Propuesta de modelo para un Sistema Inteligente de Detección de Intrusos en Redes Informáticas (SIDIRI)

Arroyave, Juan David., Herrera, Jonathan y Vásquez, Esteban.
{ifjuar, ifjoher, ifesvas}@eia.edu.co
Escuela de Ingeniería de Antioquia

Resumen—
SIDIRI es una propuesta de un modelo que utiliza sistemas inteligentes, en particular redes neuronales artificiales, como motor de análisis (A-box) de IDS con el fin de obtener una respuesta inteligente y proactiva a las necesidades de seguridad en las redes telemáticas del mundo de hoy.

Índice de Términos—IDS, Redes Neuronales Artificiales, Seguridad, Intrusos, Redes Informáticas

INTRODUCCIÓN

La información es la base de las actividades humanas, del desarrollo social y económico. Ya no nos mueve la rueda, nos mueve el impulso de unos y ceros, es el conocimiento y su posesión lo que hace girar al mundo de hoy, la bien llamada era de la información. Y así como con el crecimiento de la red mundial de comunicaciones, la aparición y rápido desarrollo del comercio electrónico y la migración de los antiguos sistemas a plataformas de servicios en línea se hace cada vez más patente la necesidad de mantener la información segura, íntegra, y disponible, una labor no muy fácil.

Las empresas tienen que pensar en proteger a sus empleados, a sus socios y clientes y sobretodo la información que mantiene el negocio, ya que la internet es desde cualquier punto de vista una pasarela de información indispensable para obtener ventajas competitivas, desarrollar y mantener nuevos mercados y crecer como organización, conocer entonces a quienes pueden atentar contra la seguridad de la información y tener medios para impedirlo es una obligación.

I. LAS AMENAZAS

Después de tener claro cuál es la importancia de la información para empresas y particulares, se debe comprender que existen innumerables factores que pueden poner en riesgo dicha información, el estar conectados al mundo nos hace blanco fácil de personas malintencionadas, virus, e incluso en algunos casos nosotros mismos somos la amenaza. Es por esta razón que conocer dichos factores nos permitirá estar preparados, tener herramientas y saber usarlas para defender la integridad de nuestra información. No conocer al enemigo es darle ventajas en su intento por hacernos daño y no estar preparados para sus eventuales ataques es como dejar la puerta de nuestra casa abierta a mitad de la noche.

A. Enemigos

Hackers:
Un hacker es una persona con altos conocimientos en diferentes ramas de la computación, en especial lo relacionado con las tecnologías de información, redes y sistemas operativos, especialista en entrar en sistemas ajenos sin permiso.

Sin entrar en conflictos ideológicos con respecto a lo que significa ser hacker y la nueva llamada ética hacker, y si bien existen intrincados desarrollos sociales alrededor de la cultura hacker en donde se diferencian "hackers buenos" (white hats) y crackers (black hats) en sus valores morales, sociales y políticos, nuestro interés al interior de la

red es estar seguros de que nuestra información sea confiable, íntegra, que esté disponible y que ninguno de estos personajes acceda a nuestra red.

Script Kiddies:

Persona que posee bajos conocimientos sobre informática y que trata de violar sistemas ajenos, generalmente se relaciona con crackers inexpertos ya que para lograr romper la seguridad de los sistemas usa generalmente exploits y programas creados por terceros.

Este tipo de personas representan una gran amenaza, en especial para redes pequeñas y cibernautas desprevenidos que son sus principales blancos por tener herramientas de seguridad poco desarrolladas.

Personal descontento y/o desprevenido:

El propio personal al interior de las empresas puede representar una de las mayores amenazas para la seguridad de la información. Ya sea por error o por descontento en su trabajo, un empleado puede causar grandes perjuicios a un sistema informático. Desde perder un password o dárselo a la persona equivocada de manera desprevenida hasta atentar contra la infraestructura de la red misma. Es aquí donde se las políticas y la gestión para el manejo de la seguridad de nuestra red cobran importancia, ya que no solo debemos defendernos de los ataques de afuera, pues de nada sirve estar a salvo de los piratas informáticos al otro lado del mundo si nuestra clave de tarjeta de crédito está en manos de una secretaria inescrupulosa.

