Seguridad en Informática

Aspectos Duros y Blandos

Dr. José Fernández G.

aprocal
Asociación de Profesionales en Compras, Abastecimiento y Logística

Octubre 2013

Agenda

- Definición de Seguridad Informática.
- Objetivos del Área de Seguridad Informática.
- Amenazas y sus distintos tipos.
- Motivadores y Actores
- Mitos y Creencias Urbanas
- Análisis de Riesgos
- Control Sinergístico
- Matriz de Riesgo
- Impacto al Negocio
- Técnicas y herramientas
- Conclusiones y Preguntas

aprocal
Asociación de Profesionales en Compras, Abastecimiento y Logística

Definición de Seguridad Informática

La **seguridad informática** o **seguridad de tecnologías de la información** es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software (bases de datos, metadatos, archivos), hardware y todo lo que la organización valore (activo) y signifique un riesgo si esta información confidencial llega a manos de otras personas, convirtiéndose, por ejemplo, en información privilegiada.

aprocal
Asociación de Profesionales en Compras, Abastecimiento y Logística

Definición de Seguridad Informática

Consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida así como su modificación solo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

aprocal
Asociación de Profesionales en Compras, Abastecimiento y Logística

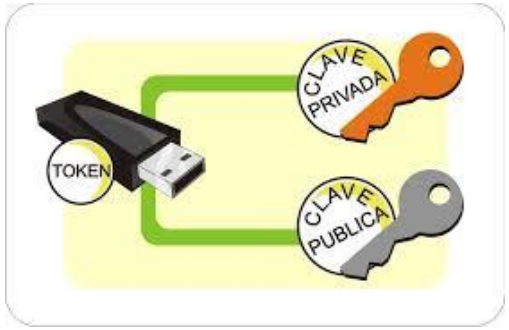
Seguridad Informática en los Datos

1. **Integridad:** La información solo puede ser modificada por quien esta autorizado y de manera controlada.

2. **Confidencialidad:** La información sólo debe ser legible para los usuarios autorizados.

3. **Disponibilidad:** Debe estar disponible siempre que se necesite.

4. **Irrefutabilidad:** El uso y/o modificación de la información por parte de un usuario debe ser irrefutable, es decir, que el usuario no puede negar dicha acción.



aprocal
Asociación de Profesionales en Compras, Abastecimiento y Logística

Objetivos del Área de Seguridad Informática

La seguridad informática debe establecer normas que minimicen los riesgos a la información o infraestructura informática. Estas normas incluyen horarios de funcionamiento, restricciones a ciertos lugares, autorizaciones, denegaciones, perfiles de usuario, planes de emergencia, protocolos y todo lo necesario que permita un buen nivel de seguridad informática minimizando el impacto en el desempeño de los trabajadores y de la organización en general y como principal contribuyente al uso de programas realizados por programadores.

Concebida para proteger los activos informáticos, entre los que se encuentran los siguientes:

- La infraestructura computacional
- Los usuarios
- La información

aprocal
Asociación de Profesionales en Compras, Abastecimiento y Logística

Amenazas

Una Amenaza es la posibilidad de ocurrencia de cualquier tipo de evento acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema, en el caso de la Seguridad Informática, los Elementos de Información.

- Las amenazas pueden ser causadas por:
- Usuarios
- Programas maliciosos
- Errores de programación
- Intrusos
- Un siniestro
- Personal técnico interno
- Fallos electrónicos o lógicos de los sistemas informáticos en general.
- Catástrofes naturales

aprocal
Asociación de Profesionales en Compras, Abastecimiento y Logística

Tipos de Amenazas

- Amenazas por el origen
  1. Amenazas Internas
  2. Amenazas Externas
- Amenazas por el Efecto
- Amenazas por el medio Utilizado

Tipos de Amenazas

Amenazas por el origen

El hecho de conectar una red a un entorno externo nos da la posibilidad de que algún atacante pueda entrar en ella, con esto, se puede hacer robo de información o alterar el funcionamiento de la red. Sin embargo el hecho de que la red no esté conectada a un entorno externo, como Internet, no nos garantiza la seguridad de la misma. De acuerdo con el Computer Security Institute(CSI) de San Francisco aproximadamente entre el 60 y 80 por ciento de los incidentes de red son causados desde dentro de la misma. Basado en el origen del ataque podemos decir que existen dos tipos de amenazas:

