CATÁLOGO Y PRIORIZACIÓN DE VULNERABILIDADES E INCIDENTES INICIALES

1. *Objetivo*

En consideración a lo establecido en los artículos 8 y 9 de la "Norma Técnica para Coordinar la Gestión de Incidentes y Vulnerabilidad que afecten a la Seguridad de las Redes y Servicios de Telecomunicaciones", el presente documento tiene por objeto definir el catálogo inicial de vulnerabilidades e incidentes que serán reportados por el EcuCERT y que deberán ser gestionados por los prestadores de servicios de telecomunicaciones.

Las vulnerabilidades e incidentes que no estén contenidos en este catálogo y que sean reportados a los prestadores de servicios de telecomunicaciones, estarán sujetos al proceso de priorización según lo establecido en el artículo No. 8 Ibídem.

2. *Consideraciones para la priorización de Incidentes y Vulnerabilidades*

2.1 Generales

Para la priorización de vulnerabilidades e incidentes se ha tomado como criterio de severidad, el hecho de que los sistemas vulnerables o atacados pertenezcan al prestador de servicios de telecomunicaciones o a sus clientes y abonados. La existencia de vulnerabilidades u ocurrencia de incidentes en la infraestructura de prestadores de servicios será calificada con mayor impacto que aquella ocurrida en la infraestructura de clientes y abonados.

El prestador de servicios de telecomunicaciones deberá definir procesos de gestión de vulnerabilidades e incidentes en consideración al número de días establecidos por la prioridad asignada en este documento, según lo establecido en el artículo 22 de la "Norma Técnica para Coordinar la Gestión de Incidentes y Vulnerabilidad que afecten a la Seguridad de las Redes y Servicios de Telecomunicaciones".

2.1 Priorización de Vulnerabilidades

En consideración al amplio espectro de plataformas, tecnologías y sistemas correspondientes a la infraestructura propia de los prestadores de servicios de telecomunicaciones, así como la de sus clientes y abonados, en el presente documento se asigna una prioridad referencial a cada vulnerabilidad, basada en métricas relacionadas con la explotación de dichas vulnerabilidades y su impacto en el ámbito de la seguridad de la información.

Para la asignación de la prioridad referencial se ha considerado los siguientes sistemas de métricas internacionales de severidad de vulnerabilidades:

No	Nombre	Acrónimo
1	Common Vulnerability and Exposure	CVE
2	Common Vulneravility Scoring System	CVSS
3	Extensible Configuration Checklist Description Format	XCCDF

No	Nombre	Acrónimo
4	Open Vulnerability Assessment Language	OVAL
5	Common Configuration Enumeration	CCE
6	Common Weakness Enumeration	CWE
7	Common Platform Enumeration	CPE
8	Common Configuration Scoring System	CCSS
9	Open Checklist Interactive Language	OCIL
10	Asset Reporting Format	ARF
11	Security Content Automation Protocol	SCAP
12	Open Web Application Security Protocol	OWASP

Tabla No. 1 Sistemas Internacionales de métricas de severidad de vulnerabilidades

2.2 Priorización de Incidentes

La priorización de incidentes ha considerado el nivel de importancia que tienen los elementos de red de los prestadores de servicios de telecomunicaciones, en relación a la prestación del servicio a sus clientes y abonados de acuerdo a lo establecido en la normativa vigente.

3. Asignación de prioridades.

3.1 Prioridades de Vulnerabilidades

3.1.1 Prioridad para infraestructura de Prestadores de Servicios de Telecomunicaciones

La Tabla No. 2 presenta las vulnerabilidades asociadas a direcciones IP que corresponden a la infraestructura del prestador de servicios de telecomunicaciones para la prestación del servicio, que inicialmente serán reportadas por el EcuCERT y su priorización referencial para la gestión correspondiente por parte del prestador.