B. Amenazas

Los principales ataques y daños a nuestros sistemas de información pueden venir de algunas de las fuentes antes mencionadas, pero el conocer los enemigos es sólo el primer acercamiento a una red segura, ahora es importante conocer que pueden hacerle estos enemigos a nuestros sistemas. En general los ataques a nuestra red se pueden clasificar de tres grupos: ataques de reconocimiento, ataques de acceso y ataques de denegación de servicio (DoS).

*Ataques de reconocimiento***:** Son ataques que no representan un daño inmediato, son el paso inicial de otros ataques y lo que buscan es identificar equipos y nodos de red, servicios y puertos activos para encontrar vulnerabilidades que puedan ser explotadas para acceder a un sistema determinado. *Ataques de acceso:* Estos ataques buscan obtener acceso remoto a determinado nodo de red para obtener privilegios, ocultar huellas, atacar otros nodos u obtener información.

Ataques DoS (Denegación de servicio): Ataque a un sistema de ordenadores o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima. Se genera mediante la saturación de los puertos con flujo de información, haciendo que el servidor se sobrecargue y no pueda seguir prestando servicios, por eso se le dice "denegación", pues hace que el servidor no de abasto a la cantidad de usuarios. [1]

Remote to Local (R2L): Ataque en el cual usando exploits, se ejecutan *shellcodes* que permiten ejecución de código en una máquina remota[1]

II. EL PRESENTE DE LOS IDS[2]

Un sistema de detección de intrusos o IDS es un programa que detecta intrusiones a una red determinada, es el guardián de nuestra red, la alarma que nos indica los posibles ataques de los cuales estamos siendo víctimas. Sus aplicaciones como herramienta de seguridad son varias y el implementarlas y mantenerlas como bastión para la seguridad de nuestra información constituyen buenas prácticas en las redes telemáticas.

En la actualidad varios de los IDS existentes utilizan la Arquitectura CIDF[3] propuesta por el Intrusion Detection Working Group, ésta arquitectura define un IDS como un conjunto de

[1] Shellcode: Conjunto de órdenes programadas generalmente en lenguaje ensamblador que se inyectan en la pila para conseguir que la máquina en la que reside se ejecute la operación que se haya programado.
[2] Intrusion Detection System
[3] Common Intrusion Detection Framework

componentes (unidades lógicas) independientes e interconectados que se comunican entre ellos a través de mensajes o eventos, pueden ser un solo cluster o estar distribuidos. Entre las unidades lógicas encontramos las siguientes:

- Generador de eventos (E-box)
- Analizador de eventos (A-box)
- Base de dados de los Eventos (D-box)
- Unidades de respuesta (R-box)

Dichos componentes como su nombre lo indican deben asegurar la obtención correcta de los eventos que sucedan en el trafico de la red, analizarlos, guardarlos y determinar una respuesta si dichos eventos constituyen o no un ataque. [Ver Anexo 1]
Por lo general los bloques E, D y R funcionan de manera muy similar en todos los IDS pero el bloque A cuenta con múltiples variables dependiendo de sus características funcionales, estructurales, de comportamiento y origen de datos, algunos ejemplos de los enfoques de IDS son:

Por función:
- Detectores de Anomalías
- Detectores de usos incorrectos

Por Origen de datos:
- HIDS[4]
- NIDS[5]
- Hybrid – IDS

Por comportamiento:
- Activos - IPS[6]
- Pasivos (Carecen de R-box)

Dado la gran variedad de tipos de IDS y el tipo de sistema que se va a proponer en este articulo sólo explicaremos el funcionamiento de los IDS de *Detección de usos incorrectos,* el cual consiste en que el IDS ha sido programado para detectar patrones, para esto la mayoría de los IDS actuales utilizan sistemas basados en firmas, los cuales contienen elementos que ayudan a identificar ataques previamente conocidos, como paquetes malformados, escaneo de puertos y comportamientos sospechosos en general.

III. LOS IDS NO SON INFALIBLES

Es importante reconocer que la seguridad es un problema que no tiene una solución mágica, ninguna herramienta de seguridad (Antivirus, Firewall, IDS) representa un sistema infalible, ya que los problemas de intrusiones están relacionados con el comportamiento humano.