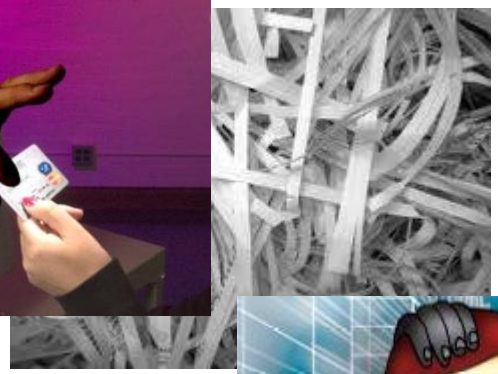
- Amenazas internas
- Amenazas externas

aprocal
Asociación de Profesionales en Compras, Abastecimiento y Logística

Tipos de Amenazas

Amenazas por el efecto

El tipo de amenazas por el efecto que causan a quien recibe los ataques podría clasificarse en:



- Robo de información.
- Destrucción de información.
- Anulación del funcionamiento de los

sistemas o efectos que tiendan a ello.

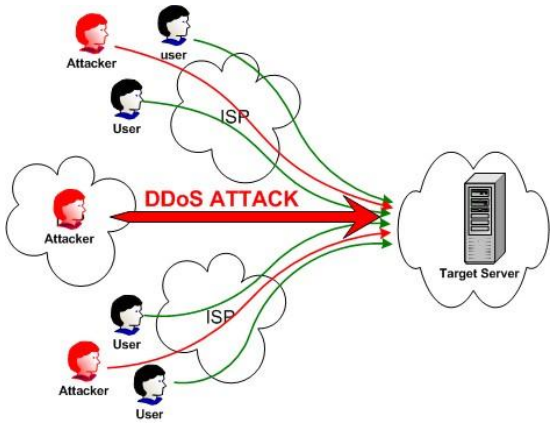
- Suplantación de la identidad, publicidad de
- datos personales o confidenciales,
- cambio de información, venta de datos personales, etc.

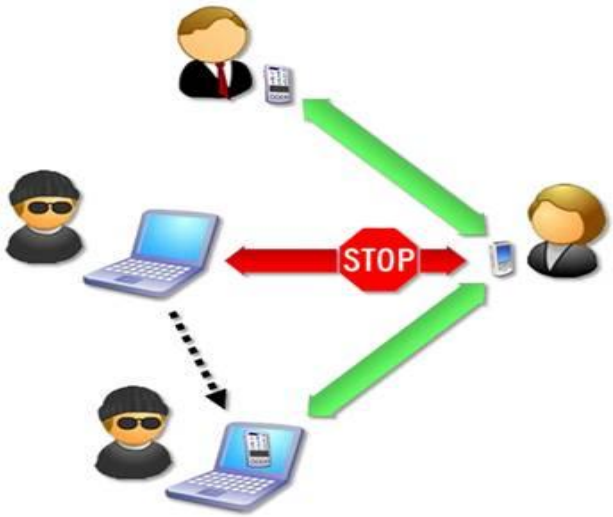
aprocal
Asociación de Profesionales en Compras, Abastecimiento y Logística

Tipos de Amenazas

Amenazas por el medio utilizado

- Virus Informático
- Ingeniería Social
- Denegación del Servicio
- Spoofing
- Etc.





aprocal
Asociación de Profesionales en Compras, Abastecimiento y Logística

Motivadores y Actores del Entorno

Atacan principalmente gobierno o iniciativa privada, con fin de evidenciar o hacer cortes en el servicio que ofrecen.

Atacan a cualquiera, su motivación es financiera así que pueden buscar cualquier información de la cual obtener ganancia.

Atacan con fines específicos, buscando en si propiedad intelectual, o información confidencial.

aprocal
Asociación de Profesionales en Compras, Abastecimiento y Logística

Mitos y Creencias Urbanas

- «Mi sistema no es importante para un hacker»

- Esta afirmación se basa en la idea de que no introducir contraseñas seguras en una empresa no entraña riesgos pues «¿quién va a querer obtener información mía?». Sin embargo, dado que los métodos de contagio se realizan por medio de programas *automáticos*, desde unas máquinas a otras, estos no distinguen buenos de malos, interesantes de no interesantes, etc. Por tanto abrir sistemas y dejarlos sin claves es facilitar la vida a los virus y de posibles atacantes. Otra consideración respecto a esta afirmación que la llevan a ser falsa es que muchos ataques no tiene otro fin que el destruir por destruir sin evaluar la importancia.