No	Vulnerabilidad	Nombre	Descripción del riesgo	Prioridad Infraestructura Prestador
1	Accesible_RDP	Accesible Remote Desktop Protocol	Un atacante podría acceder de manera no autorizada al sistema de información vulnerando la confidencialidad, integridad y disponibilidad del sistema	Critica
2	Open_MongoDB	Base de datos MongoDB	Un atacante podría hacer que un sistema de información ejecute código malicioso lo cual a su vez vulnere la confidencialidad, integridad y disponibilidad de la información de dicho sistema	Critica
3	Cisco_Smartinstall	Cisco SmartInstall	Un atacante podría hacer que un sistema de información ejecute código malicioso lo cual a su vez vulnere la confidencialidad, integridad y disponibilidad de la información de dicho sistema	Critica
4	Open_Memcached	mem-cashed memory caching system	Un atacante podría hacer que un sistema de información ejecute código malicioso lo cual a su vez vulnere la confidencialidad, integridad y disponibilidad de la información de dicho sistema	Critica

No	Vulnerabilidad	Nombre	Descripción del riesgo	Prioridad Infraestructura Prestador
5	Netis_Router	Routers Netis	Un atacante podría acceder de manera no autorizada al sistema de información vulnerando la confidencialidad, integridad y disponibilidad del sistema	Critica
6	Open_IPMI	Intelligent Platform Management Interface	Un atacante podría acceder de manera no autorizada al sistema de información vulnerando la confidencialidad, integridad y disponibilidad del sistema	Alta
7	DNS_Open_Resolver	DNS Domain Name System - Open Resolver	Un atacante podría utilizar el servidor DNS Vulnerable a fin de ejecutar ataques a sistemas de información	Alta
8	Freak_SSL	Factoring Attack on RSA Export	Un atacante podría interceptar conexiones HTTPS y posteriormente decifrar su vulnerando la confidencialidad de la información transmitida	Alta
9	LDAP	Lightweight Directory Access Protocol	Un atacante podría hacer que un sistema de información ejecute código malicioso lo cual a su vez vulnere la confidencialidad, integridad y disponibilidad de la información de dicho sistema	Alta
10	Open_SQL_Server_Resl	Microsoft SQL Server Resolution	Un atacante podría hacer que un sistema de información ejecute código malicioso lo cual a su vez vulnere la confidencialidad, integridad y disponibilidad de la información de dicho sistema	Alta
11	Mdns	Multicast Domain Name System	Un atacante podría hacer que un sistema de información ejecute código malicioso lo cual a su vez vulnere la confidencialidad, integridad y disponibilidad de la información de dicho sistema	Alta
12	NAT_PMP	Network Address Translation Port Mapping Protocol	Un atacante podría hacer que un sistema de información ejecute código malicioso lo cual a su vez vulnere la confidencialidad, integridad y disponibilidad de la información de dicho sistema	Alta
13	Open_Netbios	Network Basic Input Output System	Un atacante podría hacer que un sistema de información ejecute código malicioso lo cual a su vez vulnere la confidencialidad, integridad y disponibilidad de la información de dicho sistema	Alta
14	NTP_Version	Netwwork Timpe Protocol Version	Un atacante podría hacer que un sistema de información ejecute código malicioso lo cual a su vez vulnere la disponibilidad de la información de dicho sistema	Alta
15	Open_Chargen	Open Character Generator Protocol	Un atacante podría hacer que un sistema de información ejecute código malicioso lo cual a su vez vulnere la disponibilidad de la información de dicho sistema	Alta
16	Poodle_SSLv3	Padding on Oracle on Downgraded Legacy Encryption	Un atacante podría hacer que un sistema de información ejecute código malicioso lo cual a su vez vulnere la disponibilidad de la información de dicho sistema	Alta
17	Open_Redis	Remote Dictionary Server Redis	Un atacante podría hacer que un sistema de información ejecute código malicioso lo cual a su vez vulnere la confidencialidad de la información de dicho sistema	Alta
18	Open_Telnet	Teletype Network	Un atacante podría acceder de manera no autorizada al sistema de información vulnerando la confidencialidad, integridad y disponibilidad del sistema	Alta