Miremos las desventajas de los IDS
- Análisis limitado de tráfico, pues solo se ocupan del segmento de red al que pertenecen
- El volumen de información que circula una red es muy grande para ser procesado por algunos IDS
- Son sistemas que consumen gran cantidad de recursos de máquina

Desventajas de los IDS basados en firmas
- No están preparados para los ataques de día cero (ataques no conocidos) y requieren tiempo para actualizar los parches, cargar y actualizar las firmas
- Son vulnerables a las modificaciones de los ataques ya conocidos (variaciones de comportamiento)
- Requieren ser supervisados constantemente por personal cualificado, además de un proceso arduo de "finetunning"
- Problemas de cantidad de falsos positivos y/o falsos negativos

IV. VENTAJAS DE LAS REDES NEURONALES ARTIFICIALES

Como se ha visto hasta ahora el problema de seguridad es un problema de computación relacionado con el comportamiento humano, no es entonces descabellado pensar en una solución que se base también en el comportamiento humano, los Sistemas Inteligentes.
Para este proyecto en particular se desarrollará un modelo basado en redes neuronales artificiales, las cuales tienen una concepción que basa su

[4] Host-Based IDS
[5] Network IDS
[6] Intrusion Prevention System

versatilidad y simplicidad en el sistema nervioso animal con cualidades como: aprendizaje, auto organización, tolerancia a fallos, flexibilidad, respuesta en tiempo real [2].

La elaboración de un modelo basado en redes neuronales artificiales para la detección de intrusos tendrá entonces ventajas como:

- La red aprenderá de manera autónoma a partir de los ejemplos, lo que disminuirá el tiempo y esfuerzo del proceso de "finetunning" que se necesita para su correcto funcionamiento
- La red neuronal artificial se puede adaptar a nuevos comportamientos, la cual hace al sistema mucho más flexible a variaciones y modificaciones de los métodos de intrusión actualmente conocidos (Base de conocimiento)
- Disminuir la cantidad de falsos positivos y falsos negativos que presentan los sistemas IDS basados en firmas
- La red infiere ataques que no aprendió, y puede adaptarse a los que el administrador de red cual lo convierte en un sistema, de cierta manera, heurístico

V. MODELO SIDIRI

El modelo SIDIRI es una propuesta de A-box para un IDS basado en redes neuronales artificiales, para protocolos TCP/IP.
El algoritmo tiene los valores de las características de los paquetes IP [Anexo 2] [Anexo 3]. El modelo utilizará como E-box el algoritmo público pcap (El pcap es un interfaz de una aplicación de programación para captura de paquetes. La implementación del pcap para sistemas basados en Unix se conoce como libpcap. El libpcap puede ser utilizado por un programa para capturar los paquetes que viajan por toda la red y, en las versiones más recientes, para transmitir los paquetes en la capa de enlace de una red, así como para conseguir una lista de los interfaces de red que se pueden utilizar con el libpcap.), una vez capturados los paquetes estos pasaran a un módulo que se encargara de organizarlos de acuerdo a la conversación a la que pertenecen y los almacenaran en una base de datos externa (D-box), paralelamente a este proceso un modulo leerá 20 paquetes de cada conversación donde enviará dicho bloques de paquetes a la red neuronal híbrida Perceptron - ART [Ver Anexo 4] que especificaremos a continuación:

A. Entradas

Las entradas de la red son 20 paquetes pertenecientes a la misma conversación, cada paquete se tratara como un vector de datos donde cada posición de dicho vector será un segmento del paquete como fue especificado anteriormente.

B. Estructura

La red cuenta con una capa oculta, la cual contiene 20 neuronas las cuales poseen como función de activación la función sigmoidal, dicha capa se encuentra conectada con las entradas por medio de enlaces sencillos y con la capa de salida con enlaces dobles (back-propagation) con lo cual se pretende obtener un porcentaje de certeza sobre la autenticidad del ataque en cuestión al comparar el ataque actual con los aprendidos previamente por la red.