Mitos y Creencias Urbanas

- «Estoy protegido pues no abro archivos que no conozco»

- Esto es falso, pues existen múltiples formas de contagio, además los programas realizan acciones sin la supervisión del usuario poniendo en riesgo los sistemas, si bien la medida es en sí acertada y recomendable.

Mitos y Creencias Urbanas

- «Como tengo antivirus estoy protegido»

- En general los programas antivirus no son capaces de detectar todas las posibles formas de contagio existentes, ni las nuevas que pudieran aparecer conforme los ordenadores aumenten las capacidades de comunicación, además los antivirus son vulnerables a desbordamientos de Buffer (Buffer Overflow) que hacen que la seguridad del sistema operativo se vea más afectada aún, aunque se considera como una de las medidas preventivas indispensable.

Mitos y Creencias Urbanas

- «Como dispongo de un firewall no me contagio»

- Esto únicamente proporciona una limitada capacidad de respuesta. Las formas de infectarse en una red son múltiples. Unas provienen directamente de accesos al sistema (de lo que protege un*firewall*) y otras de conexiones que se realizan (de las que no me protege). Emplear usuarios con altos privilegios para realizar conexiones puede entrañar riesgos, además los *firewalls* de aplicación (los más usados) no brindan protección suficiente contra el spoofing. En todo caso, el uso de cortafuegos del equipo y de la red se consideran altamente recomendables.

Mitos y Creencias Urbanas

- «Tengo un servidor web cuyo sistema operativo es un Unix actualizado a la fecha y por tanto seguro»

- Puede que esté protegido contra ataques directamente hacia el núcleo, pero si alguna de las aplicaciones web (PHP, Perl, Cpanel, etc.) está desactualizada, un ataque sobre algún script de dicha aplicación puede permitir que el atacante abra una shell y por ende ejecutar comandos en el unix. También hay que recordar que un sistema actualizado no está libre de vulnerabilidades sino que se no tiene ninguna de las descubiertas hasta el momento.

Realidad al realizar análisis de riesgos

- 47,000+ Incidentes de Seguridad Analizados
- 621 Brechas de seguridad confirmadas y estudiadas.
- 19 Contribuyentes Internacionales.
- 6TO Año Consecutivo.

Solamente existen un reporte de este tipo…(DBIR)

aprocal
Asociación de Profesionales en Compras, Abastecimiento y Logística

Análisis de Riesgos

De los incidentes de seguridad fueron realizados desde un agente o instancia externa.

Fueron utilizadas tácticas sociales, tanto correo electrónico, redes sociales o inclusive llamadas telefónicas.

De las intrusiones a la red se deben a credenciales débiles o robadas.

