UNIVERSIDAD EVANGÉLICA DE EL SALVADOR

Escuela de Posgrados

MAESTRÍA EN DERECHO CORPORATIVO

Ensayo

“Ataques en Internet a los nombres de dominio de las sociedades en el salvador, aspectos legales”

Para optar al título de

“Maestra en Derecho Corporativo”

Presentado por

Licda. Keni Janeth López de Amaya

CIF: 2022011340

Coordinador

Dr. Edis Alcides Guandique Sánchez

San Salvador, 02 de julio de 2024.

UNIVERSIDAD EVANGELICA DE EL SALVADOR
AUTOR: KENI JANETH LÓPEZ DE AMAYA
LICENCIADA EN CIENCIA JURÍDICAS
Identificador ORCID: 0009-0003-6539-5648

TÍTULO.

ASPECTOS LEGALES DE LOS NOMBRES DE DOMINIO REGISTRADOS POR SOCIEDADES SALVADOREÑAS

Tabla de Contenido.

Resumen.....i
Introducción. 1
Abreviaturas.....2
Planteamiento del problema. 3
Justificación. 4
Objetivos. 5
Objetivo general del ensayo: 5
Objetivos específicos: 5
Desarrollo.....7
Definiciones y características del ciberespacio. 7
Los Nombres de Dominio y su relación con la Propiedad Intelectual y las Marcas. 9
¿Cómo funciona un Servicio de Nombre de Dominio? 12
Prácticas de abuso de DNS 14
Regulaciones y estándares internacionales. 21
Derecho comparado. 22
Derecho Comprado en la Implementación de DNS. 23
Derecho Comparado en la Regulación a los Ataques de DNS. 24
¿Qué hacer en caso de un ciberataque? 25
Legislación en El Salvador 25
Impacto de los ataques de DNS a sociedades en El Salvador. 28
Protección jurídica de dominio. 31
Conclusiones. 34
Recomendaciones. 37
Índice Bibliográfico 38
Tabla de Ilustraciones.....40

Resumen.

En el mundo digital actual, los nombres de dominio son fundamentales para la identidad y operatividad de las organizaciones. Estos dominios no solo representan la dirección en línea de una entidad, sino que también son cruciales para su marca y presencia digital. Sin embargo, estos dominios están cada vez más expuestos a diversos ataques cibernéticos que buscan interrumpir, desviar o apropiarse de la actividad en línea de las entidades. Este ensayo explora las principales formas de ataques a nombres de dominio, incluyendo el secuestro de dominios, el envenenamiento de caché DNS y los ataques de denegación de servicio.

El secuestro de dominios implica la transferencia no autorizada de un dominio, resultando en la pérdida de control. El envenenamiento de caché DNS, redirige el tráfico a sitios maliciosos manipulando las respuestas del servidor DNS. Los ataques DDoS saturan los servidores con tráfico excesivo, causando interrupciones en el servicio.

Además, se analizan las consecuencias de estos ataques para las organizaciones afectadas, tales como la pérdida de confianza, daños financieros significativos y riesgo reputacional. Se presentan recomendaciones detalladas que las organizaciones en El Salvador pueden implementar para proteger sus nombres de dominio y mitigar los impactos de posibles ataques.

Palabras claves: Secuestro de dominios, servidor, DNS, protección, legislación.

Abstract.

In today's digital world, domain names are essential for the identity and operation of organizations. These domains not only represent an entity's online address but are also crucial to its brand and digital presence. However, these domains are increasingly exposed to various cyberattacks that seek to disrupt, divert, or hijack entities' online activity. This essay explores the main forms of domain name attacks, including domain hijacking, DNS cache poisoning, and denial of service attacks.

Domain hijacking involves the unauthorized transfer of a domain, resulting in loss of control. DNS cache poisoning redirects traffic to malicious sites by manipulating DNS server responses. DDoS attacks flood servers with excessive traffic, causing service interruptions.

Additionally, the consequences of these attacks for affected organizations are analyzed, such as loss of trust, significant financial damage, and reputational risk. Detailed recommendations are presented that organizations in El Salvador can implement to protect their domain names and mitigate the impacts of potential attacks.

Keywords: Domain hijacking, server, DNS, protection, legislation.

Introducción.

El Salvador ha experimentado cambios significativos desde 2019 debido a la pandemia de Covid-19 y a las políticas gubernamentales centradas en la tecnología. Iniciativas como la adopción del Bitcoin como moneda nacional, ha colocado al país en el escenario mundial, generando tanto atención positiva como negativa. Positivo en el sentido de volverlo un país atractivo para tipos de inversionistas ligados a la tecnología, con una visión de país de volver a El Salvador en un hub tecnológico y negativo ya que está expuesto también a los peligros de internet.

Si consideramos que la mayoría de las empresas desde pequeñas a grandes tiene una identidad digital en internet, y que poseen un DNS (Sistema de Nombres de Dominio) y que este DNS de forma natural representa no solo una dirección de internet si no también un distintivo relacionado con la marca a la cual hace referencia del Servicio de Nombre de Dominio, lo podemos considerar como parte de un bien de la empresa y por ende la responsabilidad legal de lo que suceda con ese nombre de dominio y en particular con los temas asociados a la disponibilidad y abuso del dominio pueda tener repercusiones legales directas sobre el propietario del Nombre de Dominio de Internet, esto es especialmente relevante en un contexto donde la ciberseguridad y la protección de la identidad digital son cruciales para mantener la confianza de los consumidores y la integridad de la marca. La Ley de Delitos informáticos y conexos establece un marco legal para abordar estos desafíos proporcionando herramientas para combatir el cibercrimen y proteger los activos digitales de las empresas.

Mientras El Salvador avanza hacia un futuro más tecnológico, es esencial que las empresas y los individuos comprendan las implicaciones legales y de seguridad asociada con la identidad digital y el uso de DNS. La combinación de políticas innovadoras y un enfoque de la ciberseguridad puede ayudar a mitigar los riesgos y maximizar los beneficios de esta transformación digital.

Abreviaturas

Art.: Artículo.
Bits: Binary digit (Dígito binario).
CFPB: Oficina de Protección Financiera del Consumidor.
CNR: Centro Nacional de Registro.
DHCP: Dynamic Host Configuration Protocol (Protocolo de Configuración Dinámica de Host).
DDoS: Distributed Denial-of-Service (Denegación de Servicio Distribuido).
DNS: Sistema de Nombres de Dominio.
DNSSEC: Domain Namy Sysstem Security Extensions (Extensiones de Seguridad del DNS).
EEE: Espacio Económico Europeo.
EE. UU: Estados Unidos.
FCC: Comisión Federal de Comunicaciones.
FTC: Comisión Federal de Comercio.
FQDN: Fully Qualified Domain Name (Nombre de Dominio Calificado).
GDPR: Reglamento General de Protección de Datos.
gTLDs: Generic Top-Level Domains (Dominios de nivel superior genéricos).
gTLD-MoU: Generic Top-Level Domain Name-Memorandum of Understanding (Nombre de dominio de nivel superior: Memorando de entendimiento).
HTTP: Hypertex Transfer Protocol (Protcolo de transferencia Hypertex).
IAHC: International Ad Hoc Committee (Comité Internacional Ad Hoc del ICANN).
IANA: Internet Assigned Numbers Authority (Autoridad de Numeros Asignados de Internet).
ICANN: Internet Corporation for Assigned Names and Numbers (Corporación de Internet para la Asignación de Nombres y Números).
ICO: Oficina del Comisionado de Información.
IFT: Instituto Federal de Telecomunicaciones.
InterNIC: Corporación de Asignación de Nombres y Número de Internet.
ICANN (IMRS): Managed Root Server (Servidor raíz administrado).
IoT: Internet of Things (Internet de las cosas).
IP Address: Internet Protocol Address (Dirección de Protocolo de Internet).
Ip: Internet Protocol (Protocolo de internet).
Ipsec: Internet Protocol Security (Seguridad de protocolo de Internet).
IPv4: Internet Protocol version 4 (Protocolo de internet versión 4).
IPv6: Internet Protocol versión 6 (Protocolo de internet versión 6).
ISO: Organización Internacional de Estándares.
ISP: Internet Service Provider (Proveedor de servicios de internet).
NAP: Network Access Point (Punto de acceso a la red).
NAT: Network Address Translation (Traducción de Direcciones de Red).
NDP: Neighborhood Discovery (Descubrimiento de Vecindario)
NTIA: Administración Nacional de Telecomunicaciones e Información.
OMPI: Organización Mundial de Propiedad Intelectual.
OSPFv3: Open Shortest Path First (Protocolo de enrutamiento de ruta más corta).
POC: Comité de Supervisión de Políticas.
QoS: Qualty of Service (Calidad de Servicio).
RGPD: Reglamento General de Protección de Datos.
RSO: Root Server Operators (Operadores de Servidores Raíz).
RSS: Sistema de Servidores Raíz.
SEC: Securities and Exchange Commission (Comisión de aseguramiento e intercambio).
SLAAC: Stateless Addres Autoconfiguration (Configuración automática de direcciones sin estado).
SSH: Secure Shell (Cubierta Segura).
SVNet: Salvadorean Network Information Center.
tld: Top-level domain (Dominio de nivel superior).
TCP: Protocolo de control de transmisión.
TCP/IP: Protocolo de transmisión/Protocolo de internet.
TI: Tecnología de la información.
TIC: Tecnologías de la Información y la Comunicación.
UE: Unión Europea.
UDP: User Datagram Protocol (Protocolo de datagramas de usuario).
UDRP: Política Uniforme de Resolución de Controversias de la ICANN.
USPTO: United Sates Patent and Trademark Office (Oficina de Patentes y Marca de los Estados Unidos).

Planteamiento del problema.

Los ataques a Nombres de Dominio representan un riesgo significativo para la reputación, las finanzas y la confianza de clientes y proveedores de las sociedades en El Salvador. En un entorno donde los sistemas informáticos de las empresas son esenciales para su actividad económica, estos ataques, que incluyen desde el secuestro de dominio hasta el phishing, pueden tener consecuencias devastadoras. Estos delitos no solo afectan la operatividad de las empresas, sino que también ponen en peligro la confianza que los clientes y proveedores depositan en ellas.

La creciente dependencia de las empresas en sus sistemas informáticos y la globalización del ciberespacio plantean desafíos únicos para el marco jurídico salvadoreño. La relatividad de la territorialidad y la soberanía en el ciberespacio complica la determinación de competencias jurisdiccionales y la aplicación del derecho local. Esto pone en duda la capacidad del Estado para ejercer el derecho penal de manera efectiva en casos de ciberdelincuencia.

Por lo tanto, es crucial explorar las implicaciones legales de los ataques a Nombres de Dominio y comprender cómo el marco jurídico salvadoreño puede proteger a las empresas. Es necesario analizar qué medidas legales deben implementarse para garantizar la protección de los derechos de las sociedades y asegurar una justicia oportuna ante estos ataques. La pregunta central que guía este análisis es: ¿Cómo el Estado y el marco legal vigente garantizan la protección de los derechos de las sociedades y la justicia oportuna ante los ataques a Nombres de Dominio?

Justificación.

En el auge de la digitalización y el comercio electrónico ha hecho que los nombres de dominio se conviertan en un activo muy esencial para las sociedades. Los nombres de dominio representan la identidad digital de una empresa y con el crecimiento de internet están más expuestos a ataques cibernéticos.

El ensayo que presentamos resulta de suma importancia, ya que nos enfocamos en un desafío emergente y crítico dentro del panorama digital de las empresas en El Salvador. Los efectos legales de los ataques a los nombres de dominio. Estos ataques que abarcan desde el secuestro de dominio hasta el phishing están adquiriendo una relevancia sin precedentes debido a su creciente frecuencia y al peligro que representa para la reputación, las finanzas y la confianza de clientes y proveedores de las sociedades. Asimismo, resulta imperativo explorar las implicaciones legales de estos ataques, comprendiendo cómo el marco jurídico salvadoreño resguardará a las empresas y qué medidas legales deben implementarse. Este análisis incluirá la evaluación de la efectividad de la legislación existente y la identificación de posibles vacíos legales que requieran atención.

Al adentrarse en un tema que apenas ha sido explorado en el contexto salvadoreño, en este ensayo se propone sentar las bases para futuras investigaciones y regulaciones. La protección jurídica adecuada de los nombres de dominio puede ejercer una influencia considerable en la confianza de los inversionistas. Por ende, este trabajo se enfoca en proponer soluciones prácticas y jurídicas con el objetivo de fortalecer la seguridad y confianza en las transacciones de comercio electrónico y las operaciones en línea.

Objetivos.

Objetivo general del ensayo:

Es analizar los aspectos legales en El Salvador para una sociedad, al existir un abuso de su Nombre de Dominio de Internet.

Objetivos específicos:

Definir las prácticas de abuso de DNS como secuestro de dominios y otras actividades realizadas por personas con malas intenciones, incluyendo el Cibersquatting.

Identificar y analizar las vulnerabilidades legales a las que están expuestos los nombres de dominio de las sociedades en El Salvador, proporcionando una base sólida para futuras investigaciones.

Tipo de estudio jurídico.

El estudio realizado se enmarca en un ensayo con metodología de investigación jurídico documental, utilizando el método hermenéutico. Este enfoque permite una interpretación profunda y crítica de los textos legales, facilitando una comprensión detallada de los aspectos normativos relacionados con la vulnerabilidad de los nombres de dominio de las sociedades en El Salvador.

Dado que el tema es novedoso y no se dispone de medios escritos tradicionales como libros, revistas, enciclopedias o folletos, se ha llevado a cabo una investigación exhaustiva en internet. Esta revisión ha incluido la consulta de bases de datos jurídicas y tecnológicas, permitiendo acceder a información actualizada y relevante para el análisis.

En este estudio específico, el método hermenéutico se aplicó de la manera siguiente:

1. Interpretación de textos legales: Se realizó una lectura detallada y crítica de las leyes y normativas relacionadas con los nombres de dominio en El Salvador.

2. Análisis contextual: Se consideraron antecedentes, históricos, sociales y tecnológicos que influyen en la regulación de los nombres de dominio.

3. Comparación de Fuente: Se compararon diferentes fuentes tecnológicas y jurídicas para identificar posibles inconsistencias en la legislación actual. Esto ayudo a construir una visión más completa y coherente del marco legal.

También, la vulnerabilidad de los nombres de dominio en El Salvador se abordó mediante los enfoques siguientes:

1. Análisis legal: Se revisaron y analizaron las leyes y regulaciones existentes en El Salvador que afectan la gestión y protección de los nombres de dominio. Esto incluyó la Ley Especial contra los Delitos Informáticos y Conexos.

2. Identificación de Amenazas: Se identificaron las principales amenazas y riesgos a los que están expuestos los nombres de dominio, como el secuestro de dominios, phishing y ataques de denegación de servicio (DDos).

3. Estudio comparativo: Se compararon las prácticas y regulaciones de El Salvador con las de otros países para identificar posibles mejoras y adoptar mejores prácticas internacionales.

Desarrollo.

Definiciones y características del ciberespacio.

El ciberespacio se define como un espacio imaginario donde se establecen las comunicaciones en una red informática [1]. Bajo esta condición de imaginario existe una relatividad respecto a la concepción del territorio y la soberanía por parte de los Estados. Con esta premisa de ver todo lo que abarca el ciberespacio como uno solo y que prácticamente puede ser accedido desde cualquier parte del mundo, hace poco práctico el marco jurídico para determinar las competencias de una jurisdicción y la aplicación del derecho local, poniendo en duda el alcance del Estado, desde su ratio de definición, de ejercer el derecho penal. Por ende, es de vital importancia entender el carácter ubicuo del ciberespacio y los aspectos de territorialidad de los Servicios de Nombre de Dominio, conocidos como DNS[2], para que, con base a esta compresión, el profesional del derecho pueda desentrañar el imaginario del ciberespacio y analizar los casos de la aplicación de los sistemas en el derecho penal a la luz de un concepto de territorialidad más global, apoyado del derecho internacional.

