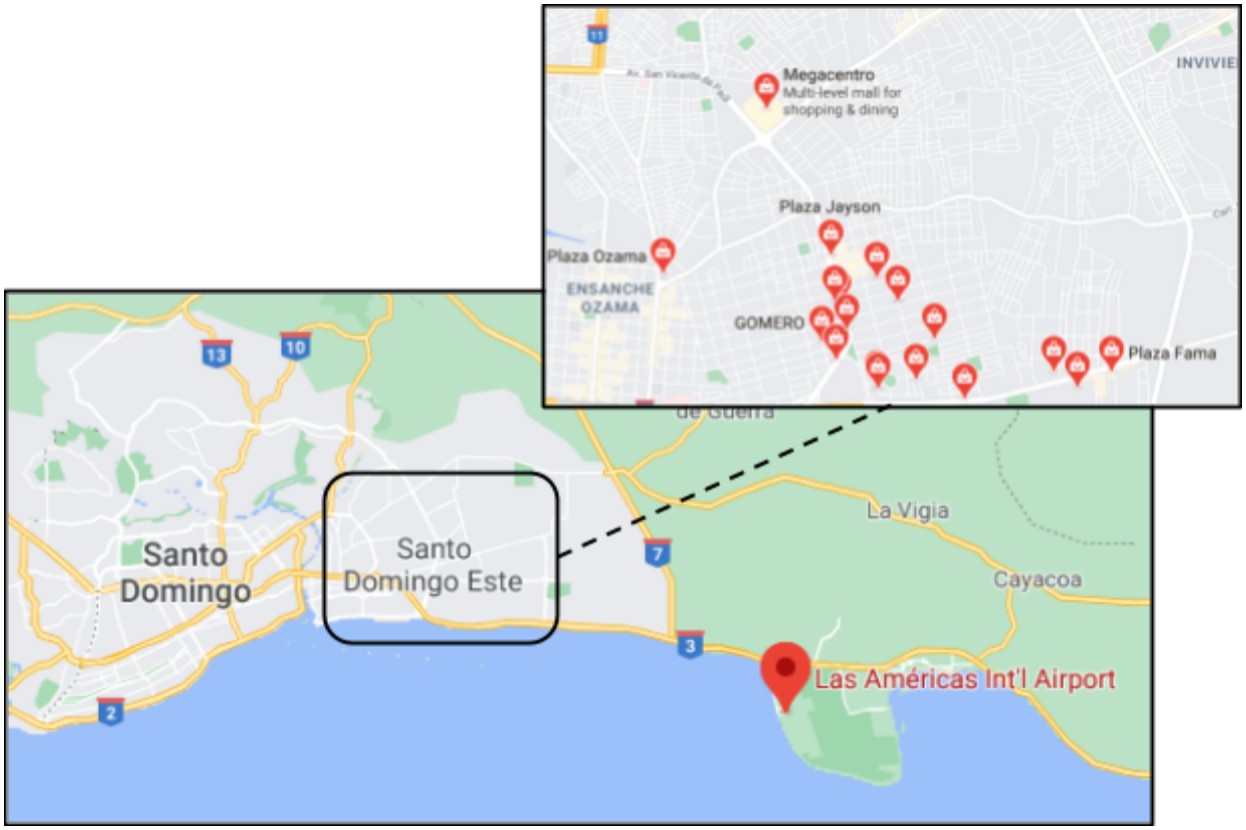


Figura 4.4: Mapa de centros comerciales y aeropuertos correspondientes al área de Santo Domingo Este.
Fuente:(Google maps, 2020).

Correspondiente al área del gran Santo Domingo, se encuentran los siguientes centros comerciales autorizados:

- Megacentro
- Coral Mall
- Baro Plaza
- Plaza Alma Rosa
- Plaza bonaire
- Plaza Ozama
- Plaza Marena
- Plaza Fama
- Plaza Villa España
- City Center San Isidro

Dentro de esta zona, se consideran como puntos vitales estratégicos las plazas: **Megacentro**, **Coral Mall** y **Plaza Fama** por su alto nivel de concurrencia y popularidad según Google maps (2020). Tomando esto como referencia, se recomienda que la fase de pruebas para la implementación de estos controles de ciberseguridad se empiece con estos lugares.

4.2.3 - Marco para fases de despliegue

Se entiende que para el despliegue de el presente marco de ciberseguridad sea de manera efectiva, este tiene que ser seccionado en fases de la siguiente forma:

Fase	Gran Santo Domingo	Santo Domingo Este
0 (de prueba)	Ágora Mall, Sambil y BlueMall	Megacentro, Coral Mall y Plaza Fama
1 (Inicial)	Galería 360, silver sun gallery, downtown center y Novo Centro	Plaza Bonaire, plaza Ozama y city center San Isidro
2 (intermedia)	Acrópolis Center, Bella Vista Mall, Plaza Naco y Unicentro plaza	Baro plaza y plaza Alma Rosa
3 (Despliegue total)	Centro Comercial Colón, Kennedy Mall, Comercial Plaza 2000, Plaza Jardines de Gazcue y Plaza Alexandra	Plaza Marena y plaza Villa españa

4.2.3 - Marco para fases de despliegue

En relación al AILA, se comenzará a trabajar con este espacio a partir de la fase 1 de despliegue, luego de recibirse los datos de retroalimentación levantados de la fase 0.

4.3 - Impacto y resultados esperados de la implementación de la Propuesta

Mediante el análisis de vulnerabilidades que afectan las redes públicas de aeropuertos y plazas comerciales hemos implementado controles de ciberseguridad rígidos en busca de mitigar ataques a las redes. Los crímenes de alta tecnología han ido aumentando a través del tiempo con nuevas técnicas por lo que la seguridad informática cada día tiene un papel más importante en la informática.

Los controles propuestos en este trabajo de investigación buscan tener un impacto positivo inmediato en la infraestructura de las redes inalámbricas de estos espacios, que son de alta prioridad para la economía.

Los resultados que se esperan tras implementar los controles de ciberseguridad que se han definido son:

- Mitigar los ataques cibernéticos a redes inalámbricas públicas en plazas y aeropuertos.

Estos ataques conllevan un gran peligro, ya que su fin principal es el robo de información que puede llevar a una gran pérdida económica para usuarios y entidades envueltas en los procesos que se realicen al utilizar la red. El impacto

económico de estos ataques, ya definidos previamente en esta investigación, pueden alcanzar grandes magnitudes si no son controlados.