aprocal
Asociación de Profesionales en Compras, Abastecimiento y Logística

Análisis de Riesgos

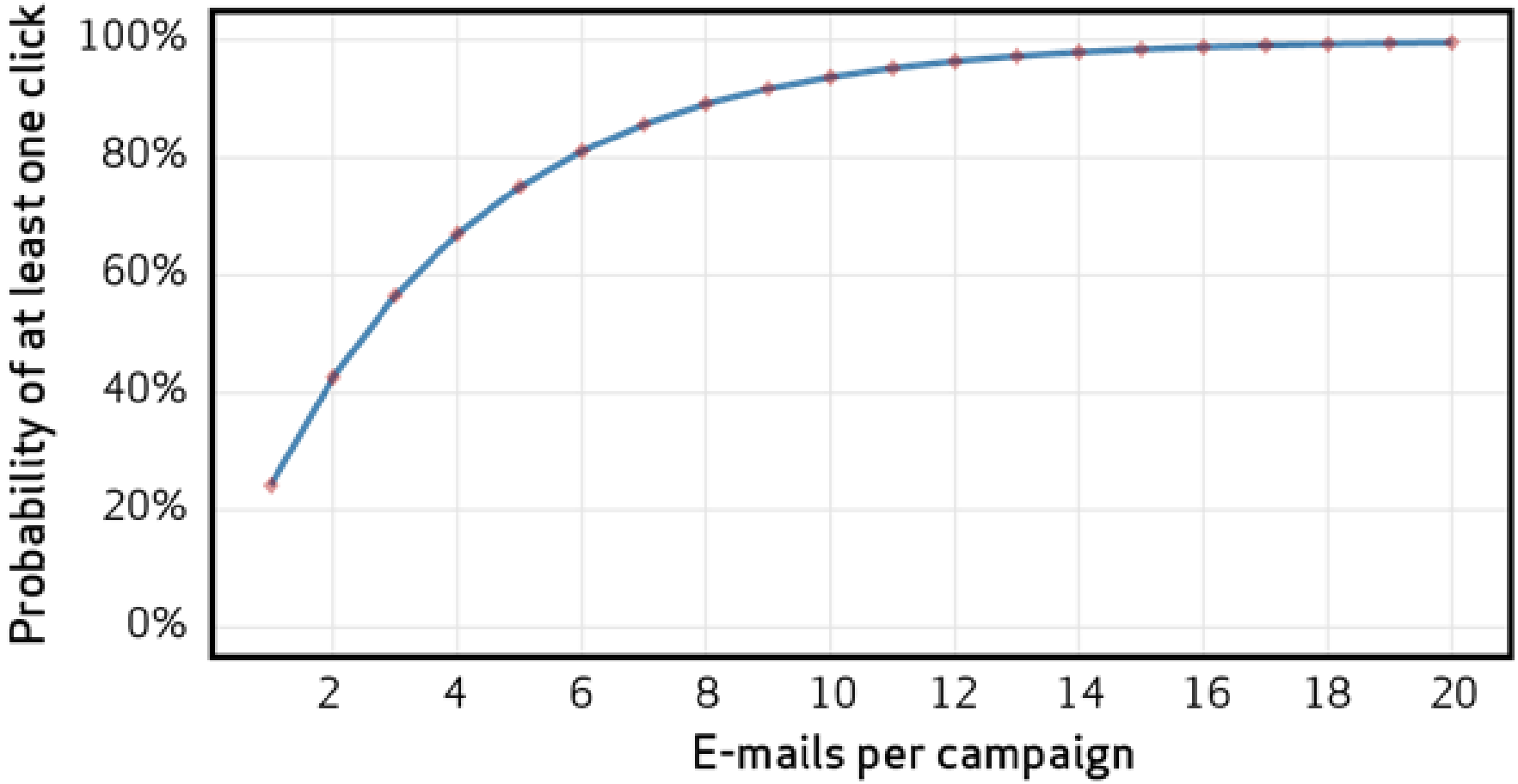
De los ataques fueron oportunistas, no orientados a un individuo o empresa especifica.

Se realizaron por vía de espionaje, en muchos de los casos de competencias directas.

Realizados por colaboradores anteriores, utilizando perfiles no desactivados o inclusive puertas traseras.

aprocal
Asociación de Profesionales en Compras, Abastecimiento y Logística

Análisis de Riesgos



aprocal
Asociación de Profesionales en Compras, Abastecimiento y Logística

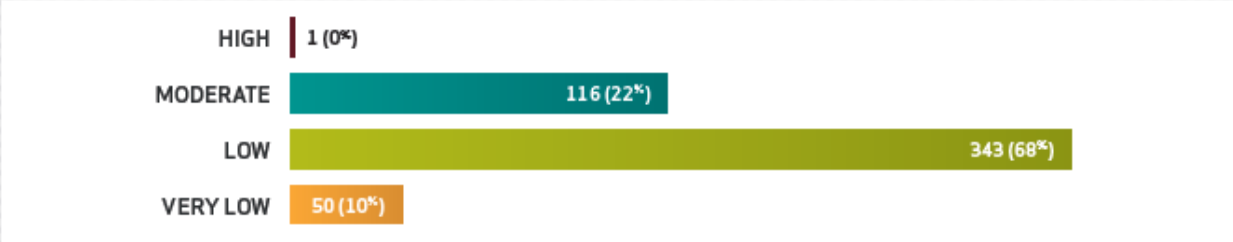
Análisis de Riesgos

THE DIFFICULTY RATING OF ATTACKS

- **Very low:** the average person could have done it.
- **Low:** basic methods, little or no customization or resources required.
- **Moderate:** some skilled techniques and customization required.
- **High:** advanced skills, significant customizations, and/or extensive resources required.