Para poder entender el carácter ubicuo del ciberespacio y mejorar la comprensión de la jurisdicción de lo que ocurre en la red informática por excelencia, internet, hay que materializar ese espacio imaginario, en donde los cables submarinos juegan un papel importante en la infraestructura global de Internet y hoy existen alrededor de 406 sistemas de cables submarinos operativos en el mundo[3]. Hoy el 99% del mundo está conectado a Internet a través de los cables submarinos y únicamente 1% lo hace mediante satélites. "El mundo se conecta a través de los océanos", se están realizando unos 100 mil kilómetros de nuevos tendidos de cables submarinos por año con una vida útil de 25 años. El costo de invertir en un cable intercontinental ronda los US$1.000 millones, instalar un cable juegan muchos factores geopolíticos y análisis de interconectividad y financiero, que conectaría ese cable, qué naciones, que población, la penetración de Internet de esos países.

La conexión de internet de Latinoamérica se hace a través del Network Access Point (NAP) de las Américas es un centro de datos de gran tamaño y punto de intercambio de Internet en Miami, Florida, dirigido por Equinix Inc. Es una empresa multinacional estadounidense con sede en Redwood City, California, que se especializa en conexión a internet y centros de datos, la compañía lidera la cuota de mercado global de centros de datos de colocación, con 200 centros de datos en 24 países en los cinco continentes.[4] Alberga una de las instancias del servidor raíz del sistema de nombres de dominio. El edificio cuenta con seis pisos y una superficie de alrededor de 70.000 metros cuadrados. Su construcción fue terminada en 2001. El NAP de las Américas sirve como un relé para Servicio de Telecomunicaciones Diplomático del Departamento de Estado de los Estados Unidos.

---

[1]Vid. "Diccionario del Estudiante" en ciberespacio | Diccionario del estudiante | RAE, con acceso el 22/05/2024. Concepto de ciberespacio según la Real Academia Española.

[2]Vid. "Nombres de Dominio" en https://www.ujaen.es/servicios/sinformatica/catalogo-de-servicios-tic/nombres-de-dominio-dns, con acceso el 01/04/2024. DNS, son las siglas en ingles de Domain Name System o mejor conocido en español como Sistema de Nombres de Dominio, el cual es un conjunto de protocolos y servicios que permiten la asignación de nombre a direcciones IP.

[3]Vid. "99% del mundo está conectado a Internet a través de cables submarinos" en https://www.camtic.org/actualidad-tic/99-del-mundo-esta-conectado-a-internet-a-traves-de-cables-submarinos/, con acceso el 25/05/2024. Hoy día el mundo está conectado a internet por medio de los cables submarinos.

[4] Vid. "Equinix" en https://es.wikipedia.org/wiki/Equinix, con acceso el 25/05/2024. Dentro de la industria es considerada como un centro de procesamiento de datos.

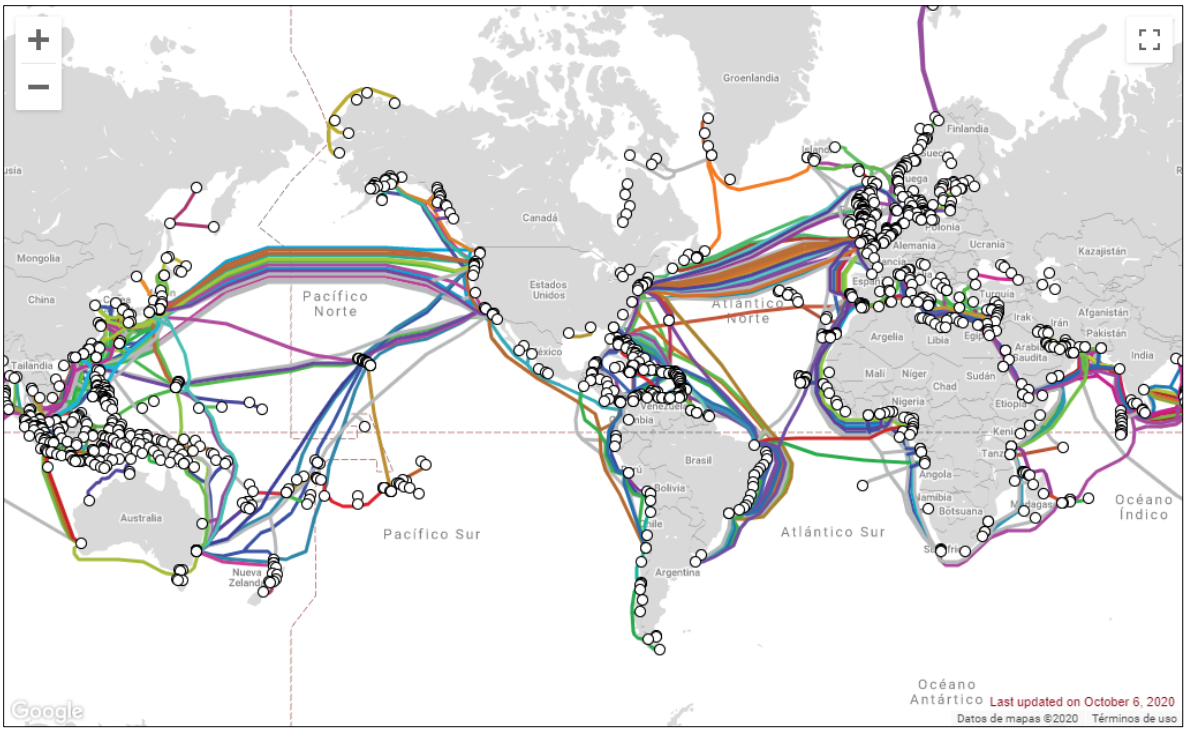


Figura 1 Cables submarinos que realizan la conexión interoceánica de internet

La conexión de internet de Latinoamérica se hace a través del Network Access Point (NAP) de las Américas es un centro de datos de gran tamaño y punto de intercambio de Internet en Miami, Florida, dirigido por Equinix Inc. Es una empresa multinacional estadounidense con sede en Redwood City, California, que se especializa en conexión a internet y centros de datos, la compañía lidera la cuota de mercado global de centros de datos de colocación, con 200 centros de datos en 24 países en los cinco continentes.[5] Alberga una de las instancias del servidor raíz del sistema de nombres de dominio. El edificio cuenta con seis pisos y una superficie de alrededor de 70.000 metros cuadrados. Su construcción fue terminada en 2001. El NAP de las Américas sirve como un relé para Servicio de Telecomunicaciones Diplomático del Departamento de Estado de los Estados Unidos.

En el ciberespacio, las fronteras físicas no existen de la misma manera que en el mundo real. Esto significa que las leyes y regulaciones de un país pueden ser difíciles de aplicar a actividades que ocurren en servidores ubicados en otros países. La soberanía de los Estados se ve desafiada porque el ciberespacio permite la comunicación y el intercambio de información sin restricciones geográficas.

Una vez se ha desmitificado el carácter virtual del ciberespacio y lo hemos traducido en territorios interconectados, la aplicación del *ius puniendi*, para los casos de delitos informáticos y en lo particular los que nos competen en cuanto a los Nombres de Dominio, puede estar definida por la jurisdicción no solo donde se materializo en delito, sino también a donde se gestó el hecho generador, que como vimos podrá ser en cualquier país interconectado en la red informática internet.

[5]Vid. “Equinix” en https://es.wikipedia.org/wiki/Equinix, con acceso el 25/05/2024. Dentro de la industria es considerada como un centro de procesamiento de datos.

Los Nombres de Dominio y su relación con la Propiedad Intelectual y las Marcas.

Una vez se ha establecido el enfoque de la jurisdicción con base a la territorialidad del internet, es importante ahora establecer qué relación tiene para las Sociedades Los Nombres de Dominio y la Propiedad Intelectual y Marcas, para esto se puede decir que un Nombre de Dominio es un nombre fácil de recordar asociado a una (IP) física de internet. Esta dirección física, permite encontrar servidores en internet y devolver las páginas web que actualmente utilizamos para consulta. Más adelante se describirá a detalle un apartado técnico de cómo funciona un Servicio de Dominio de Internet.

Los Nombres de Dominio de internet que son conocidos como DNS fueron creados en su forma más básica para trasladar de una manera fácil de leer a los humanos, los Nombres de Dominio en dirección de internet, de tal forma que cada vez que una persona quiere navegar por internet este nombre de dominio es trasladado a una dirección física de internet (IP Address), que puede ser un octeto de la siguiente forma 93.184.216.34. Esta forma tan común que actualmente conocemos data de 1987 y sigue utilizándose hoy en día en cada sitio web que las personas utilizan para poder navegar, siendo una especie de directorio telefónico donde podemos encontrar estos nombres de las páginas que deseamos consultar.

Con el auge y la explosión del Internet actualmente si inferimos 1 DNS por cada sitio web, estamos hablando que a 2021 existían 1.88 mil millones de páginas de internet con DNS.[6] A parte de la utilidad técnica de los Nombres de Dominio para encontrar sitios web, a través de una convención entendible para el usuario diario de los sitios web, el contar con un nombre de dominio de un sitio web puede traer implicaciones de derechos de propiedad intelectual, además sirven para salvaguardar la reputación y el valor comercial de las marcas y empresas que tiene presencia en línea.

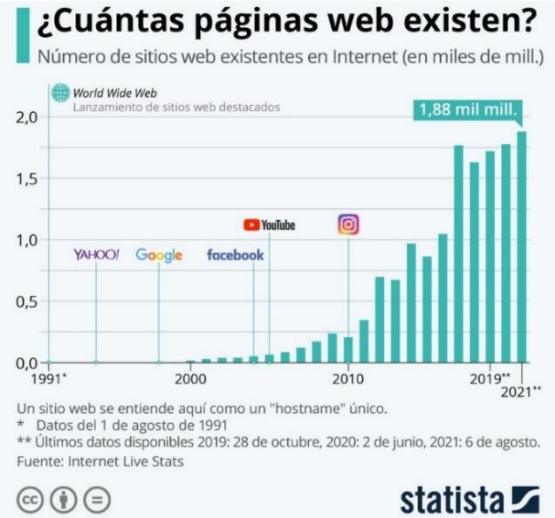


Figura 2 Sitios web creados a nivel mundial al mes de agosto de 2021

[6]Vid. "¿Cuántos sitios web hay en el mundo?", https://es.statista.com/grafico/19107/numero-de-sitios-web-existentes-en-internet/, con acceso el 01/04/2024. El articulo hace referencia a evolución que ha tenido la web desde el lanzamiento del World Wide Web por parte de físico en agosto de 1991.

Existen actualmente entidades que se encargan de velar por exclusividad y la integridad de los Nombres de Dominio precisamente para que estos cumplan con su propósito de exclusividad, valor comercial de marca. Además, el contar con un nombre de dominio puede tener implicaciones en cuanto a la privacidad y protección de los datos de los usuarios que pueden ser a nivel local o global y si bien originalmente los Nombres de Dominio estaban destinados a realizar únicamente la función técnica de facilitar la conectividad entre computadoras a través de Internet, los Nombres de Dominio, debido a su forma fácil de recordar y amigable para el ser humano, han llegado a constituir identificadores comerciales. Se utilizan habitualmente en publicidad como medio para indicar la presencia de una empresa o negocio en Internet (Ver Figura 3). Las empresas se han dado cuenta del importante potencial de un sitio web en Internet como medio para proporcionar información y ofrecer bienes o servicios directamente al público consumidor.

Con el crecimiento de Internet, los Nombres de Dominio han entrado en conflicto con las marcas. La posibilidad de que se produzca tal conflicto surge de la falta de conexión entre el sistema de registro de marcas, por un lado, y el sistema de registro de Nombres de Dominio, por otro. El primer sistema (marcas) es administrado por una autoridad (gubernamental) con carácter territorial (ya sea nacional o regional), lo que da lugar a derechos por parte del titular de la marca que pueden ejercerse dentro del territorio pertinente.

Este último sistema (Nombres de Dominio) suele ser administrado por una organización no gubernamental sin ninguna limitación funcional: los Nombres de Dominio se registran por orden de llegada y ofrecen una presencia mundial única en Internet[7].



Figura 3 Ejemplo de Resolución de Nombre de Dominio para páginas de Internet.

El potencial de conflictos inherente a los dos diferentes sistemas de registro ha sido aprovechado por personas que han adoptado la práctica de registrar, como Nombres de Dominio para ellos mismos, las

[7]Vid. "Primer Proceso de la OMPI relativo a los nombres de dominio de Internet: Archivo" en Primer Proceso de la OMPI relativo a los nombres de dominio de Internet: Archivo (wipo.int), con acceso el 01/04/2024. La OMPI desde 1998, inició con el proceso internacional para formular recomendaciones en temas de propiedad intelectual relacionadas con los DNS.

marcas de otras personas o empresas ("cybersquatting"[8], ciberocupación[9]). Los conflictos entre nombres de dominio y marcas presentan características inusuales que desafía la capacidad del sistema judicial ordinario. Este sistema, al tener una base territorial, no siempre puede ofrecer una solución integral a un conflicto de dimensiones globales. Además, los litigios pueden ser lentos y costosos, lo que puede llevar a una situación de facto en la que resulta más rápido y económico para el titular de una marcar negociar con un ciberocupante y recomprar sus derechos sobre un nombre de dominio, en lugar de intentar recuperarlos a través de litigios.

La relación entre los Nombres de Dominio de Internet y las marcas fue abordada a partir de 1996 por el Comité Internacional Ad Hoc (IAHC), que emitió su "Memorando de entendimiento sobre el espacio de Nombres de Dominio genéricos de alto nivel del sistema de Nombres de Dominio de Internet" (gTLD-MoU) en mayo de 1997. Teniendo en cuenta el asesoramiento proporcionado por la Organización Mundial de Propiedad Intelectual (OMPI) sobre propiedad intelectual y cuestiones de resolución de disputas, la IAHC (más tarde el Comité de Supervisión de Políticas (POC) desarrolló un sistema de resolución de disputas para abordar posibles conflictos entre marcas y Nombres de Dominio[10].

Para ejemplificar un caso de Cybersquatting, se puede analizar la sentencia del Juez de lo Civil y Comercial Federal 7, Secret. N° 13 el 26/11/1997 en el caso Heladerías Freddo S.A. c. Spot Network, por apropiación indebida de nombre FREDDO para internet[11]. Heladerías Freddo S.A., solicitó el cese del uso de nombre de dominio y de la marca FREDDO como nombre de domino por parte de la empresa Spot Network, ya que cuando se trató de registrar el nombre FREDDO como nombre de domino este ya había sido ocupado por Spot Network. Al no haber respuesta de la empresa, se solicita medida cautelar, ante lo cual el Juez solicita a la autoridad encargada de la administración de dominio que suspenda el registro freddo.com.ar.

Después de mediación entre las partes se dispuso la medida cautelar solicitada, suspensión preventiva del nombre de dominio freddo.com.ar, obtenido por Spot Network, siendo la razón de la resolución que a primera vista (*prima facie*) se había realizado una variante del uso indebido de la marca ajena. El Juez dio lugar a la medida ya que existía la intención de opacar la marca del demandante o existía la intensión de extorsionarlo por el uso del nombre, ya que solo existía el mero uso de dominio, sin intención de vender u ofrecer para la venta de productos o servicios que ostenten la marca por parte del demandado, más adelante en el desarrollo del ensayo se encontrarán otros ejemplos y los procesos para solventar conflictos de apropiaciones de Nombres de Dominio.

[8]Vid. "Cybersquatting, qué es y cómo protegerse" en https://www.incibe.es/empresas/blog/cybersquatting-y-protegerse, con acceso el 01/04/2024. La apropiación de nombres de dominio o cybersquatting o, básicamente consiste en registrar un nombre de dominio que simula ser uno legítimo y posteriormente utilizarlo con fines fraudulentos.
[9]Vid. "¿Qué es la ciberocupación?" en https://latam.kaspersky.com/resource-center/preemptive-safety/cybersquatting, con acceso el 01/04/2024. Es una de las formas de ciberdelito, por medio del cual alguien puede comprar o registrar un nombre de dominio idéntico o similar a un dominio que ya existe con la intención de sacar algún tipo de utilidad o una ganancia significa de una marca ya registrada.
[10]Vid. "Primer Proceso de la OMPI relativo a los nombres de dominio Internet: Archivo" en https://www.wipo.int/amc/es/processes/process1/index.html, con acceso el 01/04/2024. En junio de 1998, la Organización Mundial de la Propiedad (OMPI) inició el proceso internacional para formular las recomendaciones de propiedad intelectual que tengan relación con los nombres de dominio de internet.
[11] Vid. FERNANDEZ DELPECH. H. *Manual de Derecho Informático.* 1a ed. Abeledo Perrot, Buenos Aires, 2014, p.146.