- Proteger la información personal de cada usuario que esté navegando por la red, así como también la compañía que ofrezca este servicio.
- Crear una base para la infraestructura de la seguridad informática en otros sectores públicos que no posean controles.
- Educar a los usuarios a cómo navegar de una forma más segura por el internet, ya que muchos ataques pueden prevenirse con la concientización adecuada.
- Utilizar la información recolectada de los reportes generados de vulnerabilidades para fortalecer la seguridad informática en la República Dominicana

Descripción	Indicadores	Fuentes de verificación
Mitigar ciberataques en espacios públicos	Número de ataques a las redes reducidos.	Datos de retroalimentación, Registros de ataques y vulnerabilidades [DICAT]

Tabla 4.6: Indicadores de impacto

Conclusiones

En relación a todas las soluciones de ciberseguridad que se presentan en el país a través de instituciones públicas y privadas, no se pudo encontrar dentro de los registros de visibilidad pública parámetros que cubran específicamente las necesidades de protección cibernética que poseen los espacios públicos. El aspecto más crítico que se pudo encontrar es en la respuesta a los reportes de ataques, ya que según menciona Dawson (2018) en su investigación:

> *"En 2017, había aproximadamente 42 uniformados[Policías] y civiles dedicados a la ciberseguridad. Sin embargo, están titulados principalmente usuarios de aplicaciones que en lugar de desarrolladores. Por lo tanto, si hubo ataques más severos a la infraestructura en forma de malware, gusanos, etc., nadie tenía el conocimiento para hacer ingeniería inversa. Ni el personal de esta división podría realizar análisis de código de bajo nivel o asesorar a una empresa sobre prácticas de codificación seguras para garantizar que estén más seguras una vez que implementen su Además, hay talento en ciberseguridad en el personal de servicio gubernamental y desinformado."*

Por tanto, es vital que para la mitigación y control efectivo de cualquier tipo de amenaza de esta índole, se vea necesaria la capacitación y reclutamiento de personal competente y actualizado con las últimas novedades en materia de seguridad informática. En adición a esta premisa, es importante que también se considere que para que una nación y/o organización esté preparada para responder ante las necesidades de la seguridad cibernética, es necesario que la necesidad se perciba en los niveles más altos de gobierno. Debe haber un marco integral que cree una atmósfera de uniformidad entre el gobierno y las entidades comerciales.

En relación a la medidas de ciberseguridad más reciente tomada por el gobierno, el decreto no. 230-18, es vital que se te tome más en cuenta el pilar de la educación ciudadana en cuestión formación de conocimientos preventivos, ya que como se pudo notar en las estadísticas levantadas por *Kaspersky* , gran parte de las amenazas principales en el país tienen que ver con la facilidad con la que los ciudadanos dominicanos pueden acceder a links, paginas y/o redes maliciosas.

Esta última premisa, en conjunto con la facilidad de realizar cibercrimen desde cualquier punto del país y en evidente apreciación de que los lugares públicos como los centros comerciales y los aeropuertos son zonas con gran posibilidad de impacto por parte de e individuos con intenciones maliciosas, se recomienda al gobierno dominicano y a las empresas privadas la elaboración de un marco de seguridad informática con enfoque primordial en este tipo de espacios.

Por último, es vital señalar que en República Dominicana la falta de acceso de información sobre ciberseguridad a nivel nacional es un problema de carácter crítico. Se entiende que a causa del nivel de importancia del internet en la presente era, los ciudadanos dominicanos requieren ser informados con datos estadísticos de cómo se encuentra la ciberseguridad a nivel nacional, pero la privatización de dicha información en conjunto con la descentralización de los planes de seguridad informática a través de la diversificación de instituciones, hacen imposible cubrir esta necesidad.

Recomendaciones

- ➔ Deshabilitar y bloquear todos los puertos que no están siendo utilizados, físicos como lógicos, para evitar el uso no autorizado de estos, y mitigar Rogue APs.
- ➔ Invertir en equipos de red adecuados, capaces de soportar una red de gran tamaño y tráfico, con Sistema de Detección de Intrusos (IDS).
- ➔ Configurar sus *Network Appliances,* para identificar ciertos tipos de tráfico que considere sospechoso y bloquearlo o crear alertas automáticamente.
- ➔ Utilizar un Gestor de contraseñas como *Dashlane* o *Lastpass*[12] para facilitar la utilización de contraseñas complejas, autogeneradas y evitar la reutilización.
- ➔ Establecer, límites fijos de tiempo, datos, y dispositivos a cada usuario.
- ➔ Auditar con frecuencia los registros de configuración de los equipos de red, para asegurar que las medidas de seguridad hayan sido configuradas correctamente y detectar cambios no autorizados. Herramientas de Software como *SolarWinds SEIM* [13] pueden ayudar a gestionar este proceso.
- ➔ Segmentación de redes. Utilizar VLANs (Virtual LAN) para separar las redes internas de negocio, la red de acceso público y la red de configuración de equipos de red; dando solo acceso a las funciones realmente necesarias en cada red. La red de acceso público solo debe tener acceso al internet y los clientes conectados a esta deben ser aislados, previniendo la comunicación e identificación entre estos.
- ➔ Crear un plan de Actualización de dispositivos de red para asegurarse que tengan los parches de seguridad más recientes según surjan nuevas amenazas. Un retraso de días puede tener resultados catastróficos.

---

[12] **Dashlane / Lastpass:** Son administradores de contraseñas, que ayudan a generar y recuperar contraseñas complejas.

[13] ***SolarWinds SEIM :*** Es una solución integral de gestión de eventos e información de seguridad (SIEM) diseñada para recopilar y consolidar todos los registros y eventos de firewalls, servidores, enrutadores en tiempo real.

Bibliografía

- Afaqui, M. S., Garcia-Villegas, E., & López-Aguilera, E. (2016). IEEE 802.11 ax: Challenges and requirements for future high efficiency WiFi. IEEE Wireless Communications, 24(3), 130-137. Recuperado de: https://ieeexplore.ieee.org/document/7792393

- Agyemang, J., Kponyo, J. & Logo, G. (2019). A Lightweight Rogue Access Point Detection Algorithm for Embedded Internet of Things (IoT) Devices. Information Security and Computer Fraud 2019, 7(1), 7-12. Recuperado de: researchgate.net/publication/331555503_A_Lightweight_Rogue_Access_Point_Detection_Algorithm_for_Embedded_Internet_of_Things_IoT_Devices

- Banach, Z. (2019). What Is Session Hijacking: Your Quick Guide to Session Hijacking Attacks. Netsparker. Recuperado de: https://www.netsparker.com/blog/web-security/session-hijacking/

- Centro nacional de ciberseguridad (CNCS). (2020). *CSIRT-RD*. Cncs.gob.do, 1

- Cisco (2018). Reporte Anual de Ciberseguridad. Recuperado de: https://www.cisco.com/c/dam/global/es_mx/solutions/pdf/reporte-anual-cisco-2018-espan.pdf

- Dawson, Maurice & Taveras, Pedro. (2018). Issues in Cybersecurity: Security Challenges and Problems in the Dominican Republic. Land Forces

Academy Review. 23. 173-180. 10.2478/raft-2018-0020. Recuperado de: https://www.researchgate.net/publication/328211905_Issues_in_Cybersecurity_Security_Challenges_and_Problems_in_the_Dominican_Republic

- Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (DICAT). (2020). ¿Quiénes somos?. Recuperado de: http://www.dicat.gob.do/

- Decreto No. 230-18. (2018). Establece y regula la Estrategia Nacional de Cibesdeseguridad.com/2016/11/seguridad-tecnologia-centros-comerciales

ENISA (2016). Securing Smart Airports. Recuperado de: https://www.enisa.europa.eu/publications/securing-smart-airports

- Escrivá Gascó, G. (2013). Seguridad informática. Madrid, España: Macmillan Iberia, S.A.

