

Agencia de Regulación y Control de las Telecomunicaciones

DIRECCIÓN TÉCNICA DE CONTROL DE SEGURIDAD DE REDES DE TELECOMUNICACIONES



La información conlleva un riesgo mínimo o inexistente aplicables para publicación pública. Sujeto a las normas de copyright estándar, puede distribuirse sin restricciones.

CATÁLOGO Y PRIORIZACIÓN DE VULNERABILIDADES E INCIDENTES INICIALES - VERSIÓN 2.0

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 reportadas a los prestadores de servicios de telecomunicaciones, estarán sujetas 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”.

2.2. **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 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 se ha considerado los siguientes sistemas de métricas internacionales de severidad de vulnerabilidades:

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

2.3. 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 para la gestión correspondiente por parte del prestador.

No	Vulnerabilidad	Nombre	Descripción del riesgo	Prioridad Infraestructura Prestador
1	Accesible_RDP	Accesible Remote Desktop Protocol	Servicio RDP accesible remotamente, que podría permitir intentos de acceso no autorizado mediante ataques de fuerza bruta o la explotación de vulnerabilidades asociadas al servicio.	Critica

No	Vulnerabilidad	Nombre	Descripción del riesgo	Prioridad Infraestructura Prestador
2	Cisco_Smartinstall	Cisco SmartInstall	Servicio Cisco Smart Install accesible desde la red, lo que podría permitir a un atacante obtener información de configuración o realizar acciones no autorizadas sobre el dispositivo.	Critica
3	Netis_Router	Routers Netis	Exposición de dispositivos Netis vulnerables, con riesgo de acceso no autorizado y compromiso de la configuración o servicios del router.	Critica
4	Open_Elasticsearch	Instancia Elasticsearch Expuesta a Internet	Elasticsearch expuesto (Open Elasticsearch) Puerto: 9200	Critica
5	Open_Memcached	mem-cached memory caching system	Servicio Memcached accesible remotamente desde la red, lo que podría permitir accesos no autorizados y exposición o manipulación de información almacenada en caché.	Critica
6	Open_MongoDB	Base de datos MongoDB	Servicio MongoDB accesible remotamente, que podría permitir accesos no autorizados o exposición de información almacenada en la base de datos.	Critica
7	Open_MYSQL	Servicio MySQL Expuesto a Internet	Bypass de autenticación en versiones antiguas. Ejecución remota de código en ciertas configuraciones.	Critica
8	Pop_Open_MSMQ_IPv6	Servicio Microsoft Message Queuing (MSMQ) Expuesto sobre IPv6	Infraestructura con puertos de gestión o servicios internos expuestos a la WAN sin controles de filtrado.	Critica
9	Sistema_Vulnerable_Dominio_IPv6	Dominio con Configuración Vulnerable sobre IPv6	Los ataques de dominio suelen estar vinculados al secuestro o manipulación de DNS.	Critica
10	Sistema_Vulnerable_SMTP	Servicio SMTP Vulnerable	Fallo de seguridad o de configuración en el protocolo de transferencia SMTP en correo electrónico.	Critica
11	CWMP	CPE Customer Premise Equipment WAN Management Protocol	Servicio CWMP (CPE WAN Management Protocol) accesible desde la red, que podría permitir la exposición de información de los dispositivos o facilitar accesos y acciones no autorizadas sobre su configuración.	Alta