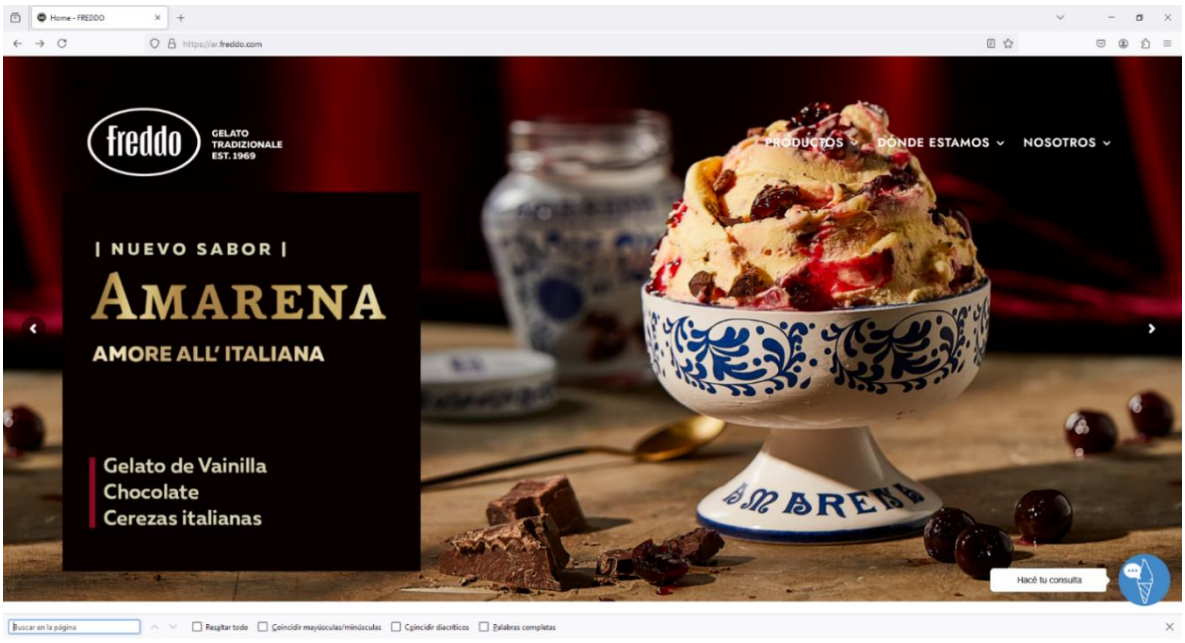


Figura 4 Pagina web de la Heladería Freddo S.A.

¿Cómo funciona un Servicio de Nombre de Dominio?

Antes de entrar en detalle del funcionamiento de los Servicios de Nombre de Dominio (DNS), es importante tomar en cuenta que, a partir de esta descripción de la operación de DNS, será más fácil comprender los tipos de ataques en internet que pueden sufrir los Nombres de Dominio y como se deberían tipificar los delitos derivados del uso inapropiado de las Tecnologías de la Información y las Comunicaciones (TIC).

De una manera resumida un servicio de dominio tiene varios nodos que se buscan entre si hasta llegar al Servidor de Nombre de Dominio que devuelve conforme al nombre digitado por el usuario en el navegador, la dirección de internet (*dirección ip*) que lo llevará hasta el servidor que contiene las páginas web que traerán las páginas web consultadas por el usuario.

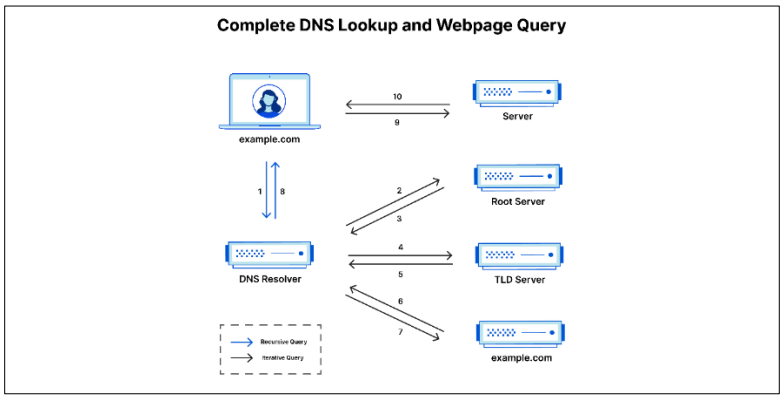


Figura 5 Consulta DNS para encontrar un sitio web

Los usuarios generalmente no se comunican directamente con el servidor DNS: la resolución de nombres se hace de forma transparente por las aplicaciones del cliente (por ejemplo, navegadores, clientes de correo y otras aplicaciones que usan Internet). El espacio de nombres de dominio tiene una estructura arborescente. Las hojas y los nodos del árbol se utilizan como etiquetas de los medios. El punto en el extremo derecho de un nombre de dominio separa la etiqueta raíz de la jerarquía.

Este primer nivel es también conocido como dominio de nivel superior (TLD, por sus siglas en inglés). Los objetos de un dominio DNS (por ejemplo, el nombre del equipo) se registran en un archivo de zona, ubicado en uno o más servidores de nombres.[12]

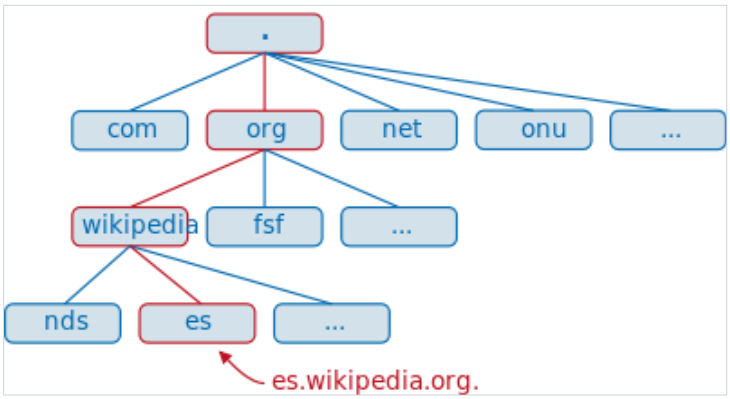


Figura 6 Jerarquía de nombres de dominio

Como ejemplo de la estructura de Nombres de Domino podemos considerar el ejemplo del sitio http://elsalvador.com, el cual tiene el ¨.¨ como un servidor principal llamado servidor raíz, que están distribuidos a nivel mundial y luego van los servidores de nivel superior (Top Level Domain, TLD), que para el ejemplo en cuestión seria .com (comercial), luego se identifican los servidores de segundo nivel que llevan el nombre que identifica el Nombre de Dominio y que por lo general es el que está identificado con el nombre que representa la Marca, en este caso , el servidor raíz es [.] , servidor gcTLD es [com] y como servidor de segundo nivel [elsalvador] , así se resuelve el nombre completo que identifica al sitio web en cuestión. Para los casos de servidores TLD, que hacen referencias a países, estos se denominan ccTLD, country code Top Level Domain. Para un sitio web como http://vidri.com.sv , el servidor ccTLD sería [sv] que describe a El Salvador como país del dominio y como servidor de segundo nivel [vidri.com] para clasificarlo dentro del dominio de El Salvador como un sitio comercial.

Un servidor raíz (root server en inglés) es un servidor de nombres para la zona raíz del Sistema de nombres de dominio de Internet (DNS). Los servidores de nombres raíz son una parte fundamental de Internet, ya que son el primer paso en la traducción (resolución) de los nombres de host legibles en direcciones IP que se utilizan en la comunicación entre los hosts de Internet.[13]

[12]Vid. “Sistemas de nombres de dominio” en https://es.wikipedia.org/wiki/Sistema_de_nombres_de_dominio, con acceso el 25/05/2024. La función más importante de los nombres de dominio es la resolución de los nombres de dominio.
[13]Vid. “Servidor raíz” en https://es.wikipedia.org/wiki/Servidor_ra%C3%ADz, con acceso el 25/05/2024. Son servicios de red que proveen respuestas a nuestros dispositivos.

Dada una consulta de cualquier dominio, el servidor raíz proporciona al menos el nombre y la dirección del servidor autorizado de la zona de más alto nivel para el dominio buscado. De manera que el servidor del dominio proporcionará una lista de los servidores autorizados para la zona de segundo nivel, hasta obtener una respuesta razonable. Existen 13 servidores raíz en toda Internet, cuyos nombres son de la forma letra.root-servers.net, aunque siete de ellos no son realmente servidores únicos, sino que representan múltiples servidores distribuidos a lo largo del globo terráqueo (ver tabla siguiente). Estos servidores reciben miles de consultas por segundo y a pesar de esta carga la resolución de nombres trabaja con bastante eficiencia.[14]

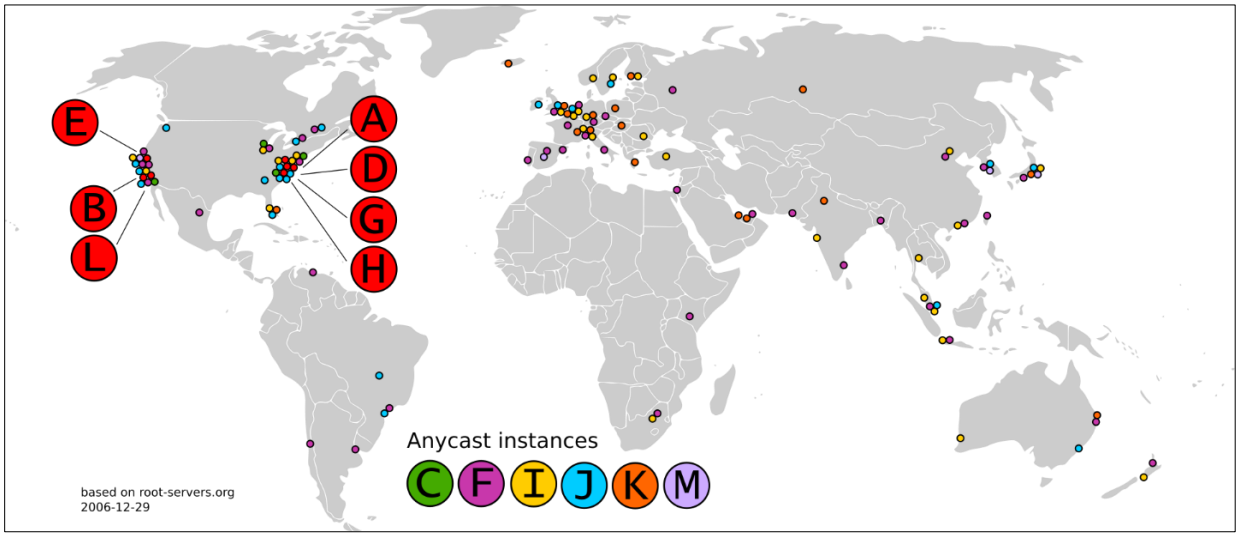


Figura 7 Localización de los servidores raíz de internet

Prácticas de abuso de DNS

Para entender las prácticas de abuso de DNS, es importante considerar que los delitos cibernéticos organizados pueden incluir grupos delictivos organizados que participan en el delito y delincuentes cibernéticos u otros grupos que no cumplen los criterios establecidos en la Convención contra la Delincuencia Organizada, que realizan actividades típicamente asociadas con la delincuencia organizada[15]. De tal manera que los grupos delictivos organizados pueden o no operar en el ciberespacio y en cuanto a los delitos cibernéticos organizados aún no se tiene claro su alcance al momento de operar. A continuación, se explicará cómo están organizados los nuevos grupos de ciberdelicuentes, las técnicas que actualmente se usan para poder llevar ataques a diferentes blancos y que tipos de ataques pudiesen llevarse a cabo contra los DNS de las Sociedades.

[14]Vid. "Servidor raíz" en https://es.wikipedia.org/wiki/Servidor_ra%C3%ADz, con acceso el 25/05/2024. Son servicios de red que proveen respuestas a nuestros dispositivos.

[15]Vid. "Grupos delictivos que participan en los delitos cibernéticos organizados" en https://www.unodc.org/e4j/es/cybercrime/module-13/key-issues/criminal-groups-engaging-in-cyber-organized-crime.html, con acceso el 02/04/2024. El articulo menciona que los estudios también han demostrado que los grupos delictivos han aprovechado de los beneficios que la tecnología brinda para cometer delitos cibernéticos o para facilitar las actividades de la delincuencia organizada fuera del ciberespacio.

Según estudio publicado por Trend Micro, empresa especialista en software de protección contra ciberataques, los grupos criminales pueden operar como verdaderas empresas, inclusive poseen una estructura formal, pagan salarios a sus miembros (hasta el 80% según el estudio, tienen un departamento dedicado a la gestión administrativa, para ponerse en perspectiva, una empresa mediana de cibercriminales puede tener de 6 a 49 empleados y hasta 50 millones de facturación, producto de las actividades cibercriminales. Quienes componen estas empresas son verdaderos profesionales del cibercrimen de todas partes del mundo. En este sentido, estas empresas tienen diferentes modelos de ataques, hoy se vuelve muy común el uso de negocios como Ransomware as a Service, Malware as a service, donde las empresas ya no realizan los ataques directamente, sino que se vuelven traficantes de los programas que permiten realizar los ataques, vendiéndolos por un precio accesible o si se prefiere ellos ejecutan los ataques directamente.

Estas empresas delictivas tienen códigos estrictos de conducta, por ejemplo, los pagos no pueden cancelarse una vez se dé la orden de ataque, además hay grupos que tienen prohibido realizar ataques a los países que son miembros del grupo delictivo. Otro punto interesante para considerar es que los ciber atacantes se vuelven especialistas por sectores de la economía, los hay que atacan los sectores energéticos, finanzas, salud, etc., importante también considerar la motivación, hemos hablado de aquellos grupos que tienen motivaciones económicas, como los que mencionamos en estos párrafos, otros lo hacen por notoriedad, también los hay que realizan estos tipos de ataque por temas políticos que son identificados con el tema hacktivistas, cuyos blancos son países y figuras políticas de dichos países.

Un ejemplo de estos grupos delictivos es el grupo Ransomhub, que en abril de este año 2024, ataco a la Financiera Constelación de El Salvador [16], este grupo se proclama estar formado por hackers de diferentes países que tiene como finalidad el lucro, además se abstienen de que países como Cuba, China, Corea del Norte, sean sus blancos. Según el perfilamiento de este grupo se sugiere que podrían ser rusos, los cuales son reclutados en el foro de la Darkweb llamado RAMP[17] Es importante conocer el perfil del atacante y como opera ya que es difícil en un caso de estos ataques establecer la jurisdicción del ataque y más establecer la individualización del delito, como en el caso de este ataque realizado en El Salvador y que se ha adjudicado el grupo Ramsonhub.

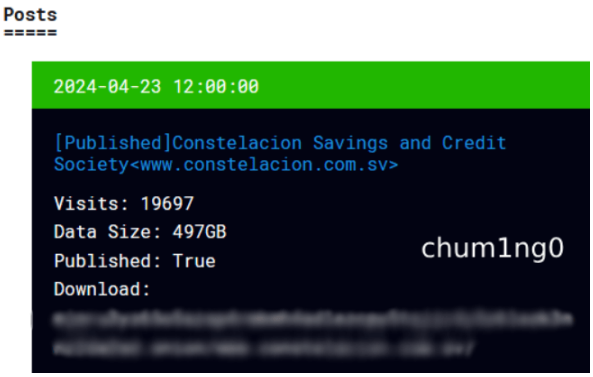


Figura 8 Imagen de un foro de la deep web donde se han filtrado los datos de FInanciera Constelación

[16] Vid. "Hackers exponen datos de clientes de la Sociedad de Ahorro y Crédito Constelación S.A. de C.V." en Hackers exponen datos de clientes de la Sociedad de Ahorro y Crédito Constelación S.A. de C.V. - La Prensa Gráfica (laprensagrafica.com), con acceso el 22/06/2024. La información de la institución financiera fue extraída por un grupo de hackers que roba información y luego pide dinero a cambio de no liberarla

[17] Vid. "Dark Web Profile: RansomHub", en https://socradar.io/dark-web-profile-ransomhub/, con acceso el 22/06/2024. RansomHub afirma que se debe de cumplir con los acuerdos y requisitos establecidos durante las negociaciones.