- Forecast, G. M. D. T. (2019). Cisco visual networking index: global mobile data traffic forecast update, 2017–2022. Update, 2017, 2022. Recuperado de: https://s3.amazonaws.com/media.mediapost.com/uploads/CiscoForecast.pdf

- Ghering, M. (2016). Evil Twin vulnerabilities in Wi-Fi Networks. Radboud University, 1 Recuperado de: https://www.cs.ru.nl/bachelors-theses/2016/Matthias_Ghering___4395727___Evil_Twin_Vulnerabilities_in_Wi-Fi_Networks.pdf

- Google. (s.f.). [Mapas de Santo Domingo, República Dominicana en Google maps]. Recuperado el 11 de Noviembre, 2020.

- INCIBE (2017). Amenaza vs Vulnerabilidad. INCIBE Blog. Recuperado de: incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

- ITU (2010). Ciberseguridad: Definiciones y terminología relativas a la creación de confianza y seguridad en la utilización de las tecnologías de la información y la comunicación. ITU News, Nov 2010, 1. Recuperado de: https://www.itu.int/net/itunews/issues/2010/09/pdf/201009_20-es.pdf

- Juanes, G. G. (2016). Seguridad y tecnología para centros comerciales. Cuadernos de seguridad, 1. Recuperado de: Cuaderno

- Kaspersky Lab. (2020). CIBERAMENAZA MAPA EN TIEMPO REAL EN EL ÚLTIMO MES [República Dominicana]. Recuperado el 11 de Noviembre, de: https://cybermap.kaspersky.com/es

- Lemonnier, J. & Latto, N. (2020). What is Adware and How to Get Rid of it?. AVG Signal Blog. Recuperado de: https://www.avg.com/en/signal/what-is-adware

- Ley No. 53-07. (2007). Contra crímenes y delitos de alta tecnología, de fecha 23 de abril del año 2007. Santo Domingo, República Dominicana.

- Malwarebytes (2018). Malware. Malwarebytes Cybersecurity Basics, Recuperado de: https://www.malwarebytes.com/cybersecurity/
- Malwarebytes (2020). 2020 State of Malware Report. Malwarebytes Labs. Recuperado de: resources.malwarebytes.com/files/2020/02/2020_State-of-Malware-Report.pdf
- Mohamad Noor, M. & Hassan, W. (2018). Wireless Networks: Developments, Threats and Countermeasures. IJDIWC 3(1), 125-128. Recuperado de: https://www.researchgate.net/publication/328090396_Wireless_Networks_Developments_Threats_and_Countermeasures
- Nohe, P. (2018). Executing a Man-in-the-Middle Attack in just 15 Minutes. The SSL Store, HashedOut. Recuperado de: https://www.thesslstore.com/blog/man-in-the-middle-attack-2/
- Parno B., Kuo C., Perrig A. (2006) Phoolproof Phishing Prevention. In: Di Crescenzo G., Rubin A. (eds) Financial Cryptography and Data Security. FC 2006. Lecture Notes in Computer Science, vol 4107. Springer, Berlin, Heidelberg.
- Pau García, E. (2019). Redes WiFi,¿ Realmente se pueden proteger?. Universitat oberta de catalunya (UOC), 6. Recuperado de: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/81269/3/fbnafriaTFM0618memoria.pdf

- Rivas, E. (27 de Abril de 2018). Los peligros de usar un wifi desconocido. *Diario Libre*. Recuperado de: https://listindiario.com/tecnologia/2018/04/17/510904/los-peligros-de-usar-un-wifi-desconocido

- Swinhoe, D. (2019). What is a man-in-the-middle attack? How MitM attacks work and how to prevent them. CSO. Recuperado de: https://www.csoonline.com/article/3340117/what-is-a-man-in-the-middle-attack-how-mitm-attacks-work-and-how-to-prevent-them.html

- Trend Micro (2020). Emotet Now Spreads via Wi-Fi. Trend Micro Security News. Recuperado de: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/emotet-now-spreads-via-wi-fi

- Velázquez , A. I. (2011, Agosto 18). *CLASIFICACIÓN DE LOS PRINCIPALES RIESGOS DE LA SEGURIDAD INFORMÁTICA,* 1.

-Verizon (2020). Data breach investigations Report: Official

- WI-FI ALLIANCE. (2019). *Wi-Fi CERTIFIED Passpoint® Deployment Guidelines* (Rev 1.3), 14. Recuperado de: https://www.wi-fi.org/file/wi-fi-certified-passpoint-deployment-guidelines

rseguridad 2018-2021. Santo Domingo, República Dominicana.

- World Economic Forum (2018). World economic forum annual report. Geneva, Suiza.

Anexos

★ Recursos visuales

❑

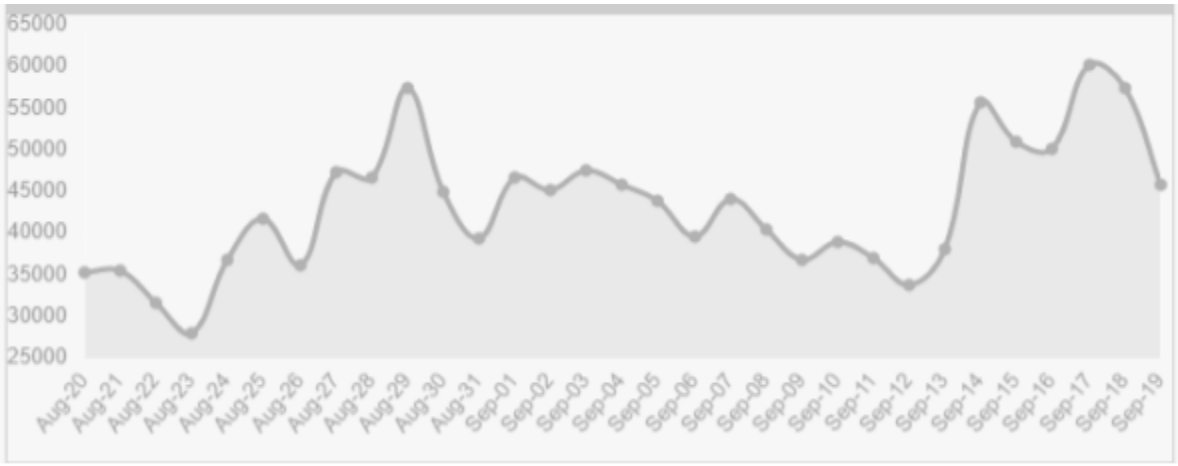


Gráfico de ciberataques en República Dominicana.
Fuente: (Kaspersky, 2020)

❑

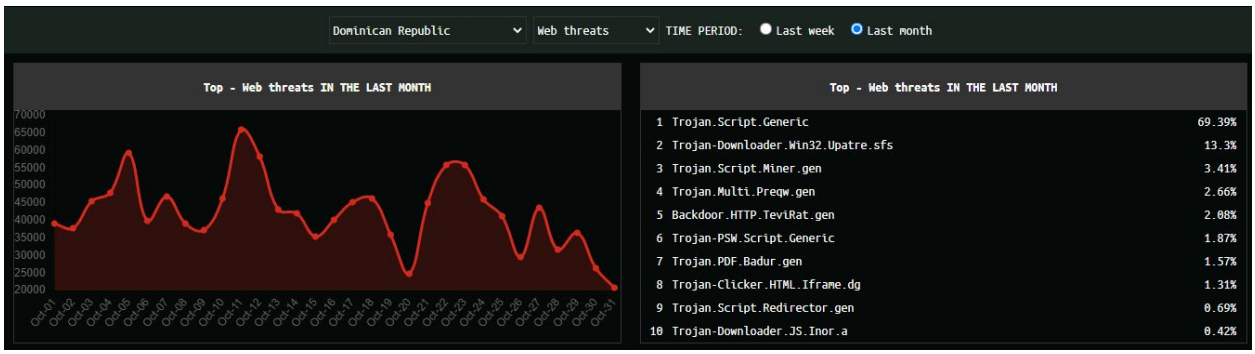


Gráfico de amenazas de red en República Dominicana. Fuente: (Kaspersky,2020)

