GESTIÓN DE INCIDENTES Y VULNERABILIDADES v2

ELABORADO POR	REVISADO POR	APROBADO POR
Nombre: Fernando Hernández	**Nombre:**	**Nombre:**
Cargo: Técnico de Soporte	**Cargo:**	**Cargo:**

1. OBJETIVO
   Establecer procedimientos relacionados con vulnerabilidad e incidentes, en los que se considere el registro, priorización, análisis, escalamiento y gestión.

2. PROCEDIMIENTOS
   a. **NOTIFICACIONES**
      - ARCOTEL a SPEED FIBER. El Arcotel notificará sobre vulnerabilidades e incidentes presentes en la red del prestador o vinculados a sus abonados o clientes.
      - SPEED FIBER al ARCOTEL. Se debe notificar al ARCOTEL sobre cualquier incidente que afecten a la seguridad de la red y sus servicios, este reporte se le realiza al correo **incedente@ecucert.gob.ec**

   b. **PRIORIZACION**
      - Las notificaciones y reportes deben ser priorizadas de acuerdo al siguiente detalle:
        - Prioridades de Vulnerabilidades
          - Prioridad para Infraestructura

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	Media
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

- Prioridad para abonados y clientes

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	Media
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 podria 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 podria 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 podria 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 podria 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 podria 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 podria 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 podria 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 podria 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 podria 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 podria 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 podria 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 podria 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 podria 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 podria 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 podria 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 podria 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

- Prioridades de Incidentes
  - Prioridad para Infraestructura

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 especifico 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

- Prioridad para abonados y clientes

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

No	Incidente	Descripción	Riesgos	Prioridad Clientes /Abonado
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 especifico de malware	Vulneración de la confidencialidad, integridad y disponibilidad de la información contenida en el host / server	Media
15	Scanners	La dirección IP detectada hace referencia a un host el cual estaria analizando puertos abiertos y cerrados de un sistema de información especifico	Ejecución de varias técnicas de ataques a sistemas de información.	Media

No	Incidente	Descripción	Riesgos	Prioridad Clientes /Abonado
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

c. **CATEGORIZACIÓN**

- Las notificaciones y reportes deben ser categorizadas:

Color	¿Cuándo utilizar?	¿Cómo debe ser compartida la información?	Ejemplo
TLP:ROJO	**DIFUSIÓN RESTRINGIDA** Cuando la información está limitada a personas concretas, debido a que su difusión a terceras personas podría tener un impacto en la privacidad, reputación u operaciones si es mal utilizada.	Los destinatarios no pueden compartir información de TLP: ROJO con nadie fuera del intercambio, reunión o conversación específica en la que se reveló originalmente. En caso de que se necesite dar a conocer a otra persona se deberá pedir autorización al emisor de la información. En la mayoría de los casos, TLP:ROJO debe intercambiarse de manera verbal o en persona. Los destinatarios no pueden compartir información con nadie, incluso en un nivel jerárquico superior.	1. Información compartida en una reunión o conversación. 2. Correo electrónico directo. (Con etiqueta TLP:ROJO)

TLP:ÁMBAR	**DIFUSIÓN LIMITADA** Cuando la información requiere apoyo para que se actúe de manera efectiva, pero conlleva riesgos para la privacidad, la reputación o las operaciones, si se comparte fuera de las organizaciones involucradas.	Los destinatarios solo pueden compartir información de TLP:ÁMBAR con miembros de su propia organización, y otros actores que necesiten conocerla para protegerse o evitar daños mayores. Las fuentes tienen la libertad de especificar límites adicionales para compartirla.	Acuerdos de confidencialidad entre Centros de Respuesta a Incidentes Informáticos.
TLP:VERDE	**DIVULGACIÓN LIMITADA DENTRO DE LA COMUNIDAD** Cuando la información es útil para el conocimiento de todas las organizaciones participantes.	La información recibida con etiqueta TLP:Verde puede circular libremente dentro de una comunidad en particular, pero no implica que sea información pública. Los beneficiarios pueden compartir la información con sus compañeros y organizaciones asociadas dentro de su sector o comunidad, pero no fuera de ella o a través de canales accesibles públicamente.	Compartir un análisis de malware dentro de una comunidad objetivo determinada.
TLP:BLANCO	**DIVULGACIÓN SIN RESTRICCIÓN** Cuando la información no supone ningún riesgo de mal uso, dentro de las reglas y procedimientos establecidos para su difusión pública.	Se debe tener en consideración que al momento de su difusión, se deben respetar los derechos de autor.	

