C.I.S.O.
Chief Information Security Officer

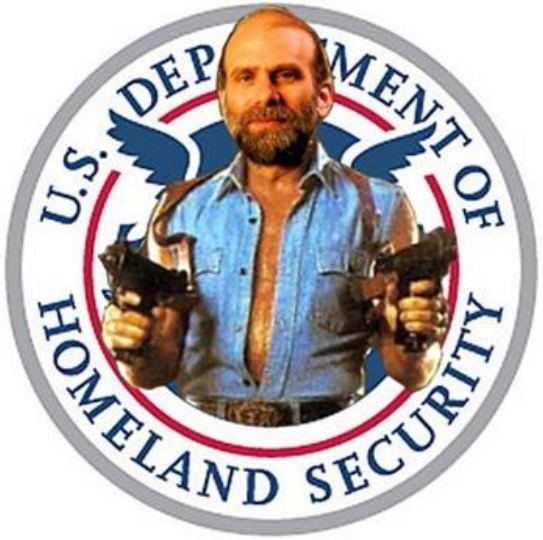
Los 10 puntos críticos en el management de Seguridad Informática

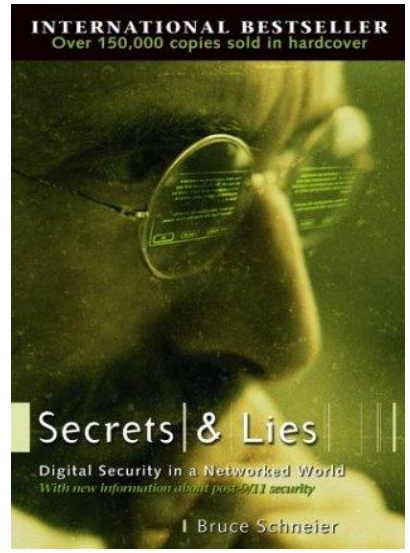
Por: Jesús Torrecillas (D.S.E.)
(C.I.S.O. en AXTEL)

Antes de comenzar…

Introducción:

Si usted piensa que la Tecnología puede resolver sus problemas de Seguridad, entonces usted no entiende los problemas de Seguridad y tampoco entiende la Tecnología.





(2004) Schneier, Bruce. Secrets & lies. Digital Security in a networked world. John Wiley & Sons Inc.

Introducción:

- Aclarando posturas desde el principio.
- La Seguridad Informática en su evolución histórica.
- ¿Qué no es un C.I.S.O.?
- ¿Qué es un C.I.S.O.?
- ¿La labor de un C.I.S.O?
- Tipos de C.I.S.O.
- ¿A quién reporta un C.I.S.O.?
- ¿Por qué las empresas deben tener a un experto en Seguridad Informática?
- Beneficios en el negocio.
- ¿Inversión o gasto?
- ¿Qué certificaciones debería contar?
- Los 10 puntos fuertes.
- Referencias.

Aclarando posturas desde el principio:

La Seguridad de la Información debe ser considerada como Factor Estratégico para la continuidad del negocio.

La Seguridad Informática en su evolución:

- Nada.
- Vigilante.
- Antivirus.
- Negocio de las certificaciones.
- Personal Firewall.
- IDS.
- IPS.
- Ataques volumétricos y toda la fauna esa…
- Firewalls de tercera generación.
- C.I.S.O.
- R.O.I.

¿Qué no es un C.I.S.O:

- Reparador de computadoras.
- Soporte telefónico de help desk.
- Cambiador del tonner.
- Desconocedor de las tecnologías.
- Recién egresado o graduado.
- Presuntuoso y afrentoso.
- Charlatan.
- Desconocedor estratégico del negocio.
- Bueno para nada.
- Joven y lleno de certificaciones de lo más variopinto.
- Con asuntos sucios escondidos.