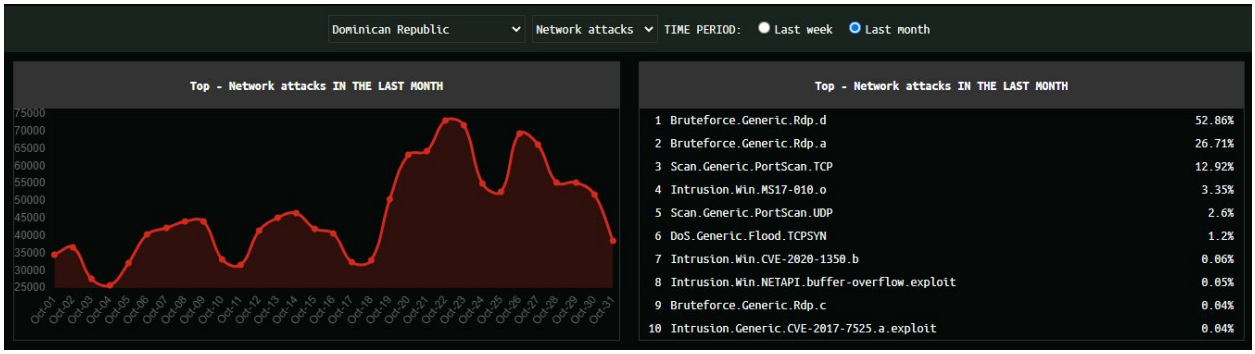


Gráfico de Ataques a redes en República Dominicana. Fuente: (Kaspersky,2020)

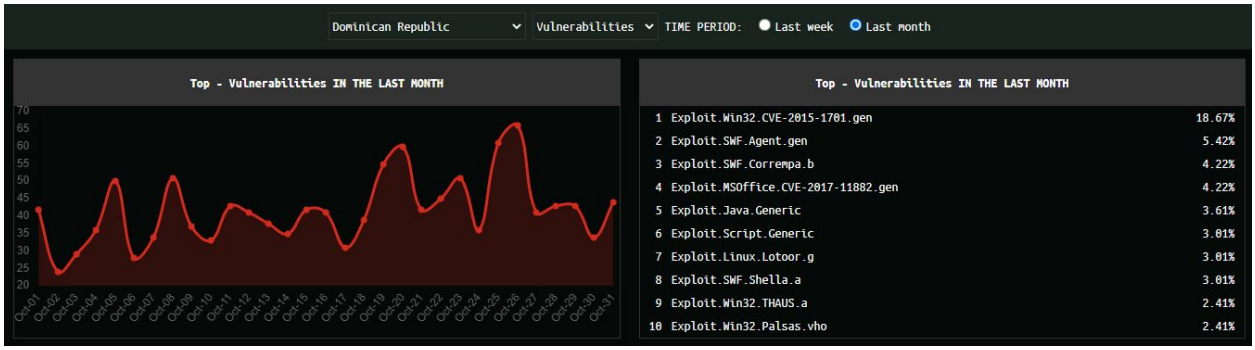
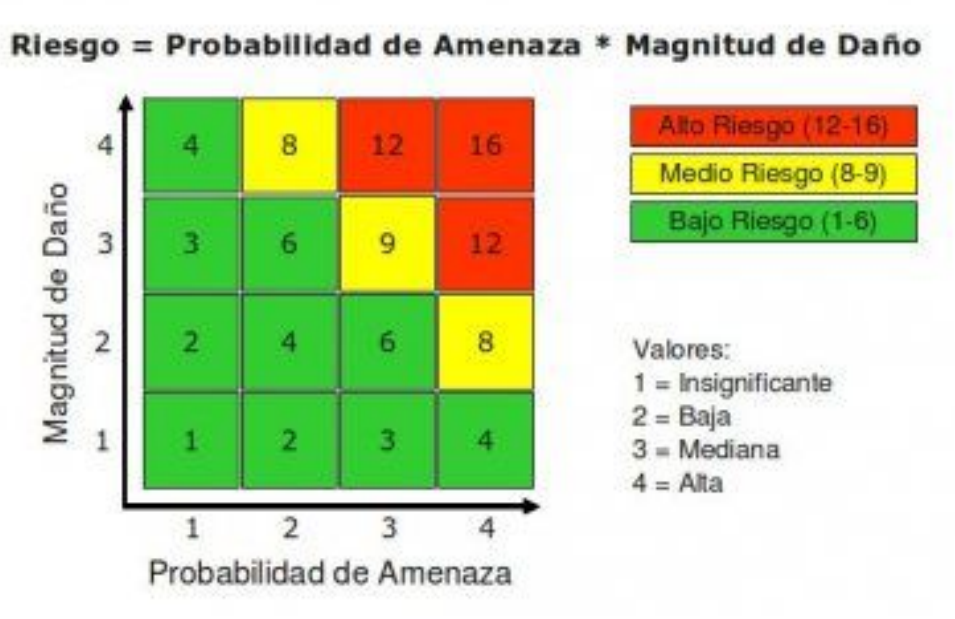
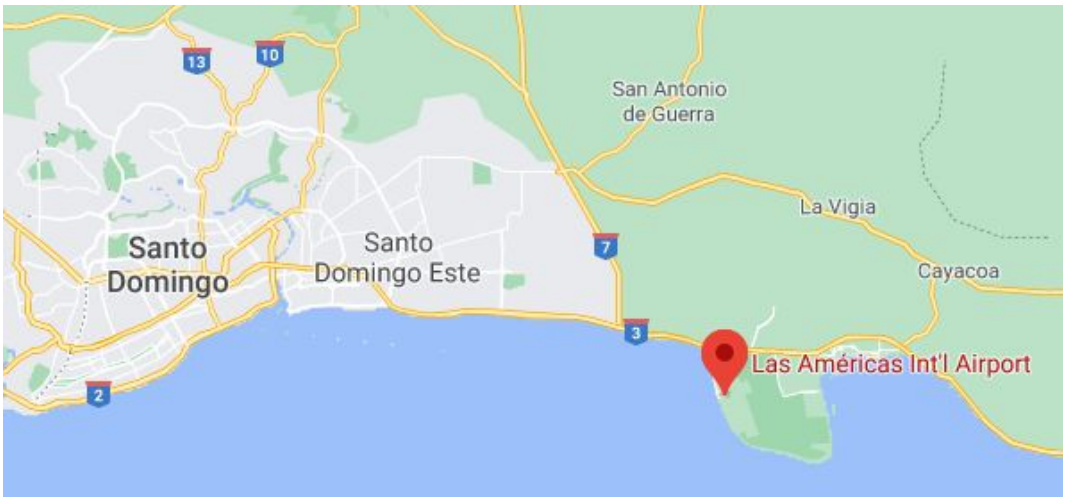