Mientras que los autores van subiendo la apuesta, probando nuevas técnicas y teniendo un aprovechamiento de recursos mucho mayor - menos del 1% de las infracciones analizadas en el estudio de este año, utilizaron tácticas clasificadas como "alto" en la escala de dificultad para VERIS. De hecho, el 78% de las técnicas que vimos estaban en categorías "baja" o "muy baja". Las barreras de entrada para convertirse en un hacker son bastante bajas.

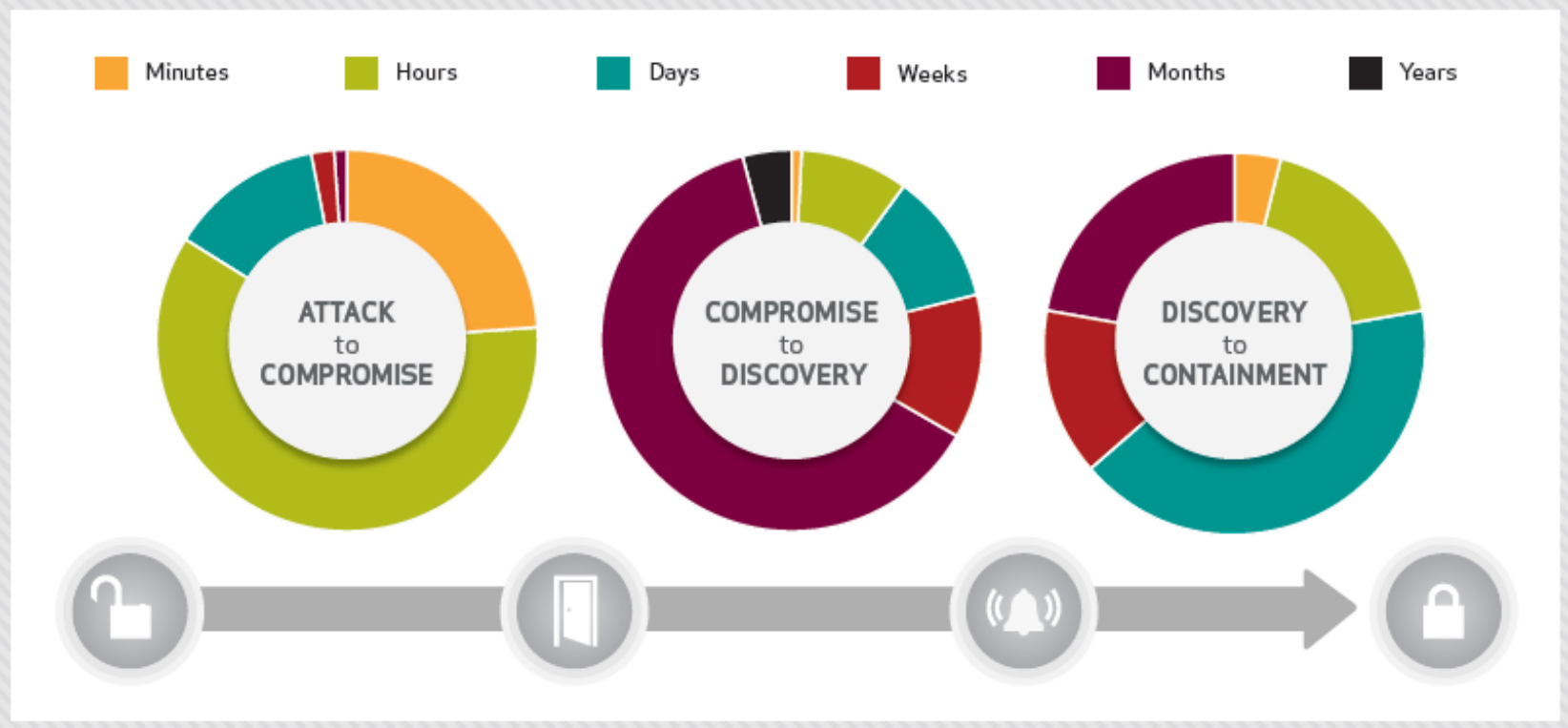
Figure 3: Difficulty of tactics used in initial compromise