¿Qué es un C.I.S.O.?:

- Veterano en tecnologías de computación.
- Experto en comunicaciones informáticas.
- Conocedor de la Ingeniería Social y la malicia humana.
- Mayor de 40 años. (bien toreado)
- Con gran reputación y liderazgo bien reconocido.
- Gran observador de los acontecimientos.
- Capacidad de abstracción.
- Poco impresionable.
- Líder con don de gentes.
- Insobornable.
- Visión estratégica del negocio.

El C.I.S.O. Como director de orquesta:

La labor de un C.I.S.O.:

- Administración de la seguridad de la información.
  - Desarrollo y gestión de las políticas de seguridad informática.
  - Crear conciencia en materia de seguridad entre el personal de la organización y las partes interesadas.
  - Evaluación de riesgos y control de los activos de información de la organización.
  - Implementar medidas preventivas respecto a la vulnerabilidad de los activos de la empresa.
- Colaboración con la alta dirección en investigaciones y emitiendo informes que describan los incidentes de Seguridad y su mitigación.
- Saber socializar con TODOS los directivos y mandos intermedios de la empresa para realizar una alianza estratégica de protección de los activos de información.

Tipos de C.I.S.O.:

- De manera concreta existen tres tipos básicos de CISO.
- El primero de ellos corresponde a un perfil empresarial, pues su conocimiento y experiencia se encuentran enfocados a participar en el correcto cumplimiento de los objetivos de la organización. Este tipo de CISO se encuentra estrechamente vinculado con el área jurídica, de recursos humanos e informática.
- Existe también el tipo técnico al cual se le denomina CSO. En este caso su perfil le permite ubicar las vulnerabilidades, verificar su corrección y salvaguardar la integridad de la información que reside y viaja sobre redes, equipos y sistemas informáticos de la compañía. Por supuesto, su función dentro de la empresa no es menos importante, pues se encarga de buscar y custodiar las pruebas electrónicas necesarias para poder impugnar a quienes han hecho mal uso de la información.
- También está el tipo metodológico. Este último utiliza diversos procedimientos para la protección de los datos tales como ITIL, Cobit e ISO27001 y el plan de recuperación en casos de desastres (DRP, por sus siglas en inglés). De acuerdo a la necesidad de cada empresa, en cuanto a resguardo de la información, será el tipo de CISO que se contrate para cumplir con los objetivos en ese rubro.
- El CISO unificador de todo lo anterior (debe contar con un equipo de “governance”).

¿A quién reporta un C.I.S.O.?

- En la mayoría de los casos el CISO reporta al CIO de la compañía.
- También es ideal que reporte a la alta dirección.
- Otra opción es al departamento de Control Interno, o Auditoría.
- Sería ideal que el C.I.S.O. y su equipo no dependieran de IT para tener independencia a la hora de tomar decisiones en auditorías. Una estructura así debería permitir a IT disponer de sus propios expertos operativos que periódicamente reportasen al C.I.S.O. las actividades.

¿Por qué las empresas deben tener a un experto en Seguridad Informática?

- Imagen corporativa de la salvaguarda de los activos de Información.
- Concentrar el conocimiento en Seguridad en una sóla persona y en un solo equipo.
- Lo exigen las nuevas reglamentaciones y auditorías a nivel Internacional.
- Repercute la credibilidad de la compañía a nivel de organización, accionista, imagen pública.
- Poner orden en la casa desde un único punto de vista integrador.
- Da muchos beneficios para el negocio.

Beneficios para el negocio:

- Ahorra costos frente a desastres por pérdida de activos de información.
- Da tranquilidad al accionariado y repercute en la imagen empresarial.
- Factor estratégico para la continuidad del negocio.
- Factor estratégico para recuperación del negocio tras un desastre.