Gráfico de vulnerabilidades en República Dominicana. Fuente: (Kaspersky,2020)

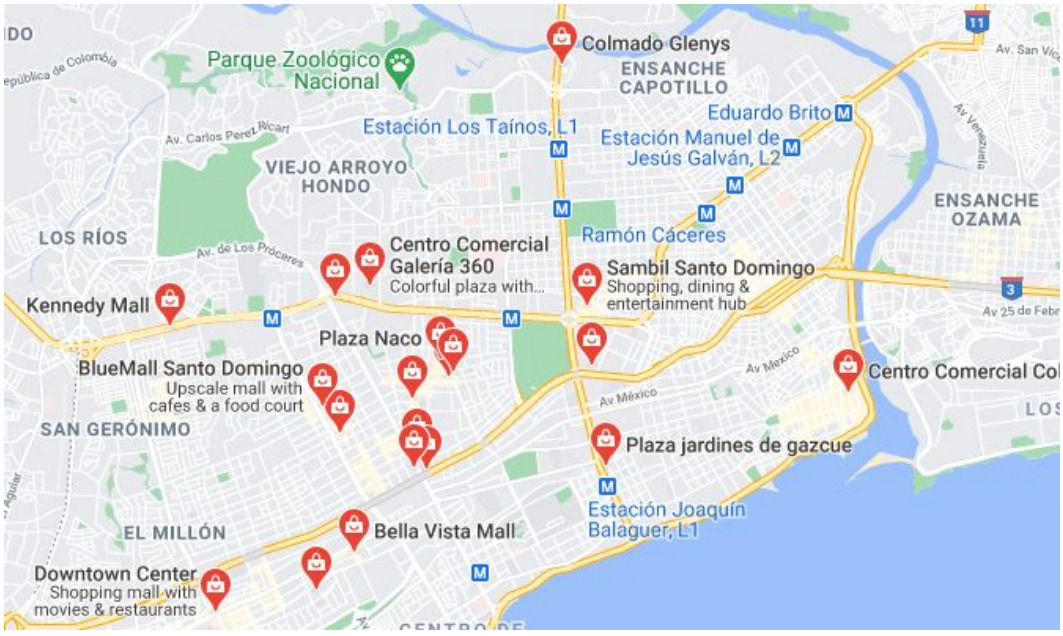


Matriz de riesgo. Fuente(Velazquez, 2011)

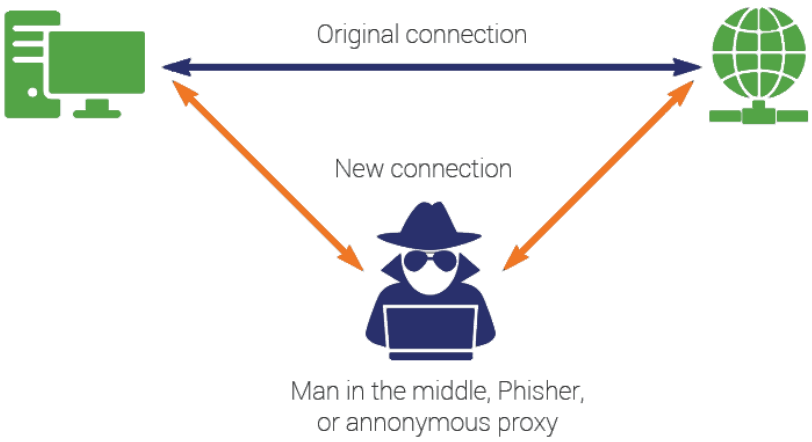


Google. (s.f.). [Mapa de ubicación del AILA, Santo Domingo, República Dominicana en Google maps]. Recuperado el 11 de Noviembre, 2020.

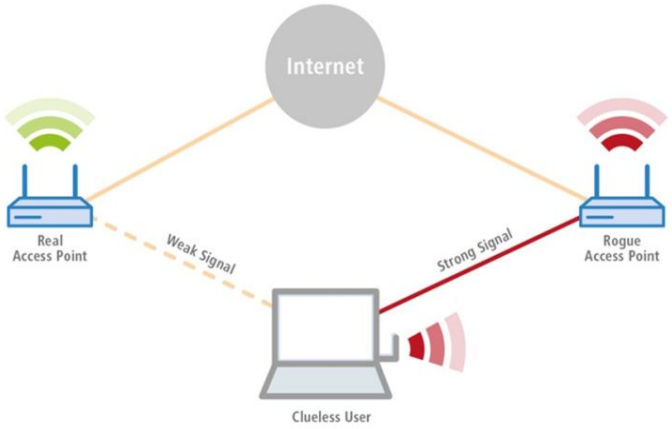
Google. (s.f.). [Mapa de centros comerciales del Santo Domingo Este, República Dominicana en Google maps]. Recuperado el 11 de Noviembre, 2020.



Google. (s.f.). [Mapa de centros comerciales del gran Santo Domingo, República Dominicana en Google maps]. Recuperado el 11 de Noviembre, 2020.