Entre 2018 y 2019, otro estudio, pero de la empresa de ciberseguridad Kaspersky, reveló un aumento significativo en los ataques dirigidos a datos, con incrementos del 33% y 112%. Sin embargo, este incremento en los ataques no se ha visto acompañado por un aumento en la protección y los esfuerzos en ciberseguridad por parte de las empresas. El estudio mostró que más del 57% de los encuestados no cuenta con una política de ciberseguridad, y en el caso de las medianas empresas, esta cifra asciende al 71%. Esto implica que las pequeñas y medianas empresas están en mayor riesgo de enfrentar consecuencias legales si no cumplen con las leyes pertinentes del país.

Dado que el ciberespacio es extremadamente dinámico, la legislación cibernética debería evolucionar continuamente para garantizar una protección óptima. No garantizar la seguridad de los datos de los clientes de una empresa contra ciberataques sofisticados podría generar multas significativas y daños en la reputación de la empresa. Todas las empresas, pero especialmente las pequeñas y medianas, deben conocer las consecuencias legales de una violación de datos y las soluciones disponibles que pueden protegerse de los ciberataques y sus consecuencias.

Además de la ciberocupación ("Cybersquatting") existen otros tipos de abusos contra los Nombres de Dominio de Internet, ya sea que se realicen a través de técnicas genéricas como el uso de malware, phishing, ramsomware, a ataques específicos de DNS como, inundación, envenenamiento de cache, DNS fantasma, etc. Todos estos ataques tienen su particularidad, sin embargo, al igual que las implicaciones legales varían dependiendo del alcance del ataque y este a su vez de la motivación del atacante. Las motivaciones de los atacantes como se mencionó anteriormente pueden ser desde lucrarse, afectar la reputación ya sea por venganza, competencia, política (hacktivismo) o el deseo de ganar reputación en la comunidad de hackers.

Se definen algunos tipos de ataques relacionadas al abuso del DNS, estos ataques pueden variar en complejidad y alcance, pero todos tienen el objetivo común de explotar vulnerabilidades para causar daño o robar información.

Ataques DNS:

Las técnicas vistas anteriormente se realizan para atacar diferentes objetivos, en este caso en particular los ataques van dirigidos a los Servicios de Nombres de Dominio. A continuación, se presentan los ataques contra Servicios de Nombre de Dominio que se consideran más importantes:

1. Secuestro DNS:

Un secuestro DNS sucede cuando un atacante tiene control de a donde una dirección de internet redirige las páginas permitiendo al atacante redirigir al usuario a una página similar para obtener sus datos.

Un ejemplo de estos ataques fue el realizado a la billetera de criptomonedas Waves en 2018, que eran redirigidos a una página falsa donde se les pedía que introdujeran sus palabras claves para recuperar fondos[18].

[18] Vid. "Página de Waves fue víctima de un secuestro DNS por algunas horas" en https://www.criptonoticias.com/seguridad-bitcoin/pagina-waves-victima-secuestro-dns-algunas-horas/ con acceso el 22/06/2024. Ejemplo de ataque de secuestro de DNS.

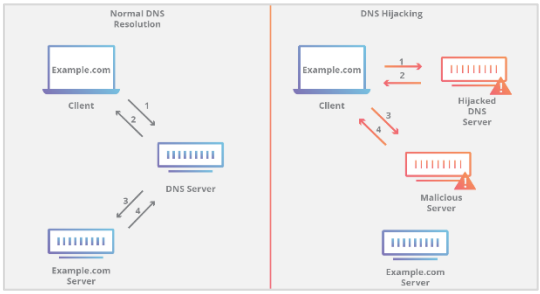


Figura 9 9 Secuestro DNS

2. Secuestro del enrutador (router):

Este secuestro suele ser el primer punto de ataque de muchos ciberdelincuentes. Esto se debe a que muchos enrutadores tienen contraseñas predeterminadas o vulnerables, por lo tanto, pueden ser descifradas fácilmente. Una vez obtenido el acceso los atacantes se apropian del router y modifican la configuración de DNS, afectando a todos los usuarios conectados a este dispositivo ya infectado.

En mayo 2018 el FBI y empresas privadas de ciberseguridad, alertaron del troyano Roaming Mantis, posiblemente de Asia, que buscaba obtener información de los usuarios enrutándolos por DNS a nuevas paginas maliciosas para obtener datos, por lo que el FBI hizo pública la solicitud que se reiniciaran los enrutadores de varias marcas en todo el mundo para poder eliminar 2 de tres variantes[19].

3. Ataque DDoS al servidor DNS:

Un ataque DDOS, o de denegación de servicios, no es más que un ataque realizando millones de peticiones a un sitio web, hasta que este no tenga la capacidad de poder atenderlas y entonces comienza a mostrar el famoso error 404 "*Page not found*".

En junio de 2023, Microsoft sufrió uno de estos ataques afectando servicios como Azure, Outlook y OneDrive, el ataque apunta al grupo de hackers Anonymous Sudan que promueven las ideologías musulmanas o el grupo Killnet, hackers rusos que usan al grupo Anonymous Sudan como cortina de humo. Sin embargo, Microsoft logro contener el ataque si brevemente afecto algunos servicios.

[19]Vid. "FBI lanza alerta mundial por ciberataque y pide reiniciar los routers" en https://www.laprensagrafica.com/techlife/FBI-lanza-alerta-mundial-por-ciberataque-y-pide-reiniciar-los-routers-20180528-0063.html, con acceso el 22/06/2024. Ejemplo de secuestro de un enrutador.

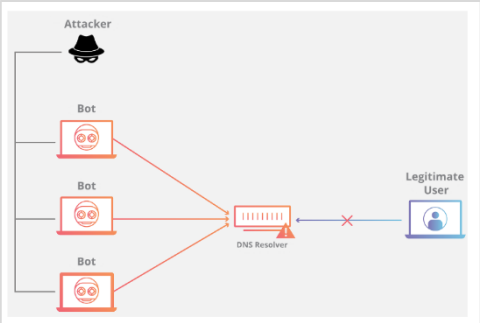


Figura 10 10 Modo de ataque DDoS para DNS.

4. Ataque de tipo intermediario (MitM Man-in-the-Middle):

Mediante el uso de herramientas especializadas, el ciberdelincuente intercepta la comunicación entre el usuario y el servidor DNS y responde con direcciones IP falsas, redirigiendo así el tráfico hacia su propio servidor[20].

En 2023 datos de pago de clientes fueron sustraídos de Air Europa, usando esta técnica, se supone que se secuestró un equipo intermedio por donde pasaban los datos de los clientes y fueron sustraídos. Massanet recomendó a los usuarios cancelar las tarjetas con las que reservaron sus viajes, además se encuentran en el escrutinio público y judicial en cuanto si realizaron todo lo necesario para resguardar la información de sus clientes[21].

5. Túnel de DNS:

Este ataque usa otros protocolos para transmitir consultas y respuestas DNS a través de un túnel. Los atacantes pueden utilizar SSH, TCP o HTTP para pasar malware o información robada a consultas DNS, sin que los detecten la mayoría de los firewalls[22].

El pirata informático infecta la computadora de la víctima prevista con malware, pero es difícil de detectar porque no bloquea las solicitudes de DNS. Luego, el usuario continúa enviando solicitudes al resolutor de DNS para obtener direcciones IP, pero el resolutor reenvía las solicitudes al servidor del delincuente, desde donde comienza el túnel: se crea un corredor «seguro» con la computadora de la víctima y se accede a él para fines malintencionados.

[20]Vid. "Secuestro de DNS: Una amenaza silenciosa en el mundo digital" en https://www.accessq.com.mx/secuestro-dns/, con acceso el 20/05/2024. El secuestro de DNS es una tácita utilizada por ciberdelincuentes, y lo utilizan para redireccionar el tráfico de internet, desde un sitio web legítimo hacia uno malicioso.
[21]Vid. "¿Cómo fue hackeada Air Europa? Hipótesis de experto" en https://www.hosteltur.com/159724_como-fue-hackeada-air-europa-hipotesis-de-experto.html, con acceso el 27/06/2024. Ejemplo, de ataque de tipo intermediario.
[22]Vid. "Secuestro de DNS: Una amenaza silenciosa en el mundo digital" en https://www.accessq.com.mx/secuestro-dns/, con acceso el 05/05/2024. El secuestro de DNS es una tácita utilizada por ciberdelincuentes, y lo utilizan para redireccionar el tráfico de internet, desde un sitio web legítimo hacia uno malicioso.

6. Ataque zero-day:

Este tipo de ataque explota las vulnerabilidades desconocidas de un sistema o software. Una vulnerabilidad de día cero (también llamada amenaza de día cero) es un ataque que se aprovecha de una vulnerabilidad de seguridad que no tiene solución. Se denomina amenaza de "día cero" porque una vez que se descubre el fallo, el desarrollador o la organización dispone de "cero días" para dar con una solución. Una vulnerabilidad es un fallo involuntario de software o hardware a causa de un error de programación o de una configuración inadecuada. Como las vulnerabilidades no son intencionadas, son difíciles de detectar, y pueden pasar desapercibidas durante días, meses o incluso años. Una táctica habitual es distribuir malware a través de correos electrónicos de phishing que contengan archivos adjuntos o enlaces que tengan las vulnerabilidades incrustadas. Estas cargas útiles maliciosas se ejecutan cuando un usuario interactúa con el archivo adjunto o el enlace[23].

Un famoso ataque de día cero afectó a Sony Pictures Entertainment en 2014, cuando se hizo pública información confidencial, como copias de películas no estrenadas, comunicaciones por correo electrónico entre empleados de alto nivel y planes de negocio. Los atacantes utilizaron una vulnerabilidad de día cero para obtener esta información.

Las vulnerabilidades de día cero pueden tener un impacto devastador en una empresa. Estas vulnerabilidades, que son fallos de seguridad desconocidos para el desarrollador del software, pueden ser explotadas por atacantes antes de que se disponga de una solución. La consecuencia de un ataque de día cero incluyen la pérdida de datos valiosos o confidenciales, lo que puede resultar en daños financieros y legales significativos. Además, los clientes pueden perder la confianza en la empresa, afectando su reputación y relaciones comerciales.

Una vez definidas las técnicas y tipos de ataque, hay que responder la siguiente pregunta, ¿Qué implicaciones tiene para una Sociedad que su DNS sea secuestrado? El secuestro de DNS puede tener graves consecuencias para las empresas, incluyendo la interrupción significativa del negocio, lo que resulta en tiempo de inactividad y pérdida de productividad debido al cierre de aplicaciones en la nube o incluso en sus propias instalaciones. Los ciberdelincuentes pueden robar datos al redirigir a las víctimas a servidores maliciosos, recolectando credenciales e información sensible. Este tipo de ataque también puede dañar la reputación de la empresa, ya que los clientes, socios,

Aunque un DNS no es un bien jurídico por sí mismo, está estrechamente relacionado con varios aspectos legales que sí lo son. Por ejemplo, un DNS está vinculado a la propiedad intelectual, ya que un nombre de dominio puede ser una marca registrada y, por lo tanto, gozar de protección legal. Además, los DNS son esenciales para el funcionamiento de internet y la economía digital, lo que los convierte en componentes críticos de la infraestructura tanto nacional como internacional.

[23]Vid. "¿Qué es un ataque de día cero? en https://www.cloudflare.com/es-es/learning/security/threats/zero-day-exploit/ con acceso el 02/05/2023. Un ataque de día cero siempre se aprovecha de una vulnerabilidad de seguridad que no es conocida.

A continuación, un cuadro resumen donde se vincula el tipo de ataque DNS, su descripción, la técnica utilizada para realizar el ataque y un ejemplo de ataques que se han realizado.

Tipo de ataque	Descripción	Técnica	Ejemplo
Secuestro DNS	En un secuestro de DNS, el atacante redirige las consultas a un servidor de nombre de dominio diferente. Se puede llevar a cabo con malware o con una modificación no autorizada de un servidor DNS	Infección con Malware	Investigadores han descubierto que cibercriminales han estado ejecutando ataques de DNS hijacking para distribuir malware. Las víctimas han manifestado que su navegador web abría un sitio por sí solo que ofrecía descargar una app para mantenerse informado sobre el coronavirus (COVID-19), en nombre de la Organización Mundial de la Salud (OMS). Inyectaba un malware que malware se hacía de los datos financieros almacenados en el navegador, billeteras de criptomonedas, el historial del navegador y las cookies, archivos de texto y la información que el navegador almacena para autocompletar formulario, entre otra información.
Secuestro de enrutador	Este secuestro suele ser el primer punto de ataque de muchos ciberdelincuentes. Esto se debe a que muchos enrutadores tienen contraseñas predeterminadas o vulnerables, por lo tanto, pueden ser descifradas fácilmente. Una vez obtenido el acceso los atacantes se apropian del router y modifican la configuración de DNS, afectando a todos los usuarios conectados a este dispositivo ya infectado	Infección con Malware	La compañía de ciberseguridad Kaspersky Lab ha alertado sobre la expansión del 'malware' Roaming Mantis, de ciberataques a routers mediante la técnica de secuestro del sistema de nombres de dominio (DNS), que ha comenzado a afectar a usuarios europeos y que ha incorporado minería de criptomoneda.
Ataque DDoS al servidor DNS	Los servidores se ven saturados, ya que su tráfico se hace excesivo e incontrolable. Un ataque DDoS es un ataque volumétrico de denegación de servicio distribuido (DDoS)	Ataque de fuerza bruta	El mayor ataque DDoS hasta la fecha ocurrió en septiembre de 2017. Su tamaño fue de 2,54 Tbps y se dirigió a los servicios de Google. Google Cloud comunicó el ataque en octubre de 2020. Los atacantes enviaron paquetes falsificados a 180.000 servidores web, que a su vez enviaron respuestas a Google. No fue un incidente aislado. Los atacantes habían dirigido varios ataques DDoS a la infraestructura de Google durante los seis meses anteriores.
Ataque de tipo intermediario (MitM Man-in-the-Middle)	Mediante el uso de herramientas especializadas, el ciberdelincuente intercepta la comunicación entre el usuario y el servidor DNS y responde con direcciones IP falsas, redirigiendo así el tráfico hacia su propio servidor	Explotación de vulnerabilidades	En 2017, se detectó una importante vulnerabilidad en las aplicaciones de banca móvil de numerosos bancos de renombre, que dejaba a los clientes de iOS y Android expuestos a ataques MITM. El problema estaba relacionado con la tecnología de fijación de certificados diseñada para evitar el uso de certificados fraudulentos. Debido a que la fijación de certificados ocultaba la ausencia de una verificación adecuada del

			nombre de host, las pruebas de seguridad no identificaban a los atacantes, lo que en última instancia permitía que se produjeran ataques MITM.
Servidor DNS fraudulento	Este tipo de delito cibernético es mucho más complicado que el secuestro local porque no se puede controlar desde el dispositivo objetivo	Infección con Malware	El malware DNSChanger: Este ataque de pharming infectó millones de ordenadores en todo el mundo y redirigió el tráfico web de los usuarios a sitios fraudulentos. Modificaba la configuración DNS de las máquinas infectadas, redirigiendo a los usuarios a servidores malintencionados controlados por los atacantes. Esto les permitió interceptar información delicada y llevar a cabo diversas actividades fraudulentas
Sustracción de información mediante DNS	En este tipo de ataque informático, los hackers se aprovechan de las vulnerabilidades del servidor para robar datos	Infección con Malware	APT29 es un grupo sofisticado de atacantes que se cree que está patrocinado por el gobierno ruso. En 2015, los investigadores descubrieron que APT29 estaba utilizando un túnel DNS para comunicarse con su servidor C&C. El grupo estaba utilizando malware personalizado llamado Hammertoss para extraer datos de redes comprometidas mediante consultas y respuestas de DNS.
Túnel de DNS	Este ataque usa otros protocolos para transmitir consultas y respuestas DNS a través de un túnel. Los atacantes pueden utilizar SSH, TCP o HTTP para pasar malware o información robada a consultas DNS, sin que los detecten la mayoría de los firewalls. El pirata informático infecta la computadora de la víctima prevista con malware	Infección con Malware	El malware llamado GhostDNS se utiliza con frecuencia para apoderarse de servidores DNS y redirigir el tráfico a sitios web maliciosos. Los investigadores descubrieron que el virus GhostDNS se comunicaba con su servidor de control a través de un túnel DNS en 2018. Para recibir órdenes y robar datos de las PC comprometidas, el virus utilizaba solicitudes y respuestas de DNS.