No	Vulnerabilidad	Nombre	Descripción del riesgo	Prioridad Infraestructura Prestador
12	DNS_Open_Resolver	DNS Domain Name System - Open Resolver	Servicio DNS configurado como resolutor abierto, accesible desde la red, que podría ser utilizado para realizar consultas DNS no autorizadas o participar en ataques de amplificación y denegación de servicio.	Alta
13	Freak_SSL	Factoring Attack on RSA Export	Servicio SSL/TLS vulnerable a FREAK (Factoring Attack on RSA-EXPORT Keys), que podría permitir a un atacante debilitar el cifrado de las comunicaciones y obtener información sensible transmitida entre el cliente y el servidor.	Alta
14	LDAP	Lightweight Directory Access Protocol	Servicio LDAP accesible remotamente desde la red, lo que podría permitir accesos no autorizados o exposición de información relacionada con usuarios, grupos y recursos del directorio.	Alta
15	Mdns	Multicast Domain Name System	Servicio mDNS accesible desde la red, que podría permitir la divulgación de información sobre dispositivos, servicios y recursos disponibles en la red local.	Alta
16	NAT_PMP	Network Address Port Mapping Protocol	Servicio NAT-PMP accesible desde la red, que podría permitir la modificación no autorizada de configuraciones de traducción de direcciones y facilitar la exposición de servicios internos a redes externas.	Alta
17	NTP_Version	Network Time Protocol Version	Servicio NTP con una versión identificada, que podría presentar vulnerabilidades conocidas o configuraciones inseguras dependiendo de la versión utilizada.	Alta
18	Open_Chargen	Open Character Generator Protocol	Servicio CHARGEN accesible desde la red, que podría ser utilizado para generar tráfico excesivo y participar en ataques de denegación de servicio o amplificación de tráfico.	Alta
19	Open_IPMI	Intelligent Platform Management Interface	Servicio IPMI accesible remotamente desde la red, lo que podría permitir accesos no autorizados y afectar la administración o configuración del sistema.	Alta
20	Open_Netbios	Network Basic Input Output System	Servicio NetBIOS accesible desde la red, que podría permitir la exposición de información sobre dispositivos, nombres de equipos y recursos compartidos, así como facilitar intentos de acceso no autorizado.	Alta
21	Open_Port	Exposición de Puerto de Red	Es un servicio perimetral expuesto a internet que tiene activada o permite una función de decodificación o traducción de peticiones sin autenticación.	Alta

No	Vulnerabilidad	Nombre	Descripción del riesgo	Prioridad Infraestructura Prestador
22	Open_Redis	Remote Dictionary Server Redis	Servicio Redis accesible remotamente desde la red, que podría permitir accesos no autorizados, exposición o manipulación de la información almacenada en la base de datos.	Alta
23	Open_SQL_Server_Resl	Microsoft SQL Server Resolution	Servicio Microsoft SQL Server accesible remotamente desde la red, lo que podría permitir accesos no autorizados o exposición de información almacenada en la base de datos.	Alta
24	Open_SSH	Exposición de Servicio SSH	Puerto 22 abierto: Permite enumerar usuarios válidos. Posible ejecución de comandos en ciertos escenarios.	Alta
25	Open_Telnet	Teletype Network	Acceso no autorizado a dispositivos o sistemas mediante un servicio Telnet expuesto, con riesgo de compromiso de la información y configuración.	Alta
26	Poodle_SSLv3	Padding on Oracle on Downgraded Legacy Encryption	Servicio SSL/TLS que permite el uso del protocolo SSLv3, vulnerable al ataque POODLE, lo que podría permitir a un atacante obtener información sensible mediante la explotación de las comunicaciones cifradas.	Alta
27	Sistema_Vulnerable_IMAP	Vulnerabilidad en Servicio IMAP	Servicio IMAP vulnerable, que podría permitir accesos no autorizados, exposición de información o compromiso de las cuentas de correo electrónico, dependiendo de la vulnerabilidad identificada.	Alta
28	HTTP_Vulnerable	Vulnerabilidad en Servicio HTTP	Configuraciones inseguras o posibles vulnerabilidades asociadas al protocolo web, lo que podría permitir accesos no autorizados, exposición de información o explotación de fallas en la aplicación o servidor.	Media
29	ISAKMP	Internet Security Association and Key Management Protocol	Servicio ISAKMP accesible desde la red, utilizado para la negociación y establecimiento de asociaciones de seguridad IPsec, que podría incrementar la superficie de exposición del sistema ante posibles accesos o ataques no autorizados.	Media
30	Open_DB2	Relational DataBase Management System	Servicio IBM Db2 accesible remotamente desde la red, que podría permitir accesos no autorizados o exposición y manipulación de la información almacenada en la base de datos.	Media