The simplicity of attacks doesn't take anything away from their effectiveness or impact. Even well-known techniques can be used to devastating effect.

aprocal
Asociación de Profesionales en Compras, Abastecimiento y Logística

Análisis de Riesgos



En el 84% de los casos, el compromiso inicial tomo unas cuantas horas, o incluso menos.
En el 66% de los casos, la brecha no fue descubierta en varios meses o incluso años.
En el 22% de los casos, tomo varios meses contener una brecha.

aprocal
Asociación de Profesionales en Compras, Abastecimiento y Logística

Análisis de Riesgos

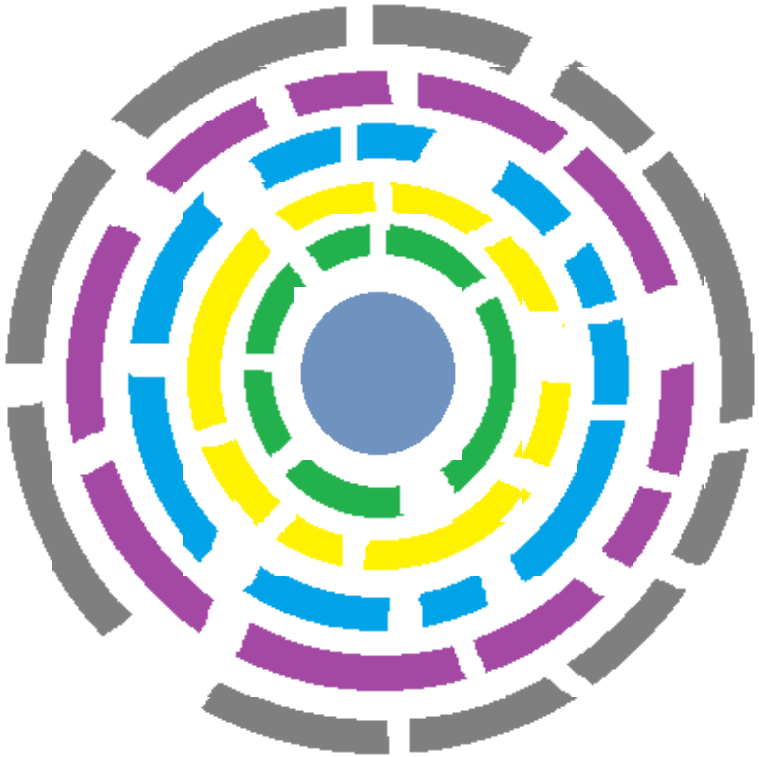
- El análisis de riesgos informáticos es un proceso que comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo.
- Teniendo en cuenta que la explotación de un riesgo causaría daños o pérdidas financieras o administrativas a una empresa u organización, se tiene la necesidad de poder estimar la magnitud del impacto del riesgo a que se encuentra expuesta mediante la aplicación de controles.
- Dichos controles, para que sean efectivos, deben ser implementados en conjunto formando una arquitectura de seguridad con la finalidad de preservar las propiedades de confidencialidad, integridad y disponibilidad de los recursos objetos de riesgo.