d. **PROTECCIÓN DE INFORMACIÓN**

El encargado de seguridad, previo al comienzo de las actividades en la gestión de incidentes y vulnerabilidades, firmará un acuerdo de confidencialidad, en donde se establezcan las obligaciones respecto a la no divulgación y tratamiento de la información.

MODELO DE ACUERDO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE INFORMACIÓN.

ACUERDO SUSCRITO ENTRE EL ENCARGADO DE SEGURIDAD DEL PRESTADOR DE SERVICIOS Y LA MÁXIMA AUTORIDAD DE LA EMPRESA.

Intervienen en la celebración del presente Acuerdo de Confidencialidad, por una parte el Sr. XXXXX, en calidad de Encargado de Seguridad de la Información, de la empresa XXXXXX, designado a través del Acta o Documento #####, suscrita el ########, mayor de edad y domiciliado(a) en la ciudad de XXXX, identificado(a) como aparece al pie de su respectiva firma; en adelante conocido como "EL ENCARGADO DE SEGURIDAD DE LA INFORMACIÓN"; y por la otra, el Sr. XXXXX, en calidad de Representante Legal de la Empresa XXXXXXXXXXXXXXXXXXXXXXX, mayor de edad y domiciliado(a) en la ciudad de XXXXXXX, identificado(a) como aparece al pie de su firma.

PRIMERA.- ANTECEDENTES.

- La empresa XXXXXX dispone del correspondiente Título Habilitante otorgado con fecha XXXXXXX por la ARCOTEL para la provisión de los servicios de telecomunicaciones de XXXXXXX. El señor XXXXXX, con documento de identidad Nro. XXXXXX, fue nombrado representante legal de la empresa XXXXXX, según consta en la documentación de respaldo que se adjunta.

- El señor XXXXX, con documento de identidad No. XXXXXX, fue designado Encargado de Seguridad de la empresa XXXXXX, mediante Acta o Documento ##### de fecha XXXXXX, cuya copia se adjunta.

- Conforme el artículo 76 de la Ley Orgánica de Telecomunicaciones "*Medidas técnicas de seguridad e invulnerabilidad. Las y los prestadores de servicios ya sea que usen red propia o la de un tercero, deberán adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad de sus servicios y la invulnerabilidad de la red y garantizar el secreto de las comunicaciones y de la información transmitida por sus redes. Dichas medidas garantizarán un nivel de seguridad adecuado al riesgo existente.*".

- Artículo 84 de la Ley Orgánica de Telecomunicaciones "*Obligaciones adicionales. La Agencia de Regulación y Control de las Telecomunicación establecerá y reglamentará los mecanismos para supervisar el cumplimiento de las obligaciones tanto de secreto de las comunicaciones como de seguridad de datos personales y, en su caso, dictará las instrucciones correspondientes, que serán vinculantes para las y los prestadores de servicios, con el fin de que adopten determinadas medidas relativas a la integridad y seguridad de las redes y servicios…*".

SEGUNDA.- OBJETO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE INFORMACIÓN.

- El objeto del presente acuerdo se refiere al compromiso y obligación que asume el Encargado de Seguridad y la empresa XXXXXXXXXX, respecto a la confidencialidad y no divulgación de información que en ejercicio de las funciones obtienen o reportan para la gestión de vulnerabilidades o incidentes.

- El Encargado de Seguridad utilizará la información recibida con fines de generación de estadísticas, administración, manejo y gestión de vulnerabilidades o incidentes de seguridad de la información.