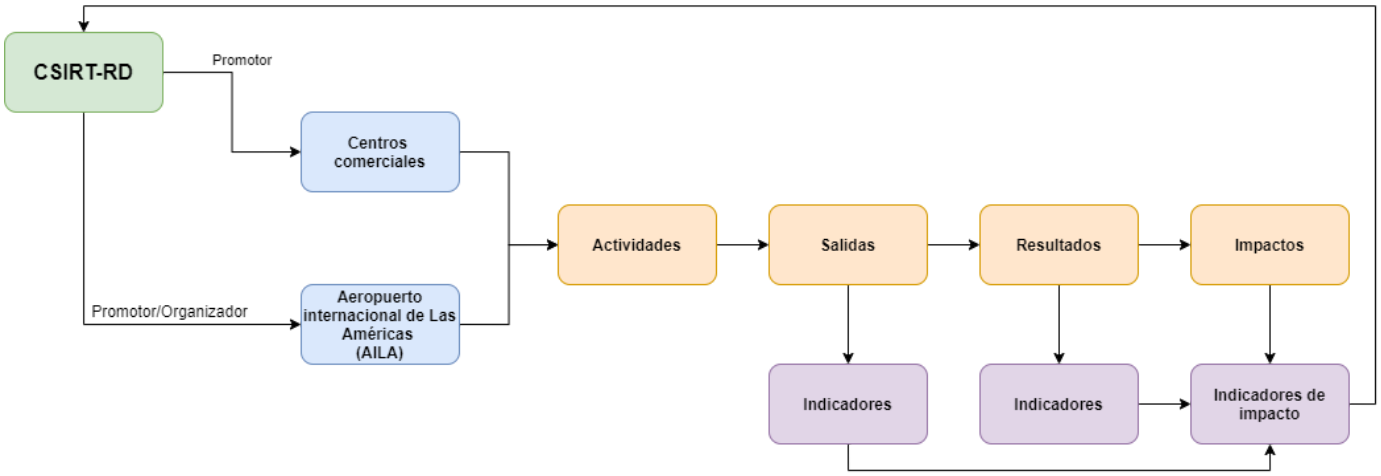


❑ *Diagrama de un ataque Man-in-the-Middle. Fuente: The SSL Store, 2018*



❑ *Ataque mediante el uso de Puntos de Acceso no Autorizados*

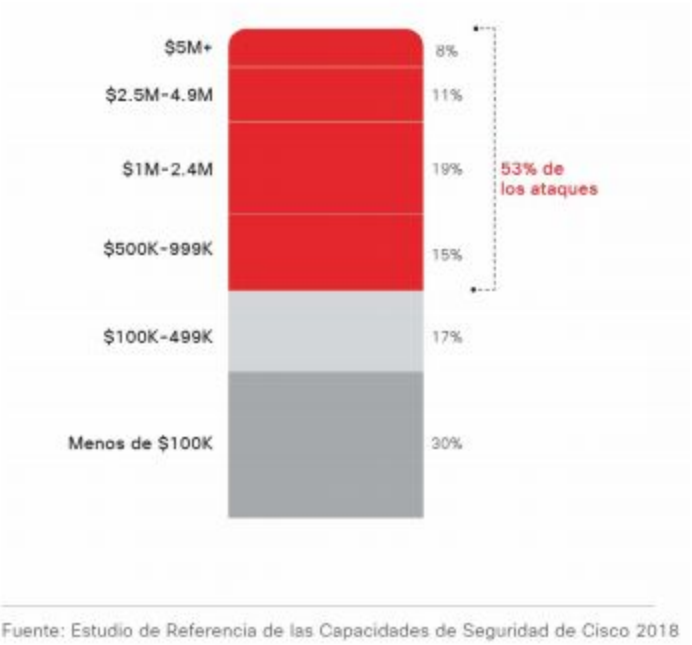
Fuente: ISCF, 2019



❑ Diagrama de Retroalimentación de distribución.Fuente: Elaboración Propia

☐ Áreas de ciberseguridad más difíciles de defender

Fuente: Cisco vulnerabilities report (2018)



Fuente: Estudio de Referencia de las Capacidades de Seguridad de Cisco 2018

- Costo de ataques cibernéticos en 2018. Fuente: Cisco annual report 2018

★ Instrumentos utilizados en el Monográfico

❑ Entrevista realizada a Luis arias, especialista en redes públicas

La siguiente entrevista se realizó el jueves 19 de noviembre del 2020 a las 8:32 PM a través de Zoom con el Ing. Luis Arias, especialista en el area de instalacion y diseño de sistemas audiovisuales, y sistemas de redes inalámbricas públicas y privadas. Luis también es fundador de la compañía Latech, donde trabaja realizando estas distintas labores.

1. **¿Considera las redes públicas del país vulnerable a ciberataques?**

   -Arias: *Si, en general, salvo algunas excepciones, las redes inalámbricas en el país son muy vulnerables, demasiado vulnerables. Personalmente he tenido la experiencia de encontrarme con redes sumamente desprotegidas donde cualquier persona puede hacer lo que quiera con esa red. Y no te hablo de empresas pequeñas sino de sitios con 200 o 300 empleados. Todo esto gracias a la falta de cultura de seguridad preventiva en este país.*

2. **¿Cuáles ataques considera pueden ser más posibles a este tipo de redes?**

   -Arias: *Definitivamente, el ransomware. De cada 10 ataques de este tipo estoy seguro que por lo menos 3 van a responder a la demanda. El Ransomware es un ataque que es lamentablemente rentable. Otro ataque siempre va a ser una amenaza es el Phishing, debido a que no se puede parar fácilmente con un firewall u otras medidas de seguridad tradicionales.*

3. **¿Los establecimientos con los que ha trabajado poseen alguna regla, reglamento o política sobre redes inalámbricas que deba seguirse?**

-Arias: *Eso depende, en este país hay todo tipo de casos. He visto muchas empresas que se toman en serio la seguridad de redes, tienen encargados de seguridad responsables, y leyes y políticas bien elaboradas a partir de normas internacionales como la ISO o la IEEE. También existen instituciones de gran tamaño y dinero que tienen estructuras de seguridad mediocre, pobre y vieja; tanto la seguridad lógica como la física.*
Las empresas internacionales típicamente vienen con sus estándares de allá, ellos mandan su estructura de red, sus firewalls, sus routers con vpn configurados desde allá, solamente contratan los sistemas de red y los switches.

Hablando específicamente de centros comerciales, es deficiente. Las plazas no invierten dinero en sus redes públicas.

4. **Con qué frecuencia son auditados los sistemas de red inalámbrica?**
   -Arias: *Las empresas grandes que considero responsables, hacen auditorías externas de seguridad y calidad con bastante regularidad.*

5. **¿Con cuáles estándares(IEEE/ISO) están trabajando?**
   -Arias: *A nivel de calidad de software: ISO 9001, 1207, 9126, 27001.*
6. **¿Cuál es el estándar con mayor importancia en su estructura de red?**
   -Arias: *Para este tipo de redes, consideró que los más relevantes serían IEEE 802.11n o 802.11ac.*
   En términos de seguridad, la Segmentación de Redes (VLAN) es un fundamento esencial para la seguridad de redes de acceso público. La red que maneja los equipos de red, routers, computadoras internas debe ser una red aparte, y la red de acceso público solo debe ser capaz de conectarse a internet, cero acceso a los equipos u otros dispositivos conectados a la red. Ese es el primer toque del manual de seguridad.

7. **Se han presentado ataques en las redes que ha trabajado?**

-Arias: *Si. Me ha tocado vivir ciertas experiencias desagradables en establecimientos de clientes: escaneo de puertos, repetidores Wi-Fi in-autorizados, ataques de fuerza bruta, intentos de phishing, entre otros. Creo que en todas partes siempre aparece alguna persona tratando de escanear tus redes, por eso hay que estar siempre atento.*

8. **¿Posee dicha red un plan de respuesta contra ataques de red inalámbrica?**
   -Arias: *Los appliances y firewalls de alta gama son capaces de realizar respuestas a ataques automáticamente si son configurados adecuadamente, el plan de respuestas es más un diseño adecuado de la estructura y configuración de red. A nivel medio es necesario tener y mantener un plan de respuesta manual. También es de gran importancia educar y controlar a los usuarios y saber bloquear efectivamente los permisos de estos en la red.*

9. **Cómo manejan el surgimiento de algún rogue ap (Puntos de Acceso no Autorizados)?**
   -Arias: *Lo más ideal sería bloquear todos los puertos que no se estén utilizando y a su vez, utilizar equipos de red que tengan medidas de seguridad automáticas contra este tipos de ataques alertar/responder ante cualquier actividad sospechosa relacionada a los puertos.*

10. **¿Cuál cree que es su mayor reto a nivel de seguridad ahora mismo?**
    -Arias: *Falta de inversión monetaria en la seguridad de las redes. La mayoría de los hotspot públicos en este país no sirven, no están bien diseñados ni estructurados, son de mala calidad y simplemente no funcionan. Los appliances y equipos de red para trabajar una red decente con calidad de servicio y seguridad cuesta dinero, y las compañías no están dispuestas a invertir. Se conforman con dispositivos de baja gama, que no son suficientes para soportar adecuadamente el tipo de redes que tienen. También es importante no solo invertir en los equipos sino también invertir en un buen diseño y una buena implementación.*