Inversión o gasto:

- **La Seguridad de la Información es Factor estratégico para la continuidad del negocio.**
- Por tanto empresas con facturaciones importantes deben contar en su comité directivo con un C.I.S.O. con el fin de disponer de un esquema de Seguridad Informática reconocido y cumpliendo los más altos estándares posibles en prevención de pérdidas Informáticas y con un proceso de recuperación frente a desastres adecuado. (D.R.P. Disaster Recovery Plan)

¿Qué certificaciones debería contar?:

- No hay una sóla certificación que avale la credibilidad y experiencia de un C.I.S.O.
- La Seguridad de la Información es una carrera de vida, no una moda.
- CISPP, CISA, COBIT, 27001,Todas son buenas pero no son la panacea.
- Tener muchas certificaciones no garantiza ser un buen C.I.S.O.
- La mejor certificación, es la experiencia, la edad, el trabajo constante y honesto.
- Tú reputación hablará más de ti que todas las certificaciones que tengas.

Los 10 puntos críticos.

1° La gestión del Gobierno: Un buen marco de referencia NIST SP800-100.

- ¿Saben ustedes lo que es la gestión de gobierno?
- ¿Saben ustedes moverse por las complicadas estructuras empresariales de su compañía?
- ¿Se siente seguro a la hora de hablar con la alta dirección de problemas de fuga de información estratégica?
- Consulte lo relacionado en ele NIST SP800-100

http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf

2° El código de ética.

- Antes de ser contratado, exija firmar un NDA con la empresa que le contrata.
- Usted verá cosas que posiblemente le cambien la visión de empresa responsable y ética que publicitan. ¿Les suena conocido?
- Posiblemente las empresas que más publicitan su código de ética, son las que tienen mayores “áreas de oportunidad”.
- No entre en shock si lo que encuentra va en contra de su moralidad. Eso es parte del “show”. Siempre puede irse a otro lugar que sí sean más éticos.
- Empresas que presumen la fe y se respire un ambiente humanista, posiblemente sean las más éticas sin hacer tanta publicidad.

3° La mejores prácticas.

- Las mejores prácticas no se publicitan, se perciben como clima laboral.
- Si la imagen de la empresa es que es “un mugrero” tal vez lo sea.
- Nunca hablar mal de su empresa, salvo que lo que usted hable sea ante un tribunal y por orden judicial.
- Sea honesto de verdad, sea honorable, sea respetuoso, sea un referente y un líder.
- Hablar mal de la empresa contagia el desánimo y esto redunda en mejores condiciones para la fuga de talentos, y aumente el fraude interno.
- Con sus informes no exagere, sea honesto, y proponga soluciones.

3° La mejores prácticas. (i)

- Las cosas se planean, nacen, crecen, maduran, y luego qué…
- La flexibilidad y el seguimiento es la base del éxito.
- Y una vez documentado vuelta a empezar.

3° La mejores prácticas. (ii)

- http://csrc.nist.gov/publications/PubsSPs.html#800-30
- NIST SP800-14 (Principles and Practices for Securing Information Technology Systems)
- http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf
- NIST SP800-53.3ª (Guide for Assessing the Security Controls in Federal Information Systems and Organizations)
- http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf
- NIST SP800-30 rev 1. (Análisis de riesgos)
- http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf
- NIST SP800-66
- http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf
- NIST SP800-27 rev A (Engineering Principles for Information Technology Security)
- http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf
- NIST SP800-88 (Sanitizacion) (Destrucción segura de la información)
- http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf
- NIST SP800-137 (Monitorizaje contínuo)
- http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf

3° La mejores prácticas. (iii)