Regulaciones y estándares internacionales.

A continuación, se analizan las regulaciones y estándares internacionales a cerca de los ataques informáticos en particular los ataques dirigidos a los Servicios de Nombre de Dominio (DNS).

Las regulaciones y estándares internacionales de DNS son fundamentales para garantizar la seguridad y estabilidad del sistema de nombres de dominio a nivel global. Las más importantes son:

ICANN (Internet Corporation for Assigned Names and Numbers): Supervisa la asignación de nombres de dominio y direcciones IP a nivel global.

IETF (Internet Engineering Task Force): Son recomendaciones adoptadas para mejorar la seguridad y la integridad del sistema DNS.

ISO/IEC 27001: Norma internacional de gestión de la seguridad de la información es relevante para las organizaciones que gestionan estructuras críticas de DNS, asegurando que se implementen controles de seguridad adecuados.

RFC (Request for comments): Son documentos publicados por el IETF, que contienen especificaciones técnicas para la implementación de directrices de los protocolos y servicios de internet, incluyendo el DNS.

Best Current Practices (BCP): Son las mejores prácticas actuales, como las publicadas por el IETF y otras organizaciones, a su vez, proporcionan directrices para la correcta configuración y operación de los servidores DNS.

Convenio Sobre Delitos Informáticos mejor conocido como Convenio de Budapest sobre delitos cibernéticos o simplemente Convenio de Budapest: es el primer tratado internacional que aborda de manera integral los delitos informáticos y los delitos cometidos a través de Internet. Este tratado tiene como objetivos principales la armonización de las leyes entre las naciones, la mejora de las técnicas de investigación y el aumento de la cooperación entre los países firmantes.

Derecho comparado.

El derecho comparado en la implementación o registro de los Servicios de Nombres de Dominio (DNS) y en la regulación de los ataques a los DNS presenta diferencias significativas debido a la naturaleza y objetivos de cada aspecto.

La implementación de los DNS se centra en la administración y gestión de los nombres de dominio que los diferentes países han adoptado diversas normativas para regular esta área, con el objetivo de garantizar un sistema de nombres de dominio eficiente y seguro.

Por ejemplo, en Estados Unidos, la Corporación de Internet para la Asignación de Nombres y Número (ICANN) juega un papel crucial en la supervisión de los DNS a nivel global. En la Unión Europea, el Reglamento General de Protección de Datos (GDPR), también influye en la gestión de los datos de registro de nombres de dominio.

Por otro lado, la regulación de los ataques a los DNS se enfoca en la ciberseguridad y la protección contra diversas amenazas. Los ataques a los DNS, como el envenenamiento de caché, el secuestro de DNS y los ataques de denegación de servicio (DDoS), requieren medidas legales y técnicas específicas para su mitigación.

Mientras que la implementación de los DNS se centra en la administración y regulación de los nombres de dominio para asegurar su correcto funcionamiento, la regulación de los ataques a los DNS se enfoca en la protección y defensa contra ciberamenazas. Ambos aspectos requieren un enfoque legal y técnico, pero con objetivos y desafíos distintos.

La implementación de los DNS busca mantener un sistema ordenado y accesible mientras que la regulación de los ataques a los DNS se orienta a salvaguardar la integridad y disponibilidad del sistema frente a posibles amenazas, es por ello por lo que a continuación desarrollamos de forma independiente.

Derecho Comprado en la Implementación de DNS.

Estados Unidos

La regulación del cambio de DNS se rige principalmente por la Ley de Asignación de Números de Internet, la cual establece los procedimientos y requisitos legales para la gestión de nombres de dominio. En este contexto, la Corporación de Internet para la Asignación de Nombres y Números (ICANN) juega un papel fundamental en la supervisión de la administración de los servidores DNS a nivel global, asegurando la estabilidad y seguridad del sistema de nombres de dominio.

Dentro de los Estados Unidos, la Administración Nacional de Telecomunicaciones e Información (NTIA) supervisa asuntos relacionados con el dominio de nivel superior .gov, garantizando que los dominios gubernamentales se gestionen de manera segura y eficiente. Por otro lado, la Autoridad de Números Asignados en Internet (IANA), una división de ICANN, es responsable de la gestión de los dominios .us, asegurando su correcta asignación y funcionamiento.

Además, la Corporación de Asignación de Nombres y Números de Internet (InterNIC) actúa como el registro central para los nombres de dominio .com, .net y .org, facilitando la coordinación y administración de estos dominios comerciales y organizacionales. Este sistema de regulación y supervisión asegura que el cambio de DNS se realice de manera ordenada y conforme a las normativas internacionales y nacionales.

Unión Europea

Aunque no se especifica en los resultados de búsqueda, las regulaciones sobre Nombres de Dominio varían entre los estados miembros de la Unión Europea. Las leyes y regulaciones sobre Nombres de Dominio están en gran parte regidas por las políticas de la Comisión Europea y las disposiciones de la legislación nacional de los estados miembros. Por ejemplo, el Registro de Internet para el Reino Unido (Nominet) es responsable de los dominios .uk, que incluyen. co.uk., org.uk y otros. Por otro lado, el European Registry for Internet Domains (EuRid) es responsable de los dominios .eu.

Es importante mencionar que la Unión Europea cuenta con el Reglamento General de Protección de Datos (GDPR), que establece normas estrictas sobre la protección de datos y la privacidad en línea. Este reglamento no solo afecta la gestión de los datos personales, sino que también tiene implicaciones significativas para la gestión de DNS y la respuesta a los ataques de DNS. Es importante mencionar que la Unión Europea cuenta con el Reglamento General de Protección de Datos (GDPR), que establece normas estrictas sobre la protección de datos y la privacidad exige que los datos personales recopilados durante el registro de dominios sean manejados con un alto nivel de protección y transparencia.

El Salvador:

La implementación del DNS en El Salvador, específicamente para dominios bajo .sv, se gestiona a través de SVNet, que es la entidad administradora de nombres de dominio en el país. Aunque El Salvador gestione sus propios dominios de nivel superior de código de país (ccTLD), es decir el “sv”, sigue las directrices y políticas establecidas por la ICANN.

Es crucial para las empresas y particulares que deseen realizar cambios en sus servidores DNS conocer y cumplir con las regulaciones establecidas en cada jurisdicción. La legalidad de modificar los servidores DNS puede estar sujeta a directrices específicas que buscan proteger la seguridad de la red, la propiedad intelectual y la privacidad de los usuarios. Además, es importante considerar las políticas de resolución de disputas de nombres de dominio, que pueden variar según la jurisdicción y el tipo de dominio.

Derecho Comparado en la Regulación a los Ataques de DNS.

País y/o Estado	Leyes	Ventajas	El Salvador
Estados Unidos	Cyber Security Act of 2015 (Ley de Ciberseguridad de EE. UU.).	Fue creada para mejorar la ciberseguridad facilitando el intercambio de información sobre amenazas cibernéticas entre el sector privado y el gobierno federal.	No existe.
	The National Cyber Incident Response Plan de 2017 (Plan de Respuesta a Incidentes Cibernéticos de 2017).	Coordina la respuesta a los incidentes cibernéticos.	No existe.
	NIST Cybersecurity Framework, Assesment, and Auditing Act of 2017 (Ley de Ciberseguridad, Evaluación y Auditoría del Instituto Nacional de Estándares y Tecnología de 2017).	Sirve de guía a las agencias federales en la implementación del maro de ciberseguridad.	No existe.
España	Código de Derecho de la Ciberseguridad.	Establece las principales normas para la protección del ciberespacio.	No existe.
China	Ley de Ciberseguridad China.	Regula el uso de Internet en China.	No existe.
México	Ley Federal de Protección de Datos Personales en Posesión de Particulares	La regulación de los servicios de Nombres de Dominio y la infraestructura relacionada está a cargo del Instituto Federal de Telecomunicaciones (IFT), el cual es un organismo autónomo encargado de regular y supervisar el sector de las telecomunicaciones y la radiodifusión.	Veto al Decreto Legislativo No. 875 de fecha 07 de mayo de 2021. "Ley de Protección de Datos Personales".
	Ley Federal de Telecomunicaciones y Radiodifusión		Ley de Telecomunicaciones. Regula y supervisa las actividades relacionadas con el sector de las Telecomunicaciones y las tecnologías de la información.
	Ley Federal de Delitos Informáticos		Ley Especial Contra los Delitos Informáticos y Conexos. Incluye delitos relacionados con el mal uso de los DNS.
Rusia	Ley Federal de la Federación sobre la Comunicación.	Son algunas de las leyes y regulaciones con los servicios de Nombres de Dominio (DNS) y están principalmente vinculadas a las regulaciones de internet, a la privacidad de los datos y la seguridad cibernética.	Ley de Telecomunicaciones. Regula y supervisa las actividades relacionadas con el sector de las Telecomunicaciones y las tecnologías de la información.
	Ley Federal de Protección de Datos Personales.		No existe.
	Ley de Seguridad de la Información		No existe.

Unión Europea	Directiva sobre las redes y sistema de información (Directiva (UE) 2016/1148.	Establece las obligaciones de seguridad para los operadores de servicios de servicios digitales.	No existe.
	Reglamento de Ciberseguridad de la UE.	Se introdujo el sistema de certificación para toda la UE.	No existe.

A pesar de que las Sociedades están consciente de los riesgos que implican los ataques cibernéticos, se pueden iniciar acciones legales si no se notifica de forma oportuna primero a las personas y autoridades interesadas sobre la violación de datos. La falta de una respuesta rápida para mitigar los daños y las medidas de seguridad de los datos podrían ser otros motivos de litigio. En algunas jurisdicciones regionales, los clientes y accionistas podrían iniciar acciones legales. El demostrar el más alto nivel de cumplimiento y contar con un plan de respuesta eficaz, puede reducir la cantidad de multas y otros costos.

A nivel mundial, las grandes empresas cuentan con un equipo jurídico que se encarga de todos los trámites legales necesarios. Sin embargo, si se trata de una pequeña o mediana empresa, no se trata sólo de multas, sino también del mayor valor del negocio: su propiedad intelectual.

¿Qué hacer en caso de un ciberataque?

A nivel de otros países si una organización o sistema sufre un ciberataque que conduce a una violación de datos, se está legalmente obligado a notificar a las personas afectadas lo antes posible.

Si la empresa reside en la Unión Europea, según el Reglamento General de Protección de Datos (RGPD), debe informar a la Oficina del Comisionado de Información (ICO) dentro de las 72 horas posteriores a la violación de datos.

En los Estados Unidos, se debe notificar al fiscal general del estado en cuestión dentro del plazo prescrito. Dado que se trata de privacidad y protección de datos del consumidor, se supone que debe notificar a los reguladores como la Comisión Federal de Comercio (FTC), la Oficina de Protección Financiera del Consumidor (CFFPB) y la Comisión Federal de Comunicaciones (FCC) para garantizar la divulgación oportuna de los datos de ataques cibernéticos.

Actualmente, en El Salvador, existe una ausencia de un proceso formal y regulado para manejar ciberataques. Esto significa que las empresas pueden enfrentar desafíos adicionales al intentar gestionar las consecuencias legales y operativas de un ciberataque sin un marco legal claro que guie sus las acciones.

Legislación en El Salvador.

En el contexto de El Salvador, la gestión de los Nombres de Dominio ".sv" debe realizarse de manera técnicamente competente y los servidores de DNS deben permanecer operativos y accesibles en Internet. Esto implica que hay una responsabilidad legal y técnica en el mantenimiento de los DNS, lo que podría considerarse un bien jurídico en términos de la importancia de su correcto funcionamiento para la sociedad y la economía.

Además, la Ley Especial Contra los Delitos Informáticos y Conexos de El Salvador protege contra conductas delictivas que pueden afectar los sistemas informáticos y, por extensión, los DNS, lo que refleja la importancia de los DNS como parte de los bienes jurídicos protegidos por la ley.

El Dr. Santiago Acurio del Pino, establece que la tendencia es que la protección a los bienes jurídicos, se le haga desde la perspectiva de los delitos tradicionales, con una re-interpretación teleológica de los tipos penales ya existentes, para subsanar las lagunas originadas por los novedosos comportamientos delictivos[24].

Como resultado, los bienes jurídicos protegidos tendrán un enfoque nuevo para facilitar su persecución y su respectiva sanción por parte del órgano jurisdiccional competente. Esto implica que la legislación puede evolucionar para adaptarse a las nuevas formas de criminalidad y mejorar la eficacia del sistema judicial en la protección de los intereses sociales.

Por lo tanto, aunque un DNS no es un bien jurídico per se, está estrechamente relacionado con varios bienes jurídicos protegidos por la legislación salvadoreña.

En El Salvador, la regulación de los servicios de internet, incluyendo los DNS, se encuentra dentro del marco legal de las Telecomunicaciones y la Protección de Datos. Aunque no hay una ley específica que regule únicamente los DNS, existe la Ley Especial Contra los Delitos Informáticos y Conexos[25], que tiene como objetivo proteger los bienes jurídicos frente a conductas delictivas cometidas mediante tecnologías de la información y comunicación, lo que podría abarcar delitos relacionados con el mal uso de los DNS.

En el caso del cibersquatting al tener como fin lucrarse al registrar Nombres de Dominios que las empresas aún no han utilizado para luego venderlo por un valor muy superior al nombre de la marca, puede generar en los clientes y proveedores confusión por ejemplo venderlo al mejor postor a una marca de otro país que coincida con el nombre de marca, esto pude traer confusión en los clientes al encontrar correos empresariales y sitio web con nombre de dominio de la marca de su preferencia pero que pertenecen a otra empresa, además puede afectar sus estrategias de marketing al no estar en línea su nombre de dominio con el nombre de marca.

En El Salvador, la propiedad Intelectual es reconocida y garantizada como un derecho fundamental de las personas, por medio de la Constitución de la República, en su Artículo 103; en el que: *"se reconoce y garantiza el derecho a la propiedad privada en función social. Asimismo, se reconoce la propiedad intelectual y artística, por el tiempo y en la forma determinados por la Ley…[26]",* y cuenta con los siguientes instrumentos legales para el resguardo de un nombre de dominio:

- Ley de Propiedad Intelectual.
- Ley de Marcas y Otros Signos Distintivos; (Disposición especificas: Nombres de Dominio en Internet: Artículo 113-A).
- Ley de Procedimiento Uniformes para la Presentación, Trámite, Registro o Deposito de instrumentos, de los Registros de la Propiedad Raíz e Hipotecas, Social de Inmuebles, de Comercio y de Propiedad Intelectual.

[24]Vid. ACURIO DEL PINO, S, *Delitos Informáticos: Generalidades.* 2 ed. Quito: Pontificia Universidad de Católica de Ecuador. 2016, p.20

[25]Vid. "Ley Especial Contra Los Delitos Informáticos y Conexos" en https://www.asamblea.gob.sv/leyes-y-decretos/resultado-busqueda/, con acceso el 20/5/2024. Tiene como objeto principal proteger los bienes jurídicos de conductas delictivas que se comenten por medios tecnológicos.

[26]Vid. "Constitución de la República de El Salvador" en 171117_072857074_archivo_documento_legislativo.pdf (asamblea.gob.sv), con acceso el 21/05/2024.