No	Vulnerabilidad	Nombre	Descripción del riesgo	Prioridad Infraestructura Prestador
31	Open_IPP	Exposición del Servicio IPP	"Enumeración de impresoras. Acceso no autorizado a servicios de impresión. Impresión remota no autorizada. Exposición de información del sistema. Ataques sobre el servidor de impresión".	Media
32	Open_NTP_monitor	Network Time Protocol Monitor	Servicio de monitoreo NTP accesible remotamente desde la red, que podría permitir la obtención de información sobre el sistema y aumentar la superficie de exposición ante posibles ataques.	Media
33	Open_Proxy	Open Proxy Server	Servicio proxy accesible remotamente desde la red, que podría permitir conexiones no autorizadas, ser utilizado para ocultar el origen del tráfico o facilitar actividades maliciosas.	Media
34	Open_SMB	Server Message Block SMB	Servicio SMB accesible remotamente desde la red, que podría permitir accesos no autorizados, exposición de información o acceso a recursos compartidos del sistema.	Media
35	Open_SNMP	Simple Network Management Protocol SNMP	Servicio SNMP accesible remotamente desde la red, que podría permitir la exposición de información sobre dispositivos y configuraciones de red, así como facilitar accesos no autorizados dependiendo de su configuración.	Media
36	Open_SSDP	Open Simple Service Discovery Protocol	Servicio SSDP accesible remotamente desde la red, que podría permitir la exposición de información sobre dispositivos y servicios disponibles, así como facilitar actividades de reconocimiento de la red.	Media
37	Sandbox_URL	URL Asociada a Contenido Potencialmente Malicioso	Posible comportamiento malicioso relacionado con phishing, malware, descarga de archivos maliciosos o comunicación con infraestructura sospechosa.	Media
38	Scan_Elasticsearch	Elastic search	Servicio Elasticsearch detectado durante un escaneo de red, que permite identificar su presencia y accesibilidad, sin que esto implique necesariamente la existencia de una vulnerabilidad.	Media
39	Scan_MYSQL_IPv6	Servicio MySQL Detectado sobre IPv6	"Puerto 3306 abierto Bypass de autenticación en versiones antiguas Ejecución remota de código en ciertas configuraciones"	Media

No	Vulnerabilidad	Nombre	Descripción del riesgo	Prioridad Infraestructura Prestador
40	Sistema_Vulnerable_POP3	Vulnerabilidad en Servicio POP3	Un atacante puede provocar el fallo de un controlador de notificaciones push mediante un correo electrónico manipulado, debido a una desreferenciación de puntero nulo.	Media
41	Sistema_Vulnerable_Web	Vulnerabilidad en Aplicación Web	Neutralización incorrecta de la entrada durante la generación de la página web (Cross-site Scripting)	Media
42	Open_Port mapper	Remote Procedure Call RCP Port mapper	Servicio Portmapper accesible remotamente desde la red, que podría permitir la enumeración de servicios RPC disponibles y facilitar el reconocimiento o accesos no autorizados al sistema.	Baja
43	Open_Qotd	Open Quote of the Day QOTD	Servicio QOTD (Quote of the Day) accesible remotamente desde la red, que podría ser utilizado para generar tráfico no solicitado y aumentar la superficie de exposición del sistema ante posibles ataques.	Baja
44	Open_TFTP	Trivial File Transfer Protocol	Servicio TFTP accesible remotamente desde la red, que podría permitir la transferencia no autorizada de archivos y la exposición de información debido a la ausencia de mecanismos de autenticación y cifrado.	Baja
45	Open_VNC	Virtual Network Computing	Servicio VNC accesible remotamente desde la red, que podría permitir accesos no autorizados al sistema mediante la explotación de credenciales débiles o vulnerabilidades del servicio.	Bajo
46	XDMCP	X Display Manager Control Protocol	Servicio XDMCP accesible remotamente desde la red, que podría permitir conexiones no autorizadas y exposición de información relacionada con sesiones y sistemas gráficos remotos.	Bajo

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

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 para la gestión correspondiente por parte del prestador.

No	Vulnerabilidad	Nombre	Descripción del riesgo	Prioridad Clientes / Abonado
1	Netis_Router	Routers Netis	Exposición de dispositivos Netis vulnerables, con riesgo de acceso no autorizado y compromiso de la configuración o servicios del router.	Critica
2	Open_Elasticsearch	Exposición de Servicio Elasticsearch	Elasticsearch expuesto (Open Elasticsearch) Puerto: 9200	Critica
3	Open_MYSQL	Exposición de Base de Datos MySQL	Bypass de autenticación en versiones antiguas. Ejecución remota de código en ciertas configuraciones.	Critica
4	Pop_Open_MS MQ_IPv6	Exposición de Servicio Microsoft Message Queuing (MSMQ) sobre IPv6	Infraestructura con puertos de gestión o servicios internos expuestos a la WAN sin controles de filtrado.	Critica
5	Sistema_Vulnerable_Dominio_IPv6	Vulnerabilidad en Dominio con IPv6 Habilitado	Los ataques de dominio suelen estar vinculados al secuestro o manipulación de DNS.	Critica
6	Sistema_Vulnerable_SMTP	Vulnerabilidad en Servicio SMTP	Fallo de seguridad o de configuración en el protocolo de transferencia SMTP en correo electrónico.	Critica
7	Accesible_RDP	Accesible Remote Desktop Protocol	Servicio RDP accesible remotamente, que podría permitir intentos de acceso no autorizado mediante ataques de fuerza bruta o la explotación de vulnerabilidades asociadas al servicio.	Alta
8	Cisco_Smartinstall	Cisco SmartInstall	Servicio Cisco Smart Install accesible desde la red, lo que podría permitir a un atacante obtener información de configuración o realizar acciones no autorizadas sobre el dispositivo.	Alta
9	Open_Memcached	mem-cached memory caching system	Servicio Memcached accesible remotamente desde la red, lo que podría permitir accesos no autorizados y exposición o manipulación de información almacenada en caché.	Alta
10	Open_Netbios	Network Basic Input Output System	Servicio NetBIOS accesible desde la red, que podría permitir la exposición de información sobre dispositivos, nombres de equipos y recursos compartidos, así como facilitar intentos de acceso no autorizado.	Alta
11	Open_Port	Exposición de Puerto de Red	Es un servicio perimetral expuesto a internet que tiene activada o permite una función de decodificación o traducción de peticiones sin autenticación.	Alta
12	Open_VNC	Virtual Network Computing	Servicio VNC accesible remotamente desde la red, que podría permitir accesos no autorizados al sistema mediante la explotación de credenciales débiles o vulnerabilidades del servicio.	Alta