No	Vulnerabilidad	Nombre	Descripción del riesgo	Prioridad Infraestructura Prestador
19	CWMP	CPE Customer Premise Equipment WAN Management Protocol	Un atacante podría hacer que un sistema de información ejecute código malicioso lo cual a su vez vulnere la confidencialidad, integridad y disponibilidad de la información de dicho sistema	Media
20	Scan_Elasticsearch	Elastic search	Un atacante podría hacer que un sistema de información ejecute código malicioso lo cual a su vez vulnere la confidencialidad, integridad y disponibilidad de la información de dicho sistema	Media
21	ISAKMP	Internet Security Association and Key Management Protocol	Un atacante podría hacer que un sistema de información ejecute código malicioso lo cual a su vez vulnere la confidencialidad, integridad y disponibilidad de la información de dicho sistema	Media
22	Open_NTP_monitor	Network Time Protocol Monitor	Un atacante podría hacer que un sistema de información ejecute código malicioso lo cual a su vez vulnere la confidencialidad, integridad y disponibilidad de la información de dicho sistema	Media
23	Open_Proxy	Open Proxy Server	Un atacante podría hacer que un sistema de información ejecute código malicioso lo cual a su vez vulnere la confidencialidad, integridad y disponibilidad de la información de dicho sistema	Media
24	Open_SSDP	Open Simple Service Discovery Protocol	Un atacante podría hacer que un sistema de información ejecute código malicioso lo cual a su vez vulnere la confidencialidad, integridad y disponibilidad de la información de dicho sistema	Media
25	Open_DB2	Relational DataBase Management System	Un atacante podría hacer que un sistema de información ejecute código malicioso lo cual a su vez vulnere la confidencialidad, integridad y disponibilidad de la información de dicho sistema	Media
26	Open_SMB	Server Message Block SMB	Un atacante podría hacer que un sistema de información ejecute código malicioso lo cual a su vez vulnere la confidencialidad, integridad y disponibilidad de la información de dicho sistema	Media
27	Open_SNMP	Simple Network Management Protocol SNMP	Un atacante podría hacer que un sistema de información ejecute código malicioso lo cual a su vez vulnere la confidencialidad, integridad y disponibilidad de la información de dicho sistema	Media
28	Open_Qotd	Open Quote of the Day QOTD	Un atacante podría hacer que un sistema de información ejecute código malicioso lo cual a su vez vulnere la disponibilidad de la información de dicho sistema	Baja
29	Open_Portmapper	Remote Procedure Call RCP Port mapper	Un atacante podría acceder de manera no autorizada al sistema de información vulnerando la confidencialidad, integridad y disponibilidad del sistema	Baja
30	Open_TFTP	Trivial File Transfer Protocol	Un atacante podría hacer que un sistema de información ejecute código malicioso lo cual a su vez vulnere la confidencialidad, integridad y disponibilidad de la información de dicho sistema	Baja
31	Open_VNC	Virtual Network Computing	Un atacante podría acceder de manera no autorizada al sistema de información vulnerando la confidencialidad del sistema	Bajo
32	XDMCP	X Display Manager Control Protocol	Un atacante podría acceder de manera no autorizada al sistema de información vulnerando la confidencialidad del sistema	Bajo

Tabla No. 2 Listado inicial de vulnerabilidades y su priorización referencial

3.1.2 Prioridad para abonados y clientes

La Tabla No. 3 presenta las vulnerabilidades asociadas a direcciones IP que corresponden a clientes y abonados del prestador de servicios de telecomunicaciones, que inicialmente serán reportadas por el EcuCERT y su priorización referencial para la gestión correspondiente por parte del prestador.