- Código Penal (Disposiciones específicas: Acceso ilícito: Artículos 184, 185, Interferencia en los Datos: Artículo 186. Interferencia en el Sistema: Artículo 222. Fraude Informático: Artículo 216 numeral 5).

- Código Procesal Penal (Disposición especifica, Obtención y Resguardo de información electrónica: Articulo 201).

Por tanto, al revisar la Ley de Marca y Otros Signos Distintivos, es importante tomar en cuenta que para reforzar la identidad y presencia de la Marca en línea, el articulo "Art. 5.- La propiedad de las marcas y el derecho a su uso exclusivo se adquiere mediante su registro de conformidad con esta Ley…"[27], por tanto para cualquier proceso de reclamo ante un caso Cibersquatting tanto a nivel de jurisdicción local o que trascienda el uso de la marca a las fronteras, es necesario el registro de marca, por lo que se deberá hacer la solicitud de registro de marca en el Centro Nacional de Registro y cumplir con los requisitos establecidos en el artículo 10 de la referida Ley de Marca y Otros Signos Distintivos los cuales son :

"a) Designación de la autoridad a que se dirige; b) Nombre, razón social o denominación, nacionalidad, domicilio y demás generales del solicitante y el nombre, profesión y domicilio del representante legal o mandatario cuando la petición se haga por su medio; c) LA MARCA CUYO REGISTRO SE SOLICITA, DEBIENDO ADHERIRSE UN MODELO O EJEMPLAR. CUANDO LA MARCA ESTUVIESE CONSTITUIDA ÚNICAMENTE POR UN DISEÑO, EL SOLICITANTE LE ASIGNARÁ UNA FORMA DE IDENTIFICACIÓN. CUANDO LA MARCA ESTUVIESE CONSTITUIDA POR SONIDOS, LA REPRODUCCIÓN DE LA MISMA DEBERÁ SER NECESARIAMENTE DE CARÁCTER GRÁFICO, PUDIENDO EFECTUARSE MEDIANTE SU REPRESENTACIÓN EN PENTAGRAMA O POR CUALQUIER OTRO MEDIO CONOCIDO O POR CONOCERSE, ADEMÁS DEBERÁ ANEXARSE LA MARCA SONORA EN UN SOPORTE MATERIAL. CUANDO LA MARCA ESTUVIESE CONSTITUIDA POR ALGÚN ELEMENTO DENOMINATIVO Y ÉSTE TUVIESE SIGNIFICADO EN UN IDIOMA DISTINTO DEL CASTELLANO, SE DEBERÁ INCLUIR UNA SIMPLE TRADUCCIÓN DEL MISMO.(1); d) Una lista que contenga el nombre de los productos o servicios que distinguirá la marca, conforme a la clasificación establecida en el Art. 85 de esta Ley, con indicación de la clase a que correspondan; e) Las reservas que se hagan respecto del tipo de letra, color o combinación de colores, diseños o características de la marca, en la misma disposición en que aparezcan en el modelo, cuando fuese el caso. Las reservas que se formulen sobre elementos que no aparezcan en el modelo carecerán de valor; f) Indicación concreta de lo que se pide; g) Dirección exacta para recibir notificaciones; y h) Lugar y fecha de la solicitud y firma autógrafa del solicitante, apoderado o representante legal. Con la solicitud a que se refiere el inciso anterior deberá presentarse lo siguiente: a) Fotocopia certificada del poder legalmente otorgado, si la solicitud se hiciere por medio de mandatario, salvo que la personería de éste estuviere ya acreditada en el Registro, caso en el cual se indicará en la solicitud la fecha y el número del registro. Cuando el interesado presente original del poder podrá pedir que éste se razone en autos y se le devuelva; b) Quince modelos o ejemplares de la marca; y, c) Los documentos o autorizaciones requeridos en los casos previstos en los Artículos 8 y 9 de la presente Ley, cuando fuese pertinente. LOS SOLICITANTES PODRÁN GESTIONAR ANTE EL REGISTRO, POR SÍ O POR MEDIO DE MANDATARIO QUE SEA ABOGADO DE LA REPÚBLICA Y QUE NO SE ENCUENTRE DENTRO DE LAS INHABILIDADES A QUE HACE REFERENCIA EL ART. 67 DEL CÓDIGO PROCESAL CIVIL Y MERCANTIL. (3)"[28]

[27]Vid. "Ley de Marcas y Otros Signos Distintivos" en https://www.asamblea.gob.sv/leyes-y-decretos/resultado-busqueda/, con acceso el 18/04/2025. Su objetivo es regular la adquisición, mantenimiento, protección, modificación y licencias de marcas.

[28] Vid. "Ley de Marcas y otros signos distintivos" en http://infotrade.minec.gob.sv/wp-content/uploads/ley-marcas.pdf, con acceso el 10/04/2024. Su objetivo es regular la adquisición, mantenimiento, protección, modificación y licencias de marcas.

Luego descargar los formularios que pone a disposición al Centro Nacional de Registro (CNR) para el registro de marca, para luego poder asociar la marca al nombre de dominio, la realización de este acto le permite al dueño de la marca ejecutar un procedimiento establecido por la ICANN (Corporación de Internet para la Asignación de Nombres y Números) para resolver disputas relacionadas con el registro de dominios de Internet a través de La Política Uniforme de Resolución de Disputas de Nombres de Dominio (UDRP), esta política permite que los titulares de marcas registradas puedan iniciar procedimientos administrativos expeditivos contra registros de dominios que consideren abusivos o de mala fe, como el Cibersquatting.[29]

Bajo la Política UDRP, si un titular de una marca registrada considera que un nombre de dominio ha sido registrado de mala fe, tiene la opción de presentar una queja ante uno de los proveedores de servicios de resolución de disputas aprobados por la ICANN. Este proceso está diseñado para abordar disputas relacionadas con el registro abusivo de nombres de dominio.

Para que la queja tenga éxito, el reclamante debe demostrar tres elementos esenciales:

1. Identidad o similitud confusa con una marca registrada.
2. Falta de derechos o intereses legítimos del registrante.
3. Registro y uso de mala fe.

Si una queja bajo la UDRP es exitosa, el dominio puede ser cancelado o transferido al titular de la marca registrada. Este proceso es preferido por su rapidez y costo de efectividad en comparación con la litigación tradicional. La UDRP se aplica a todos los nombres de dominio acreditados por la ICANN, proporcionando una protección global para las marcas en internet.

En el caso de dominios locales .sv las disputas por ciberocupación puede ser resueltas a través de SVNet, la entidad delegada por ICANN para administrar estos dominios. La política de resolución de controversias de SVNet está alineada con la de ICANN. Según esta política, SVNet puede cancelar, ceder o cambiar el estado de un dominio bajo ciertas circunstancias, como recibir instrucciones del propietario, una orden de arbitraje, o una resolución de un tribunal arbitral.

Para presentar una demanda en El Salvador relacionada con disputas de DNS, es crucial determinar la naturaleza exacta del conflicto, como la propiedad de un nombre de dominio o la administración de registros DNS. Es esencial tener un registro de marca y recopilar toda la documentación relevante, como contratos y registros de DNS. La Fiscalía General de El Salvador tiene personal capacitado para investigar delitos en la red, pero no cuenta con una unidad especializada en ciberdelitos.

El Salvador no es signatario de tratados internacionales de ciberdelitos, aunque ha expresado su intención de adherirse al Convenio de Budapest. La American Chambero f Commerce de El Salvador y el estado son signatarios del Llamamiento de Paris para la confianza y la seguridad en el ciberespacio

Impacto de los ataques de DNS a sociedades en El Salvador.

Las violaciones de datos afectan la reputación de la empresa. La falta de información o la presentación tardía podrían empeorar las cosas en forma de multas adicionales en otras regiones. ¿Qué podemos esperar en El Salvador respecto a los impactos de ataques de Nombres de Dominio de las Sociedades? Para contestar esta pregunta hemos establecido primero que los Nombres de Dominio para internet al ser parte de la marca de la Sociedad tienen una relación con la misma y son considerados activos, al igual que en

[29] Vid. “Políticas Uniforme para Resolución de Controversias” en https://svnet.sv/politicas-uniforme-para-resolucion-de-controversias/, con acceso el 25/05/2024. Todo conflicto entre particulares en torno a nombres de dominio registrados bajo el dominio SV, deberán ser resueltos con la debida aplicación de la citada política.

otras regiones, es importante de un ciberataque al Nombre de Dominio, considerar el alcance del ataque, si ha llevado a incumplimiento de servicios ofrecidos al cliente, o incumplimientos a contratos, e incluso considerar que cibercriminales pudieran hacer uso del Dominio para actividades ilícitas.

A continuación, vamos a tipificar los de ataques en dos categorías: Primero los que son técnicas que puedan llevar a secuestrar información, denegar servicios, etc. y que pueden traer como consecuencia el secuestro y uso indebido de los Servicios de Nombre de Dominio. Segundo, aquellos ataques dirigidos explícitamente hacia los Servicios de Nombre de Dominio. En la primera categoría se tienen los ataques de: Spam y Phising. Ambos pueden hacer uso de DNS falsos muy parecidos a los DNS verdaderos, puede utilizarse para obtener información de la misma empresa, y lograr obtener información de los clientes o empleados, e incluso tomar posesión del DNS original. Esto equivale, en el mundo real, a tener una identificación que valide las acciones que se ejecuten, ya sea correos electrónicos o instrucciones dadas desde sitios web. Al ser usados para hechos criminales estarían comprometiendo directamente a la empresa a la cual se le ha secuestrado su DNS.

Las implicaciones legales podrían ser las siguientes: Demandas por robo de información o fraude financiero a través de medios digitales. Ante ese tipo de demandas, los abogados de la sociedad deberán demostrar que no fue la sociedad quien está participó en las actividades delictivas y que la Sociedad ha tomado las medidas necesarias para salvaguardar la información de los clientes y que han sido suficientes para protegerse ante este tipo de ataques**.** En el caso de que, a través del secuestro de DNS, se realizaran estafas utilizando el Nombre de Dominio de la sociedad, los clientes de la sociedad podrían establecer denuncias e interponerla en la Fiscalía General de la Republica o presentar una demanda en el Juzgado pertinente. En el caso que el hecho se iniciara fuera del país, las personas afectadas podrían interponer una demanda basada en el artículo 2 de la Ley Especial contra Delitos Informáticos y Conexos.

"*Ámbito de Aplicación. Art. 2.- La presente Ley se aplicará a los hechos punibles cometidos total o parcialmente en el territorio nacional o en los lugares sometidos a su jurisdicción. También se aplicará a cualquier persona, natural o jurídica, nacional o extranjera, por delitos que afecten bienes jurídicos del Estado, de sus habitantes o protegidos por Pactos o Tratados Internacionales ratificados por El Salvador. De igual forma, se aplicará la presente Ley si la ejecución del hecho se inició en territorio extranjero y de consumó en territorio nacional o si se hubieren realizado, utilizando Tecnologías de la Información y la Comunicación instaladas en el territorio nacional y el responsable no ha sido juzgado por el mismo hecho por tribunales extranjeros o ha evadido el juzgamiento o la condena".*[30]

Estos delitos inclusive pudieran estar ocurriendo sin que la Sociedad dueña del DNS lo sepa. Imaginemos que el DNS de la Sociedad fuera capturado o se utilizaran sus logos y distintivos en un sitio web pirata para realizar operaciones fraudulentas a salvadoreños residentes en EE. UU., Estas personas identificaran a la empresa dueña y podrían emprender acciones legales. Como en la mayoría de los casos, es importante demostrar que no se tenía conocimiento del secuestro o usurpación de DNS y que la Sociedad tomó las medidas necesarias para evitar un ataque. En caso de estar enterados que se ha perdido el control de su DNS, es importante acercarse a las autoridades correspondientes a denunciar el delito, evitando así la presunción de dolo por parte de la Sociedad.

En este sentido, se debe considerar que la responsabilidad subjetiva en el ámbito del derecho se refiere a la obligación que tiene una persona o entidad de responder por los daños o perjuicios que causa a otra como consecuencia de una conducta intencional o imprudente. Esta responsabilidad se basa en la teoría de la

[30]Vid. "Ley Especial Contra Los Delitos Informáticos y Conexos" en https://www.fiscalia.gob.sv/medios/portal-transparencia/normativas/normativas-de-interes/ley-especial-contra-delitos-ciberneticos.pdf, Su objetivo principal es proteger los bienes jurídicos de las conductas delictivas que son cometidas por medios las TIC.

culpa, es decir, la culpa es un elemento subjetivo y de ahí proviene el nombre de responsabilidad subjetiva. En el contexto del derecho corporativo, la responsabilidad subjetiva puede implicar que una empresa es responsable por los daños que causa a terceros como resultado de sus acciones o negligencias. Esto puede incluir, por ejemplo, daños causados por productos defectuosos, violaciones de contratos, prácticas comerciales desleales, entre otros; lo que para nuestro caso serían las consecuencias de los ataques de DNS.

Es importante destacar que para establecer la responsabilidad subjetiva se deben demostrar tres elementos:

1. Causa y efecto: Se debe acreditar que el daño ocasionado al reclamante fue una derivación directa e inmediata del acto u omisión de cuidado del demandado.

2. La culpa: Debe existir un deber de cuidado del demandado, o también que no debe existir imprudencia por parte del actor que haya ocasionado el hecho que lo dañó.

3. El daño causado: Que puede traducirse a un daño patrimonial en el sentido de pérdida o menoscabo de patrimonio o daño moral.

Es importante mencionar que la responsabilidad subjetiva se diferencia de la responsabilidad objetiva, la cual se caracteriza por prescindir del requisito de la infracción como punto de partida y por no recurrir a la culpabilidad como criterio de imputación subjetiva.

Ya que se han abordado los tipos de ataques de DNS, considerarse la responsabilidad subjetiva de la empresa al no cumplir con el grado de protección del bien vinculado a ella y que la representa, en este caso, el nombre de dominio Además, está la presunción de su participación directa con conocimiento de causa, considerando que ya se estableció que su nombre de dominio tiene una relación contractual y una relación con la marca y los distintivos de la empresa, con los que se ha cometido un perjuicio contra clientes, proveedores, etc., volviendo ambas situaciones como un problema a nivel penal o civil, en cuanto a los reclamos de restitución, daños o perjuicios provenientes de los ataques DNS que derivaron en daños a terceros.

El régimen de responsabilidad subjetiva tiene su fundamento en la noción de “culpa”, es decir, en la intención de inferir daño por parte de su causante o el grado de impericia o negligencia que genera tal daño. Así, el mecanismo principal para determinar la ausencia de responsabilidad por parte del causante del daño es la demostración de la diligencia que le es exigida en el caso particular. Teniendo en cuenta que la responsabilidad contractual parte de presumir la culpa, se invierte la carga de la prueba y entonces no corresponde al titular del DNS probarla, sino a quien recibe, o usa los servicios, comprobar su diligencia.

Esto permite concluir que lo que se plantea no compromete la diligencia del titular del DNS en su custodia; basta su manifestación en torno al hecho generador, que derivó en el fraude electrónico. Sin embargo, si el tercero afectado realiza la acusación y establece un monto de los perjuicios, con el propósito de que surja la responsabilidad civil como fuente de la obligación a cargo del dueño del DNS de indemnizar los perjuicios, obligará a este a demostrar el mayor grado de diligencia en la protección de su nombre de dominio. Esto siempre y cuando exista un contrato como única fuente normativa de la relación jurídica entre el titular del DNS y el afectado, que además es en la mayoría de los casos, de adhesión. No es del todo sencillo acreditar que una de las obligaciones del dueño de DNS es brindar a sus clientes completa seguridad en la utilización de medios electrónicos, incluido su nombre de dominio.

Al respecto, teniendo en cuenta que el dueño de DNS mismo se pone en riesgo de sufrir fraudes al exponer su marca en línea que puede ser de mucho o poco riesgo, según los niveles de seguridad que utilice, es

necesario destacar que, ante cualquier ataque, es claro que siempre habrá culpa de la empresa, Esta será determinante en la medida que los niveles de seguridad sean dependientes del riesgo asimilado. En consecuencia, la culpa del usuario por negligencia debe probarse en las condiciones legalmente exigidas, con excepción del dolo; porque, en este caso, el perjuicio no provendría del riesgo propio de exposición del DNS, sino de una mala intención por parte del usuario o su impericia.