No	Vulnerabilidad	Nombre	Descripción del riesgo	Prioridad Clientes / Abonado
13	Poodle_SSLv3	Padding on Oracle on Downgraded Legacy Encryption	Servicio SSL/TLS que permite el uso del protocolo SSLv3, vulnerable al ataque POODLE, lo que podría permitir a un atacante obtener información sensible mediante la explotación de las comunicaciones cifradas.	Alta
14	CWMP	CPE Customer Premise Equipment WAN Management Protocol	Servicio CWMP (CPE WAN Management Protocol) accesible desde la red, que podría permitir la exposición de información de los dispositivos o facilitar accesos y acciones no autorizadas sobre su configuración.	Media
15	DNS_Open_Resolver	DNS Domain Name System - Open Resolver	Servicio DNS configurado como resolutor abierto, accesible desde la red, que podría ser utilizado para realizar consultas DNS no autorizadas o participar en ataques de amplificación y denegación de servicio.	Media
16	Freak_SSL	Factoring Attack on RSA Export	Servicio SSL/TLS vulnerable a FREAK (Factoring Attack on RSA-EXPORT Keys), que podría permitir a un atacante debilitar el cifrado de las comunicaciones y obtener información sensible transmitida entre el cliente y el servidor.	Media
17	HTTP_Vulnerable	Vulnerabilidad en Servicio HTTP	Configuraciones inseguras o posibles vulnerabilidades asociadas al protocolo web, lo que podría permitir accesos no autorizados, exposición de información o explotación de fallas en la aplicación o servidor.	Media
18	ISAKMP	Internet Security Association and Key Management Protocol	Servicio ISAKMP accesible desde la red, utilizado para la negociación y establecimiento de asociaciones de seguridad IPsec, que podría incrementar la superficie de exposición del sistema ante posibles accesos o ataques no autorizados.	Media
19	LDAP	Lightweight Directory Access Protocol	Servicio LDAP accesible remotamente desde la red, lo que podría permitir accesos no autorizados o exposición de información relacionada con usuarios, grupos y recursos del directorio.	Media
20	Mdns	Multicast Domain Name System	Servicio mDNS accesible desde la red, que podría permitir la divulgación de información sobre dispositivos, servicios y recursos disponibles en la red local.	Media
21	NAT_PMP	Network Address Translation Port Mapping Protocol	Servicio NAT-PMP accesible desde la red, que podría permitir la modificación no autorizada de configuraciones de traducción de direcciones y facilitar la exposición de servicios internos a redes externas.	Media