No	Vulnerabilidad	Nombre	Descripción del riesgo	Prioridad Clientes /Abonado
1	Netis_Router	Routers Netis	Un atacante podría acceder de manera no autorizada al sistema de información vulnerando la confidencialidad, integridad y disponibilidad del sistema	Critica
2	Accesible_RDP	Accesible Remote Desktop Protocol	Un atacante podría acceder de manera no autorizada al sistema de información vulnerando la confidencialidad, integridad y disponibilidad del sistema	Alta
3	Cisco_Smartinstall	Cisco SmartInstall	Un atacante podría hacer que un sistema de información ejecute código malicioso lo cual a su vez vulnere la confidencialidad, integridad y disponibilidad de la información de dicho sistema	Alta
4	Open_Memcached	mem-cashed memory caching system	Un atacante podría hacer que un sistema de información ejecute código malicioso lo cual a su vez vulnere la confidencialidad, integridad y disponibilidad de la información de dicho sistema	Alta
5	Open_Netbios	Network Basic Input Output System	Un atacante podría hacer que un sistema de información ejecute código malicioso lo cual a su vez vulnere la confidencialidad, integridad y disponibilidad de la información de dicho sistema	Alta
6	Open_VNC	Virtual Network Computing	Un atacante podría acceder de manera no autorizada al sistema de información vulnerando la confidencialidad del sistema	Alta
7	Poodle_SSLv3	Padding on Oracle on Downgraded Legacy Encryption	Un atacante podría hacer que un sistema de información ejecute código malicioso lo cual a su vez vulnere la disponibilidad de la información de dicho sistema	Alta
8	CWMP	CPE Customer Premise Equipment WAN Management Protocol	Un atacante podría hacer que un sistema de información ejecute código malicioso lo cual a su vez vulnere la confidencialidad, integridad y disponibilidad de la información de dicho sistema	Media
9	DNS_Open_Resolver	DNS Domain Name System - Open Resolver	Un atacante podría utilizar el servidor DNS Vulnerable a fin de ejecutar ataques a sistemas de información	Media
10	Freak_SSL	Factoring Attack on RSA Export	Un atacante podría interceptar conexiones HTTPS y posteriormente decifrar su vulnerando la confidencialidad de la información transmitida	Media
11	ISAKMP	Internet Security Association and Key Management Protocol	Un atacante podría hacer que un sistema de información ejecute código malicioso lo cual a su vez vulnere la confidencialidad, integridad y disponibilidad de la información de dicho sistema	Media
12	LDAP	Lightweight Directory Access Protocol	Un atacante podría hacer que un sistema de información ejecute código malicioso lo cual a su vez vulnere la confidencialidad, integridad y disponibilidad de la información de dicho sistema	Media
13	Mdns	Multicast Domain Name System	Un atacante podría hacer que un sistema de información ejecute código malicioso lo cual a su vez vulnere la confidencialidad, integridad y disponibilidad de la información de dicho sistema	Media
14	NAT_PMP	Network Address Translation Port Mapping Protocol	Un atacante podría hacer que un sistema de información ejecute código malicioso lo cual a su vez vulnere la confidencialidad, integridad y disponibilidad de la información de dicho sistema	Media

