SECRETARÍA
NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CERT-PY

GOBIERNO NACIONAL
Construyendo Juntos Un Nuevo Rumbo
agendaDigital

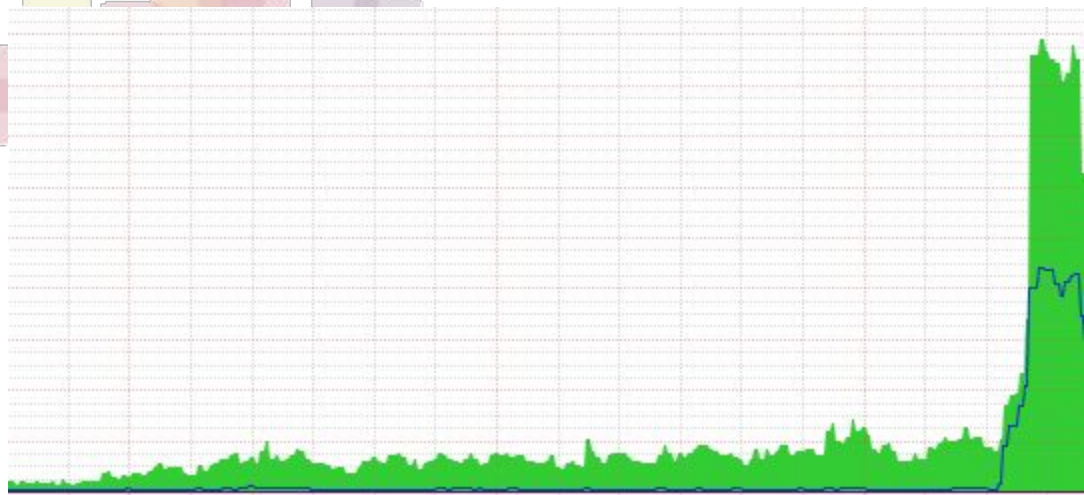
# BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD

## TALLER PARA GERENTES DE TI

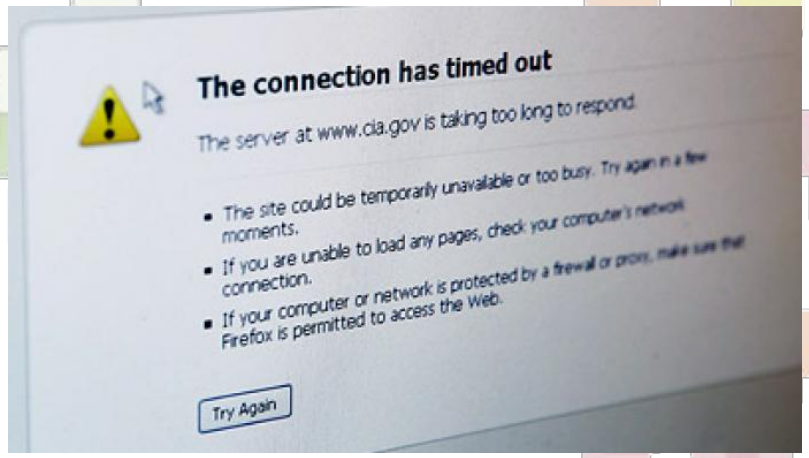
# Qué es un ataque DDoS y cómo funciona?

Un ataque de denegación causa la interrupción de uno o varios servicios mediante el consumo excesivo de alguno de estos recursos en el servidor o elementos de red intermedios:

- Ancho de banda
- Ciclos de CPU
- Memoria
- Espacio en disco



# Qué es un ataque DDoS y cómo funciona? (2)




# Qué es un ataque DDoS y cómo funciona? (3)

En el mundo actual existe algo llamado "guerra informática", "guerra digital" o "ciberguerra"

***Un ataque DDoS puede ser dirigido a cualquier tipo de host conectado a Internet.***

# Seguridad Perimetral (Firewall)

***La paz y prosperidad del imperio romano dependió durante siglos de la defensa de sus fronteras, que se protegían gracias a fortificaciones, murallas y torres vigía.***

# Seguridad Perimetral (Firewall)

Un sistema firewall contiene un conjunto de reglas predefinidas que permiten:

* **Autorizar una conexión (allow);**
* **Bloquear una conexión (deny);**
* **Redireccionar un pedido de conexión sin avisar al emisor (drop).**