11. **¿Su marco de seguridad está regulado por alguna institución del país?**

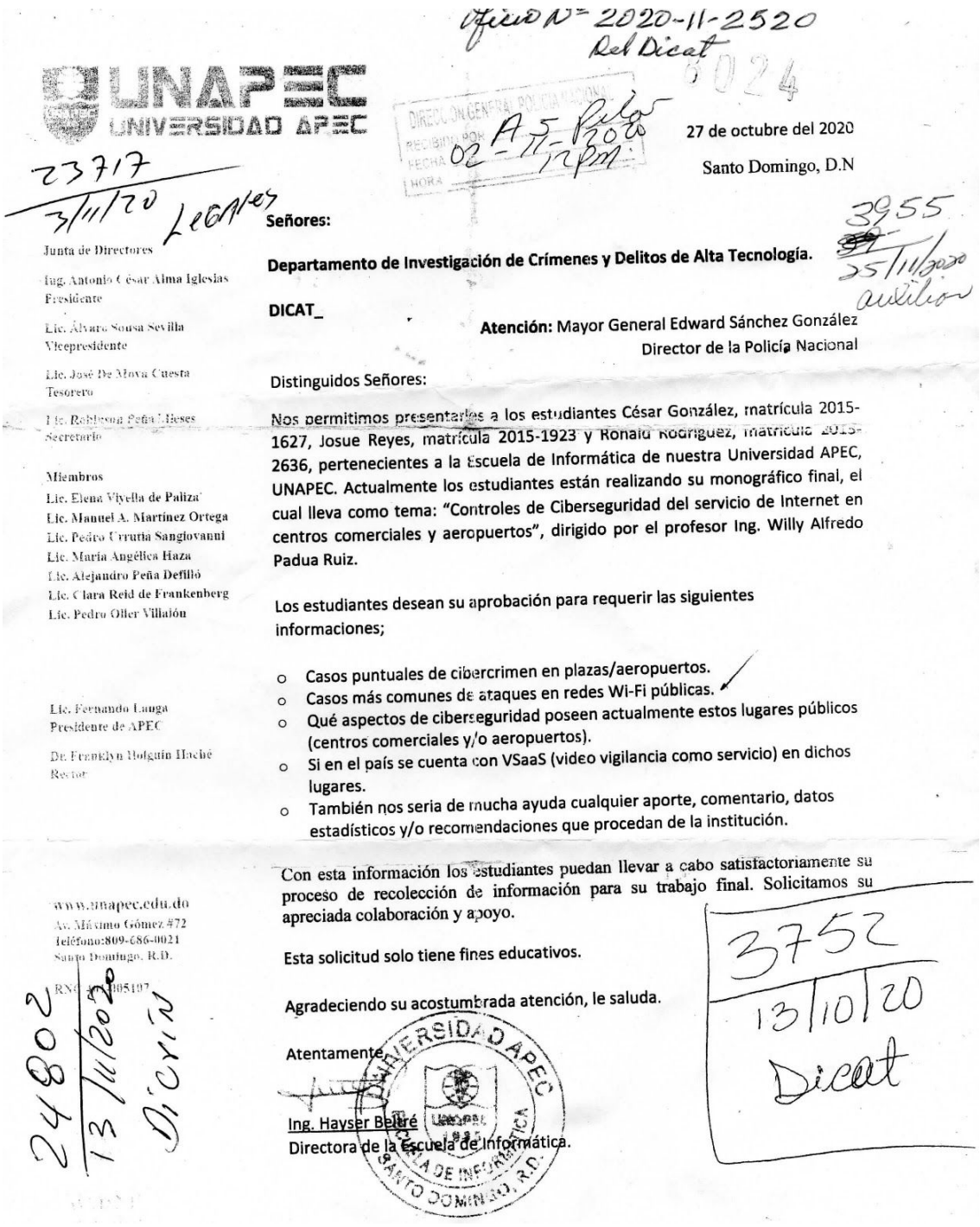
    -Arias: *El gobierno no tiene mucha regulación o estándares a nivel de seguridad. Indotel tiene algunas regulaciones pero son muy generales y básicas. En términos de reportar incidentes y tratar con crímenes cibernéticos, siempre nos hemos comunicado con el DICAT.*

12. **¿Cree necesaria la incorporación, reforzamiento o refinamiento del contacto gubernamental con este establecimiento a nivel de ciberseguridad?**

    -Arias: *Dirección. El gobierno debe dar dirección, a través de una misma entidad, para fortalecer la ciberseguridad. El OPTIC (Oficina Presidencial de Tecnologías de la Información y Comunicación), es un buen comienzo de lo que podría ser organización por parte del gobierno, deberían establecer patrones de seguridad a nivel gubernamental y luego pueden expandirse a sectores generales/privados para fortalecer la ciberseguridad en todos los ámbitos: privados, públicos, etc.. Necesitan integración, un solo ángulo, una sola cabeza liderando y diciendo que es lo que se va a hacer para mejorar la ciberseguridad del país y el gobierno.*

- ★ **RESULTADOS DE ESTUDIOS ANTERIORES DEL AUTOR SOBRE EL TEMA**
- ★ **VALIDACIÓN DE LOS RESULTADOS OBTENIDOS**

❑ Solicitud y Respuesta de Información al DICAT



UNAPEC
UNIVERSIDAD APEC

Oficio N° 2020-11-2520
Del Dicat
5024

DIRECCIÓN GENERAL POLICÍA NACIONAL
RECIBIDO POR
FECHA 02-11-2020
HORA 12pm

27 de octubre del 2020

Santo Domingo, D.N

23717
3/11/20 Legales

3955
25/11/2020
auxilio

Señores:

Departamento de Investigación de Crímenes y Delitos de Alta Tecnología.

DICAT_

Atención: Mayor General Edward Sánchez González
Director de la Policía Nacional

Distinguidos Señores:

Nos permitimos presentarles a los estudiantes César González, matrícula 2015-1627, Josue Reyes, matrícula 2015-1923 y Ronald Rodriguez, matrícula 2015-2636, pertenecientes a la Escuela de Informática de nuestra Universidad APEC, UNAPEC. Actualmente los estudiantes están realizando su monográfico final, el cual lleva como tema: "Controles de Ciberseguridad del servicio de Internet en centros comerciales y aeropuertos", dirigido por el profesor Ing. Willy Alfredo Padua Ruiz.

Los estudiantes desean su aprobación para requerir las siguientes informaciones;

- Casos puntuales de cibercrimen en plazas/aeropuertos.
- Casos más comunes de ataques en redes Wi-Fi públicas.
- Qué aspectos de ciberseguridad poseen actualmente estos lugares públicos (centros comerciales y/o aeropuertos).
- Si en el país se cuenta con VSaaS (video vigilancia como servicio) en dichos lugares.
- También nos seria de mucha ayuda cualquier aporte, comentario, datos estadísticos y/o recomendaciones que procedan de la institución.

Con esta información los estudiantes puedan llevar a cabo satisfactoriamente su proceso de recolección de información para su trabajo final. Solicitamos su apreciada colaboración y apoyo.

Esta solicitud solo tiene fines educativos.

Agradeciendo su acostumbrada atención, le saluda.

Atentamente,

Ing. Hayser Beltré
Directora de la Escuela de Informática.