- TOGAF (Open Source Group Architecture Framework)
- http://www.vanharen.net/Samplefiles/9789087537104SMPL.pdf
- SABSA (Ciclo de vida para arquitecturas de seguridad)
- http://sabsa.org/
- Zachman Framework for Enterprise Architecture.
- http://www.businessrulesgroup.org/BRWG_RFI/ZachmanBookRFIextract.pdf
- http://www.exinfm.com/training/M2C4/zachman-poster.pdf
- Common Criteria Portal. (CC)
- https://www.commoncriteriaportal.org/
- https://www.commoncriteriaportal.org/files/ccfiles/ccpart2v3.1r4.pdf
- Rainbow Series. (libros de Seguridad como el famoso “libro rojo de Seguridad”
- http://fas.org/irp/nsa/rainbow.htm
- OWASP (análisis de seguridad entornos web)
- https://www.owasp.org/index.php/Main_Page
- https://www.owasp.org/index.php/OWASP_Top_10_Privacy_Risks_Project

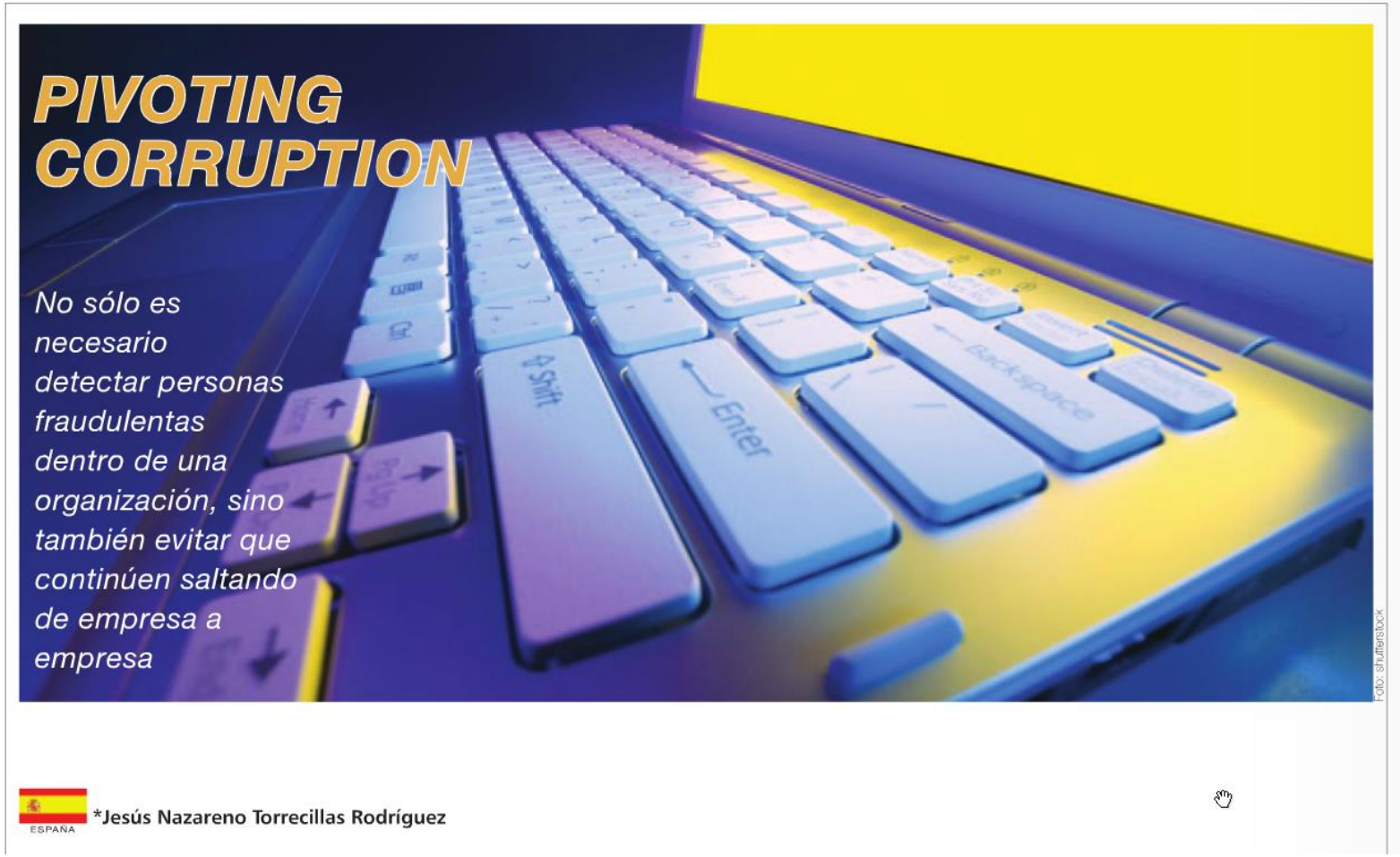
4° Las mejores prácticas (las suyas).