- El Encargado de Seguridad, únicamente utilizaran la información para el fin mencionado en la condición anterior, comprometiéndose a mantener la más estricta confidencialidad, advirtiendo que dicha obligación se extiende a cualquier persona que por su relación con EL PRESTADOR, deba tener acceso a la información entregada, obtenida o elaborada.

- El Encargado de Seguridad no podrá reproducir, modificar, hacer pública o divulgar ya sea en forma oral, visual, escrita, grabada en medios magnéticos o en cualquier otra forma tangible, la información objeto del presente acuerdo, en cumplimiento con lo dispuesto en la Norma Técnica para la gestión de incidentes y vulnerabilidades.

- El Encargado de Seguridad asume la obligación de guardar secreto sobre cuanta información pudieran disponer con relación a la gestión de vulnerabilidades e incidentes y no comunicarlos a terceros, aún después de cinco (5) años de la finalizada la relación entre las partes.

TERCERA.- EXCEPCIONES.

Sin prejuicio de lo establecido en el presente Acuerdo, las partes aceptan que la obligación de confidencialidad no se aplicara en el siguiente caso:

- Cuando la información fuera de dominio público en el momento de su suministro al PRESTADOR, o una vez suministrada la información, esta acceda al dominio público sin transgredir ninguna de las condiciones del presente Acuerdo.

- Cuando un mandato judicial exija su divulgación. En este caso EL PRESTADOR proporcionará la información solicitada salvaguardando sus propiedades de seguridad e indicando la categorización de información.

CUARTA.- VIGENCIA Y PLAZO.

- El Acuerdo entrará en vigor en el momento de la firma del mismo por ambas partes y tiene validez hasta cinco (5) años después del cese de las funciones del encargado de seguridad.

QUINTA.- CONFLICTO.

En caso de cualquier conflicto o discrepancia que pueda surgir en relación con la interpretación y/o cumplimiento del presente Acuerdo, las partes se someten expresamente a los Jueces competentes de la ciudad de XXXXXX, con renuncia a su fuero propio, aplicándose la legislación vigente en la República del Ecuador.

SÉPTIMA.- INCUMPLIMIENTO.

El incumplimiento de las obligaciones establecidas en el presente Acuerdo de no Divulgación, dará lugar al inicio de las acciones administrativas, civiles y penales contempladas en la normativa jurídica vigente en el estado ecuatoriano.

Y en señal de expresa conformidad y aceptación de los términos recogidos en el presente acuerdo, lo firman las partes por duplicado.

Dado y firmado en Quito, a XX de XXX de 201X

Sr Encargado de Seguridad de la Prestadora de Servicios	Sr. Prestador/a de Servicios

e. **RESPALDO Y CONSERVACIÓN DE LA INFORMACIÓN**

Toda la información relacionada con incidentes y vulnerabilidades debe estar respaldada de manera que garantice la confidencialidad, integridad y disponibilidad de la misma.

Speed Fiber deberá conservar dicha información de acuerdo al siguiente detalle:

- Información Pública General o Pública Comunitaria: durante 6 (seis) meses.
- Información Sensible: durante 1 (un) año.
- Información Confidencial: durante 3 (tres) años.

Speed Fiber almacenará por el lapso de 1 (un) año, la información relativa a la asignación de las direcciones IP de sus clientes o abonados, la información incluirán la fecha y hora que fue asignada la IP.

f. **DIFUSIÓN DE LA INFORMACIÓN**

Las notificaciones realizadas por SPEED FIBER a sus abonados o clientes debe ser comunicada de manera simultánea al Centro de Respuestas de Incidentes Informáticos de la ARCOTEL, al correo electrónico **notificaciones@ecucert.gob.ec**

g. **FORMATO NOTIFICACIONES**

Las notificaciones enviadas del ARCOTEL a SPEED FIBER contendrán al menos la siguiente información:

Campo	Posibles valores del campo
Número de ticket-comprobante	Número de notificación
Evento	Incidente o vulnerabilidad
Prioridad	Crítica, alta, media o baja
Confidencialidad (TLP)	Rojo, ámbar, verde o blanco
Tipo de usuario	Abonados o clientes, Infraestructura propia.