Junta de Directores
Ing. Antonio César Aima Iglesias
Presidente
Lic. Álvaro Sousa Sevilla
Vicepresidente
Lic. José De Moya Cuesta
Tesorero
Lic. Rebecca Peña Reyes
Secretario

Miembros
Lic. Elena Viyella de Paliza
Lic. Manuel A. Martínez Ortega
Lic. Pedro Urruria Sangiovanni
Lic. María Angélica Haza
Lic. Alejandro Peña Defilló
Lic. Clara Reid de Frankenberg
Lic. Pedro Oller Villalón

Lic. Fernando Lauga
Presidente de APEC

Dr. Franklyn Holguín Haché
Rector

www.unapec.edu.do
Av. Máximo Gómez #72
Teléfono:809-686-0021
Santo Domingo, R.D.
RNC [illegible]105107

24802
13/11/2020
DICAT

3752
13/10/20
Dicat

UNIVERSIDAD APEC
ESCUELA DE INFORMÁTICA
SANTO DOMINGO, R.D.

★

(Carta de solicitud de información firmada y sellada por la Policía Nacional Dominicana.)

POLICIA NACIONAL
REPUBLICA DOMINICANA

OFICINA DEL DIRECTOR GENERAL

"Todo por la Patria"

"Año de la Consolidación de la Seguridad Alimentaria"

26409

27 de noviembre del 2020.

SEPTIMO ENDOSO:

A la : **Ing. HAYSER BELTRE,**
Directora de la Escuela de Informática de la Universidad APEC. SU DESPACHO.

Asunto : Remisión de información.

Anexo : Oficio No.3955 de fecha 25 del mes en curso, del Director Central de Investigación, P.N., y anexo.

1.- DEVUELTO cortésmente, para su conocimiento y fines que estime de lugar.

Lic. EDWARD R. SANCHEZ GONZALEZ,
Mayor General,
Director General de la Policía Nacional.

SGPV:
BB.LS:
cr.

★

(Carta de confirmación emitida por el director de la Policía Nacional, Edward Sanchez Gonzalez)

"REPUBLICA DOMINICANA"
POLICÍA NACIONAL
DIRECCIÓN CENTRAL DE INVESTIGACION, P.N.
SUBDIRECCIÓN CENTRAL DE INVESTIGACION, POLICÍA CIENTÍFICA
DEPARTAMENTO DE INVESTIGACIÓN DE CRÍMENES Y DELITOS DE ALTA TECNOLOGÍA, P.N. (DICAT)
"AÑO DE LA CONSOLIDACION DE LA SEGURIDAD ALIMENTARIA"

25 de noviembre del 2020.-

No. 2020-11-2520:
QUINTO ENDOSO :

Al	:	Director de Investigación, Dicrim, P.N. **SU DESPACHO. -**
Asunto	:	Solicitud de información.
Anexo	:	a)Su oficio **No.3 7 5 2** de fecha 13-11-2020 y anexos. b)Informe detallado.

1.- **D E V U E L T O respetuosamente**, con las informaciones detalladas en el oficio base, con relación a los casos puntuales de cibercrimen en plazas y aeropuertos, casos más comunes de ataques en redes WIFI públicas, aspectos de ciberseguridad que poseen actualmente estos lugares públicos (centros comerciales y/o aeropuertos), si en el país se cuenta con VSaaS (video vigilancia como servicio) en dichos lugares. Lo que informo para su conocimiento y fines

PORFIRIO BOTIER ESTEVEZ,
Tte. Coronel, P.N.
Comandante Departamento de Investigación Crímenes
y Delitos de Alta Tecnología, (DICAT), P.N.

BE/Jr

★

(Carta de confirmación emitida al DICRIM por el Director del DICAT, Profirio Botier Estevez)

POLICIA NACIONAL
DIRECCION CENTRAL DE INVESTIGACIONES
DEPARTAMENTO DE INVESTIGACION DE CRIMENES Y DELITOS DE ALTA TECNOLOGIA, P.N.

"AÑO DE LA INNOVACION Y LA COMPETECIA"

23 de Noviembre 2
Santo Domingo

RELACION DE LAS DENUNCIAS RECIBIDAS, CASOS RESUELTOS y CASOS PENDIENTE, SEGÚN EL TIPO DE DELITOS, DESDE EL 01 DE ENERO 2018 HASTA LA FECHA

NO.	TIPOS DE DELITOS	TOTAL GENERAL 2018			TOTAL GENERAL 2019			TOTAL GENERAL 2020			TOTAL GENERAL		
		TOTAL DENUNCIAS RECIBIDAS	TOTAL CASOS RESUELTOS	TOTAL PENDIENTES	TOTAL DENUNCIAS RECIBIDAS	TOTAL CASOS RESUELTOS	TOTAL PENDIENTES	TOTAL DENUNCIAS RECIBIDAS	TOTAL CASOS RESUELTOS	TOTAL PENDIENTES	TOTAL DENUNCIAS RECIBIDAS	TOTAL CASOS RESUELTOS	TOTAL PENDIENTES
1	DIFAMACION Y / O AMENAZA VIA PAGINA WEB	52	68	-16	19	4	17	0	20	-20	71	92	-21
2	EXTORSION VIA PAGINA WEB	28	24	4	3	1	3	119	29	90	150	54	96
3	ESTAFA VIA PAGINA WEB	502	85	417	137	25	118	596	86	510	1235	196	103
4	HACKING	12	0	12	0	1	0	0	1	-1	12	2	10
6	DIFAMACION Y/O AMENAZA VIA E-MAIL	4	3	1	0	0	0	0	3	-3	4	6	-2
8	SUSTRACCION DE EQUIPOS ELECTRONICOS	6	8	-2	0	0	0	0	0	0	6	8	-2
9	FRAUDES ELECTRONICOS A PERSONAS E EMPRESAS	8	7	1	0	0	0	0	3	-3	8	10	-2
10	CERTIFICACION DE CORREO ELECTRONICO	0	40	-40	0	5	0	0	3	-3	0	48	-48
11	LLAMADAS MOLESTOSAS Y/O AMENAZANTES	44	5	39	6	6	4	21	4	17	71	15	56
12	ROBO DE E-MAIL	0	0	0	0	0	0	0	0	0	0	0	0
13	PHISHING	179	76	103	57	7	50	174	15	159	410	98	312
14	ROBO DE IDENTIDAD	51	21	30	3	1	2	27	3	24	81	25	56
15	ACCESO ILICITO Y SABOTAJE	23	8	15	4	3	4	79	6	73	106	17	89
16	PORNOGRAFIA INFANTIL	0	7	-7	0	0	0	0	0	0	0	7	-7
17	CLONACION DE TARJETAS (SKIMMING)	100	75	25	1	8	1	16	6	10	117	89	28
18	ESTAFA VIA TELEFONICA	29	4	25	14	4	10	7	2	5	50	10	40
	TOTAL DE LOS AÑOS 2017, 2018, 2019 Y 2020	1038	431	607	244	65	209	1039	183	856	2321	677	164

TOTAL GENERAL DE LOS AÑOS 2018, 2019 Y 2020			
DENUNCIAS RECIBIDAS	CASOS RESUELTOS	CASOS PENDIENTES	TOTAL GE
2321	679	3107	610

DEPTO. DE INV. DE CRIMENES Y DELITOS DE ALTA TECNOLOGIA, P.N.
(DICAT)

★ (Respuesta a la solicitud de información, emitida por el DICAT. Pagina 2)