C. Etapa de aprendizaje y funcionamiento

La red neuronal será del tipo de aprendizaje Off-Line, lo cual significa que la red tendrá separadas sus etapas de aprendizaje y de funcionamiento, es decir que la red no aprenderá (ni olvidará lo aprendido) durante el funcionamiento normal de la misma.
La red neuronal tendrá un aprendizaje de tipo supervisado, es decir que la red recibe al momento de su entrenamiento tanto las entradas como las salidas y de acuerdo a los errores que encuentre entre las salidas de la red y de las salidas esperadas por el entrenador, la red ajustará sus enlaces para cumplir con las salidas esperadas.
Como entrenamiento inicial de la red neuronal se utilizarán ataques comunes a todas las redes de telecomunicaciones, para ello se utilizará el conjunto de datos KDD 1999 el cual es una recopilación de la base de datos del Programa de

Evaluación de Detección de Intrusiones de DARPA, colectada y gestionada por el Laboratorio Lincoln del MIT [4]
La red neuronal en su fase inicial también recibirá algunas conversaciones comunes en las redes informática para que aprenda a diferenciar entre un patrón de red no peligroso y uno peligroso.

D. *Salidas*

La red neuronal cuenta únicamente con una neurona de salida la cual tiene como función de activación la función escalonada (limitador duro), es decir que únicamente da resultados booleanos (1 ó 0) con lo cual determinamos si existe un ataque o no y dado al resultado de similitud obtenido en la capa oculta determinas qué porcentaje de similitud tiene este con los ataques aprendidos previamente.

E. *Desventajas del modelo SIDIRI*

- Variabilidad del sistema
- Posee muchos parámetros configurables y esto crea muchos problemas a la hora de hacerle *finetunning*.
- La representación de los datos para que el sistema opere con ellos, y su adquisición por medio de los elementos de E-box
- Posible pérdida de información discriminante valiosa al hacer conversión de datos
- Poca o nula trazabilidad de los ataques.

VI. CONCLUSIONES

El desarrollo de IDS es un complejo campo que debe ser abordado con una perspectiva que ayude a enfrentar el problema gigante que representa la seguridad de la información, es por esta razón que se hace necesario abordar el problema de manera distinta a la que se usa actualmente, una opción para hacerlo son los sistemas inteligentes, en nuestro caso las redes neuronales artificiales.

Esta investigación y propuesta de modelo SIDIRI será desarrollada como trabajo de grado por los ponentes del presente artículo.

RECONOCIMIENTO

Agradecemos a nuestro profesor Manuel Humberto Santander Peláez por su orientación y formación, por enseñarnos la importancia de la seguridad de la información, el mundo de las redes y el valor del espíritu investigativo.
A nuestro profesor Alejandro Peña Palacio por su orientación y aporte en el desarrollo del modelo del sistema inteligente.
A nuestros compañeros Camilo Rodríguez y Daniel Londoño por sus aportes, correcciones y constante motivación.

REFERENCIAS

[1] Wikipedia: La Enciclopedia Libre. *Ataque de denegación de servicio* [en línea]. [ref. de 27 de Abril de 2007]. http://es.wikipedia.org/wiki/Ataque_de_denegaci%C3%B3n_de_servicio
[2] Wikipedia: La Enciclopedia Libre. *Red neuronal artificial* [en línea]. [ref. de 21 de Abril de 2007]. http://es.wikipedia.org/wiki/Red_neuronal_artificial
[3] BARRERA GARCÍA-OREA, Alejandro. Universidad Politécnica de Madrid. *Presente y Futuro de los IDS* [en línea]. 2005. [ref. de 16 de Febrero de 2007] http://www.neurosecurity.com/whitepapers/futureIDS.pdf
[4] BALUJA GARCÍA, Walter; ESCANDÓN BON, Rebeca. Instituto Superior Politécnico José Antoni Echevarría. *Empleo de las redes neuronales en la detección de intruso*. VIII Seminario Iberoamericano de Seguridad en las TICs 2007. http://www.segurmatica.co.cu/descargas/info2007/redesneuronales_ids.ppt
[5] PINACHO, Pedro Pablo; VALENZUELA Tito. Universidad de Santiago (Chile). *Una Propuesta de IDS Basado en Redes Neuronales Recurrentes* [en línea]. México DF, Octubre de 2003. [ref. de 13 de Marzo de 2007] http://www.criptored.upm.es/guiateoria/gt_m291b.htm