# Seguridad Perimetral (Firewall)

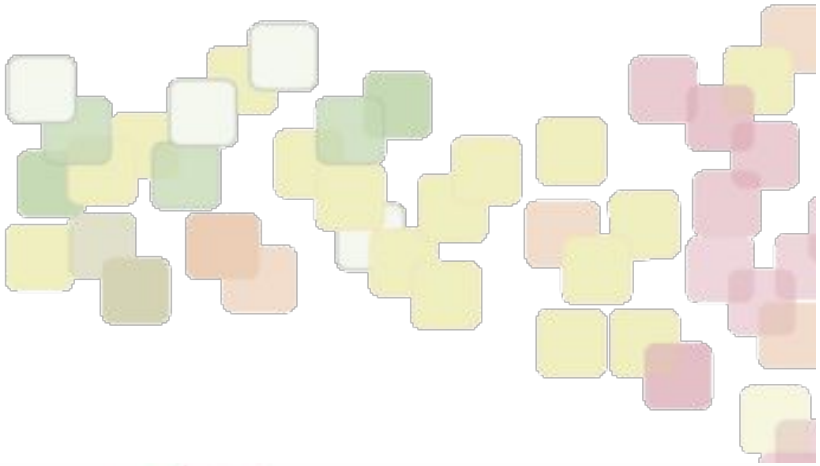
***Seguridad Perimetral Firewall***

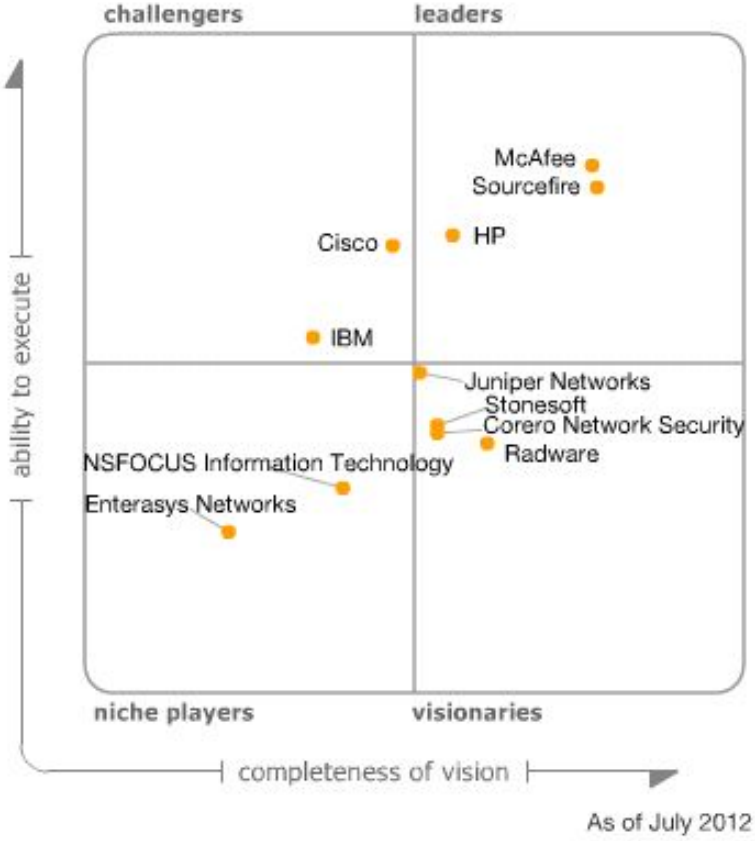
- Control de tráfico de red desde y hacia Internet (Firewall*), seguridad perimetral.
- Protección contra ataques externos.
- Control de usuarios.
- Generación y administración de VPN**.
- Conexión para equipos remotos (portátiles).
- Gestión de ancho de banda de internet.

# Sistemas de detección y prevención de intrusión (IDS/IPS)

**¿Qué es un sistema de detección/prevención de intrusiones (IDS/IPS)?**

# Sistemas de detección y prevención de intrusión (IDS/IPS)



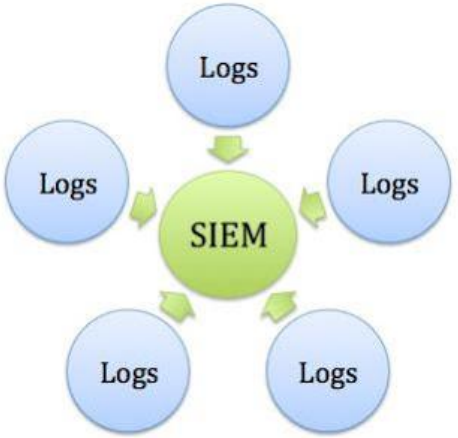




# Análisis y centralización de logs

**¿Que es un SIEM?**

La tecnología SIEM proporciona un análisis en tiempo real de las alertas de seguridad generadas por el hardware y software de red.