No	Vulnerabilidad	Nombre	Descripción del riesgo	Prioridad Clientes /Abonado
15	NTP_Version	Netwwork Timpe Protocol Version	Un atacante podría hacer que un sistema de información ejecute código malicioso lo cual a su vez vulnere la disponibilidad de la información de dicho sistema	Media
16	Open_Chargen	Open Character Generator Protocol	Un atacante podría hacer que un sistema de información ejecute código malicioso lo cual a su vez vulnere la disponibilidad de la información de dicho sistema	Media
17	Open_DB2	Relational DataBase Management System	Un atacante podría hacer que un sistema de información ejecute código malicioso lo cual a su vez vulnere la confidencialidad, integridad y disponibilidad de la información de dicho sistema	Media
18	Open_IPMI	Intelligent Platform Management Interface	Un atacante podría acceder de manera no autorizada al sistema de información vulnerando la confidencialidad, integridad y disponibilidad del sistema	Media
19	Open_MongoDB	Base de datos MongoDB	Un atacante podría hacer que un sistema de información ejecute código malicioso lo cual a su vez vulnere la confidencialidad, integridad y disponibilidad de la información de dicho sistema	Media
20	Open_NTP_monitor	Network Time Protocol Monitor	Un atacante podría hacer que un sistema de información ejecute código malicioso lo cual a su vez vulnere la confidencialidad, integridad y disponibilidad de la información de dicho sistema	Media
21	Open_Proxy	Open Proxy Server	Un atacante podría hacer que un sistema de información ejecute código malicioso lo cual a su vez vulnere la confidencialidad, integridad y disponibilidad de la información de dicho sistema	Media
22	Open_Redis	Remote Dictionary Server Redis	Un atacante podría hacer que un sistema de información ejecute código malicioso lo cual a su vez vulnere la confidencialidad de la información de dicho sistema	Media
23	Open_SMB	Server Message Block SMB	Un atacante podría hacer que un sistema de información ejecute código malicioso lo cual a su vez vulnere la confidencialidad, integridad y disponibilidad de la información de dicho sistema	Media
24	Open_SNMP	Simple Network Management Protocol SNMP	Un atacante podría hacer que un sistema de información ejecute código malicioso lo cual a su vez vulnere la confidencialidad, integridad y disponibilidad de la información de dicho sistema	Media
25	Open_SQL_Server_Resl	Microsoft SQL Server Resolution	Un atacante podría hacer que un sistema de información ejecute código malicioso lo cual a su vez vulnere la confidencialidad, integridad y disponibilidad de la información de dicho sistema	Media
26	Open_Telnet	Teletype Network	Un atacante podría acceder de manera no autorizada al sistema de información vulnerando la confidencialidad, integridad y disponibilidad del sistema	Media
27	Scan_Elasticsearch	Elastic search	Un atacante podría hacer que un sistema de información ejecute código malicioso lo cual a su vez vulnere la confidencialidad, integridad y disponibilidad de la información de dicho sistema	Media
28	Open_Portmapper	Remote Procedure Call RCP Port mapper	Un atacante podría acceder de manera no autorizada al sistema de información vulnerando la confidencialidad, integridad y disponibilidad del sistema	Baja
29	Open_Qotd	Open Quote of the Day QOTD	Un atacante podría hacer que un sistema de información ejecute código malicioso lo cual a su vez vulnere la disponibilidad de la información de dicho sistema	Baja
30	Open_SSDP	Open Simple Service Discovery Protocol	Un atacante podría hacer que un sistema de información ejecute código malicioso lo cual a su vez vulnere la confidencialidad, integridad y disponibilidad de la información de dicho sistema	Baja

No	Vulnerabilidad	Nombre	Descripción del riesgo	Prioridad Clientes /Abonado
31	Open_TFTP	Trivial File Transfer Protocol	Un atacante podría hacer que un sistema de información ejecute código malicioso lo cual a su vez vulnere la confidencialidad, integridad y disponibilidad de la información de dicho sistema	Baja
32	XDMCP	X Display Manager Control Protocol	Un atacante podría acceder de manera no autorizada al sistema de información vulnerando la confidencialidad del sistema	Bajo

Tabla No. 3 Listado inicial de vulnerabilidades y su priorización referencial

3.2 Incidentes.

3.2.1 Prioridad para infraestructura de Prestadores de Servicios de Telecomunicaciones

La Tabla No. 4 presenta los incidentes asociados a direcciones IP que corresponden a la infraestructura del prestador de servicios de telecomunicaciones para la prestación del servicio, que inicialmente serán reportadas por el EcuCERT y su priorización referencial para la gestión correspondiente por parte del prestador.