No	Vulnerabilidad	Nombre	Descripción del riesgo	Prioridad Clientes / Abonado
22	NTP_Version	Network Time Protocol Version	Servicio NTP con una versión identificada, que podría presentar vulnerabilidades conocidas o configuraciones inseguras dependiendo de la versión utilizada.	Media
23	Open_Chargen	Open Character Generator Protocol	Servicio CHARGEN accesible desde la red, que podría ser utilizado para generar tráfico excesivo y participar en ataques de denegación de servicio o amplificación de tráfico.	Media
24	Open_DB2	Relational DataBase Management System	Servicio IBM Db2 accesible remotamente desde la red, que podría permitir accesos no autorizados o exposición y manipulación de la información almacenada en la base de datos.	Media
25	Open_IPMI	Intelligent Platform Management Interface	Servicio IPMI accesible remotamente desde la red, lo que podría permitir accesos no autorizados y afectar la administración o configuración del sistema.	Media
26	Open_IPP	Exposición del Servicio Impresión IPP	"Enumeración de impresoras. Acceso no autorizado a servicios de impresión. Impresión remota no autorizada. Exposición de información del sistema. Ataques sobre el servidor de impresión".	Media
27	Open_MongoDB	Base de datos MongoDB	Servicio MongoDB accesible remotamente, que podría permitir accesos no autorizados o exposición de información almacenada en la base de datos.	Media
28	Open_NTP_monitor	Network Time Protocol Monitor	Servicio de monitoreo NTP accesible remotamente desde la red, que podría permitir la obtención de información sobre el sistema y aumentar la superficie de exposición ante posibles ataques.	Media
29	Open_Proxy	Open Proxy Server	Servicio proxy accesible remotamente desde la red, que podría permitir conexiones no autorizadas, ser utilizado para ocultar el origen del tráfico o facilitar actividades maliciosas.	Media
30	Open_Redis	Remote Dictionary Server Redis	Servicio Redis accesible remotamente desde la red, que podría permitir accesos no autorizados, exposición o manipulación de la información almacenada en la base de datos.	Media
31	Open_SMB	Server Message Block SMB	Servicio SMB accesible remotamente desde la red, que podría permitir accesos no autorizados, exposición de información o acceso a recursos compartidos del sistema.	Media

No	Vulnerabilidad	Nombre	Descripción del riesgo	Prioridad Clientes / Abonado
32	Open_SNMP	Simple Network Management Protocol SNMP	Servicio SNMP accesible remotamente desde la red, que podría permitir la exposición de información sobre dispositivos y configuraciones de red, así como facilitar accesos no autorizados dependiendo de su configuración.	Media
33	Open_SQL_Server_Resl	Microsoft SQL Server Resolution	Servicio Microsoft SQL Server accesible remotamente desde la red, lo que podría permitir accesos no autorizados o exposición de información almacenada en la base de datos.	Media
34	Open_SSH	Exposición de Servicio SSH	Puerto 22 abierto: Permite enumerar usuarios válidos. Posible ejecución de comandos en ciertos escenarios.	Media
35	Open_Telnet	Teletype Network	Acceso no autorizado a dispositivos o sistemas mediante un servicio Telnet expuesto, con riesgo de compromiso de la información y configuración.	Media
36	Sandbox_URL	URL Asociada a Contenido Potencialmente Malicioso	Posible comportamiento malicioso relacionado con phishing, malware, descarga de archivos maliciosos o comunicación con infraestructura sospechosa.	Media
37	Scan_Elasticsearch	Elastic search	Servicio Elasticsearch detectado durante un escaneo de red, que permite identificar su presencia y accesibilidad, sin que esto implique necesariamente la existencia de una vulnerabilidad.	Media
38	Scan_MYSQL_IPv6	Servicio MySQL Detectado sobre IPv6	"Puerto 3306 abierto Bypass de autenticación en versiones antiguas. Ejecución remota de código en ciertas configuraciones".	Media
39	Sistema_Vulnerable_IMAP	Vulnerabilidad en Servicio IMAP	Servicio IMAP vulnerable, que podría permitir accesos no autorizados, exposición de información o compromiso de las cuentas de correo electrónico, dependiendo de la vulnerabilidad identificada.	Media
40	Sistema_Vulnerable_POP3	Vulnerabilidad en Servicio POP3	Un atacante puede provocar el fallo de un controlador de notificaciones push mediante un correo electrónico manipulado, debido a una desreferenciación de puntero nulo.	Media
41	Sistema_Vulnerable_Web	Vulnerabilidad en Aplicación Web	Neutralización incorrecta de la entrada durante la generación de la página web (Cross-site Scripting).	Media
42	Open_Portmapper	Remote Procedure Call RCP Port mapper	Servicio Portmapper accesible remotamente desde la red, que podría permitir la enumeración de servicios RPC disponibles y facilitar el reconocimiento o accesos no autorizados al sistema.	Baja