aprocal
Asociación de Profesionales en Compras, Abastecimiento y Logística

Análisis de Riesgos

aprocal
Asociación de Profesionales en Compras, Abastecimiento y Logística

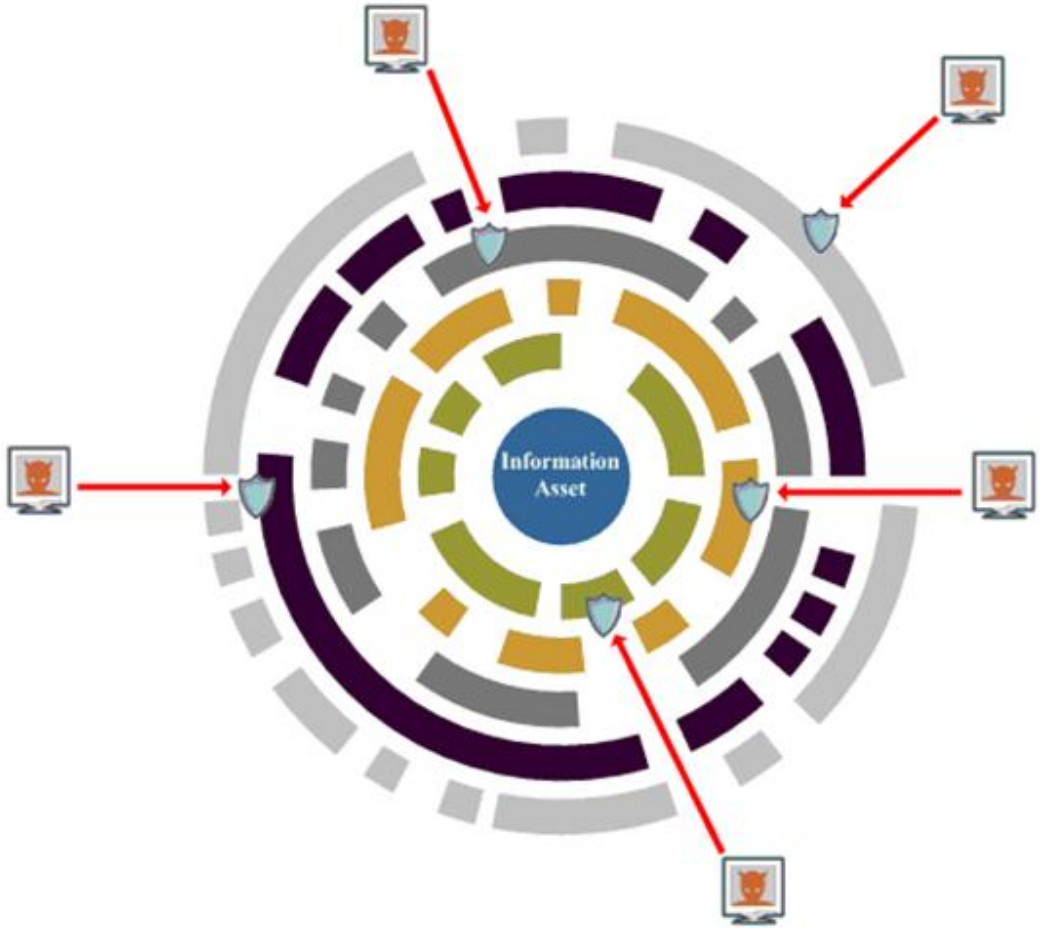
Controles Sinergísticos



- Controles Físicos y Ambientales
- Controles de Red Lógicos
- Controles de Plataforma y Sistemas
- Controles de Aplicaciones y Servicios
- Controles Administrativos