No	Incidente	Descripción	Riesgos	Prioridad Infraestructura Prestador
1	Defacement	La dirección IP detectada hace referencia a un sitio web cuyo contenido fue manipulado por un actor malicioso	Daño a la reputación del propietario de la infraestructura tecnológica.	Critica
2	Fraude IPPBX	La dirección IP detectada hace referencia a una central telefónica IP PBX la cual ha sido comprometida por actores maliciosos	Perjuicio económico a los administradores de la Central Telefónica	Critica
3	Botnet	La dirección IP detectada hace referencia a un host comprometido y manipulado remotamente por un actor malicioso	Realización de ataques informáticos utilizando infraestructura ubicada en el territorio ecuatoriano	Alta
4	Phishing	La dirección IP detectada hace referencia a un host/servidor ubicado en el territorio ecuatoriano que almacena un sitio web fraudulento	Engaño a usuarios para obtener información personal	Alta
5	Ataque DNS	La dirección IP detectada hace referencia a un host que ha realizado actividad maliciosa contra un sistema DNS	Realización de ataques informáticos utilizando infraestructura ubicada en el territorio ecuatoriano	Alta
6	Compromised Website	La dirección IP detectada hace referencia a un servidor web el cual ha sido comprometido y manipulado por un actor malicioso	Vulneración de la confidencialidad, integridad y disponibilidad de la información contenida en el servidor web	Alta
7	Command and Control	La dirección IP detectada hace referencia a un host / servidor el cual controla a otros sistemas con fines maliciosos	Ejecución de varias técnicas de ataques a sistemas de información.	Alta
8	DDoS	La dirección IP detectada hace referencia a un host el cual ha atacado un sistema de información con el objetivo de suspender sus servicios	Vulneración de disponibilidad de servicios y operación de un sistema de información	Alta
9	Blacklisted	La dirección IP detectada hace referencia a un host que ha sido bloqueado internacionalmente debido	Bloqueo a infraestructura de comunicaciones de prestadores de servicios de telecomunicaciones	Alta

No	Incidente	Descripción	Riesgos	Prioridad Infraestructura Prestador
		a actividad maliciosa contra sistemas de información		
10	SPAM	La dirección IP detectada hace referencia a un host desde el cual se origina el envió de información no solicitada	Engaño a usuarios para obtener información personal y ejecución de técnicas de ataque a sistemas de información	Alta
11	Malware	La dirección IP detectada hace referencia a un host / server en el cual se ha detectado un tipo específico de malware	Vulneración de la confidencialidad, integridad y disponibilidad de la información contenida en el host / server	Media
12	Bruteforce	La dirección IP detectada hace referencia a un host el cual ha intentado acceder a un sistema de información de manera no autorizada	Acceso no autorizado a sistemas y la consecuente vulneración de la confidencialidad, integridad y disponibilidad de la información	Media
13	SQL Injection	La dirección IP detectada hace referencia a un host desde el cual se transmite código malicioso hacia sistemas de información	Ejecución de varias técnicas de ataques a sistemas de información.	Media
14	Fast_Flux	La dirección IP detectada hace referencia a un host el cual abusa de un servicio DNS para ejecutar técnicas de ataques a sistemas de información	Ejecución de varias técnicas de ataques a sistemas de información.	Media
15	Inyección de Código	La dirección IP detectada hace referencia a un host desde el cual se transmite código malicioso hacia sistemas de información	Ejecución de varias técnicas de ataques a sistemas de información.	Media
16	Scanners	La dirección IP detectada hace referencia a un host el cual estaría analizando puertos abiertos y cerrados de un sistema de información especifico	Ejecución de varias técnicas de ataques a sistemas de información.	Media
17	Sinkhole	La dirección IP detectada hace referencia a un host que enruta tráfico de su destino original hacia otro lugar con intenciones maliciosas	Realización de ataques informáticos utilizando infraestructura ubicada en el territorio ecuatoriano	Baja

Tabla No. 4 Listado inicial de incidentes y su priorización referencial

3.2.2 Prioridad para Abonados y Clientes

La Tabla No. 5 presenta los incidentes asociados a direcciones IP que corresponden a clientes y abonados del prestador de servicios de telecomunicaciones, que inicialmente serán reportadas por el EcuCERT y su priorización referencial para la gestión correspondiente por parte del prestador.