- Conocimiento de lo que es Seguridad.
- Honestidad profesional.
- Reputación en el mercado.
- Independencia de proveedores.
- Integridad personal.
- Mejora continua.

5° La corrupción interna.

- Denunciar a un corrupto no es tarea fácil. Tiene sus redes de protección internas. Pero como todo, si usted cuenta con todos los elementos, apoyos, y evidencias (legalmente obtenidas) ¡¡¡ ACTÚE SIN PIEDAD!!!
- La corrupción interna comienza cuando las medidas de consecuencias no están claras. Si se permite el delito una vez, esté será como la semilla del cáncer que ya será difícil de erradicar.
- La imagen de una empresa se fortalece cuando pone en la calle a delincuentes.
- Prevenga la corrupción interna y fuga de información estratégica como parte de sus funciones. (NDA Non-disclosure agreement)

5° La corrupción interna.



- http://content.yudu.com/Library/A2r3hf/EdicionImpresaNo83Re/resources/74.htm

6° Domine el lenguaje financiero.

- No hable de, Bit, Bits, Byte, etc… a la alta dirección pues los aburriría.
- Tenga claro que el no invertir en seguridad hoy, mañana será causa de costosas inversiones para remediar lo que no hizo ayer.
- ROI, ROI, ROI, y nada más que ROI. (Return On investment)

ROI = (Utilidad neta o Ganancia / Inversión) x 100

Un buen modelo de Gestión del Riesgo: http://ishandbook.bsewall.com/risk/index.html

6° Domine el lenguaje financiero. (ROI, TCO…)

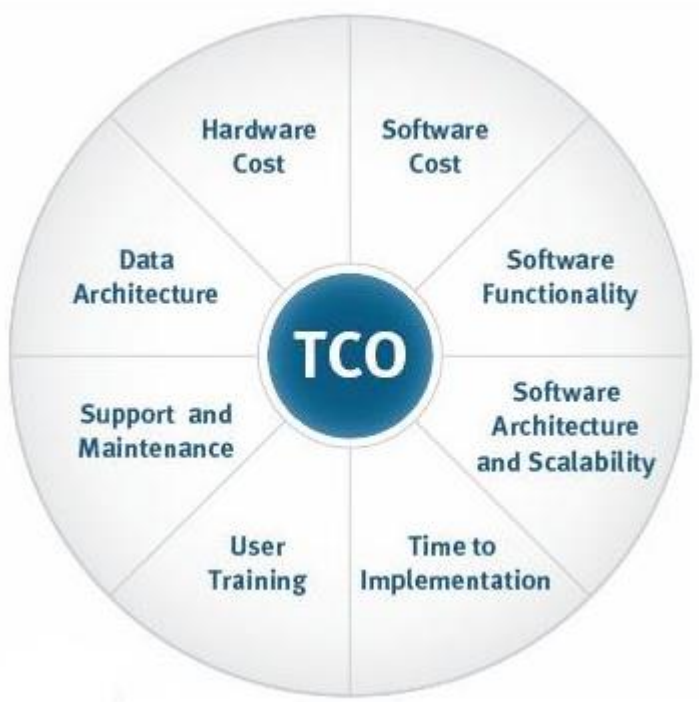
Determinar AV
- AV (*Asset Value*).
- Se determina el costo del activo a evaluar.