Ahora bien, circunscribiéndonos al ámbito de la culpa, queda por ver qué tan viable es legalmente el reproche de las actuaciones del usuario. Vale la pena mencionar que el usuario es responsable cuando se demuestra la no observancia y de las buenas prácticas de seguridad. Por ejemplo, ante un evento de phishing el dueño del DNS es la víctima, no quien se vuelve el usuario del nombre de dominio.

Protección jurídica de dominio.

Para abordar nuestra interrogante sobre ¿Cómo el Estado y el marco legal vigente garantizan la protección de los derechos de las sociedades y la justicia oportuna ante los ataques a Nombres de Dominio?, es importante considerar aspectos claves, ya que, dentro de los aspectos legales, tenemos la protección jurídica de dominios ante los diferentes procesos judiciales que se puedan dar, considerando que no se mencionan en los contratos de servicios de nombre de dominio la posibilidad de un ataque. Además, se deja de lado la consideración de que un Nombre de Dominio de Internet, al margen de ser un elemento técnico, guarda una relación con la empresa como un distintivo de marca.

En primer lugar, es necesario determinar si existe alguna estipulación contractual que otorgue al titular del nombre de dominio las herramientas jurídicas necesarias para protegerlo contra ataques provenientes de otros nombres de dominio, derechos de propiedad industrial, derechos de autor, entre otros. Cabe destacar que los derechos conferidos por el contrato de registro al titular del nombre de dominio son limitados, abarcando principalmente el derecho de uso, la transferencia y la licencia de este. No obstante, no se contempla específicamente ninguna disposición contractual que ofrezca alternativas concretas de protección o acciones jurídicas para la defensa del nombre de dominio.

Los contratos de registro de nombres de dominio bajo gTLDs, como por ejemplo .net y .com, presentan dos características principales:

La primera es la falta de previsión respecto a la posibilidad de ataques a los nombres de dominio, aunque antes de registrarse se advierten las condiciones sobre el registro abusivo de nombres de dominio.

La segunda característica común es la adhesión generalizada a la Política Uniforme de Resolución de Disputas de la ICANN (UDRP) para la resolución de conflictos relacionados con nombres de dominio.

Esta política se entiende incorporada al contrato, aunque no se especifica claramente qué tipos de conflictos pueden solucionarse mediante ella, dejando abierta la posibilidad de utilizarla para resolver controversias derivadas de ataques a nombres de dominio.

En este contexto, es pertinente analizar la UDRP para determinar si su interpretación dentro de las regulaciones contractuales puede aplicarse como un mecanismo de protección jurídica para los nombres de dominio.

Es importante resaltar la ausencia de una disposición explícita en la política que se refiera a la protección de los nombres de dominio contra ataques provenientes de otras instituciones jurídicas. No obstante, en el primer apartado de la política, que describe su objetivo, se menciona: *"... se incorpora mediante referencia en su acuerdo de registro y establece las cláusulas y condiciones en relación con una controversia que surja entre usted y cualquier otra parte distinta a la nuestra (el registrador) sobre el registro y utilización*

de un nombre de dominio de Internet registrado por usted…"[31]. De esta lectura, se deduce que la política es plenamente aplicable para proteger los nombres de dominio, ya que sus cláusulas y condiciones se aplican a cualquier controversia en la que una de las partes sea el titular del nombre de dominio y la otra sea distinta al registrador, siempre que la disputa esté relacionada con el registro y uso del nombre de dominio.

Numerosos supuestos pueden encajar en esta política, ya que no limita la protección a ataques provenientes de otros nombres de dominio o de sus titulares. Al indicar esto, se presenta una proposición tan amplia que sugiere que, siempre que el conflicto derive del registro o uso del nombre de dominio, su titular podrá invocar el procedimiento regulado por la UDRP. Esto implica que, ante la utilización de un nombre de dominio por otra persona distinta al titular, ya sea como un nombre de dominio similar, como signo distintivo o con fines de explotación, el titular podría buscar protección mediante la acción judicial de la UDRP.

Si hacemos una interpretación extensiva, podríamos considerar aplicables para la protección de los nombres de dominio los supuestos de controversias mencionados en el numeral cuarto, literal a) de la política: *"… en caso de que un tercero (un demandante) sostenga ante el proveedor competente, en cumplimiento del Reglamento, que: i) usted posee un nombre de dominio idéntico o similar hasta el punto de crear confusión con respecto a una marca de productos o servicios sobre la que el demandante tiene derechos; ii) usted no tiene derechos o intereses legítimos respecto del nombre de dominio, y iii) usted posee un nombre de dominio que ha sido registrado y utilizado de mala fe"*[32]. Esto, teniendo en cuenta el objetivo de la política, permite al titular de un nombre de dominio reclamar que cualquier otra persona posee un nombre de dominio similar al suyo, cuyo objetivo es generar confusión sobre los servicios que ofrece, utilizando el nombre de dominio similar de mala fe.

Este análisis sugiere que existen muchos otros supuestos de aplicación que podrían derivarse del estudio minucioso de las problemáticas de ataques a los nombres de dominio, conforme a lo regulado en la política, y mediante una interpretación extensiva de sus prescripciones. Sin embargo, es importante criticar la UDRP por la amplitud y falta de concreción de su regulación en este punto. La formulación de un objetivo tan amplio crea una ventana excesivamente grande para la protección del nombre de dominio, lo que genera inseguridad jurídica al someter la resolución de estos ataques a este procedimiento extrajudicial.

Como se ha expuesto, el nombre de dominio puede actuar en el mercado virtual como un identificador comercial. Es decir, en ciertos casos, un nombre de dominio puede tener una capacidad distintiva similar a la de los signos distintivos como las marcas, los nombres comerciales, y los lemas comerciales.

En este contexto, se propone que quien utiliza un nombre de dominio sin tener un derecho específico para diferenciar productos y servicios en el mercado, puede obtener un derecho de exclusividad sobre ese signo, típicamente a través del registro de una marca en la oficina nacional, regional o internacional correspondiente, sin perjuicio de registrarlo también como denominación o razón social al constituir una sociedad.

Así, se estima que cuando un nombre de dominio se usa para distinguir servicios y productos de una persona o empresa de los de otra, lo que es común en servicios ofrecidos a través de la red, debería ser posible obtener una marca sobre el mismo, siempre que se cumplan los requisitos legales establecidos. En concreto, este mecanismo de protección jurídica para los nombres de dominio ya ha sido implementado en Estados Unidos, donde se permite al titular del nombre de dominio que cumpla con las condiciones establecidas por la entidad correspondiente para registrar el nombre de dominio como marca, determinando así, en cada caso

[31]Vid. "Política de Solución de Controversias en materia de nombres de dominio" en https://www.icann.org/resources/pages/policy-2012-02-25-es , con acceso el 22/05/2024.
[32]Ibidem.

las clases oficiales de productos o servicios en las que se puedan incluir los distintos servicios o informaciones técnicas prestadas por medio de Internet.

Esta política de la Oficina de Patentes y Marcas Registradas de Estados Unidos (USPTO) confirma la tesis de que el nombre de dominio no puede gozar de una protección autónoma como signo distintivo. Solo obtiene protección como signo distintivo, es decir como un derecho de exclusividad, por el contrario, si se registra como marca. En ese momento, dejará de ser simplemente un nombre de dominio para convertirse en una marca de productos o servicios a los ojos de la ley.

Por lo tanto, en ausencia de un régimen jurídico específico para los nombres de dominio, esta alternativa se convierte en una herramienta valiosa para que el titular del nombre de dominio, que ofrece servicios o comercializa productos a través de un sitio web, obtenga mayor seguridad jurídica. Esto asegura que su actividad comercial no será objeto de registro como marca, registro como nombre de dominio similar, u otra actividad que pueda causar confusión, y que, en caso de conflicto, contará con las herramientas necesarias para su defensa.

El objetivo es lograr que el nombre de dominio reciba la protección propia de los signos distintivos, como las marcas o los nombres comerciales, sin necesidad de registrar el dominio como tal. Esto se logra simplemente a través de las funciones que desempeña de hecho en el tráfico comercial de un territorio específico y conforme a su sistema jurídico. Es decir, la protección del nombre de dominio frente a ataques y que se puedan derivarse regular gracias al uso del nombre de dominio bajo características propias de esas instituciones.

No obstante, esta alternativa se limita a los ordenamientos jurídicos que permiten adquirir derechos sobre signos distintivos, especialmente marcas, mediante su uso en el comercio de dicho territorio. En estos casos, el registro de la marca ante la autoridad nacional es meramente declarativo. Esta forma de protección es equivalente a la anterior, pero se basa en la posibilidad que algunos sistemas jurídicos ofrecen al considerar el registro de signos distintivos como meramente declarativo. Así, en ausencia de mecanismos autónomos de protección de los nombres de dominio, este enfoque es viable. No obstante, al contrario de lo que argumentan sus detractores, el nombre de dominio no recibiría una protección indiscriminada, sino que tendría que cumplir con requisitos rigurosos y específicos, similares a los mencionados previamente. Por lo tanto, no se obtendría protección únicamente por el uso del nombre de dominio.

La posibilidad de proteger los nombres de dominio es generalmente rechazada. Esta postura considera que el nombre de dominio, aunque no está consagrado en la normativa de propiedad industrial, puede desempeñar funciones importantes en el tráfico comercial, destacándose su capacidad distintiva respecto a bienes y servicios. Por ello, se argumenta que merece protección jurídica bajo el régimen específico de los signos distintivos, sin exigir las mismas condiciones que se aplican a marcas o nombres comerciales, sino simplemente en virtud de su uso. Sin embargo, esta alternativa es meramente teórica, ya que en la práctica no puede aplicarse debido a las profundas diferencias entre el régimen de propiedad industrial, especialmente en lo que respecta a las marcas, y los nombres de dominio. Como resultado, no es viable equiparar estas dos instituciones ni extender directamente el régimen de protección de las marcas a los nombres de dominio. Por esta razón, son más aceptados los sistemas que moderan la aplicación del régimen de propiedad industrial, considerando ciertos requisitos que debe cumplir el nombre de dominio para ser registrado y obtener protección como signo distintivo.

Conclusiones.

Los ataques cibernéticos en el mundo y particularmente en El Salvador, se han vuelto frecuentes y cada vez más especializados. Se ha visto cómo, inclusive, los cibercriminales operan de manera organizada formando bandas criminales. Hay modalidades inclusive de Hacking as a service (HaaS),[33] que no es más que la comercialización de habilidades de hacking, donde el Hacker se convierte en contratista, siendo la darkweb un lugar donde se comercializan estos servicios, e inclusive programas y herramientas se venden para vulnerar empresas con diferentes motivaciones: fines económicos, políticos, reconocimiento, etc.

Otro punto importante para considerar en la exposición a nivel país que El Salvador tiene actualmente haciendo énfasis en este ensayo específicamente en lo referente de la adopción de tecnologías crypto. La adopción de tecnología como pilar estratégico, apostándole a traer inversionistas extranjeros, da una vitrina al mundo tanto para las situaciones positivas como país como las negativas. Esto último en el sentido que El Salvador se vuelve blanco de ciberataques, por la notoriedad y prestigio que pueda traer, el lucro y el hacktivismo.[34]

De este contexto y lo definido en este ensayo se puede concluir, primero, que las Sociedades en El Salvador tienen una necesidad de exponerse al mundo de internet no solo por la naturaleza de sus negocios, si no por el uso de herramientas y mejoras de sus procesos como una forma natural de su evolución. Por tanto, están altamente expuestas a ciberataques, aun tomando todas las salvaguardas técnicas. De ahí que existirá un riesgo inherente que se materialice una amenaza cibernética, por lo que es importante considerar la protección no solo técnica y económica sino también la protección jurídica de los bienes.

A partir de esta protección jurídica de los bienes, considerando la marca y distintivos de las sociedades como un bien per se dé la empresa y siendo los Nombres de dominio una representación de la marca y distintivos en internet es importante y una prioridad la protección de Nombres de dominio. Debe tenerse claro que los Nombres de dominio, hoy en día, no solo representan una relación de la marca y los distintivos de la Sociedad, sino también representan las identidades de los miembros de estas, usando el Nombre de Dominio como un identificador y distintivo inequívoco de la relación contractual que existe entre un miembro de la Sociedad o un empleado de esta, tal cual como se hace con el correo electrónico y la dirección de internet.

Esto puede llevar a la Sociedad, ante un ataque cibernético a sus Nombres de Dominio a consecuencias legales de orden civil, mercantil y hasta penal, debido a temas de suplantación, secuestro y denegación de servicios. Estos ataques pueden derivar en incumplimientos de contrato por denegación de servicio. Por ejemplo, la tienda electrónica de Apple que utiliza bots para analizar continuamente las páginas web de las empresas que tienen sus aplicaciones en la tienda, verificando que las políticas de privacidad de los clientes estén publicadas en internet. Un ataque de DNS de denegación de servicio puede impedir que estos bots realicen su trabajo, lo que podría llevar a Apple a eliminar la aplicación de la tienda, de acuerdo con las políticas aceptadas en el acuerdo con Apple. Esto tendría consecuencias directas dependiendo, de la naturaleza de la aplicación, incluyendo temas reputacionales, económicos y posibles demandas contra la Sociedad, considerando el tipo de servicio, y los derechos adquiridos por los clientes a través de sus contratos con la Sociedad por el uso de la aplicación que ya no estará disponible en la tienda electrónica.

Esto puede acarrear otras consecuencias, como la imposición de sanciones administrativas y multas por parte de las entidades reguladoras, para el caso de los bancos y las aseguradoras. Otros casos que pudieran darse incluyen demandas por daños y perjuicios si un cliente de una aseguradora padeciera una enfermedad o tuviera que ser atendido de emergencia y no pudiera recibir la atención al no tener activo el sistema para

[33] Vid. "Hacking as a service (Haas)" en https://www.techtarget.com/whatis/definition/hacking-as-a-service-HaaS, con acceso el 28/05/2024. Es la comercialización de piratería en las cuales el hacker sirve como contratista.
[34] Vid. "Hacktivismo" en https://es.wikipedia.org/wiki/Hacktivismo, con acceso el 28/05/2024. Es un acrónimo de hacker y activismo, también conocido como ciberactivismo.

validar la póliza de seguro, debido a un ataque de inundación de DNS que no ha permitido que el sitio web de la aseguradora se encuentre disponible. En el peor de los casos, si la persona fallece, podría acusar a la aseguradora de no haber hecho todo lo necesario para mantener habilitados sus sistemas u ofrecer vías alternas para poder garantizar el servicio.

El correo electrónico, como se estableció anteriormente es una identidad que puede establecer una relación contractual, en el caso de secuestro de Nombre de Dominio puede generar consecuencias ya que los atacantes podrían generar correos electrónicos o tomar posesión de estos, creando sitios fachada para estafas o incluso adquirir obligaciones a nombre de la Sociedad al robar información de esta. En el primer caso, los clientes pueden ser estafados a través de un correo o un sitio con el Nombre DNS legítimo de la empresa, lo que inclusive podría llevar a demandas civiles o penales a la Sociedad. Aunque es difícil comprobar el dolo en el actuar, esto puede incluir temas de peritaje de expertos, donde también se puede establecer responsabilidad, si se determina que no se tomaron las medidas necesarias para la protección de los programas o sistemas informáticos, lo que permitió que el ataque se perpetrara y tuviera consecuencias por negligencia o impericia según el artículo 7 de la Ley Especial Contra los Delitos Informáticos y Conexos.