Autores

Juan David Arroyave Molina
Estudiante

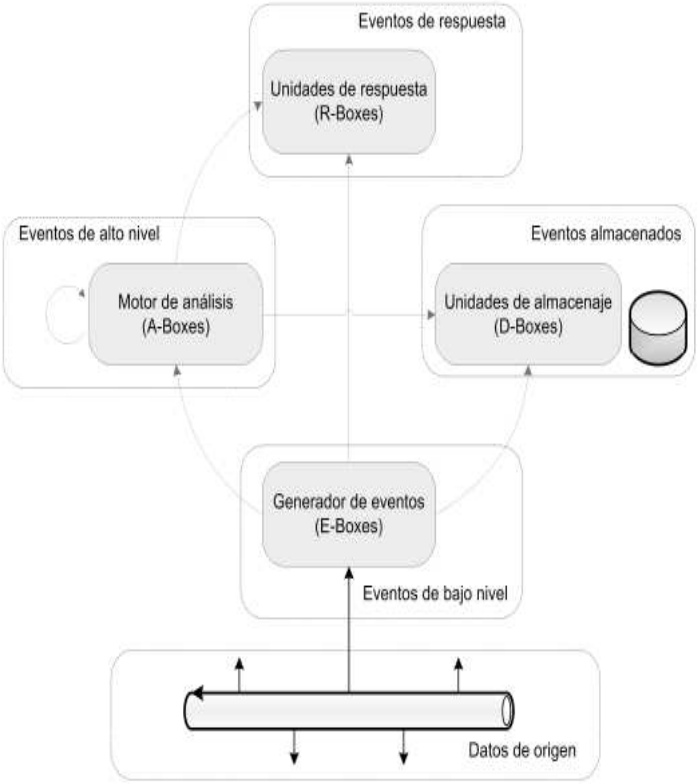
Jonathan Steven Herrera Román
Estudiante

Esteban Vásquez González
Estudiante

IX Semestre
Ingeniería Informática
Escuela de Ingeniería de Antioquia

ANEXOS

Anexo 1
Arquitectura CIDF [3]



El Common Intrusion Detection Framework (CIDF) es un esfuerzo por desarrollar protocolos y aplicaciones de interfaz para que los proyectos de investigación y detección puedan compartir información y recursos y así los componentes de detección de intrusiones puedan reutilizarse en otros sistemas.
Bajo este *framework* de IDS se desarrollará la propuesta de modelo para el SIDIRI , ya que se desea un A-box basado en redes neuronales artificiales.

Anexo 2
Cabeceras de protocolos TCP/IP que servirán de entradas a la red neuronal [5]

Característica	*Descripción*
Puerto Origen	Puerto desde donde se origina el paquete
Puerto Destino[1]	Puerto destino del paquete
Protocolo	TCP, UDP o ICMP
TTL	Tiempo de vida del paquete
TOS	Tipo de Servicio
IPlen	Largo de paquete IP
DgmLen	Longitud de cabecera UDP
RB	Bit reservado
MF	Más fragmentos
DF	No fragmentar
Opciones IP	Número de opciones del paquete IP
F1	Bit reservado
F2	Bit reservado
U	Flag Urg
A	Flag Ack
P	Flag Push
R	Flag Reset
S	Flag Syn
F	Flag Fin
Win	tamaño de la ventana deslizante
TCP Len	Largo de cabecera TCP
Opciones TCP	Número de opciones TCP
UDP Len	Largo de opciones UDP
Type	Tipo de mensaje ICMP
Code	Código de tipo de mensaje ICMP

Para el formato de las cabeceras IP según la RFC 791 para IPv4 se usará para el reconocimiento y como entradas de la red neuronal los anteriores atributos de la misma.