Determinar EF
- EF (*Exposure Factor*).
- Se determina el factor de exposición de cada activo con cada riesgo.

Calcular SLE
- SLE (*Single Loss Excpectancy*).
- Se calcula la expectativa de una perdida mediante: SLE = AV x EF

Determinar ARO
- ARO (*Annualized Rate of Ocurrence*).
- Se determina la taza de ocurrencia anualizada.

Calcular ALE
- ALE (*Annualized Loss Expectancy*).
- Se anualiza la expectativa de perdida mediante: ALE = SLE x ARO



6° Domine el lenguaje financiero.

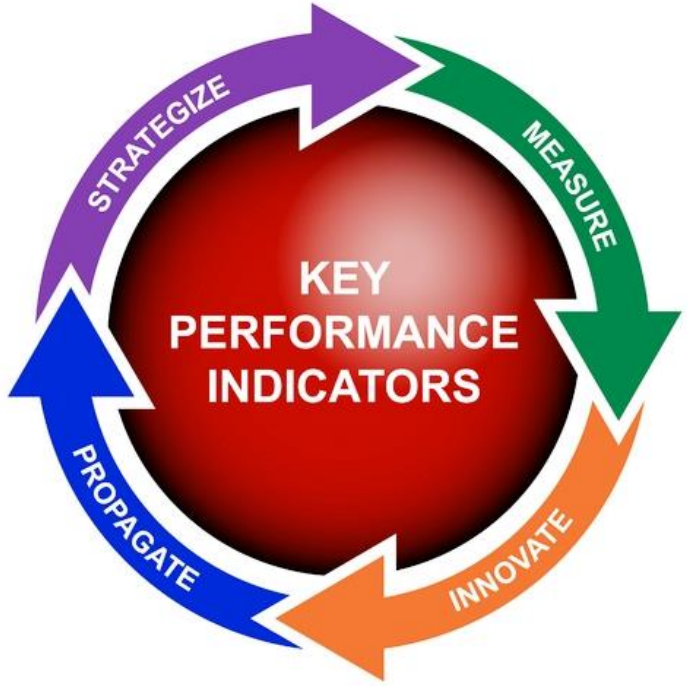
- ¿Sabe usted lo que es el ROI? **Return on Investment.**
- ¿Sabe usted lo que es el TCO? **Total Cost of Ownership.**
- ¿Sabe usted lo que es el EVA? **Economic Value Added.**
- ¿Sabe usted lo que es el SLE? **Single Loss Expectancy.**
- ¿Sabe usted lo que es el ARO? **Annualized Rate of Ocurrence.**
- ¿Sabe usted lo que es el ALE? **Annualized Loss Expectancy.**

7° No prometa aquello inalcanzable.

- La Seguridad es una percepción social.
- Si usted promete una burra, posiblemente cometa una burrada.
- La Seguridad de la Información no es una ciencia exacta ni precisa, pero hay unos lineamientos mínimos que usted debe seguir.
- Si usted dice que se puede tal vez se pueda.
- Si usted dice que no se puede tal vez se esté equivocando.

Puntos a exponer a la Alta Dirección

- La Seguridad como factor estratégico para la continuidad del negocio.
- Hacer que ellos piensen que tú “morirás” por la Seguridad.
- Reflexionar que la Información es nuestro producto clave.
- Mostrar el resultado de un anterior Análisis de Riesgo.
- Usted será el responsable por no proveer Seguridad.
- Deberá apoyar una política que Vd. Apruebe.
- Proteger el valor de la Propiedad Intelectual.
- Tensiones por responsabilidades jurídicas.
- Económicas y perdidas no económicas.
- Costo de la reputación e integridad.
- Pérdida de ventajas competitivas.
- Citar a expertos.



8° El Retorno de la Inversión (R.O.I.)