"Daños a Sistemas Informáticos. Art. 7.- EL QUE DESTRUYA, DAÑE, MODIFIQUE, EJECUTE UN PROGRAMA O REALICE CUALQUIER ACTO QUE ALTERE EL FUNCIONAMIENTO O INHABILITE PARCIAL O TOTALMENTE UN SISTEMA INFORMÁTICO QUE UTILICE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN O CUALQUIERA DE LOS COMPONENTES QUE LAS CONFORMAN, SERÁ SANCIONADO CON PRISIÓN DE TRES A CINCO AÑOS. SI EL DELITO PREVISTO EN EL PRESENTE ARTÍCULO SE COMETIERE EN CONTRA DE CUALQUIERA DE LOS COMPONENTES DE UN SISTEMA O PROGRAMA INFORMÁTICO QUE UTILICEN LAS TECNOLOGÍA DE LA INFORMACIÓN Y DE LA COMUNICACIÓN QUE ESTÉN DESTINADAS A LA PRESTACIÓN DE SERVICIOS PÚBLICOS O FINANCIEROS O LA REALIZACIÓN DE TRANSACCIONES EN BITCOIN U OTRAS CRIPTOMONEDAS QUE PERMITAN SU CONVERTIBILIDAD AUTOMÁTICA E INSTANTÁNEA A MONEDA DE CURSO LEGAL, O QUE CONTENGAN INFORMACIÓN PERSONAL, CONFIDENCIAL, RESERVADA, PATRIMONIAL TÉCNICA O PROPIA DE PERSONAS NATURALES O JURÍDICAS, SERÁ SANCIONADO CON PRISIÓN DE CUATRO A SIETE AÑOS. SI EL DELITO PREVISTO EN EL PRESENTE ARTÍCULO SE EJECUTARE POR IMPRUDENCIA, SERÁ SANCIONADO CONTRA PRISIÓN DE UNO A TRES AÑOS."[35],

La ley deja un amplio espectro de su aplicación si se considera que la negligencia, impericia o inobservancia pueden incluir la falta de aprobación de un presupuesto de ciberseguridad por parte de una Junta Directiva, o la falta de esta de seguir leyes y normas como es el caso de la norma NRP-23 Normas técnicas para la Gestión de la Seguridad de la Información o la NRP-32 Normas técnicas sobre Medidas de Ciberseguridad en Canales Digitales, para bancos, financieras, aseguradoras. El articulo no especifica si las normas establecidas como tales a parte de las dispuestas por la ley, incluyen las buenas prácticas y costumbres, lo que ampliaría el alcance de la presente ley si se consideran las mejores prácticas de ciberseguridad. La inobservancia de estas debería ser probada por un peritaje como se mencionó arriba.

Las empresas que manejan datos de consumidores tienen la responsabilidad e implementar medidas de seguridad adecuadas para proteger esta información sensible. Tal y como se observa en el apartado asignado al Derecho Comparado, las leyes de protección de datos varían significativamente según el país.

[35] VASQUEZ LOPEZ, Luis, *Ley especial contra los delitos informáticos y conexos*, Editorial Lis, El Salvador 2023.

En Estados Unidos, las empresas deben cumplir con leyes estatales específicas. Como ejemplos de estas leyes incluyen la Ley de Protección al Consumidor de Nevada y la Ley de Privacidad del Consumidor de California (CCPA). Estas leyes exigen transparencia en la divulgación de ciberataques y la preparación para mitigar riesgos. La CCPA, por ejemplo, otorga a los consumidores derechos sobre sus datos personales, incluyendo el derecho a saber qué información se recopila, el derecho a solicitar la eliminación de sus datos y el derecho a optar no vender su información personal.

En la Unión Europea, las empresas deben seguir el Reglamento General de Protección de Datos (GDPR). Este reglamento establece estrictas directrices sobre cómo se deben manejar y proteger los datos personales. Según el GDPR, en caso de una violación de datos, la empresa debe informar a la Oficina del Comisionado de Información (ICO) dentro de las 72 horas posteriores a la detención de la violación. Además, el GDPR impone sanciones significativas por incumplimiento, lo que subraya la importancia de la protección de datos en la región.

Mientras que las leyes de protección de datos de Estados Unidos pueden variar de un estado a otro, en la Unión Europea existe un marco regulatorio unificado bajo el GDPR. Ambas regiones, sin embargo, enfatizan la importancia de la transparencia y la preparación para mitigar riesgos en la gestión de datos de consumidores

Las sociedades que son nuevas en el ámbito digital deben conocer las leyes de protección de datos en todas las jurisdicciones relevantes en las que operen. La gravedad de las multas por infracciones varía según la región y el número de las personas afectadas.

Es crucial contar con un equipo legal para definir responsabilidades y asegurar una respuesta adecuada a las violaciones de datos, Esto incluye la notificación oportuna a las personas y autoridades afectadas, la implementación de medidas correctivas para prevenir futuras violaciones y la cooperación con las autoridades reguladoras durante las investigaciones. Además, las empresas deben realizar auditorías regulares de seguridad y capacitaciones para empleados sobre las mejores prácticas en ciberseguridad y protección de datos.

Por tanto, podemos concluir que: a) El país actualmente tiene una exposición importante a nivel internacional que lo vuelva blanco de ataques cibernéticos. b) Los Nombres de Dominio son un bien de las Sociedades en cuanto que guardan relación con las marcas y distintivos de estas, además de establecer una relación contractual de servicio con quien provee los servicios de resolución de Nombres de Dominio. Además, forman parte del correo electrónico, lo que se vuelve también una identidad de un empleado de la Sociedad que lo identifica y puede llegar a establecer una relación contractual, por lo que es de vital importancia su protección. c) Los ataques a los Nombres de Dominio pueden tener impactos legales en las Sociedades que pueden derivar en demandas, civiles o penales, como consecuencia de estafas, incumplimiento de obligaciones contractuales, o contravenciones de normas establecidas por entes reguladores entre otras. d) El marco legal vigente en El Salvador, carece de herramientas que protejan a las Sociedades ante casos especializados de ciberataques donde puede existir una presunción de dolo, negligencia, impericia o inobservancia, en perjuicios de las Sociedades, que deberán comprobar la ausencia de dolo y que han hecho todo lo necesario para el cumplimiento de las normas establecidas, las cuales no quedan especificadas en la ley. Además, los tipos de ataques cibernéticos son cada vez más sofisticados y variados, lo que hace que las leyes tradicionales con sus procesos actuales no puedan permitir la aplicación oportuna de la ley a la que todos tienen derecho. Considerando también el alcance de esta, ya que en la mayoría de los casos los ataques cibernéticos pueden abarcar diferentes jurisdicciones, es importante también la suscripción de convenios y tratados referentes a ciberseguridad que también permitan ampliar el alcance del brazo de la ley más allá de las fronteras del país. e) Por ultimo y no menos importante, es la ausencia de especialistas peritos, en ataques informáticos, no solo a nivel ofensivo y defensivo, sino también en la parte forense para determinar el alcance de la responsabilidad a la hora de determinar el hecho generador del delito.

Recomendaciones.

1. Las sociedades deben de tener en orden los registros de marca y distintivos, así como los formularios de servicio de SVNet para la resolución de Nombres de Dominio, actualizando oportunamente al administrador del servicio.

2. Establecer cláusulas claras en los contratos: Para las sociedades es crucial incluir en los contratos con clientes y proveedores cláusulas de aceptación de acuerdo de servicio que especifiquen y delimiten responsabilidades. Además, incluir en el caso de proveedores cláusulas de observancia de medidas de seguridad de la información.

3. Crear acuerdos de servicio de los sitios web y aplicaciones: Las sociedades deben desarrollar acuerdos de servicio que incluyan la aceptación implícita de los usuarios de los riesgos al momento de acceder a los sitios web y aplicaciones como una medida de derivación de responsabilidad ante riesgos que no puedan ser mitigados por parte de las Sociedades.

4. Definir una instancia de evaluación de riesgos en el Gobierno Corporativo: Establecer una instancia encargada de realizar evaluaciones de riesgo, y asegurar el fiel cumplimiento de normas de seguridad de la información. Garantizar la creación y ejecución de planes de continuidad de negocio y planes de recuperación ante desastres, destinando un monto de su presupuesto destinado a la ciberseguridad.

5. Gestionar un Comité de crisis en el Gobierno Corporativo: Se recomienda a las sociedades manejar un comité de crisis que permite manejar la adecuada comunicación hacia todos los interesados, clientes, proveedores, instituciones de control o gubernamentales, con el fin de cumplir con normativas y reducir la posibilidad de demandas.

6. Contratar pólizas de seguros contra ciberseguridad: Establecer contratos de pólizas de seguros que cubran un porcentaje del patrimonio de la sociedad en caso de perdidas o legales por posibles demandas o sanciones administrativas en caso de ser regulados.

7. Reportar ciberataques a las autoridades: En caso de ser víctimas de un ciberataque, es importante presentar la denuncia del delito ante la FGR, con el propósito de reforzar la ausencia de dolo.

8. Ampliar la Ley Especial de Delitos Informáticos y Conexos: A nivel país, es importante ampliar la Ley para tipificar mejor los tipos de delito informáticos y sus causales, buscando alternativas para la protección de las Sociedades.

9. Legislar la protección de datos personales: Es necesario contar con una legislación que regule la protección de datos personales, similar a otros países, y que otorgue a las sociedades un plazo para notificar a los clientes sobre incidentes con sus datos.

10. Suscribir convenios internacionales: Firmar convenios o tratados internacionales que permitan la colaboración con otros países y extiendan la aplicación de la ley salvadoreña más allá de las fronteras nacionales.

Índice Bibliográfico

1. ACURIO DEL PINO, Santiago, *Delitos Informáticos: Generalidades.* 2 ed. Quito: Pontificia Universidad de Católica de Ecuador. 2016.
2. FERNANDEZ DELPECH, horacio. *Manual de Derecho Informático.* 1a ed. Buenos Aires Argentina, 2014.
3. MENDOZA ORANTES, Ricardo, *Código Penal,* Editorial Jurídica Salvadoreña, El Salvador, 2023.
4. MENDOZA ORANTES, Ricardo, *Código Procesal Penal*, Editorial Jurídica Salvadoreña, El Salvador, 2023.
5. VASQUEZ LOPEZ, Luis, *Ley especial contra los delitos informáticos y conexos*, Editorial Lis, El Salvador 2023.
6. VASQUEZ LOPEZ, Luis, *Recopilación de Leyes en Materia Registral*, Editorial Lis, El Salvador, 2024.

Bibliografía de páginas web

1. Constitución de la República de El Salvador" en 171117_072857074_archivo_documento_legislativo.pdf (asamblea.gob.sv), con acceso el 21/05/2024.
2. "Cybersquatting, qué es y cómo protegerse" en https://www.incibe.es/empresas/blog/cybersquatting-y-protegerse, con acceso el 01/04/2024.
3. "Dark Web Profile: RansomHub", en https://socradar.io/dark-web-profile-ransomhub/, con acceso el 22/06/2024.
4. "Diccionario del Estudiante" en ciberespacio | Diccionario del estudiante | RAE, con acceso el 22/05/2024.
5. "Equinix" en https://es.wikipedia.org/wiki/Equinix, con acceso el 25/05/2024.
6. "FBI lanza alerta mundial por ciberataque y pide reiniciar los routers" en https://www.laprensagrafica.com/techlife/FBI-lanza-alerta-mundial-por-ciberataque-y-pide-reiniciar-los-routers-20180528-0063.html, con acceso el 22/06/2024.
7. "Grupos delictivos que participan en los delitos cibernéticos organizados" en https://www.unodc.org/e4j/es/cybercrime/module-13/key-issues/criminal-groups-engaging-in-cyber-organized-crime.html, con acceso el 02/04/2024.
8. "Hackers exponen datos de clientes de la Sociedad de Ahorro y Crédito Constelación S.A. de C.V." en Hackers exponen datos de clientes de la Sociedad de Ahorro y Crédito Constelación S.A. de C.V. - La Prensa Gráfica (laprensagrafica.com), con acceso el 22/06/2024.
9. "Ley de Marcas y otros signos distintivos" en http://infotrade.minec.gob.sv/wp-content/uploads/ley-marcas.pdf, con acceso el 10/04/2024.
10. "Ley de Marcas y Otros Signos Distintivos" en https://www.asamblea.gob.sv/leyes-y-decretos/resultado-busqueda/, con acceso el 18/04/2025.
11. "Ley Especial Contra Los Delitos Informáticos y Conexos" en https://www.asamblea.gob.sv/leyes-y-decretos/resultado-busqueda/, con acceso el 20/5/2024.

12. "Microsoft ha sufrido un ataque DDOS. ¿La información de los usuarios está comprometida? en https://cincodias.elpais.com/cincodias/2023/06/19/lifestyle/1687170387_114007.html, con acceso el 22/06/2024.
13. "Nombres de Dominio" en https://www.ujaen.es/servicios/sinformatica/catalogo-de-servicios-tic/nombres-de-dominio-dns, con acceso el 01/04/2024.
14. "NRP-23 Normas técnicas para la Gestión de la Seguridad de la Información" en https://ssf.gob.sv/descargas/Normas/Normas_Prudenciales/Bancos/NRP-23.pdf, con acceso el 28/05/2024.
15. "NRP-32Normas técnicas sobre Medidas de Ciberseguridad en Canales Digitales" en https://ssf.gob.sv/descargas/normas/NRP-32.pdf, con acceso el 28/05/2024.
16. "Página de Waves fue víctima de un secuestro DNS por algunas horas" en https://www.criptonoticias.com/seguridad-bitcoin/pagina-waves-victima-secuestro-dns-algunas-horas/ con acceso el 22/06/2024.
17. "Política de Solución de Controversias en materia de nombres de dominio" en https://www.icann.org/resources/pages/policy-2012-02-25-es , con acceso el 22/05/2024.
18. "Políticas Uniforme para Resolución de Controversias" en https://svnet.sv/politicas-uniforme-para-resolucion-de-controversias/, con acceso el 25/05/2024.
19. "Primer Proceso de la OMPI relativo a los nombres de dominio de Internet: Archivo" en Primer Proceso de la OMPI relativo a los nombres de dominio de Internet: Archivo (wipo.int), con acceso el 01/04/2024.
20. "Primer Proceso de la OMPI relativo a los nombres de dominio Internet: Archivo" en https://www.wipo.int/amc/es/processes/process1/index.html, con acceso el 01/04/2024.
21. "Secuestro de DNS: Una amenaza silenciosa en el mundo digital" en https://www.accessq.com.mx/secuestro-dns/, con acceso el 20/05/2024.
22. "Secuestro de DNS: Una amenaza silenciosa en el mundo digital" en https://www.accessq.com.mx/secuestro-dns/, con acceso el 05/05/2024.
23. "Servidor raíz" en https://es.wikipedia.org/wiki/Servidor_ra%C3%ADz, con acceso el 25/05/2024.
24. "Sistemas de nombres de dominio" en https://es.wikipedia.org/wiki/Sistema_de_nombres_de_dominio, con acceso el 25/05/2024.
25. "¿Cómo fue hackeada Air Europa? Hipótesis de experto" en https://www.hosteltur.com/159724_como-fue-hackeada-air-europa-hipotesis-de-experto.html, con acceso el 27/06/2024.
26. "¿Cuántos sitios web hay en el mundo?", https://es.statista.com/grafico/19107/numero-de-sitios-web-existentes-en-internet/, con acceso el 01/04/2024.
27. "¿Qué es la ciberocupación?" en https://latam.kaspersky.com/resource-center/preemptive-safety/cybersquatting, con acceso el 01/04/2024.
28. "¿Qué es un ataque de día cero? en https://www.cloudflare.com/es-es/learning/security/threats/zero-day-exploit/ con acceso el 02/05/2023.
29. "99% del mundo está conectado a Internet a través de cables submarinos" en https://www.camtic.org/actualidad-tic/99-del-mundo-esta-conectado-a-internet-a-traves-de-cables-submarinos/, con acceso el 25/05/2024.

Tabla de Ilustraciones

Figura 1 Cables submarinos que realizan la conexión interoceánica de internet 8
Figura 2 Sitios web creados a nivel mundial al mes de agosto de 2021 9
Figura 3 Ejemplo de Resolución de Nombre de Dominio para páginas de Internet. 10
Figura 4 Pagina web de la Heladería Freddo S.A. 12
Figura 5 Consulta DNS para encontrar un sitio web 12
Figura 6 Jerarquía de nombres de dominio 13
Figura 7 Localización de los servidores raíz de internet 14
Figura 8 Imagen de un foro de la deep web donde se han filtrado los datos de FInanciera Constelación .. 15
Figura 9 Secuestro DNS 17
Figura 10 Modo de ataque DDoS para DNS. 18