No	Vulnerabilidad	Nombre	Descripción del riesgo	Prioridad Clientes / Abonado
43	Open_Qotd	Open Quote of the Day QOTD	Servicio QOTD (Quote of the Day) accesible remotamente desde la red, que podría ser utilizado para generar tráfico no solicitado y aumentar la superficie de exposición del sistema ante posibles ataques.	Baja
44	Open_SSDP	Open Simple Service Discovery Protocol	Servicio SSDP accesible remotamente desde la red, que podría permitir la exposición de información sobre dispositivos y servicios disponibles, así como facilitar actividades de reconocimiento de la red.	Baja
45	Open_TFTP	Trivial File Transfer Protocol	Servicio TFTP accesible remotamente desde la red, que podría permitir la transferencia no autorizada de archivos y la exposición de información debido a la ausencia de mecanismos de autenticación y cifrado.	Baja
46	XDMCP	X Display Manager Control Protocol	Servicio XDMCP accesible remotamente desde la red, que podría permitir conexiones no autorizadas y exposición de información relacionada con sesiones y sistemas gráficos remotos.	Bajo

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

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 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.	Crítica
2	Fraude IPPBX	La dirección IP detectada está asociada a un sistema IPPBX involucrado en actividades fraudulentas, como el uso no autorizado del servicio de telefonía para realizar llamadas o generar tráfico irregular.	Perjuicio económico a los administradores de la Central Telefónica.	Crítica

No	Incidente	Descripción	Riesgos	Prioridad Infraestructura Prestador
3	Pass_LEAK	La dirección IP detectada está asociada a la exposición o filtración de credenciales de acceso, posiblemente comprometidas y divulgadas por un actor malicioso.	Filtración de una o más credenciales de acceso (usuarios y/o contraseñas) asociadas a la organización.	Critica
4	Ataque DNS	La dirección IP detectada está asociada a actividades de ataque contra servicios DNS, que podrían afectar la disponibilidad, integridad o funcionamiento de los servicios de resolución de nombres.	Realización de ataques informáticos utilizando infraestructura ubicada en el territorio ecuatoriano.	Alta
5	Blacklisted	La dirección IP, dominio o servicio detectado se encuentra incluido en una lista negra debido a su asociación con actividades sospechosas, maliciosas o no confiables.	Bloqueo a infraestructura de comunicaciones de prestadores de servicios de telecomunicaciones.	Alta
6	Botnet	La dirección IP detectada está asociada a una botnet o a infraestructura utilizada para controlar dispositivos comprometidos y realizar actividades maliciosas.	Compromiso de dispositivos y utilización no autorizada de recursos.	Alta
7	Command and Control	La dirección IP detectada está asociada a una infraestructura de Command and Control (C2), utilizada para establecer comunicaciones con dispositivos comprometidos y permitir el envío de instrucciones o ejecución de actividades maliciosas.	Compromiso y control remoto de sistemas afectados.	Alta
8	Compromised Website	La dirección IP detectada está asociada a un sitio web comprometido, cuyo contenido, funcionamiento o infraestructura podría haber sido alterado o utilizado de manera no autorizada por un actor malicioso.	Vulneración de la confidencialidad, integridad y disponibilidad de la información contenida en el servidor web.	Alta
9	DDoS	La dirección IP detectada está asociada a actividades de denegación de servicio distribuido (DDoS), dirigidas a afectar la disponibilidad de sistemas, servicios o recursos mediante la generación de un volumen elevado de tráfico o solicitudes.	Vulneración de disponibilidad de servicios y operación de un sistema de información.	Alta

No	Incidente	Descripción	Riesgos	Prioridad Infraestructura Prestador
10	Phishing	La dirección IP detectada está asociada a un sitio web o infraestructura utilizada para realizar actividades de phishing, con el objetivo de engañar a los usuarios y obtener información sensible o credenciales de acceso.	Robo de credenciales o información sensible de los usuarios.	Alta
11	SPAM	La dirección IP detectada está asociada al envío masivo de mensajes no solicitados (SPAM), que podría afectar la reputación del servicio, generar tráfico no deseado o ser utilizado para distribuir contenido malicioso.	Engaño a usuarios para obtener información personal y ejecución de técnicas de ataque a sistemas de información.	Alta
12	Bruteforce	La dirección IP detectada está asociada a intentos reiterados de acceso mediante ataques de fuerza bruta, orientados a obtener credenciales válidas o acceso no autorizado a sistemas y servicios.	Acceso no autorizado a sistemas y la consecuente vulneración de la confidencialidad, integridad y disponibilidad de la información.	Media
13	Fast_Flux	La dirección IP detectada está asociada a actividades de inyección de código, dirigidas a introducir y ejecutar código no autorizado en sistemas o aplicaciones, lo que podría comprometer su funcionamiento, integridad o seguridad.	Dificultad para identificar y bloquear infraestructura maliciosa.	Media
14	HTTP_Vulnerabl e	La dirección IP detectada está asociada a un servicio HTTP que presenta vulnerabilidades o configuraciones inseguras, lo que podría permitir accesos no autorizados, explotación del servicio o exposición de información.	Configuraciones inseguras o posibles vulnerabilidades asociadas al protocolo web, lo que podría permitir accesos no autorizados, exposición de información o explotación de fallas en la aplicación o servidor.	Media
15	Inyección de Código	La dirección IP detectada está asociada a actividades de inyección de código, orientadas a introducir o ejecutar código no autorizado en sistemas o aplicaciones, lo que podría comprometer su funcionamiento, integridad o seguridad.	Ejecución no autorizada de código en sistemas o aplicaciones.	Media
16	Malware	La dirección IP detectada está asociada a actividades relacionadas con malware, incluyendo la distribución, alojamiento o comunicación con software malicioso que podría comprometer sistemas o dispositivos.	Vulneración de la confidencialidad, integridad y disponibilidad de la información contenida en el host / server.	Media