- Es la razón financiera que compara el beneficio o la utilidad obtenida en relación a la inversión realizada.
- Representa una herramienta para analizar el rendimiento que la empresa tiene desde el punto de vista financiero.
- ¿Qué inversión debo de hacer en Seguridad de la Información para que dicha inversión me de beneficios y no sea un gasto contable?
- Rentabilice siempre los programas de Seguridad de la Información.
- No gaste a lo loco y sin sentido. Invierta con inteligencia y discreción.

8° El Retorno de la Inversión (R.O.I.)

9° La imagen empresarial va con usted.

- ¿CISO menor de 40 años? Mmm No por muchas certificaciones se es un experto en Seguridad de la Información.
- Si su vida es un desmadre ¿Qué imagen de su empresa usted proyectará?
- El hábito (vestiduras) no hace al monje, pero sí lo condiciona.
- Salga ahí fuera, conozca a otros líderes en Seguridad de la Información. Comparta experiencias, dese a conocer y aprenda de otros.
- Aprenda humildad estratégica.

10° Actualícese.

- EL LIBRO HACE LIBRES, La ignorancia esclavitud.
- Lea, participe en foros, vaya a eventos de Seguridad.
- Si usted trabaja en una empresa grande, tendrá grandes problemas. Por eso es básico conocer la opinión de otros expertos.
- El saber no ocupa lugar, pero el desconocimiento genera pérdidas enormes.
- Lea, lea, y siga leyendo.


¿Tiene alguna duda de lo que es un C.I.S.O?

Referencias:

- https://www.incibe.es/blogs/post/Empresas/BlogSeguridad/Articulo_y_comentarios/CEO_CISO_CIO_roles_ciberseguridad
- ROI-ALE: http://ishandbook.bsewall.com/risk/Assess/Risk/ROI.html
- http://www.magazcitum.com.mx/?p=1607
- http://blog.segu-info.com.ar/2008/11/cissp-ccent-cisa-ccie-ccna-lpt-giac.html
- http://www.acis.org.co/revistasistemas/index.php/ediciones-revista-sistemas/edicion-no-123/item/99-los-ciso%C2%B4s-opinan
- http://searchdatacenter.techtarget.com/es/consejo/Que-atributos-son-necesarios-para-tener-exito-en-el-rol-del-CISO

Referencias:

- http://www.isecom.org/
- https://malwr.com/
- http://www.malware-traffic-analysis.net/
- http://www.gns3.com/
- http://www.redeszone.net/2014/06/09/veracrypt-un-gran-derivado-de-truecrypt-mas-seguro/
- https://howsecureismypassword.net/
- http://www.seguridadparatodos.es/2012/02/cloudcracker-servicio-en-la-nube-de.html
- http://www.seguridadparatodos.es/2012/02/cloudcracker-servicio-en-la-nube-de.html
- https://www.privatetunnel.com/home/
- https://www.proxpn.com/index.php

Referencias:

- https://whispersystems.org/
- http://www.mspy.mx/?gclid=CKnBvtP3i8kCFQiqaQod904DJQ
- http://www.mspy.mx/features.html
- http://www.wifislax.com/
- http://www.airtightnetworks.com/home/products/AirTight-WIPS.html
- Preparación CISSP http://www.deacosta.com/files/
- http://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html
- https://cwe.mitre.org/top25/#listing (Los 25 errores de software)
- https://www.owasp.org/images/7/79/ESAPI_Book.pdf (apis seguras)
- http://www.sans.org/critical-security-controls (controles de seguridad)
- http://www.rapid7.com/
- http://www.tripwire.com/
- http://www.arachni-scanner.com/ (scanner web)

Referencias:

- http://www.cellebrite.com/es
- http://www.mspy.mx/?gclid=CKnBvtP3i8kCFQiqaQod904DJQ
- https://www.paraben.com/

¡¡¡Muchas gracias!!!

jntorrecillas@yahoo.es

amsi
asociación mexicana de seguridad informática