No	Incidente	Descripción	Riesgos	Prioridad Clientes /Abonado
1	Fraude IPPBX	La dirección IP detectada hace referencia a una central telefónica IP PBX la cual ha sido comprometida por actores maliciosos	Perjuicio económico a los administradores de la Central Telefónica	Critica
2	Ataque DNS	La dirección IP detectada hace referencia a un host que ha realizado actividad maliciosa contra un sistema DNS	Realización de ataques informáticos utilizando infraestructura ubicada en el territorio ecuatoriano	Alta
3	Blacklisted	La dirección IP detectada hace referencia a un host que ha sido bloqueado internacionalmente debido a actividad maliciosa contra sistemas de información	Bloqueo a infraestructura de comunicaciones de prestadores de servicios de telecomunicaciones	Alta
4	Botnet	La dirección IP detectada hace referencia a un host comprometido y manipulado remotamente por un actor malicioso	Realización de ataques informáticos utilizando infraestructura ubicada en el territorio ecuatoriano	Alta
5	Command and Control	La dirección IP detectada hace referencia a un host / servidor el cual controla a otros sistemas con fines maliciosos	Ejecución de varias técnicas de ataques a sistemas de información.	Alta
6	Compromised Website	La dirección IP detectada hace referencia a un servidor web el cual ha sido comprometido y manipulado por un actor malicioso	Vulneración de la confidencialidad, integridad y disponibilidad de la información contenida en el servidor web	Alta
7	Defacement	La dirección IP detectada hace referencia a un sitio web cuyo contenido fue manipulado por un actor malicioso	Daño a la reputación del propietario de la infraestructura tecnológica.	Alta
8	Phishing	La dirección IP detectada hace referencia a un host/servidor ubicado en el territorio ecuatoriano que almacena un sitio web fraudulento	Engaño a usuarios para obtener información personal	Alta
9	SPAM	La dirección IP detectada hace referencia a un host desde el cual se origina el envió de información no solicitada	Engaño a usuarios para obtener información personal y ejecución de técnicas de ataque a sistemas de información	Alta
10	Bruteforce	La dirección IP detectada hace referencia a un host el cual ha intentado acceder a un sistema de información de manera no autorizada	Acceso no autorizado a sistemas y la consecuente vulneración de la confidencialidad, integridad y disponibilidad de la información	Media
11	DDoS	La dirección IP detectada hace referencia a un host el cual ha atacado un sistema de información con el objetivo de suspender sus servicios	Vulneración de disponibilidad de servicios y operación de un sistema de información	Media
12	Fast_Flux	La dirección IP detectada hace referencia a un host el cual abusa de un servicio DNS para ejecutar técnicas de ataques a sistemas de información	Ejecución de varias técnicas de ataques a sistemas de información.	Media
13	Inyeccion de Código	La dirección IP detectada hace referencia a un host desde el cual se transmite código malicioso hacia sistemas de información	Ejecución de varias técnicas de ataques a sistemas de información.	Media
14	Malware	La dirección IP detectada hace referencia a un host / server en el cual se ha detectado un tipo específico de malware	Vulneración de la confidencialidad, integridad y disponibilidad de la información contenida en el host / server	Media

No	Incidente	Descripción	Riesgos	Prioridad Clientes /Abonado
15	Scanners	La dirección IP detectada hace referencia a un host el cual estaría analizando puertos abiertos y cerrados de un sistema de información especifico	Ejecución de varias técnicas de ataques a sistemas de información.	Media
16	SQL Injection	La dirección IP detectada hace referencia a un host desde el cual se transmite código malicioso hacia sistemas de información	Ejecución de varias técnicas de ataques a sistemas de información.	Media
17	Sinkhole	La dirección IP detectada hace referencia a un host que enruta tráfico de su destino original hacia otro lugar con intenciones maliciosas	Realización de ataques informáticos utilizando infraestructura ubicada en el territorio ecuatoriano	Baja

Tabla No. 5 Listado inicial de incidentes y su priorización referencial

4. Referencias

- https://cve.mitre.org/
- https://www.first.org/cvss/
- https://nvd.nist.gov/scap/xccdf/docs/xccdf-spec-1.1.4-20071102.pdf
- https://oval.mitre.org/
- https://cce.mitre.org/
- https://cwe.mitre.org/
- https://cpe.mitre.org/
- https://www.nist.gov/publications/common-configuration-scoring-system-ccss-metrics-software-security-configuration
- https://csrc.nist.gov/projects/security-content-automation-protocol/specifications/ocil
- https://csrc.nist.gov/projects/security-content-automation-protocol/specifications/arf
- https://csrc.nist.gov/projects/security-content-automation-protocol/scap-releases/scap-1-2
- https://www.owasp.org/index.php/Main_Page