aprocal
Asociación de Profesionales en Compras, Abastecimiento y Logística

Controles Sinergísticos

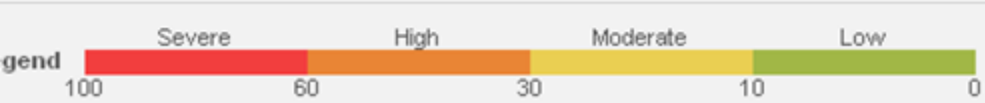


Eficiencia Total = 1-(1-80%)*(1-80%)*(1-80%)*(1-80%)*(1-80%)= 99.97%

aprocal
Asociación de Profesionales en Compras, Abastecimiento y Logística

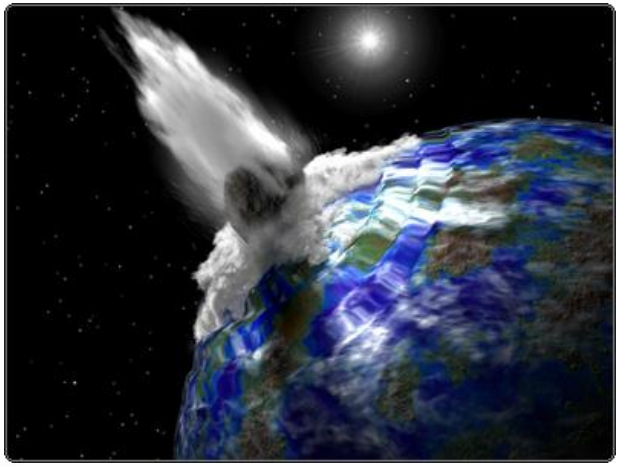
Matriz de Riesgos

Threat Scenarios		MALWARE			HACKING			SOCIAL			MISUSE			PHYSICAL			ERROR			ENVIRONMENTAL		
		External	Internal	Partner	External	Internal	Partner	External	Internal	Partner	External	Internal	Partner	External	Internal	Partner	External	Internal	Partner	External	Internal	Partner
SERVERS	Confidentiality	25	27	36	33	36	27	20	24	29	17	27	23	26	31	28	18	29	24	1	1	1
	Integrity	24	27	36	35	39	27	22	28	29	16	25	23	26	31	28	21	30	24	16	16	1
	Availability	26	29	36	38	43	26	24	28	29	22	32	23	29	35	27	22	40	21	30	38	1
NETWORK	Confidentiality	25	27	36	29	34	27	20	24	29	1	27	23	27	32	28	13	29	24	1	1	1
	Integrity	24	27	36	29	34	27	18	24	29	1	26	23	26	33	28	12	26	24	31	29	1
	Availability	26	29	36	34	40	26	22	26	29	1	30	23	30	36	27	14	41	28	37	44	33
END-USER	Confidentiality	31	29	56	29	29	36	32	34	37	1	29	36	34	36	35	1	29	37	1	1	1
	Integrity	31	28	56	29	29	36	28	32	37	1	25	36	32	35	35	1	28	37	8	9	1
	Availability	34	31	56	38	38	35	34	36	37	1	33	36	38	40	34	20	41	36	36	33	1
OFFLINE	Confidentiality	52	65	33	56	66	23	40	48	41	34	43	26	40	48	28	28	37	30	1	1	1
	Integrity	52	65	33	64	76	23	42	52	41	1	43	26	40	51	28	1	48	30	1	1	1
	Availability	52	65	33	72	86	22	43	51	40	1	45	25	41	50	27	37	48	29	30	29	1



Impacto al Negocio

- El reto es asignar estratégicamente los recursos para cada equipo de seguridad y bienes que intervengan, basándose en el impacto potencial para el negocio, respecto a los diversos incidentes que se deben resolver.
- Para determinar el establecimiento de prioridades, el sistema de gestión de incidentes necesita saber el valor de los sistemas de información que pueden ser potencialmente afectados por incidentes de seguridad. Esto puede implicar que alguien dentro de la organización asigne un valor monetario a cada equipo y un archivo en la red o asignar un valor relativo a cada sistema y la información sobre ella. Dentro de los valores para el sistema se pueden distinguir: confidencialidad de la información, la integridad (aplicaciones e información) y finalmente la disponibilidad del sistema.



aprocal
Asociación de Profesionales en Compras, Abastecimiento y Logística

Controles Críticos de Seguridad*

- Inventario de dispositivos autorizados y no autorizados.
- Inventario de Software autorizado y no autorizado.
- Configuraciones seguras para hardware y software en los dispositivos móviles, ordenadores portátiles , estaciones de trabajo y servidores.
- Evaluación de la vulnerabilidad continua y Remediación.
- Defensas de malware.
- Software de Seguridad para Aplicaciones.
- Control de dispositivos Inalámbricos.
- Capacidad de recuperación de datos.
- Evaluación de habilidades de seguridad y formación adecuadas.
- Configuraciones seguras para los dispositivos de red , tales como firewalls , routers y switches.

*fuentes: www.sans.org, http://www.verizonenterprise.com/DBIR/2013/

aprocal
Asociación de Profesionales en Compras, Abastecimiento y Logística

Controles Críticos de Seguridad*

- Limitación y Control de los puertos de red , protocolos y servicios.
- Uso Controlado de privilegios administrativos.
- Defensa de fronteras.
- Mantenimiento , Monitoreo y Análisis de registros de auditoría.
- Acceso controlado basado en la necesidad de conocer.
- Monitoreo y control de cuentas.
- Prevención de Pérdida de Datos.
- Respuesta a Incidentes y Gestión.
- Ingeniería de Red Segura.
- Pruebas de Penetración y ejercicios de equipo.

*fuentes: www.sans.org, http://www.verizonenterprise.com/DBIR/2013/

Conclusiones y Preguntas

Muchas Gracias

Fuentes: www.sans.org

www.verizonenterprise.com

www.wikipedia.com

www.calasis.com

aprocal

Asociación de Profesionales en Compras, Abastecimiento y Logística