En el caso que SPEED FIBER envíe una notificación al ARCOTEL, este deberá realizar un análisis previo y una vez que se determine como precedentes, deberán ser comunicadas a los prestadores de servicios de telecomunicaciones involucrados, en un tiempo no mayor a tres días contados desde que se recibió la notificación inicial.

h. **INFORMACIÓN DIRECCIONES IP**

SPEED FIBER entregará al ARCOTEL la información del bloque o bloques de direcciones IP que son asignados a sus clientes e infraestructura propia.

De presentarse cambio o actualizaciones en las direcciones IP, deberá informarse al ARCOTEL en un término de 15 (quince) días para su actualización.

i. **TIEMPOS DE RESPUESTA, GESTION Y RESPUESTA DE NOTIFICACIONES**
SPEED FIBER deberá cumplir con los siguientes términos para notificar las acciones implementadas o a implementar para la gestión de incidentes y vulnerabilidades reportadas por el ARCOTEL

- Para Vulnerabilidades:

Vulnerabilidad	Tiempos máximos
Prioridad	Recepción, Gestión y Respuesta a la ARCOTEL
Crítica	4 días hábiles
Alta	8 días hábiles
Media	Informativa
Baja	Informativa

- Para Incidentes:

Incidente	Tiempos máximos
Prioridad	Recepción, Gestión y Respuesta a la ARCOTEL
Crítica	1 día calendario
Alta	2 días hábiles
Media	4 días hábiles
Baja	Informativa

j. **ESTADOS DE GESTIÓN**
Se podrá tener los siguientes estados:

- Atendido. Se establece cuando la vulnerabilidad o incidente fue gestionado en su totalidad.

- Pendiente. Se establece cuando la vulnerabilidad o incidente fue realizada de manera parcial, SPEED FIBER informará una fecha en la que completará la gestión total.

- En Análisis. Se establece cuando la gestión de la vulnerabilidad o incidente requiere de la toma de acciones que están fuera del alcance de SPEED FIBER.

k. **RESPUESTA DE NOTIFICACIONES**
Los reportes de incidentes o vulnerabilidades detectados por SPEED FIBER y que tengan una prioridad crítica o alta o que requieran apoyo del ARCOTEL, deberán ser enviadas al correo **incedente@ecucert.gob.ec** para su registro.

Los reportes de vulnerabilidades con prioridad crítica o alta, detectados por SPEED FIBER, serán reportados mensualmente al ARCOTEL de manera consolidada por cada tipo de vulnerabilidad y tipo de usuario dentro de los 10 (diez) primeros días, del siguiente mes, en el formato que la ARCOTEL establezca.

Los reportes de incidentes con prioridad crítica o alta, detectados por SPEED FIBER, serán reportados en el término de 7 (siete) días luego de su gestión al ARCOTEL, en el formato que la ARCOTEL establezca.

I. ESCALAMIENTO DE INCIDENTES

1) SPEED FIBER al ARCOTEL

    a. Incidente existente

    b. Priorizar el incidente

        i. Prioridad para Infraestructura

        ii. Prioridad para abonados o clientes

    c. Notificar al Arcotel sobre el incidente (**incedente@ecucert.gob.ec)** empleando la categorización correspondiente.

    d. Validar que el encargado de seguridad haya firmado el acuerdo de confidencialidad.

    e. El encargado de seguridad deberá brindar soporte para solventar el incidente.

    f. Almacenar y respaldar la información relacionada con el incidente.

    g. Enviar una notificación de las acciones implementadas o a implementar para la gestión del incidente de acuerdo a los tiempos máximos establecidos.

2) ARCOTEL a SPEED FIBER

    a. Notificación de Incidente existente

    b. Priorizar el incidente

        i. Prioridad para Infraestructura

    ii. Prioridad para abonados o clientes

c. Validar que el encargado de seguridad haya firmado el acuerdo de confidencialidad.

d. El encargado de seguridad deberá brindar soporte para solventar el incidente.

e. Almacenar y respaldar la información relacionada con el incidente.

f. Enviar una notificación de las acciones implementadas o a implementar para la gestión del incidente de acuerdo a los tiempos máximos establecidos.