No	Incidente	Descripción	Riesgos	Prioridad Infraestructura Prestador
17	Sandbox_URL	La URL detectada está asociada a contenido sospechoso o potencialmente malicioso, identificado mediante su análisis en un entorno controlado (sandbox), que podría estar relacionado con phishing, malware u otras actividades maliciosas.	Posible comportamiento malicioso relacionado con phishing, malware, descarga de archivos maliciosos o comunicación con infraestructura sospechosa.	Media
18	Scanners	La dirección IP detectada está asociada a actividades de escaneo o reconocimiento de sistemas y servicios, orientadas a identificar puertos, aplicaciones, vulnerabilidades o recursos expuestos en la red.	Identificación de servicios, sistemas o vulnerabilidades expuestas.	Media
19	SQL Injection	La dirección IP detectada está asociada a actividades de inyección SQL, dirigidas a manipular consultas hacia bases de datos con el propósito de obtener, modificar o eliminar información de manera no autorizada.	Ejecución de varias técnicas de ataques a sistemas de información.	Media
20	Sinkhole	La dirección IP detectada está asociada a una infraestructura de tipo Sinkhole, utilizada para redirigir y monitorear comunicaciones de dispositivos comprometidos, permitiendo identificar o analizar actividades relacionadas con malware o botnets.	Realización de ataques informáticos utilizando infraestructura ubicada en el territorio ecuatoriano.	Baja

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

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 para la gestión correspondiente por parte del prestador.

No	Incidente	Descripción	Riesgos	Prioridad Clientes /Abonado
1	Fraude IPPBX	La dirección IP detectada está asociada a un sistema IPPBX involucrado en actividades fraudulentas, como el uso no autorizado del servicio de telefonía para realizar llamadas o generar tráfico irregular.	Perjuicio económico a los administradores de la Central Telefónica.	Critica

No	Incidente	Descripción	Riesgos	Prioridad Clientes /Abonado
2	Pass_LEAK	La dirección IP detectada está asociada a la exposición o filtración de credenciales de acceso, posiblemente comprometidas y divulgadas por un actor malicioso.	Filtración de una o más credenciales de acceso (usuarios y/o contraseñas) asociadas a la organización.	Crítica
3	Ataque DNS	La dirección IP detectada está asociada a actividades de ataque contra servicios DNS, que podrían afectar la disponibilidad, integridad o funcionamiento de los servicios de resolución de nombres.	Realización de ataques informáticos utilizando infraestructura ubicada en el territorio ecuatoriano.	Alta
4	Blacklisted	La dirección IP, dominio o servicio detectado se encuentra incluido en una lista negra debido a su asociación con actividades sospechosas, maliciosas o no confiables.	Bloqueo a infraestructura de comunicaciones de prestadores de servicios de telecomunicaciones.	Alta
5	Botnet	La dirección IP detectada está asociada a una botnet o a infraestructura utilizada para controlar dispositivos comprometidos y realizar actividades maliciosas.	Compromiso de dispositivos y utilización no autorizada de recursos.	Alta
6	Command and Control	La dirección IP detectada está asociada a una infraestructura de Command and Control (C2), utilizada para establecer comunicaciones con dispositivos comprometidos y permitir el envío de instrucciones o ejecución de actividades maliciosas.	Compromiso y control remoto de sistemas afectados.	Alta
7	Compromised Website	La dirección IP detectada está asociada a un sitio web comprometido, cuyo contenido, funcionamiento o infraestructura podría haber sido alterado o utilizado de manera no autorizada por un actor malicioso.	Vulneración de la confidencialidad, integridad y disponibilidad de la información contenida en el servidor web.	Alta
8	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
9	Phishing	La dirección IP detectada está asociada a un sitio web o infraestructura utilizada para realizar actividades de phishing, con el objetivo de engañar a los usuarios y obtener información sensible o credenciales de acceso.	Robo de credenciales o información sensible de los usuarios.	Alta