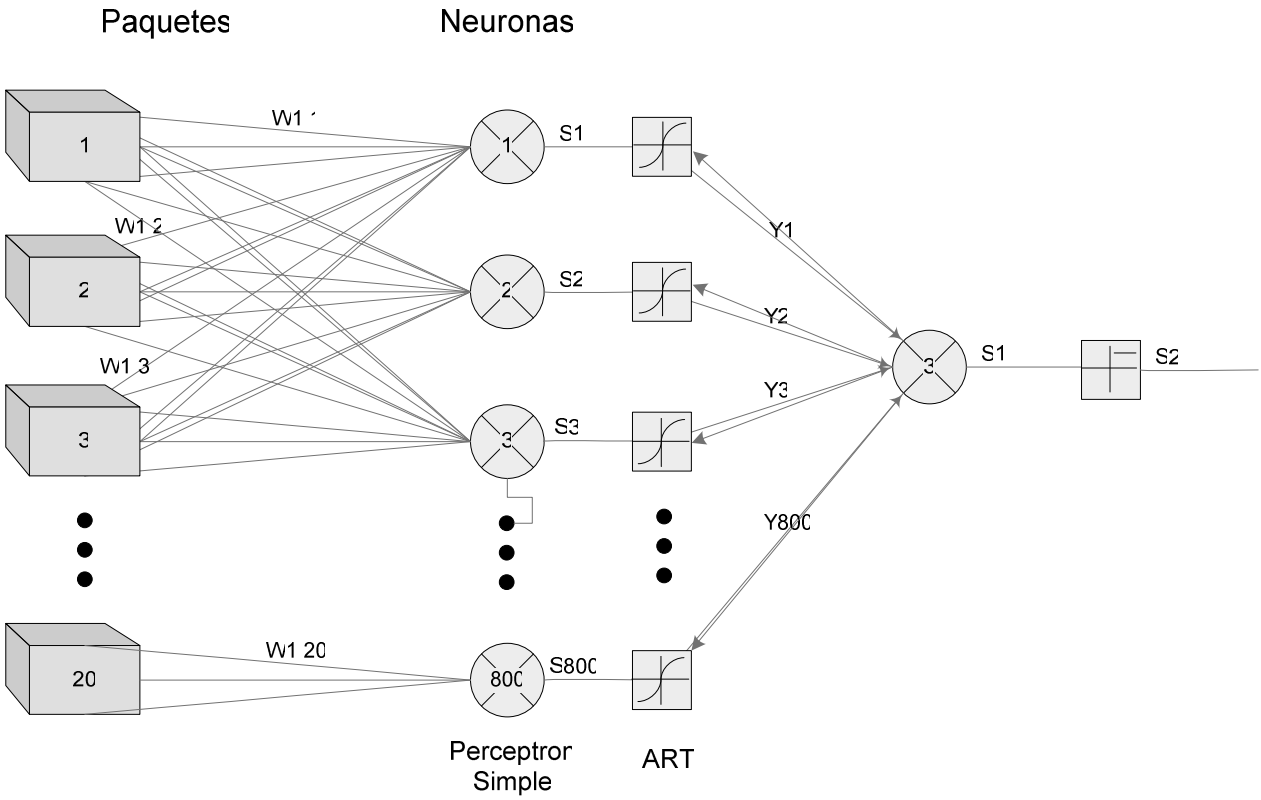
Anexo 3
Puertos más susceptibles de ataques según SANS [5]

Puerto	*Descripción*
telnet	puerto para shell remota no encriptada
ssh	puerto para shell remota segura
FTP	puerto de protocolo de intercambio inseguro de archivos
netbios	protocolo de comunicaciones Microsoft
rlogin	login remoto
RPC	Puerto de portmapper RPC
NFS	puerto de servicio de sistema de archivos en red
lockd	puerto bloqueo
netbiosWinNT	protocolo de comunicaciones Microsoft
Xwin	protocolo de servidor X Windows
DNS	puerto de servicio de nombres de dominio
ldap	puerto de servicio de autenticación ldap
SMTP	puerto de intercambio de correo
POP	puerto de intercambio de correo
IMAP	puerto de intercambio de correo
HTTP	puerto de servicio WEB
SSL	puerto de conexión segura
proxy HTTP	servicio proxy para WEB
serv	
Servicios pequeños bajo el puerto 20 time	Servidor de tiempo
TFTP	puerto de servicio Trivial FTP
finger	puerto se servicio de información de usuarios y conexiones
NNTP	puerto de servidor de noticias
NTP	servicio de tiempo de red
lpd	servicio de impresión
syslog	servicio de eventos del sistema
SNMP	servicio de administración de red
bgp	Protocolo de ruteo externo en Internet
socks	Puerto proxy

Los puertos que se muestran en la anterior tabla son los puertos que según SANS[7] se encuentran más susceptibles a ser atacados por los enemigos de la seguridad.

[7] SANS Institute (SysAdmin, Audit, Networking, and Security) marca registrada del Escal Institute of Advanced Technologies. SANS provee entrenamiento para seguridad computacional, certificación profesional, e investigación. Fue fundado en 1989.

Anexo 4
Modelo SIDIRI usando redes neuronales artificiales híbrida (Perceptron Simple + ART)



El modelo muestra la propuesta para la implementación de una red híbrida Perceptrón-ART para su funcionamiento como A-box del sistema