Hoy en día los ataques a organizaciones son cada vez más sofisticados e inmunes a la detección por parte de dispositivos IDS/IPS



# Análisis y centralización de logs

SECRETARÍA
NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CERT-PY

GOBIERNO NACIONAL
Construyendo Juntos Un Nuevo Rumbo
agendaDigital

# Implementación de Firewall de aplicación:mod_security, mod_evasive y mod_qos

SECRETARÍA
NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CERT-PY

GOBIERNO NACIONAL
Construyendo Juntos Un Nuevo Rumbo
agendaDigital

# Politicas de Seguridad

con el objeto de gestionar adecuadamente la seguridad de la información, los sistemas informáticos y el ambiente tecnológico del Organismo.

# Algunos ejemplos de politicas:

- Política de Uso de Correo Electrónico.
- Política de Uso de Contraseñas.
- Política de Control de Acceso.
- Política de Identificación y Autenticación de Usuarios.
- Política de Administración de Privilegios de Usuarios.
- Política de Seguridad en los Servicios de Red.
- Política de Protección de Puertos.
- Política de Actualización de Sistemas.
- Política de Protección Contra Software Malicioso.
- Política de Monitoreo de Uso de Sistemas.
- Política de Manejo de Incidentes.
- Política de Copias de Seguridad.
- Otros.

**POLÍTICA DE USO DE CONTRASEÑAS.-**

Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas. Las mismas constituyen un medio de validación y autenticación de la identidad de un usuario, y consecuentemente un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información.

Los usuarios deben cumplir las siguientes directivas:

1. La contraseña es personal y deber mantenerse en secreto. No se debe escribir ni reflejar la contraseña en un papel o en documentos donde puedan quedar expuestas. No deben ser incluidas en mensajes de correo electrónico, ni ningún otro medio de comunicación electrónica. Tampoco deben ser comunicadas las contraseñas en conversaciones telefónicas.
2. Cambiar la contraseña con regularidad y siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.
3. Establecer un recordatorio automático para cambiar las contraseñas de sus sitios web de correo electrónico, banca y tarjetas de crédito cada tres meses aproximadamente.
4. La contraseña debe ser lo suficientemente fuerte para no ser descifrada.
5. Una contraseña robusta debe:
6. Debe tener un mínimo 10 caracteres.
7. No debe ser ni derivarse de palabras comunes, de diccionario, nombre de usuario, de información personal o de algún pariente cercano. Ejemplos: password, admin, qwerty, abc123, etc.
8. Debe ser una combinación de números, letras mayúsculas y minúsculas, caracteres especiales (por ejemplo, ¡, @, *, =, -, etc.), etc.

**POLITICA DE USO DE CONTRASEÑAS.-**

1. Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar o reciclar viejas contraseñas.
2. No utilice la característica de “Recordar Contraseña” existente en algunas aplicaciones.
3. Cambiar las contraseñas provisorias en el primer inicio de sesión (“log on”).
4. Evitar incluir contraseñas en los procesos automatizados de inicio de sesión, por ejemplo, aquellas almacenadas en una tecla de función o macro.
5. Nunca introducir una contraseña en un sitio o programa del cual no tengamos la certeza absoluta de que es legítimo.
6. No utilizar herramientas online para crear contraseñas ni para encriptarlas.
7. Notificar, cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o indicio de pérdida de confidencialidad.

En caso posible se recomienda la utilización de Autenticación de Doble Factor. Un sistema de doble autenticación es aquel que utiliza dos de los tres factores de autenticación que existen para validar al usuario.

Debido a que han aumentado considerablemente las técnicas para romper o comprometer contraseñas, de diversas formas, las cuales son cada día más sofisticadas, las buenas prácticas muchas veces no son suficientes y nos encontramos con la realidad de que, aún habiendo tomado todas las precauciones, nuestra contraseña se vio expuesta debido a factores que escapan de nuestro control. Es por eso que surgió el concepto de autenticación de doble factor.

SECRETARÍA
NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CERT-PY

GOBIERNO NACIONAL
Construyendo Juntos Un Nuevo Rumbo
agendaDigital

# Muchas gracias!

CENTRO DE RESPUESTAS ANTE INCIDENTES CIBERNÉTICOS

CERT-PY

@CERTpy

/CERT-Py

**www.cert.gov.py**

***denuncias***: abuse@cert.gov.py
***contactos***: cert@cert.gov.py