No	Incidente	Descripción	Riesgos	Prioridad Clientes /Abonado
10	SPAM	La dirección IP detectada está asociada al envío masivo de mensajes no solicitados (SPAM), que podría afectar la reputación del servicio, generar tráfico no deseado o ser utilizado para distribuir contenido malicioso.	Engaño a usuarios para obtener información personal y ejecución de técnicas de ataque a sistemas de información.	Alta
11	Sandbox_URL	La URL detectada está asociada a contenido sospechoso o potencialmente malicioso, identificado mediante su análisis en un entorno controlado (sandbox), que podría estar relacionado con phishing, malware u otras actividades maliciosas.	Posible comportamiento malicioso relacionado con phishing, malware, descarga de archivos maliciosos o comunicación con infraestructura sospechosa.	Alta
12	HTTP_Vulnerable	La dirección IP detectada está asociada a un servicio HTTP que presenta vulnerabilidades o configuraciones inseguras, lo que podría permitir accesos no autorizados, explotación del servicio o exposición de información.	Configuraciones inseguras o posibles vulnerabilidades asociadas al protocolo web, lo que podría permitir accesos no autorizados, exposición de información o explotación de fallas en la aplicación o servidor.	Alta
13	Bruteforce	La dirección IP detectada está asociada a intentos reiterados de acceso mediante ataques de fuerza bruta, orientados a obtener credenciales válidas o acceso no autorizado a sistemas y servicios.	Acceso no autorizado a sistemas y la consecuente vulneración de la confidencialidad, integridad y disponibilidad de la información.	Media
14	DDoS	La dirección IP detectada está asociada a actividades de denegación de servicio distribuido (DDoS), dirigidas a afectar la disponibilidad de sistemas, servicios o recursos mediante la generación de un volumen elevado de tráfico o solicitudes.	Vulneración de disponibilidad de servicios y operación de un sistema de información.	Media
15	Fast_Flux	La dirección IP detectada está asociada a actividades de inyección de código, dirigidas a introducir y ejecutar código no autorizado en sistemas o aplicaciones, lo que podría comprometer su funcionamiento, integridad o seguridad.	Dificultad para identificar y bloquear infraestructura maliciosa.	Media
16	Inyección de Código	La dirección IP detectada está asociada a actividades de inyección de código, orientadas a introducir o ejecutar código no autorizado en sistemas o aplicaciones, lo que podría comprometer su funcionamiento, integridad o seguridad.	Ejecución no autorizada de código en sistemas o aplicaciones.	Media

No	Incidente	Descripción	Riesgos	Prioridad Clientes /Abonado
17	Malware	La dirección IP detectada está asociada a actividades relacionadas con malware, incluyendo la distribución, alojamiento o comunicación con software malicioso que podría comprometer sistemas o dispositivos.	Vulneración de la confidencialidad, integridad y disponibilidad de la información contenida en el host / server.	Media
18	Scanners	La dirección IP detectada está asociada a actividades de escaneo o reconocimiento de sistemas y servicios, orientadas a identificar puertos, aplicaciones, vulnerabilidades o recursos expuestos en la red.	Identificación de servicios, sistemas o vulnerabilidades expuestas.	Media
19	SQL Injection	La dirección IP detectada está asociada a actividades de inyección SQL, dirigidas a manipular consultas hacia bases de datos con el propósito de obtener, modificar o eliminar información de manera no autorizada.	Ejecución de varias técnicas de ataques a sistemas de información.	Media
20	Sinkhole	La dirección IP detectada está asociada a una infraestructura de tipo Sinkhole, utilizada para redirigir y monitorear comunicaciones de dispositivos comprometidos, permitiendo identificar o analizar actividades relacionadas con malware o botnets.	Realización de ataques informáticos utilizando infraestructura ubicada en el territorio ecuatoriano.	Baja

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

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-ccsmetrics-software-security-configuration>
- <https://csrc.nist.gov/projects/security-content-automationprotocol/specifications/ocil>
- <https://csrc.nist.gov/projects/security-content-automationprotocol/specifications/arf>
- <https://csrc.nist.gov/projects/security-content-automation-protocol/scapreleases/scap-1-2>
- https://www.owasp.org/index.php/Main_Page